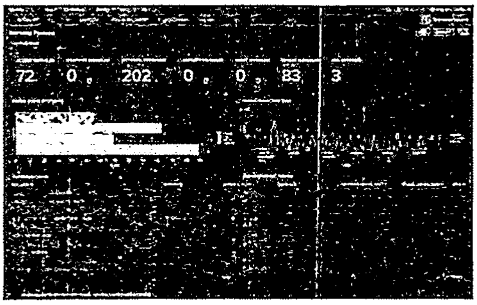
PRODUCT BRIEF

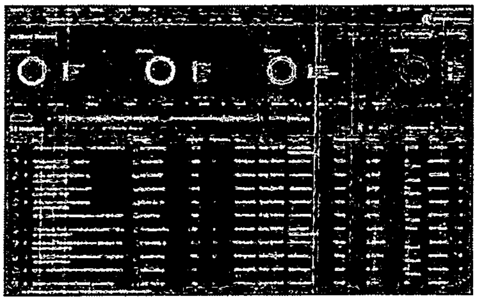
Data-Driven Security

Splunk Enterprise Security provides visibility and insights into data that powers and secures the business, enabling analysts to make critical decisions with speed and accuracy with the objective of seamlessly detecting and defending the enterprise.



Full Visibility

Break down data silos and gain actionable intelligence into the full breadth of your security posture. Monitor tens of terabytes of data per day — any data from anywhere, structured or unstructured. Backed by an unparalleled data platform, arrive at data-driven decisions that protect your business and reduce risk. Achieve outcomes inside and outside of the security organization (IT, DevSecOp, and more).

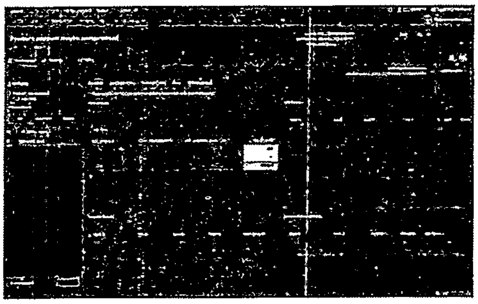


Increased Flexibility and Compatibility

Stay agile in the face of changing threats and business needs with an adaptable data platform regardless of where the organization is on their cloud or hybrid journey. Quickly gather context across your multi-vendor security ecosystem by utilizing technology integrations built by Splunk, partners, and the community on Splunkbase, which houses 2,500+ apps and add-ons.

Accelerated Threat Detection

Increase the speed of security investigations by more than 50% with unsupervised machine learning to detect unknown threats and anomalous behaviors. Accelerate investigations and gain critical context by enriching and prioritizing high-fidelity alerts with integrated threat intelligence to boost SOC productivity and drive down fatigue.



Unify Your Security Operations

Mission Control, an application available to Splunk Enterprise Security users, brings order to the chaos of your security operations. Splunk Mission Control unifies detection, investigation and response capabilities within one common work surface; simplifies security workflows by codifying your processes into easy-to-follow response templates; and empowers your team with automation to reduce analyst grunt work and increase the speed of response.

Ready to supercharge your security operations with a cloud-based data-driven SIEM solution?
Learn how to get started with Splunk.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

Threat Intelligence framework in Splunk ES

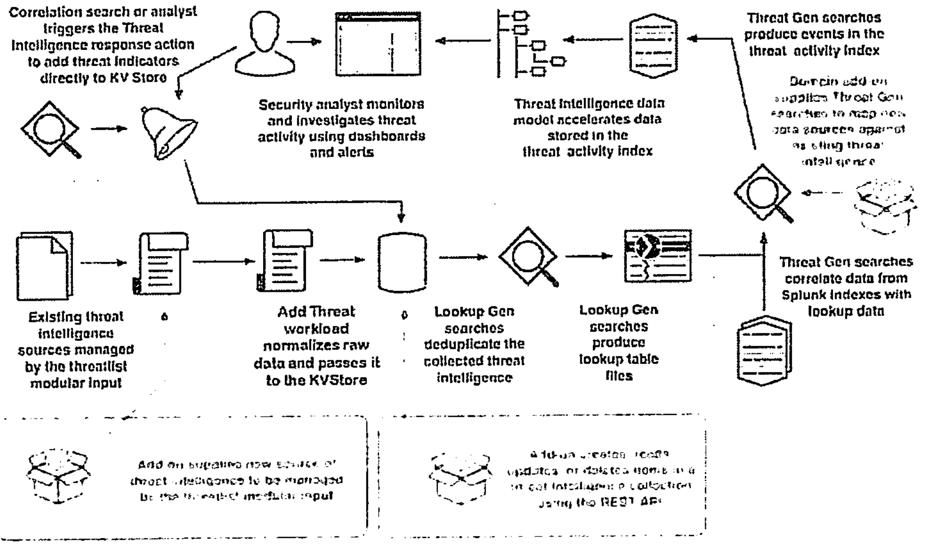
Was this page helpful?

[👍] [👎]

The Threat Intelligence framework is a mechanism for consuming and managing threat feeds, detecting threats, and alerting. The framework consists of modular inputs that collect and sanitize threat intelligence data, lookup generation searches to reduce data to optimize performance, searches to correlate data and alert on the results, and data modeling to accelerate and store results. This framawork also includes a number of audit dashboards that allow introspection into threat intelligence retrieval, normalization, persistence, and analysis.

This framework is one of five frameworks in Splunk Enterprise Security with which you can integrate. See Building Integrations for Splunk Enterprise Securty for an introduction to the frameworks.

The diagram presents an overview of the Threat Intelligence framework, with the possible integration points highlighted.


Correlation search or analyst triggers the Threat Intelligence response action to add threat indicators directly to KV Store
Security analyst monitors and investigates threat activity using dashboards and alerts
Threat intelligence data model accelerates data stored in the threat activity index
Threat Gen searches produce events in the threat activity index
Domain add-on supplies Threat Gen searches to map new data sources against existing threat intelligence
Existing threat intelligence sources managed by the threatlist modular input
Add Threat workload normalizes raw data and passes it to the KVStore
Lookup Gen searches deduplicate the collected threat intelligence
Lookup Gen searches produce lookup table files
Threat Gen searches correlate data from Splunk indexes with lookup data
Add-on supplies new source of threat intelligence to be managed by the threatlist modular input
Add-on creates, reads, updates, or deletes items in a threat intelligence collection using the REST API

How Splunk Enterprise Security processes threat

SPLUNK

Cyble Threat Intel

[illegible]

Splunk Cloud

Overview

Cyble Threat Intel, a robust cybersecurity application developed on the Splunk platform, empowers users to monitor assigned alerts effectively. By utilising this application, users can proactively avoid potential threats and acquire valuable insights that can be acted upon. It facilitates seamless collaboration, automates tasks, and ensures compliance effortlessly. By embracing Cyble Threat Intel, organisations can strengthen their security operations and confidently protect their digital assets.

The user can utilise the data received through APIs using the modular input Cyble has created. They can employ this input to design their dashboard, set up alerts, and generate reports. Additionally, the user can utilise the pre-built dashboard created by Cyble.

Developed by Cyble Inc

Release Notes

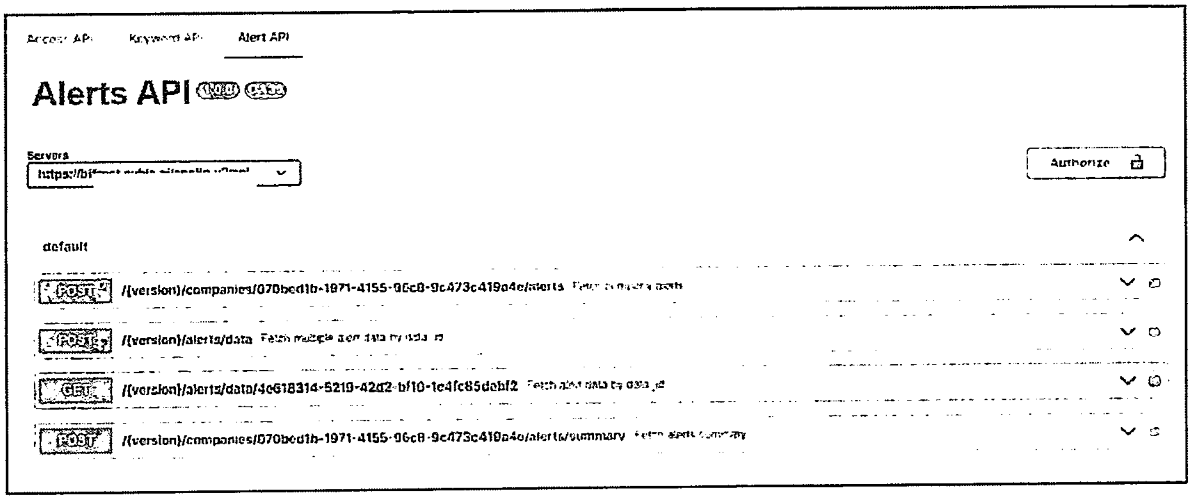
Version 1.2.1 Sept. 5, 2023

1. Removed alert_groups support
2. Fixed IOC timeout issue

- For APT groups of interest, track the latest IOCs that can be used for threat hunting in their environment and ingest them in their SIEM or perimeter security devices for alerting and blocking.

2.5.3 IOC Feed Integration

- The Cyble Vision platform also provides a curated daily feed of IOCs that clients can integrate with their cyber security monitoring platforms such as SIEM, SOAR or TIP. Cyble Vision supports a variety of out of the box integration mechanisms such as API as well as STIX 1.x and 2.x formats which are made available via the TAXII specification. Detailed documentation is also available on the platform to guide users for integrating the IOC feed with their systems, without the need for any professional service
- Each IOC will be accompanied by a Risk score that is derived from the risky behavior or activity associated with the IOC as well as Confidence Rating for the IOC based upon the credibility and reliability of the threat intelligence source and the prevalence of the IOC across multiple sources.
- The Cyble Vision platform has been successfully integrated with global technology solutions such as Palo Alto CORTEX SOAR, Anomali Cyware TIP platform as well as SIEMs such as IBM QRadar, Splunk and LogRhythm.



Alerts API

Servers
https://bi[illegible]

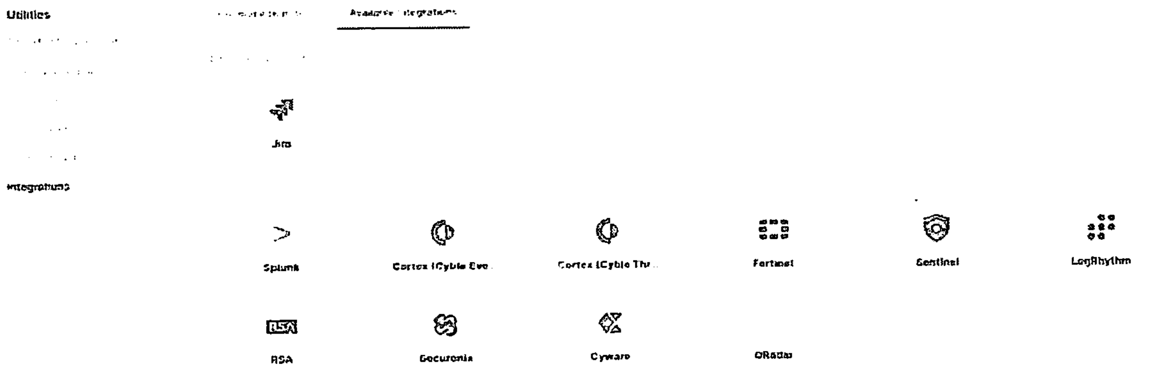
default

POST /{version}/companies/070bed1b-1971-4155-96c8-9c473c419a4e/alerts Fetch multiple alerts

POST /{version}/alerts/data Fetch multiple alert data by data_id

GET /{version}/alerts/data/4c618314-5219-42d2-bf10-1e4fc85debf2 Fetch alert data by data_id

POST /{version}/companies/070bed1b-1971-4155-96c8-9c473c419a4e/alerts/summary Fetch alerts summary



Splunk

Integration version: 44.0

Note: This integration uses one or more open source components. You can download a copy of the full source code of this integration from the storage bucket (https://storage.googleapis.com/csoar_public_integrations/Splunk.zip).

The Splunk app prepares cases with all of the relevant alerts and events from Splunk. There are two ways to ingest these cases into Chronicle SOAR: pull based, and push based methods.

The first method is called *pull based*. Using this method, in order to ingest cases into Chronicle SOAR, you need to configure the Splunk Pull Connector, which pulls cases from the Splunk app. This method doesn't require any additional configuration in the Splunk app.

The second method is called *push based*. Using this method, the Splunk app performs API calls to Chronicle SOAR to add a new case. In order to work with this method, you need to generate a Chronicle SOAR API key and add a Chronicle SOAR URI in the configuration of the app.

Create an API key:

1. Navigate to **Settings** > **Advanced** > **API**.
2. Click the plus sign on the top right to add a new API key.
3. Enter the name of the API key and click **Create**.

Note: To the push based method to work, you need to have a basic or admin level of permissions.

4. Copy the API key.

How to configure Splunk to work with Chronicle SOAR

Prerequisites for enabling or disabling token authentication

Before you can enable token authentication, you must complete the following requirements:

- The Splunk platform instance where you want to enable token authentication must not operate in legacy mode, where Splunk Web operates as a separate process. If the Splunk platform is in legacy mode, token authentication does not run. For more information on legacy mode, see the Start and Stop Splunk Enterprise (https://docs.splunk.com/Documentation/Splunk/9.0.4/Admin/StartSplunk) document in the Splunk Eneterprise Admin Manual.
- The account that you use to log into the Splunk platform must hold a role that has the edit_tokens_settings Splunk platform capability before you can turn token authentication on or off.

Enable token authentication using Splunk Web

When token authentication is off, the following message displays on the **Tokens** page in Splunk Web:

```
Token authentication is currently disabled > To enable token authentication, click Enable Token Authentication
```

Complete the following steps on the instance where you want to enable token authentication:

1. Log in to the Splunk platform instance as an administrator user, or a user that can manage tokens settings. You cannot use a token to log in to Splunk Web. You must provide a valid user name and password.
2. After you log in successfully, in the system bar, select **Settings** > **Tokens**.

splunk>

Free Splunk ×

Splunk Protects

Cloud Security at Splunk

On this page

Skip to main content ›

splunk>

Free Splunk ✕

Splunk Protects

Splunk Incident Response Framework (SIRF)

Additional Resources

More for security

- Corporate Security
- Product Security

Cloud Infrastructure

Splunk uses a range of technologies to prevent unauthorized access or compromise of Splunk's network, servers or applications, which include such things as logical and physical controls to segment data, systems and networks. Splunk monitors demarcation points used to restrict access such as firewalls and security group enforcement points. Remote users must authenticate with two-factor authentication prior to accessing Splunk networks containing customer content.

Splunk Employee Access Control

Splunk grants system privileges and permissions to users on a "least privilege" principle. Customer stacks are logically separated from each other. Splunk leverages the benefits of virtualization at the server, storage and network layers to ensure that there is strict separation for each customer instance. Logical access policies and procedures delineate Splunk's required activities and responsibilities for credential management, user access provisioning, privileged access, monitoring and intrusion detection.

Skip to main content ›

audit controls.

- You can build your own roles to map to your organization's data access policies for different classes of users. You can also map Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML) groups to different roles.

Splunk Employee and User Authentication

Authorized users supporting the delivery of Splunk services must identify and authenticate to the network, applications and platforms using their user ID and password. Splunk's enterprise password management system requires minimum password parameters. SSH key authentication and enterprise password management applications are used to manage access to the production environment and two-factor authentication (2FA) is required for remote access and privileged account access for customer content production systems.

Splunk supports single sign-on (SSO) integrations (SAML v2) with compliant identity providers such as Okta, PingFederate, Azure AD, ADFS, CA SiteMinder, OneLogin, Centrify, SecureAuth, IdentityNow, Oracle OpenSSO, Google SAML2 provider and Optimal Id. Splunk also integrates with other authentication systems, including LDAP, Active Directory and e-Directory.

- Learn how to configure single sign-on in on-premises environments with SAML.
- Learn how to configure single sign-on in Splunk Cloud with SAML.

Data Anonymization

Skip to main content ›

splunk>

Free Splunk

Privacy Policy

Splunk Privacy Policy

Updated: September 2023

Download PDF

This Privacy Policy explains how Splunk Inc. and its subsidiaries ("Splunk") collect, use, and disclose information you provide to us or which we otherwise collect ("Information"), including "Personal Data" by which we mean Information about an identified or reasonably identifiable individual.

This Privacy Policy applies to Offerings (as defined in the Splunk General Terms), splunk.com and to other websites Splunk operates that link to this Privacy Policy. This Privacy Policy does not apply to Personal Data processed by Splunk as a processor or to Splunk as an employer.

From time to time, Splunk acquires companies that may operate under their own privacy policies. You will continue to be presented with those companies' privacy policies on their offerings and websites until the integration with Splunk is complete and those offerings and websites are linked to this Privacy Policy.

The use of our products and services, including those available through other Splunk websites that link to this Privacy Policy, are subject to the terms of the applicable customer agreement. The use of our website is subject to the Splunk Websites Terms and Conditions of Use. The terms of this Privacy Policy are incorporated into and form part of those agreements.

Open All

Data Collection ⊕

Interactions ⊕

Skip to main content >

splunk>

Free Splunk

Privacy Policy

Interactions

Opting Out of Marketing Emails ⊕

Offerings ⊕

What We Collect via Our Offerings and How We Use It ⊕

Other Collection Practices ⊕

Data Collection Practices Associated with Apps ⊕

How Splunk Shares Your Information ⊕

Cookie Preferences ⊕

How We Secure Your Information ⊕

Splunk Also Observes the Following Practices ⊕

Your Rights ⊖

In certain locations, you may have rights under data protection law, such as to request access to or correction, deletion, or transfer of your Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our data request form, and we will respond as soon as reasonably practicable consistent with applicable law. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

European Economic Area, the UK, and

Skip to main content >

A.4
Security Orchestration, Automation and Response (SOAR)

Google Cloud

Chronicle SOAR

Taking Response to the Next Level

Chronicle's cloud-native security, orchestration, automation and response (SOAR) product empowers security teams to respond to cyber threats in minutes - not hours or days. Chronicle SOAR fuses a unique threat-centric approach, powerful yet simple playbook automation, and context-rich investigation to free up valuable time and ensure every security team member is informed, productive and effective.

Benefits

- Automate up to **98%** of Tier 1 tasks to free up time for strategic initiatives
- Reduce analyst caseload by up to **80%**
- Speed response **10x**

Why Chronicle SOAR?

Chronicle SOAR enables modern, fast and effective response to cyberthreats by combining playbook automation, case management and integrated threat intelligence in one cloud-native, intuitive experience.

Interpret and resolve threats faster

Shift the paradigm by uniting context with a threat-centric approach, empowering analysts to quickly focus on what's truly important instead of drowning in analysis and data.

Deploy, maintain and scale with ease

Chronicle SOAR is designed for fast initial time-to-value and ease of scaling as you grow. Pre-packaged use cases, an intuitive playbook builder, and powerful playbook lifecycle management enable teams to hit the ground running and ensure that over time SOAR increases in value, not complexity.

Capture security operations insights consistently

Empower security teams to consolidate and easily see the scope of activities, generate insights that drive improvement, and measure progress over time - enabling you to be agile, efficient and anticipate future threats.

Splunk

Integration version: 44.0

Note: This integration uses one or more open source components. You can download a copy of the full source code of this integration from the storage bucket (https://storage.googleapis.com/csoar_public_integrations/Splunk.zip).

The Splunk app prepares cases with all of the relevant alerts and events from Splunk. There are two ways to ingest these cases into Chronicle SOAR: pull based, and push based methods.

The first method is called *pull based*. Using this method, in order to ingest cases into Chronicle SOAR, you need to configure the Splunk Pull Connector, which pulls cases from the Splunk app. This method doesn't require any additional configuration in the Splunk app.

The second method is called *push based*. Using this method, the Splunk app performs API calls to Chronicle SOAR to add a new case. In order to work with this method, you need to generate a Chronicle SOAR API key and add a Chronicle SOAR URI in the configuration of the app.

Create an API key:

1. Navigate to **Settings > Advanced > API**.
2. Click the plus sign on the top right to add a new API key.
3. Enter the name of the API key and click **Create**.

Note: To the push based method to work, you need to have a basic or admin level of permissions.

4. Copy the API key.

How to configure Splunk to work with Chronicle SOAR

Prerequisites for enabling or disabling token authentication

Before you can enable token authentication, you must complete the following requirements:

- The Splunk platform instance where you want to enable token authentication must not operate in legacy mode, where Splunk Web operates as a separate process. If the Splunk platform is in legacy mode, token authentication does not run. For more information on legacy mode, see the Start and Stop Splunk Enterprise (https://docs.splunk.com/Documentation/Splunk/9.0.4/Admin/StartSplunk) document in the Splunk Eneterprise Admin Manual.
- The account that you use to log into the Splunk platform must hold a role that has the edit_tokens_settings Splunk platform capability before you can turn token authentication on or off.

Enable token authentication using Splunk Web

When token authentication is off, the following message displays on the **Tokens** page in Splunk Web:

```
Token authentication is currently disabled > To enable token authentication, click Enable Token Authentication
```

Complete the following steps on the instance where you want to enable token authentication:

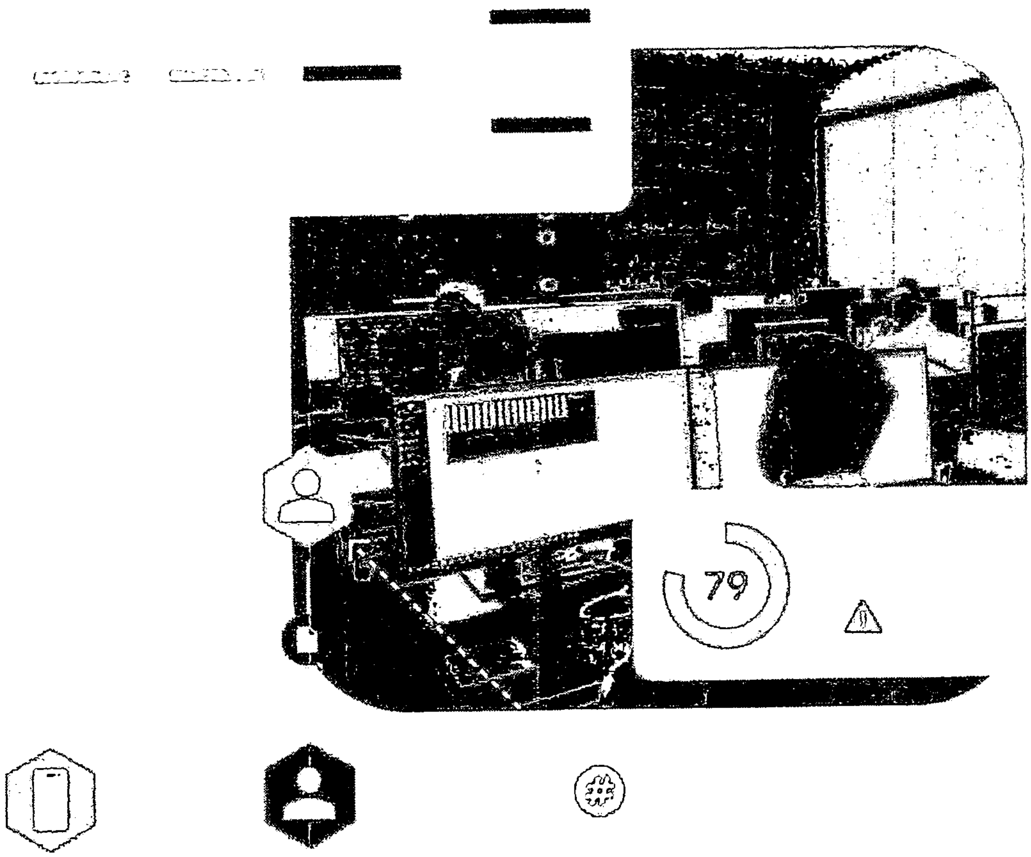
1. Log in to the Splunk platform instance as an administrator user, or a user that can manage tokens settings. You cannot use a token to log in to Splunk Web. You must provide a valid user name and password.
2. After you log in successfully, in the system bar, select **Settings > Tokens**.

Google Cloud

≡ Chronicle

Contact us

Mandiant is now part of Google Cloud. Learn More.



CHRONICLE SECURITY OPERATIONS

Respond to cyber threats in minutes, not hours or days

Chronicle enables modern, fast, and effective Security Orchestration, Automation and Response (SOAR) capabilities in one cloud-native, intuitive experience.

[illegible]

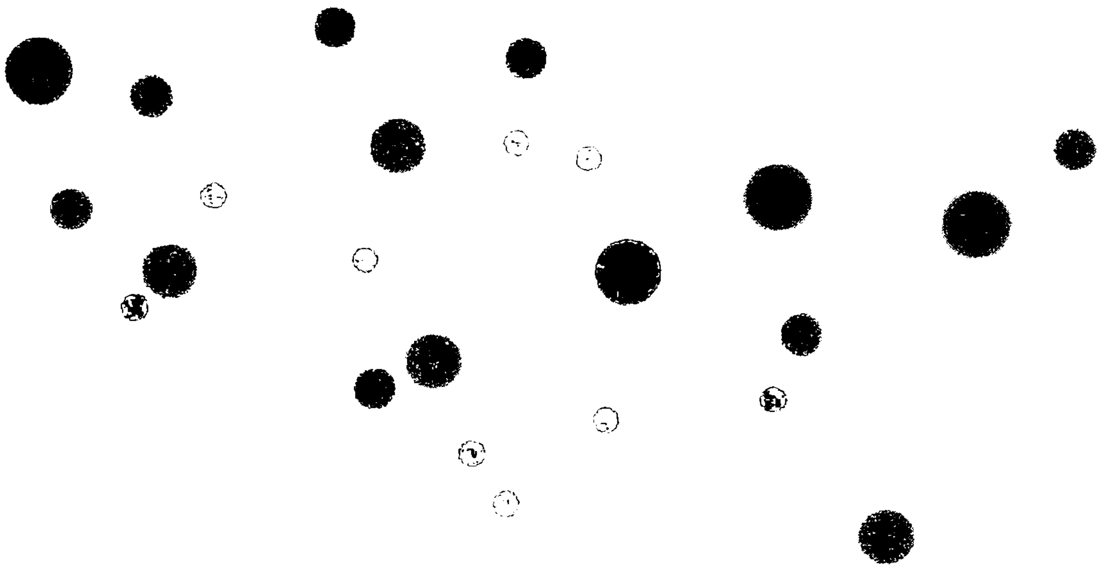
Privacy - Terms

Google Cloud

Chronicle

Contact us

Tag colleagues, assign tasks, and monitor progress of a case directly from the case wall to ensure every case is fully addressed and nothing falls through the cracks.



INSIGHTS

Capture SecOps insights consistently

Consolidate SecOps activity to easily generate insights that drive improvement and measure progress over time.

Track real-time SOC metrics and KPIs

Choose from out-of-the-box interactive reports and dashboard templates to see how your team is performing on the metrics that matter to you – from response rates to cases closed to improvement over time.

Leverage business intelligence to effectively measure and manage

Using Advanced Reports

Overview

This feature is available for all customers using the Chronicle Google Cloud license who have been given access in the Settings > Permissions screen.

Two types of permissions can be assigned to users in the Permissions screen:
View - users will only see reports that were shared with them in the Shared folder, they can also download reports and filter reports.

Edit - users can duplicate reports to the shared and personal folders, share reports, edit reports, download reports, and delete shared reports.

Advanced Reports can be accessed by all platform users through the Reports tab with no need for any prior setup.

The following folders in the Advanced Reports tab are available:

Default: Available for Admins only. Reports in this folder come predefined and cannot be edited. However, they can be duplicated and edited in a different folder. The full list of default reports together with their descriptions can be seen here. (/chronicle/docs/soar/monitor-and-report/soar-reports/default-advanced-reports-in-depth)

Personal: these are Reports that you create yourself using the Looker components. You can also duplicate reports from the Default or Shared folders and save them here.

Shared: these are reports that either you created and shared with others - or that others created and shared with you

Create a Report

1. Click the + icon.
2. Add name of report and choose a folder and an environment.
3. Click Create.
   For full information on how to create and edit Looker reports, click here (https://cloud.google.com/looker/docs).

Chronicle SOAR Overview

Chronicle Security Orchestration, Automation and Response (SOAR) is a platform designed to help organizations detect, investigate, and respond to security threats in real-time. The platform is powered by Google Cloud's infrastructure and leverages the machine learning capabilities of Google to automate and streamline security workflows.

Chronicle SOAR collects data from various security sources such as network devices, endpoint agents, and threat intelligence feeds. The platform uses this data to identify potential security incidents and initiate response actions. Chronicle SOAR also integrates with other security tools such as SIEM (Security Information and Event Management), threat intelligence platforms, and vulnerability scanners to provide a comprehensive security solution.

The platform provides an intuitive user interface that allows security analysts to investigate incidents, create workflows, and automate response actions without requiring extensive coding knowledge. Chronicle SOAR also uses machine learning to improve its accuracy and speed in identifying and responding to security incidents. The platform's automated response capabilities help organizations to reduce the time taken to detect and respond to security threats, thereby reducing the risk of data breaches and other security incidents.

Chronicle SOAR is a powerful security orchestration, automation, and response platform that helps organizations to enhance their security posture by automating security workflows, reducing response times, and improving the accuracy of security operations.

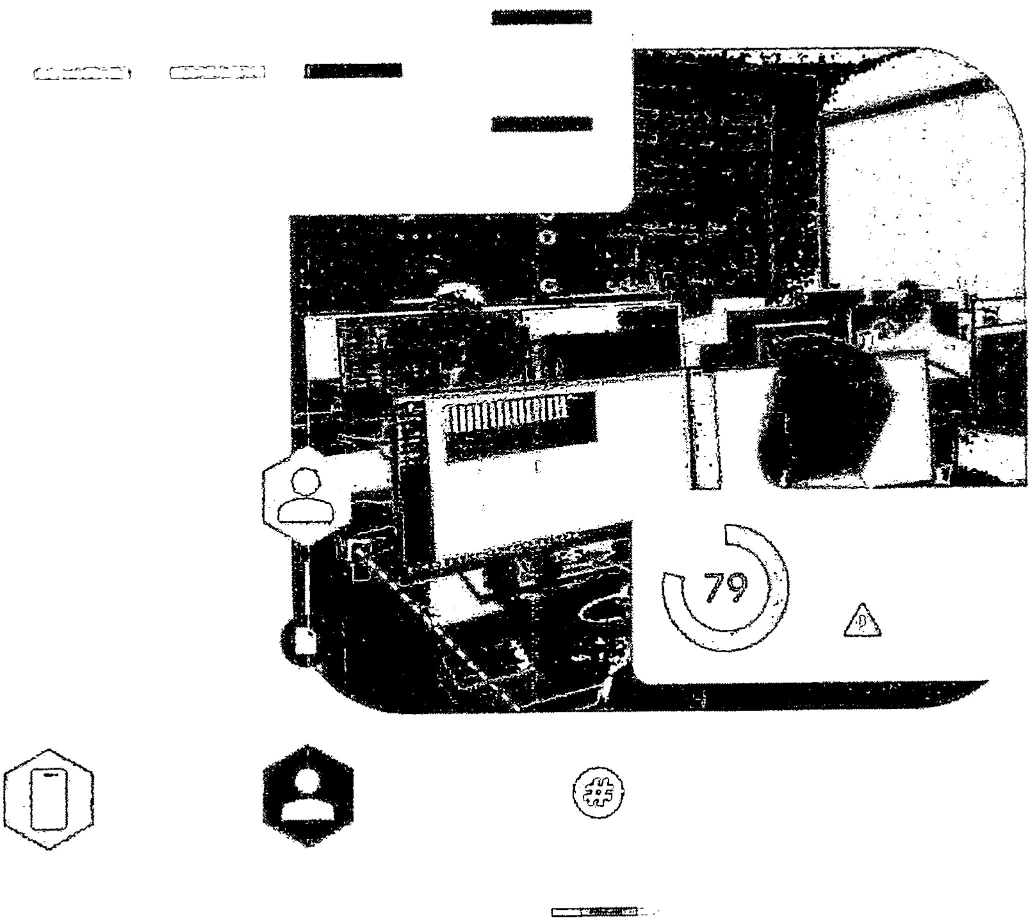
Last updated 2023-09-20 UTC.

Google Cloud

≡ Chronicle

Contact us

Chronicle is now part of Google Cloud. Learn More.



CHRONICLE SECURITY OPERATIONS

Respond to cyber threats in minutes, not hours or days

Chronicle enables modern, fast, and effective Security Orchestration, Automation and Response (SOAR) capabilities in one cloud-native, intuitive experience.

[illegible]

Privacy - Terms

Google Cloud

Chronicle

Contact us

Respond

RESOLUTION

Interpret and resolve threats faster

Case management unites the information that matters, enabling analysts to focus on what's truly important instead of drowning in data.

Automatically group related alerts into threat-centric cases

Patented technology automatically groups contextually related alerts into a single threat-centric case, enabling a single analyst to efficiently investigate and respond to a threat.

Conduct context-rich investigations

Integrate threat intelligence at every step and visualize the most important contextual data for each threat – who did what, and when – and the relationships between all involved entities attached to an event, product, or source.

Using the Chronicle Marketplace

The Chronicle Marketplace acts as the customer's toolbox, holding a wide range of utilities and options to choose from, including:

Integrations: includes integrations to third party applications and custom integrations that you have built in the IDE. In all cases you need to install them in this screen and then for those that need advanced configuration, you need to configure them in the Integrations screen via the Gear icon.

Use Cases: These are pre-built playbook workflows to integrate into the organizational security products for automated IR process and to optimize your Chronicle installation. They include predefined use cases from Chronicle and customer uploaded use cases to either test drive Chronicle functionality or incorporate into your own use cases.

Power Ups: including tools created by Chronicle Professional Services that enhance customers' ability to automate processes for more efficient Playbooks.

Integrations

There are three types of integrations you can see in the Chronicle Marketplace:

- **Commercial** – integrations to third party applications which have been developed by Chronicle – including new and updated ones
- **Community** – integrations published by users (which have been validated by Chronicle and which will appear with user details next to them)
- **Custom** – integrations which you have created and which are only displayed on your Chronicle Marketplace

Filtering Integrations

You can display the Integrations according to integration type (for example, show custom integrations, published by users) or by status (for example, installed, available update).
Integrations that have not been installed yet will have a downwards arrow on the bottom right of the box.
Click on this to successfully install the integration. For detailed information on installing and configuring an Integration, see here (/chronicle/docs/soar/respond/integrations-setup/configure-integrations).

Use Cases

Use Cases enhance your ability to shorten the time to value and to see how Chronicle experts or community users are tackling a specific attack or any other SOC challenge.
Each Use Case contains relevant items such as integrations, Playbooks etc. in order to simulate an entire workflow from end-to-end. After deploying one of these use cases, you can choose to Simulate it in the Cases tab. In addition, you can configure the Connector, and/or edit the Playbook, of a predefined Use Cases and run it on real data.

The following actions can be carried out from this screen:
Create New Use Case: You can create your own Use Case with playbook/s, test case/s and connector/s. Click Save to save locally it in your Chronicle Marketplace only. You can also export it.
Publish Use Case: Click on this option to have your Use Case published for all users. Once it's uploaded, it's sent to a dedicated Chronicle team who will analyze it and add it to the Use Case repository for all customers and community members to use. The goal of this option is to encourage all our customers to share playbooks and use cases that can help others out with their Chronicle journey. You can alter your photo and user details here before sending it. These identifiers will be published for all users.
Import Use Case: Useful for importing from other platforms such as Staging.

Power Ups

Chronicle Marketplace integrations

Chronicle Marketplace allows you to get the most out of the incorporated solutions by using integrations, investigating threats, and automating your SOC team's work.

Type here to locate a specific Chronicle SOAR Marketplace integration

- Active Directory (/chronicle/docs/soar/marketplace-integrations/active-directory)
- Alexa (/chronicle/docs/soar/marketplace-integrations/alexa)
- AlgoSec (/chronicle/docs/soar/marketplace-integrations/algosec)
- AlienVault USM Anywhere (/chronicle/docs/soar/marketplace-integrations/alienvault-usm-anywhere)
- AlienVault USM Appliance (/chronicle/docs/soar/marketplace-integrations/alienvault-usm-appliance)
- AlienVaultTI (/chronicle/docs/soar/marketplace-integrations/alienvaultti)
- Amazon Macie (/chronicle/docs/soar/marketplace-integrations/amazon-macie)
- Anomali (/chronicle/docs/soar/marketplace-integrations/anomali)
- Anomali Staxx (/chronicle/docs/soar/marketplace-integrations/anomali-staxx)
- Anomali ThreatStream (/chronicle/docs/soar/marketplace-integrations/anomali-threatstream)
- Any.Run (/chronicle/docs/soar/marketplace-integrations/any-run)
- APIVoid (/chronicle/docs/soar/marketplace-integrations/apivoid)
- AppSheet (/chronicle/docs/soar/marketplace-integrations/appsheet)
- ArcSight (/chronicle/docs/soar/marketplace-integrations/arcsight)
- ArcSight Logger (/chronicle/docs/soar/marketplace-integrations/arcsight-logger)
- Area1 (/chronicle/docs/soar/marketplace-integrations/area1)
- Armis (/chronicle/docs/soar/marketplace-integrations/armis)
- Atlassian Confluence Server (/chronicle/docs/soar/marketplace-integrations/atlassian-confluence-server)
- Attivo (/chronicle/docs/soar/marketplace-integrations/attivo)
- Automox (/chronicle/docs/soar/marketplace-integrations/automox)
- AWS Cloud Trail (/chronicle/docs/soar/marketplace-integrations/aws-cloud-trail)
- AWS CloudWatch (/chronicle/docs/soar/marketplace-integrations/aws-cloudwatch)
- AWS Elastic Compute Cloud (EC2) (/chronicle/docs/soar/marketplace-integrations/aws-elastic-compute-cloud-ec2)
- AWS GuardDuty (/chronicle/docs/soar/marketplace-integrations/amazon-guard-duty)
- AWS IAM Access Analyzer (/chronicle/docs/soar/marketplace-integrations/aws-iam-access-analyzer)
- AWS Identity and Access Management (IAM) (/chronicle/docs/soar/marketplace-integrations/aws-iam)
- AWS S3 (/chronicle/docs/soar/marketplace-integrations/aws-s3)
- AWS Security Hub (/chronicle/docs/soar/marketplace-integrations/aws-security-hub)
- AWS WAF (/chronicle/docs/soar/marketplace-integrations/aws-waf)
- Axonius (/chronicle/docs/soar/marketplace-integrations/axonius)

Chronicle SOAR Overview

Chronicle Security Orchestration, Automation and Response (SOAR) is a platform designed to help organizations detect, investigate, and respond to security threats in real-time. The platform is powered by Google Cloud's infrastructure and leverages the machine learning capabilities of Google to automate and streamline security workflows.

Chronicle SOAR collects data from various security sources such as network devices, endpoint agents, and threat intelligence feeds. The platform uses this data to identify potential security incidents and initiate response actions. Chronicle SOAR also integrates with other security tools such as SIEM (Security Information and Event Management), threat intelligence platforms, and vulnerability scanners to provide a comprehensive security solution.

The platform provides an intuitive user interface that allows security analysts to investigate incidents, create workflows, and automate response actions without requiring extensive coding knowledge. Chronicle SOAR also uses machine learning to improve its accuracy and speed in identifying and responding to security incidents. The platform's automated response capabilities help organizations to reduce the time taken to detect and respond to security threats, thereby reducing the risk of data breaches and other security incidents.

Chronicle SOAR is a powerful security orchestration, automation, and response platform that helps organizations to enhance their security posture by automating security workflows, reducing response times, and improving the accuracy of security operations.

Last updated 2023-09-20 UTC.

Working with Playbooks

Suggested articles

Using predefined widgets in Playbook views

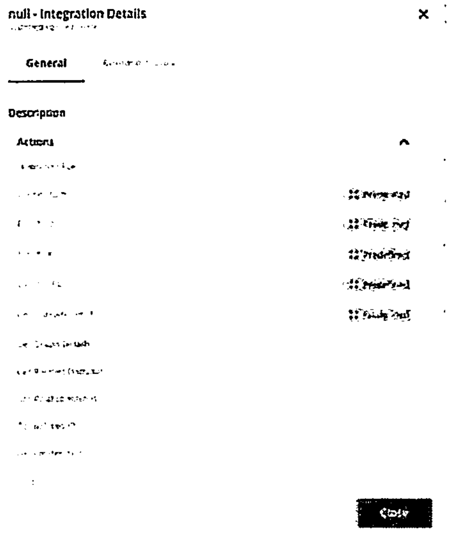
Predefined widgets are widgets that are attached to actions in an Integration in the Marketplace. They have been defined by Chronicle SOAR experts in order to return specific information for the action, thereby reducing the time required to customize and build the bespoke Playbook view

After downloading the Integration, the Actions will appear as usual for use when building the Playbook with special icons to denote if they have predefined widgets.

You can use these predefined widgets in existing Playbooks and also when building new Playbooks.

Let's take a look at how to build a new Playbook View with predefined widgets in VirusTotal actions.

1. Navigate to Marketplace > Integrations and select VirusTotal.
2. Click on the Read More. As you can see, two of the VT actions come with predefined widgets:



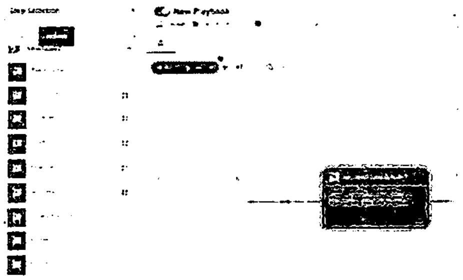
null - Integration Details

General

Description

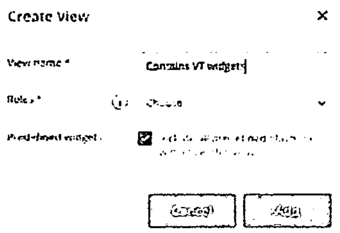
Actions

3. Make sure to download and configure the VirusTotal integration as required.
4. Now let's go to the Playbooks screen and take a look at using an Action with a predefined widget.
5. Create a new Playbook, open the Step Selector and drag and drop the VirusTotal Enrich hash Action. You can see that the action contains a special icon which lets you know it contains a predefined widget.



6. Let's now click on Add View and give it a name (Contains VT widgets) and choose a Role. In this example, we will keep the checkbox selected for including predefined widgets but note that you can always choose to opt out at this stage or even delete them after creating

the view.



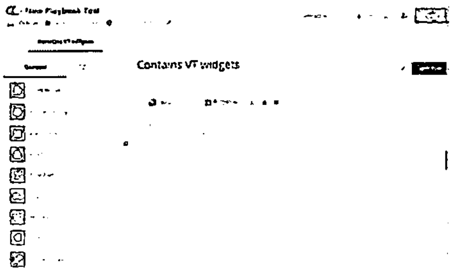
Create View

View name * Contains VT widgets

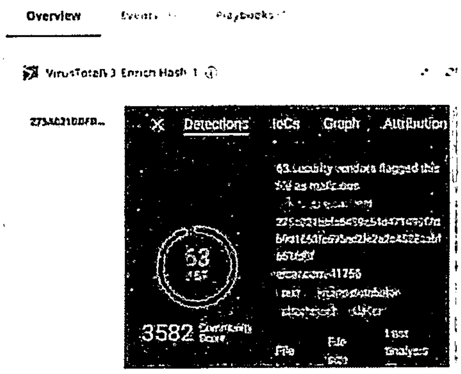
Roles * Choose

Predefined widget ☑

7. After you create the view, you can see that the widget is automatically added to the view. Note that you only can edit the following options in this widget: Name, Description, Conditions.

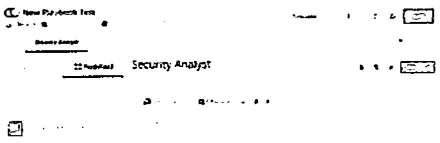


8. After the Playbook is attached to an alert, it will appear in the Alert view in the Playbook tab of the Case as shown below.



Let's now take a quick look at adding predefined widgets to existing Playbooks. Let's use VirusTotal again for this example.

1. Locate the required Playbook and open the Step Selection.
2. Drag and drop the VirusTotal Enrich URL action into the Playbook. Make sure to save!
3. Navigate to the View and you will see the predefined widget appears in the under the Predefined column on the left.



4. Drag and drop it into the View.

Working with Playbooks

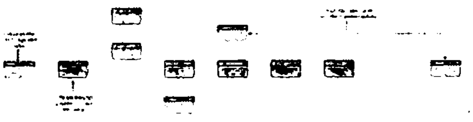
Suggested articles

Working with Playbook Blocks

Blocks are mini playbooks that users can create and reuse in other playbooks. The Blocks can implement workflows and logical decisions that might be useful in multiple playbooks. When you edit or change a Block, all playbooks using it will be affected which allows easy maintenance and playbooks improvement.
When Blocks are used within other playbooks, users can configure input parameter fields into the Block to alter its inner flow of actions.
The Block can also return an Output value into the parent playbook to allow interaction and conditioning between the two.

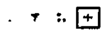
Before you create these blocks, it's advisable to spend time initially to map out specific processes that you can easily reuse in parent playbooks, as well as giving thought to input fields which can be configured per need.

The screenshot below provides an example of a reusable Block.

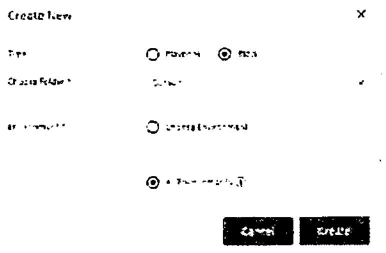


To add a new block:

1. In the Playbook screen, click the + icon on the right side of the screen.



2. For Type, select Block. Choose the folder and the environment and click Create. We recommend that Admin users click All Environments as best practice.



Create New ×

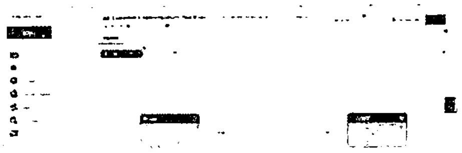
Type ○ Playbook ◉ Block

Choose Folder *

Environment * ○ Choose Environment

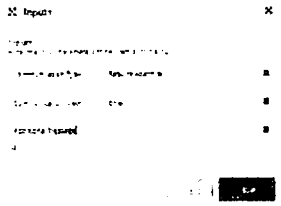
◉ All Environments

3. In the screen that opens, fill out the name of the new Playbook Block at the top of the screen. For this example, we will create a Block that handles all communication between the SOC and its clients.

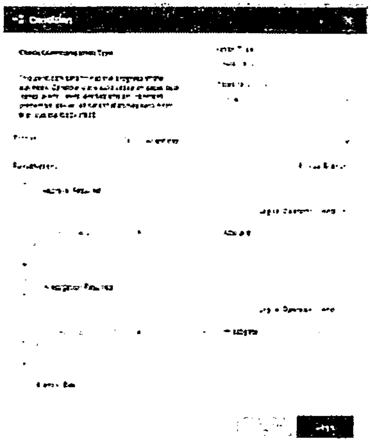


4. Let's start off by adding input parameters. Double click on the Input box and then click on the + icon to add the input name and value fields. You can add as many fields as you need. Enter the following for the name and default values in the fields and then, click Save:

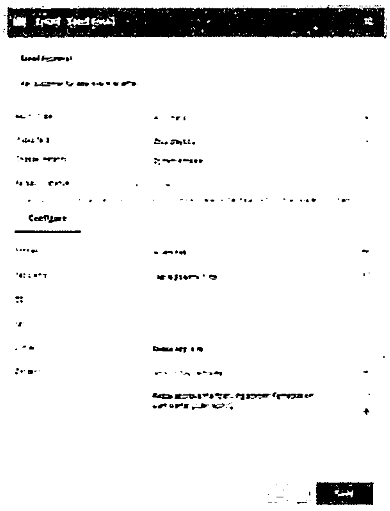
- Communication Type – Require Approval (where we have decided we will have two different communication types: Require Approval, Investigate)
- Communication Method – Email
- Additional Message – leave blank
  We will use these inputs to condition the flow of the Block
  If we add values here, they will act as default values. Note that they can be changed for each and every block after you have inserted them into the parent playbook.



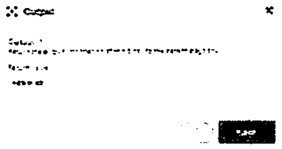
- Let's now add a Flow step which will direct the Playbook in a different direction according to which Input Type is entered.
  The types as we mentioned above are:
  Investigate
  Requires Approval
  Now let's put these into different branches. Use the placeholders to pick up the input types. As you can see in the following screenshot, we have two branches and an Else branch. The default branch which would go with the default input is branch 1.



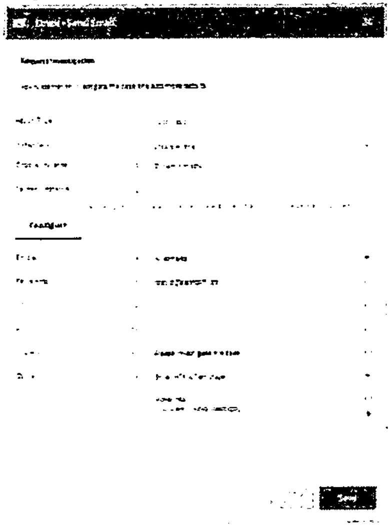
- The next stage would be to build action steps for each of the branches.
- Let's start with branch 1 which is the Require Approval branch. In the Actions column, select Email > Send Email and fill in the required parameters. This step sends an email asking the user for approval for a security analyst to perform Remediation on their machine.



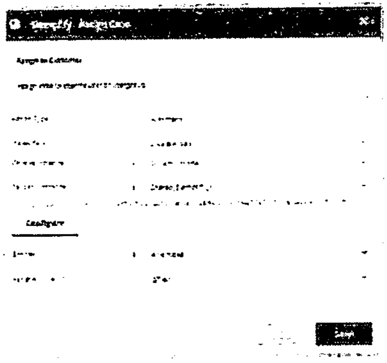
- In the next step, select Flow > Condition and fill in the required parameters. This step asks if the customer approved or not.
- In the Output step where the customer approved it, add the word Approved to be returned to the parent block.
- In the Output step of the Else branch, where the customer responded negatively, add Not Approved in the Output box.



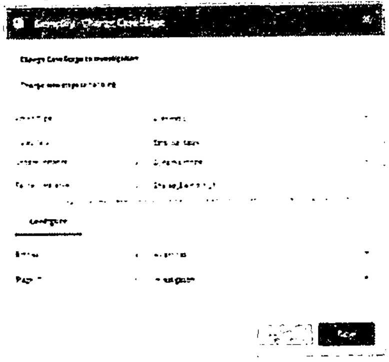
- Let's move onto the second branch. In this sequence we are defining what would happen if the Input Communication Type is Investigate. In the Actions column, select Email > Send Email and fill in the required parameters. In the screenshot below, you can see that we added the placeholder for the Additional Message. Make sure that you actually write a message in the Input Additional Message field if you change the Type to Investigate.



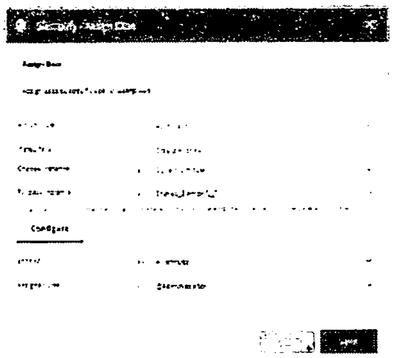
- In the next step, select Siemplify > Assign Case. Here we are going to put the responsibility for investigating the case over to the Customer to get his Tier 1 analyst to look at it.



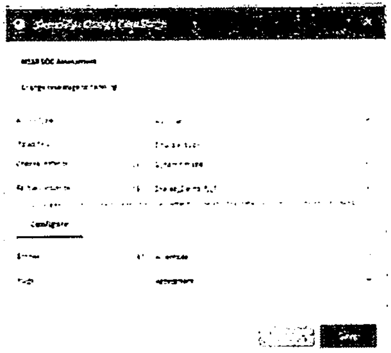
- In the next step, select Siemplify > Change Case Stage. This step presumes that we have received confirmation that the Customer is investigating and therefore we are changing the Case stage to Investigation.



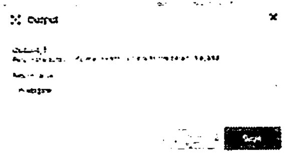
- In the next step, select Siemplify > Assign case. This step assumes that the customer has finished investigation and has asked the SOC to reclaim ownership of the case.



- In the next step, select Siemplify > Change Case Stage. This step now changes the case stage from Investigation to Assessment so that the SOC can carry on with his handling the case.



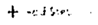
- In the Output step, add the word Investigation Completed to be returned to the parent playbook.



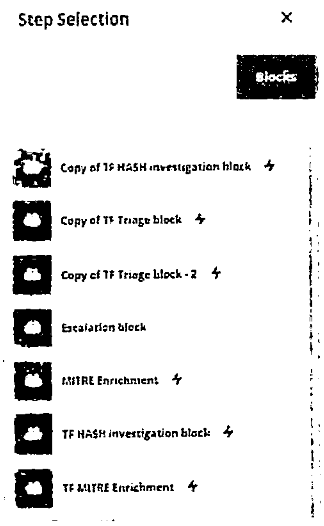
This block can now be inserted into various Playbooks.

To insert an existing block:

1. In the Playbooks screen, click Add Step.



2. In the Step Selection box, select the Blocks section.


Step Selection
×
Blocks
Copy of TF HASH investigation block ϟ
Copy of TF Triage block ϟ
Copy of TF Triage block - 2 ϟ
Escalation block
MITRE Enrichment ϟ
TF HASH investigation block ϟ
TF MITRE Enrichment ϟ

3. Drag the required block into the middle of the Playbook.

Siemplify built-in playbooks

Content:

Use-cases and their playbook

Brute force attempt

Description

Repeated attempts to log into a system using different user-names and/or passwords. The logs for the alert are gathered from the target system that some entity is trying to connect to.

Impact analysis

If the attack is successful, an attacker has access to a host machine inside the network, which could be used to launch further attacks on other machines in the network. In that case, impact is high. If the targeted machine is critical, the impact will increase to critical as well.

Enrichment

1) Source IP address – IP and is it internal or external
2) Target IP and OS information

Investigation

3) Is source IP internal?
   a. Internal:
      i. Search of any previous alerts raised on the entity (source IP), this machine might be already compromised in the past, and might still be compromised.
      ii. If the alerts are involving a malware alert – Escalate the case to TIER 2
      iii. TIER 2: Block the traffic from the source IP, disinfect the machine, verify the source of the malware and unblock the machine once no threats are found
   b. External:
      i. Search the IP using IP-reputation sites and act accordingly. (continue the next steps of this playbook to gather information for TIER 2)
4) Determine which data source was used to trigger the alert – is the alert based on network logs or actual on-host login information?
   a. Network based logs – Here we assume that the product triggering the alert cannot be sure about the traffic it monitors, as it might be encrypted. In this case, we only try to find out indicator of failure.
      i. Find out what port were used for the brute force.
      ii. Find if (and what) process is listening to the attack port.
      iii. If the attack port does not match any listening service, or and previously running service, mark the case FP (since there is no chance of success without a service listening on the port). Escalate the source IP's information to TIER 2 for further hunting, as this is still considered an indication of a malicious presence trying its 'luck' around the network

Virus found

Description

Virus found

Impact analysis

Viruses and malwares may cause harm to the resident data on the host machine which may include business critical data. As a virus does not provide anyone with the remote access to the system, severity in case of critical data affected would be **High**, and if no business-critical data was affected (although other user files may have been affected), then severity would be **Medium.**

Enrichment

1) Verify the log source (network based, antivirus, host based or ThreatIntel) and locate/extract the actual suspicious file
2) Find any other machines that triggered the same alert, and in case this alert was established as true, escalate the list of affected machines to TIER 2

Investigation

3) Study the malware/virus and variants on google to determine the severity and impact of the specific threat
4) Upload the suspicious binary to Virus Total and examine the detection ration
   a. If the detection ratio indicates of a malicious signature, escalate to TIER 2 with the gathered information
   b. If the detection ration indicates of a clean file, make the case FP and close it
5) If the case was escalated to TIER 2, supply TIER 2 with the following extra information:
   a. Binary file itself (for static/dynamic analysis)
   b. Any infected files – to determine whether business critical data was affected
   c. Victim's IP and source IP (if the source is known – in case the alert originated from a network based product)
   d. Initial information gathered about the malware type/family
   e. Potential impact on victim

Containment & Remediation: (after escalation - TIER 2)

6) If there is a source to the file, block it.
7) Disinfect the affected hosts that were found during the enrichment of TIER 1

Admin login fail

Description

A login failure attempt of an administrative account.

Impact analysis

According to the analysis results, if the attempt was successful and the admin actually logged in successfully, AND it was established as a malicious entity, only then the severity would be **High**. In other cases, while it is still a malicious entity **trying**, the severity would be medium, as it indicates of a presence of a threat which needs attention.

Enrichment

1) Determine the source of the alert – Network based or Host based
2) Note down the source and destination IPs

Investigation

3) If the log source is a host based (logs from the endpoint machine)
   a. Verify from the logs about the user of the system
      i. If the target machine is Windows, look for network information section in the win event ID 4625 (Failed logon) logs
         1. If it is blank or showing the same hostname (as the regular user), mark FP – it means that the owner of the system himself was trying to login
         2. If the network information shows another hostname/IP as the source:
            a. Verify it has any event of event ID 4624 (Successful logon)
               i. If it has, look for logon type field with value: 2, 3 or 10
               ii. If value 2 was found, mark the case FP (Highly unlikely that the logon made by the attacker himself, rather by a script)
               iii. If the value was 3 or 10, mark the case TP and escalate attacker information to TIER 2.
            b. If ID 4624 was not found, mark the case FP and search for previous malware alarms against the attacker (if any were found, investigate them according to the associated playbooks and escalate to TIER 2 if accordingly)
      ii. If target machine is Linux, look for "password check failed" login entry within the "authlog" logs.
         1. If found, notice the time difference and the user for which login failed.
            a. If same user in all attempts and the user is legitimate username (look for older entries of the same username) and time difference is in seconds – Mark the case FP (doesn't appear to be a script)

  b. Mark the case TP and escalate to TIER 2. The attempt either uses a lot of different username, 'weird' ones or just attempting to connect really quickly, which indicates on a dictionary based attack.

4) If the source of the attack is network based logs
   b. If target machine's OS is Windows:
      i. Verify the destination port (Should be 3389, default for RDP; If was not set to custom)
      ii. if destination port is 22 (ssh port, not feasible for a windows system, Network based system just saw traffic so an F.P because network based systems do not make decisions based on the target host's operating system)
         1. Mark it down as an F.P (because windows machines do not have ssh) and note down or blacklist the source IP
      iii. Escalate attacker information to tier 2 for hunting purposes (because a threat actor is present who is not successful yet but may be in future)

Containment & Remediation: (after escalation - TIER 2)

5) Use the affected hosts list for running a thorough forensic activity against each of the affected hosts.
6) Track all the changes made on the affected host, by the particular admin account(s) by analyzing host logs.
7) Hunt for any backdoors that may have been downloaded/installed, by analyzing the host's traffic (outbound and inbound connections for CnC communications)
8) Undo the changes or completely reimage the hosts, depending upon the changes made.
9) Eliminate any backdoors found and blacklist any malicious IPs found during step 7.

Excessive traffic inbound (streaming, web, etc.)

Description

An unusual amount of attempts/volume of traffic which is direction inbound is identified. This might indicate of some malicious entity downloading or trying to download files for its operation.

Impact analysis

If marked T.P, the impact would be **High** for all the cases except for the case if some file upload vulnerability was exploited successfully, in which case it should be **Critical.**

Enrichment

1. Note down the target IP and the applications deployed on affected IP

Investigation

2. Look for any known vulnerable version of any service.
    a. If found, look inside the access logs (web server) for:
        i. Any malicious strings in a pattern from same src IP. Such strings may mean there is a particular vulnerability which is being exploited or a bot attack is going on. Mark a T.P if too many requests form same IP in a very short interval are found.
        ii. Any random long strings in the web requests (GET/POST or others) as it may mean a buffer overflow exploitation scenario. Study the strings and verify if these are any known indicators of a specific attack.
    b. If found, mark T.P and escalate to Tier 2.
    c. If both of these not found, move to the next steps
3. Look for netflow logs, and src I.P wise inbound traffic volumes
    d. Study the I.P reputation, if bad mark T.P and escalate to Tier 2.
    e. Note down the src IPs which have generated the most traffic to port 80 on the victim host for escalation.

Containment & Remediation: (after escalation - TIER 2)

4. Block the malicious src IP in the firewall to prevent the malicious activity.
5. Look for FTP port open on the target machines and any related known vulnerability.
    a. Patch the vulnerability if found.
6. If target host is a web server, scan it for any file-upload vulnerability.
7. If a streaming or some other type of server, run a basic infrastructure scan using a vulnerability scanner.

Login at off hours Night: Admin login in non-working hours 22:00-06:00

Impact analysis

Same as 'Admin Login Fail'

Enrichment

1. Determine the nature of login as this information is vital in determining the nature of the attack and taking a decision later:
    a. Remote
    b. On host

Investigation

2. If on Host login:
    a. Note down the target host's IP and check:
        i. Whether the target IP is used by administrators? (Assets Inventory)
        ii. Whether the activity by administrators was prescheduled.
            1. If prescheduled and machine usage verified
            2. Mark F.P
            3. Otherwise Mark T.P and escalate the login details to Tier 2.
3. If remote login:
    a. If target machine's OS is Windows:
        iii. Verify the dest port (Should be 3389, default for RDP; If was not set to custom)
        iv. if dest port is 22 (ssh port, not feasible for a windows system, NIDS just saw traffic so an F.P)
            1. Mark it down as an F.P and note down or blacklist the source IP
            2. Escalate attacker information to tier 2 for hunting purposes
    b. If target machine's OS is Linux:
        v. Verify ssh service is running on the target system
            1. If not running, or port mismatches, mark an F.P
            2. If open, and port mismatches, mark an F.P
            3. If open and port matches to that in the alert, look for successful attempts on the target IP. If successful attempt found, mark T.P and escalate attacker information to tier 2.
4. Review the IT Security policy for timings issue.
    a. If policy allows IT administrators to perform scheduled tasks in off hours, and it was verified in above steps, mark F.P
    b. If doesn't allow, mark T.P and escalate to Tier 2.

Containment & Remediation: (after escalation - TIER 2)

5. Follow 'Admin Login Fail' playbook
6. Notify the owner of the malicious account, in case of intentional usage.
7. In case some IOCs are found, use corresponding playbook, depending upon the indicators.
8. In case of remote attempts, clean the host machine by running a thorough antivirus scan.

Login at off hours Weekend: Admin login in non-working weekend hours Friday-Sunday

Repeat same steps as for "Login at off hours Night: Admin login in non-working hours 22:00-06:00".

Malware Infections

Similar steps as "Virus Found"

Malicious Website

Impact Analysis

Sites marked malicious usually get highlighted in Threat Intel feeds for serving malicious content, like malwares and trojans etc. If the victims are users and it is confirmed that a malicious payload was delivered to the victim hosts, payload (malware, ransomware etc.) the severity will be **High** and if there are indicators that it got executed, the severity would be **Critical**. Moreover, the lists of these malicious websites also contain those domains which may have been previously compromised and are being used to run various kind of scans. In any of these cases, relevant playbooks should be followed to determine the impact.

Enrichment

9. Determine the source of the alert in order to build context and study the related rule which was triggered.
10. Determine the no. of occurrences of this alert and list down all the host's IPs.

Investigation

11. Check if source is Threat Intel feed
    a. If so, mark T.P
12. Determine if there are any previous alarms against the same dst host of the kind:
    a. Waterhole attack
    b. External to Internal Port Scan
    c. External to Internal Vulnerability Scan
13. If found, verify if the src IP is the one being investigated already.
    a. If verified, mark malicious.
14. Determine the reasons of site getting listed as malicious (e.g. unauthorized port/vulnerability scanning, served malicious content etc).
15. Whichever of the above found, follow relevant playbook.

Containment & Remediation: (after escalation - TIER 2)

16. Block the website (Public IP/IPs) in firewall.
17. Cleanup the affected hosts in your environment of the infections (if any).

Indicators of Compromise: Web server

Description

A typical web server is listening for connections on TCP port 80. The only connections you should see in firewall logs are random source IP addresses being permitted to access TCP port 80 on your server as the destination. When you open up a web browser and connect to a website your computer opens up one of these ports locally between 1024-65535 and makes a connection to TCP port 80 on the web server. So if you see a firewall log that shows your web server making a connection on a high source port to any other system someone is initiating a connection from that webserver. If they are browsing websites or hoping to other systems from here that should be frowned upon and corrected. Maybe this is someone who has already compromised the system and is sending information back to their website or FTP server. Similarly, if you see someone connect to a port other than 80 on that webserver then you have another server running. Either someone set something new up, or maybe this is a backdoor running.

Impact Analysis

If established a T.P, the severity would be **Critical** as this is a case of compromise of a web server.

Enrichment

1. Study the alert and note down the src IP(webserver) dst IP for which alarm was raised.
2. List down all the ports open on the victim host (webserver).
3. Collect Firewall logs for the time span found in alert.

Investigation

4. If dst IP has a bad reputation:
   a. Mark T.P and escalate with the collected info.
5. Look in the firewall logs:
   a. If connection was initiated by webserver to the suspicious IP (attacker), mark T.P and escalate with collected info.
6. If ports other than 80/443/22 are open on the webserver, look in the firewall logs:
   a. If there are any incoming connections on the open port on webserver from attacker IP (src IP), mark T.P and escalate with collected information. (Might be a backdoor)
7. If none of above cases are found to be true, look for any previous alarms against the webserver of type: Compromise/CnC/Malware infection and follow any relevant playbooks.

Containment & Remediation: (after escalation - TIER 2)

8. Block the dst IP (attacker's IP) in firewall.

Spear phishing campaign

Description

These alerts are raised when known phishing sites are observed to be communicating with the internal hosts or vice versa.

Impact Analysis

If marked T.P, the severity will be Critical. Such attacks are more lethal as these are targeted and show the presence of a threat actor/adversary who is targeting your organization.

Enrichment

1. Note down the src and dst IP addresses and ports.
2. List down all the email addresses against which the alerts were found.
3. Go through the email content and filter out all the URLs found in the emails.

Investigation

4. Resolve all URLs to IPs and check IP reputation for each IP.
    a. Mark T.P if bad and escalate the collected information.
    b. Otherwise continue.
5. Analyze URLs in sandboxed environment by following the URLs.
    a. Note any suspicious behavior:
        i. File downloaded.
        ii. Login page similar to famous sites, opens up.
        iii. Unknown redirections.
    b. If any of these found, mark T.P and escalate.

Containment & Remediation: (after escalation - TIER 2)

6. Once phishing is confirmed, throw a security alert email to whole organization, alarming them about the targeted activity going on.
7. Block all the malicious URLs found in the alerts (and IP addresses) in firewall.
8. Run thorough antimalware scans against the users who received the emails. (found in alerts)

Go gle Cloud

≡ Chronicle

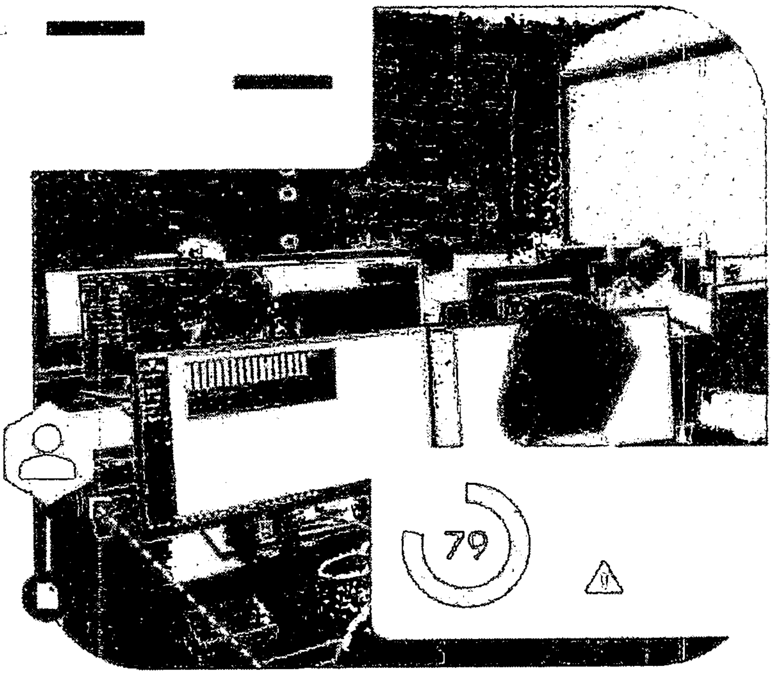
Contact us

[illegible] Learn More

[redacted]

[redacted]

[redacted]



[redacted]

CHRONICLE SECURITY OPERATIONS

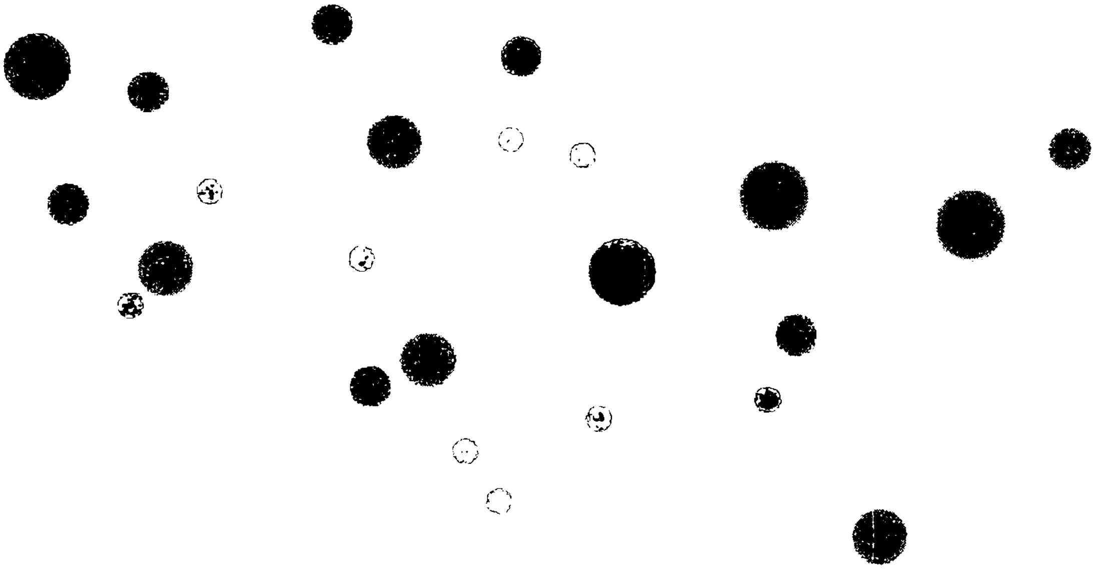
Respond to cyber threats in minutes, not hours or days

Chronicle enables modern, fast, and effective Security Orchestration, Automation and Response (SOAR) capabilities in one cloud-native, intuitive experience.

[illegible]

Privacy • Terms

Tag colleagues, assign tasks, and monitor progress of a case directly from the case wall to ensure every case is fully addressed and nothing falls through the cracks.



INSIGHTS

Capture SecOps insights consistently

Consolidate SecOps activity to easily generate insights that drive improvement and measure progress over time.

Track real-time SOC metrics and KPIs

Choose from out-of-the-box interactive reports and dashboard templates to see how your team is performing on the metrics that matter to you – from response rates to cases closed to improvement over time.

Leverage business intelligence to effectively measure and manage

Evaluation Checklist

Core SOC Management

Team Management

- □ Central View for SOC Tasks
- □ Task Delegation & Tracking
- □ Tier Management
- □ Shift Management & Handover
- □ In-App Notifications
- □ Group Chat

Access Control

- □ Shared & Classified Environments
- □ User Permissions Management
- □ Group Permissions Management

Dashboards & Metrics

- □ Customizable Large Dashboards Screen
- □ Custom KPI's & Metrics
- □ Recommended KPI's & Metrics (e.g. Human Workload, Bottlenecks etc.)
- □ SLA Tracking & Reporting
- □ Thresholds & Alerting
- □ Exporting to Report

Core Orchestration

Data Ingestion

- □ Multi Tenancy - Data Separation
- □ Source Selection (Email, SIEM, Tools etc.)
- □ Ingestion Performance Monitor
- □ Ability to Scale Up When Adding New Hardware Resources

Data & Work Prioritization

- □ Prioritization Rules Engine
- □ Automatic Case Prioritization
- □ Tasks Prioritization
- □ Workload Reduction
- □ Noise Reduction

Integrations

- □ Integrating with Existing Security Toolset
- □ 3rd Party Tools Automation
- □ Custom Integrations Editor (Python \ Scripting Based SDK)

Playbooks

- □ Drag-N-Drop Playbooks Editor
- □ Building Complex Workflows
- □ Variety of Playbook Triggers
- □ Using Security Tools in Flow
- □ Playbook Revision
- □ Playbook Testing

B. Vulnerability Management and Penetration Testing

B.1
Vulnerability Management

CrowdStrike Products

CROWDSTRIKE

Data Sheet

FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

Initiate emergency patching for critical vulnerabilities with native Falcon integrations

CROWDSTRIKE

CrowdStrike
Falcon Spotlight Vulnerability Data Add-on for Splunk

Installation and Configuration Guide v2.0+

Introduction

This guide covers the deployment, configuration and usage of the CrowdStrike Falcon Spotlight Vulnerability Data Technical Add-on (TA) for Splunk.

The CrowdStrike Falcon Spotlight Vulnerability Data Technical Add-on for Splunk allows CrowdStrike customers to retrieve CrowdStrike Spotlight Vulnerability data from CrowdStrike Falcon instance that have the Spotlight module enabled via API.

To get more information about this CrowdStrike Falcon Spotlight please refer to the documentation for the Spotlight module located in the CrowdStrike Falcon UI: https://falcon.crowdstrike.com/documentation/43/falcon-spotlight

Multitenancy - This TA is able to have multiple independent inputs enabled at the same time, each collecting data from different Falcon Instances and storing it in independent indexes.

This Technical Add-On does not currently support Falcon Flight Control Architectures. API access is direct to the Falcon Instance.

Requirements

The following are the requirements to leverage this technical add-on:

1. An active subscription to the CrowdStrike Falcon Spotlight Vulnerability module
2. A Splunk Heavy forwarder or Input Data Manager (IDM)
3. A Splunk account with proper access to deploy and configure technical add-ons
4. An active API credential with the proper API scope or access to the CrowdStrike Falcon instance to create one
5. The CrowdStrike Cloud environment that the Falcon instance resides in

If you do not have a current CrowdStrike Spotlight subscription:

1. Contact your CrowdStrike sales team to acquire one
2. Navigate to the CrowdStrike store in your falcon instance and request a trial: Click Here to See the CrowdStrike Spotlight App in the CrowdStrike Store

This Technical Add-On does not currently support Falcon Flight Control Architectures. API access needs to be direct to the Falcon Instance.

Getting Started

Spotlight Data Communication Flow

The CrowdStrike Falcon Spotlight Vulnerability Technical Add-on for Splunk leverages the 'combined' Spotlight API endpoint to collect vulnerability data. The TA communication process is as follows:

1. The TA will authenticate to the CrowdStrike API gateway for the configured CrowdStrike Cloud environment to collect an OAuth2 token
2. The OAuth2 token will then be used by the TA to connect and collect Spotlight vulnerability data from the CrowdStrike Spotlight API combined endpoint: /spotlight/combined/vulnerabilities/v1 *
3. Up to 4000 vulnerabilities will be called per API call **
4. Once all relevant data has been retrieved the TA will process the data
5. The TA will post each event to Splunk to be indexed

* The credential used to create the OAuth2 token must be scoped correctly to be able to connect to the Spotlight API
** multiple API calls maybe required to collect all available data

Data Volume Considerations

Spotlight Vulnerability data can be a large amount of data depending on the size of the environment and the time range of the data being collected. Some key considerations to take into account when collecting this data:

1. The amount of data that will be ingested
2. The available resources to collect and process the data
3. The time range or frequency of the data collection

KEY CAPABILITIES

REDUCE VULNERABILITY PRIORITIZATION EFFORT

Falcon Spotlight is a dynamic vulnerability management solution equipped with intuitive dashboards and powerful filtering capabilities, enabling you to improve your organization's security posture by serving up the most relevant information. Dashboard capabilities include:

- **ExPRT rating:** Immediately prioritize which vulnerabilities are truly relevant to your organization with a dynamic rating that more accurately shows risk levels. The rating is adjusted according to a vast database of source data.
- **Exploit status:** Using integrated vulnerability exploit and threat intelligence, you can easily identify which vulnerabilities in your environment represent the greatest risk, and build reports and dashboards that keep track of these vulnerabilities.
- **Recommended remediations:** Ensure that your remediation efforts are reducing the most risk. Falcon Spotlight intelligently recommends the highest-impact patches to deploy, reducing the chances of deploying a superseded patch.
- **Installed patches:** Use the Installed Patches page to identify which patches are active across your environment, or which patches have been installed but are pending a reboot.

AUTOMATE VULNERABILITY ASSESSMENT

Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.

IMPROVE SECURITY OPERATION EFFICIENCY

Streamline your vulnerability management program with custom dashboard features. Create and save custom filters so staff can quickly navigate and research critical issues. Use the custom team dashboards to share insights across your entire team, and set remediation timeframes to speed vulnerability resolution and increase your team's efficiency.

REDUCE OVERALL COMPLEXITY

Falcon Spotlight does not require an additional agent, and endpoints no longer need to use cumbersome hardware or weighty agents, or be on the network to be assessed. Falcon Spotlight is always on, seamlessly bridging the gap between vulnerability management and the rest of the Falcon platform, enriching threat detection and intelligence use cases. Simply select a vulnerability within the dashboard to see a wealth of data around threat actors, including threat intelligence reports and additional insights. Since all data is housed within the same console, analysts can pivot quickly to those vulnerabilities that show the most significant risk to resolve them first.

For hosts with critical vulnerabilities that need remediation instantly, IT staff can take advantage of emergency patching — it's a simple one-click action for Windows patch updates.

A SINGLE SOLUTION FOR CONTINUOUS VULNERABILITY ASSESSMENT AND MONITORING

Eliminate the need for cobbling together tools to get a complete vulnerability picture — Falcon Spotlight connects the dots, providing immediate visibility of your environment

Tap into the full power of contextual data by using threat intelligence in conjunction with Falcon Spotlight

Maintain business productivity with virtually no impact on any endpoint

Speed up your search results with custom saved searches or universal search to filter results across the entire Falcon console

Utilize the tight integration between the Falcon platform and other Falcon modules for additional in-depth research

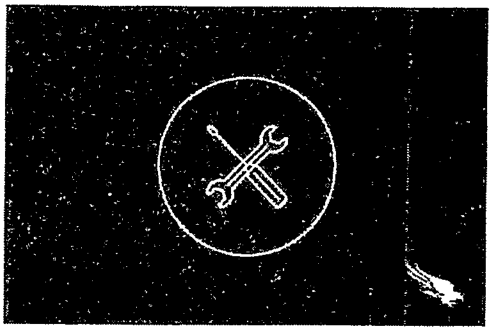
CROWDSTRIKE | BLOG

Featured Recent Videos Categories Start Free Trial

BACK TO TECH CENTER

How to Install Falcon in the Data Center

June 6 2017 Peter Ingebrigtsen Tech Center



Introduction

CrowdStrike Falcon® strikes the balance needed in today's data center: unrivaled protection from best-in-class prevention, detection and response along with security that actually contributes to the speed, flexibility, manageability and scalability benefits that IT operations expect from their modern-day data center. CrowdStrike Falcon® provides the following key benefits to data centers:

1. Speed and Simplicity.
   - No performance impact. Maximum security. Minimal impact. Data center guys typically hate security because it slows their servers down. This means that they have to purchase more servers to do the same job as one server could do before it got bogged down by security tools. CrowdStrike Falcon® is so lightweight that this problem goes away.
   - Easy to deploy. All you need is the Falcon sensor and an internet connection. There is no complex security infrastructure to manage. Just install the Falcon Sensor and go.
2. It Just Works. CrowdStrike works in all types of data centers, including on-prem, hybrid, and cloud. Falcon also works in multiple cloud platform environments, including Amazon AWS, Google Cloud Platform and Microsoft Azure. The Falcon sensor also supports Windows, Linux and macOS at the kernel level, on bare metal or as a VM, with minimal impact.
3. Ultimate Threat Protection. An organization's internet-facing servers are constantly under attack. We stand out in our ability to provide protection for the Linux OS – which especially important given its growing use in the data center. CrowdStrike Falcon® provides protection against all attack types, from the mundane opportunistic attacks to highly-targeted and sophisticated attacks. CrowdStrike provides protection against the threats that AV and Application Whitelisting miss.

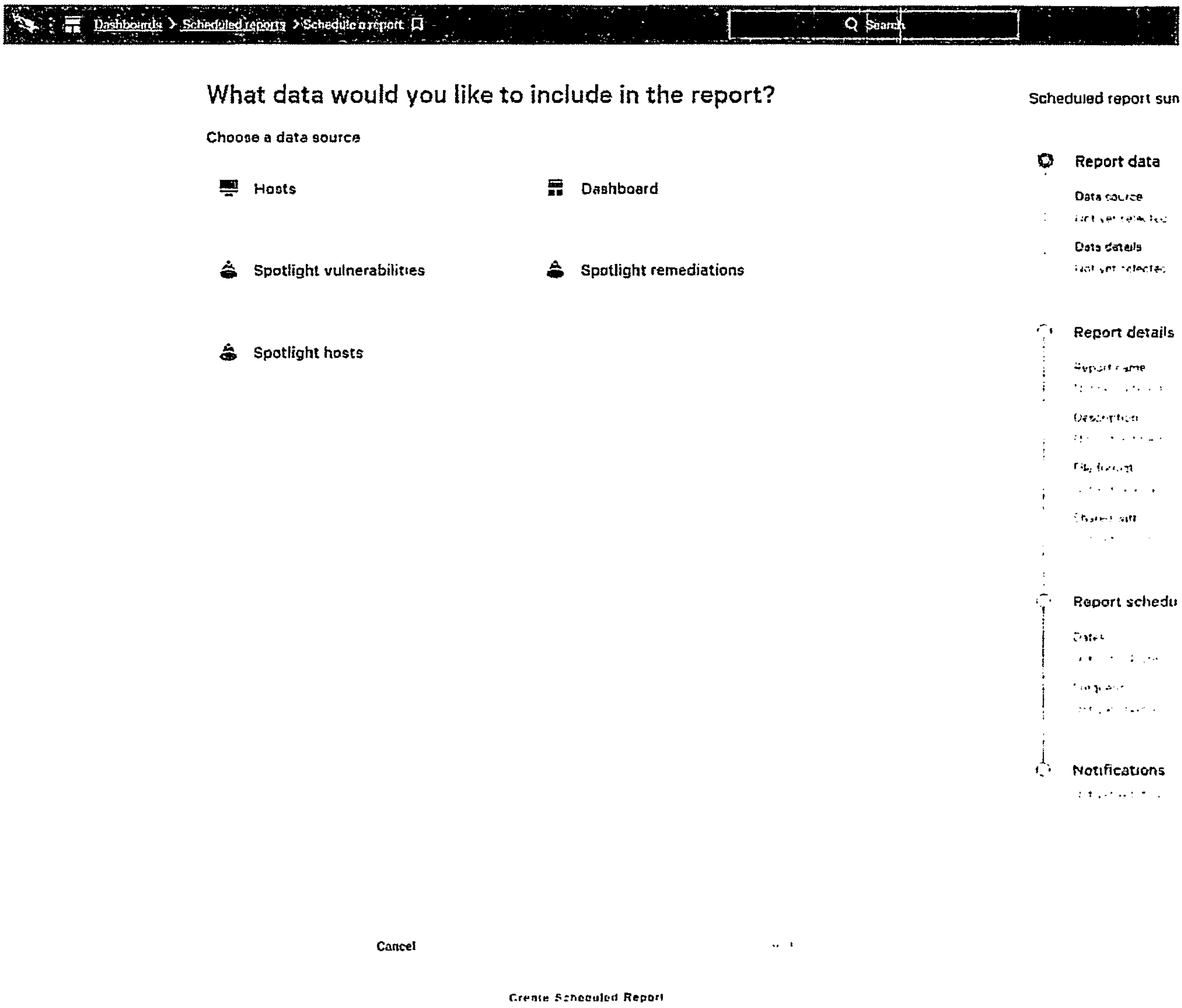
Video

Hey! What brings you to our corner of the internet today?

CROWDSTRIKE | BLOG

Customized Scheduled Reports

Reported based off dashboards or other data sources can be generated and sent automatically on a specified schedule.



Dashboards > Scheduled reports > Schedule a report

Search

What data would you like to include in the report?

Choose a data source

- Hosts
- Dashboard
- Spotlight vulnerabilities
- Spotlight remediations
- Spotlight hosts

Scheduled report sun

Report data

Data source

Not yet selected

Data details

Not yet selected

Report details

Report name

Description

File format

Shared with

Report schedu

Notifications

Cancel

Create Scheduled Report

Conclusion

As we can see, CrowdStrike's ability to customize dashboards provide high fidelity views of data for specific roles on the security team. This allows them to cut through the noise and save time while working faster to remediate attacks.

CrowdStrike Products

CROWDSTRIKE

Data Sheet

FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

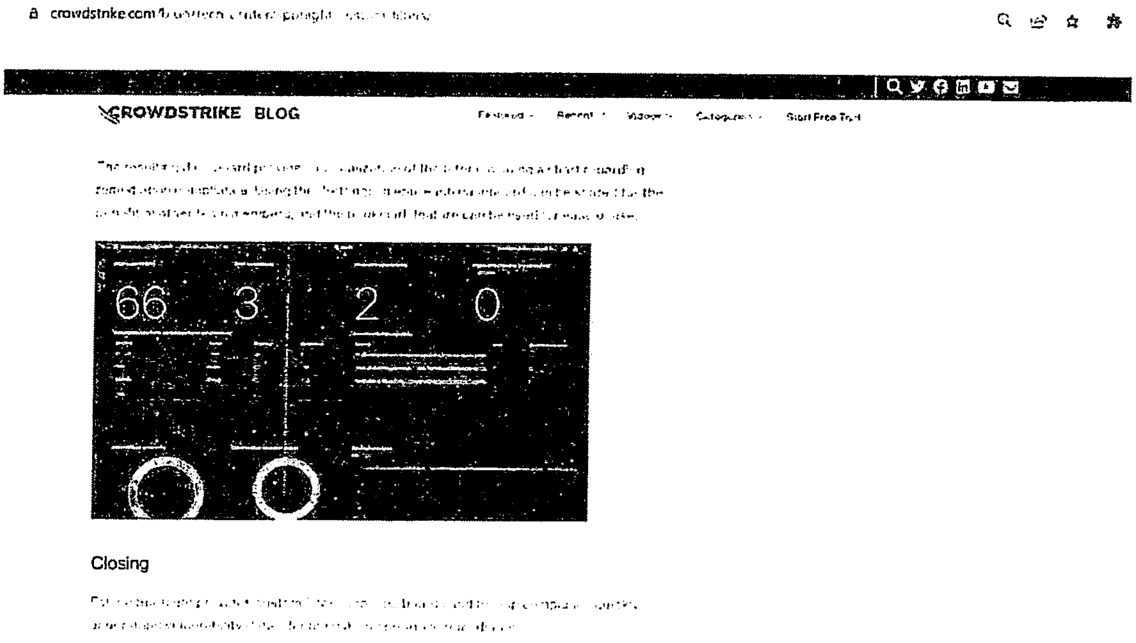
Initiate emergency patching for critical vulnerabilities with native Falcon integrations

crowdstrike.com/[illegible]

How to Use Custom Filters in Falcon Spotlight

Introduction

[illegible]



crowdstrike.com/[illegible]

[illegible]

Closing

[illegible]

Scheduled Reports

Last updated: Sep. 8, 2023

Overview

Create scheduled reports to get automatic, recurring updates of the data that matters most to you. You can download and share your scheduled reports, and receive a notification each time a new report is available.

For example, you might schedule reports for:

- A weekly summary of hosts in your environment
- Daily counts of hosts with critical vulnerabilities
- A monthly snapshot of the Executive Summary dashboard

Requirements

Default roles

- **Scheduled Report Admin:** Can assign and revoke the Scheduled Report Analyst role, create scheduled reports, view and manage any scheduled report in the CID, and view, download, and delete any generated report in the CID.
- **Falcon Administrator and Intel Admin:** Can assign and revoke the Scheduled Report Admin role plus perform any function given to **All other roles**.
- **Scheduled Report Analyst:** Can only access the Scheduled reports page and view and download generated reports of scheduled reports that have been specifically shared with them. You can assign this role to members of your team who need to access scheduled reports but do not need any other Falcon access. For example, you might assign this role to IT staff who need to access periodic reporting metrics to stay on top of vulnerabilities.
- **All other roles:** Can create scheduled reports, view and manage their own scheduled reports, and download and delete reports generated from their scheduled reports. They can also view and download reports generated from scheduled reports that have been shared with them.

CrowdStrike clouds

- Scheduled reports are supported across all CrowdStrike clouds.
- Slack, PagerDuty, Microsoft Teams, and webhook notifications are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.
- Email attachments are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.

Understanding scheduled reporting

Scheduled reports eliminate the need for manual report generation by providing automated, continuous updates of important metrics that you can share with your team. You specify the data to include, when the report runs, and who to notify when a new report is available. You can create scheduled reports with customized sets of host, vulnerability management, asset applications, or cloud security posture data. You can also schedule reports that provide a regular snapshot of various dashboards. Scheduled reports can run daily, weekly, or monthly at a time you choose, and you can notify designated recipients when new reports are available through email, Slack, PagerDuty, Microsoft Teams, or webhook. After creating a scheduled report, you can view and manage the report settings, manually run reports on demand, and download generated report files from the **Scheduled reports** page.

Scheduled report settings

When creating a new scheduled report, you customize settings in four main sections.

- Report data [/documentation/page/d31f69e2/scheduled-reports#a09c92b2]: The underlying data that populates the report

- Report details [/documentation/page/d31f69e2/scheduled-reports#i57e9fdb]: Basic report information, such as name, description, and output format
- Report schedule [/documentation/page/d31f69e2/scheduled-reports#g7f0a49e]: When to run the report and how often
- Notifications [/documentation/page/d31f69e2/scheduled-reports#d765d518]: Delivery destinations for new report notifications

Report data

A new scheduled report begins with a Falcon data source that specifies the type of data you want to see in the report. Depending on the data source you select, additional filtering options may be available to narrow the scope of the data that displays.

Data source

You can build a scheduled report from any of the following data sources you have access to:

Data source type	Description
Hosts	Schedule reports with data from the **Host Management** page at Host setup and management > Manage endpoints > Host management [/hosts/hosts].
Dashboard	Schedule automated generation of your **Private, Shared,** and **Preset** dashboards at Dashboards and reports > Dashboards [/dashboards-v2/].
Vulnerability management - vulnerabilities	Schedule reports with vulnerability data from the **Vulnerabilities** page at Exposure management > Vulnerability management > Vulnerabilities [/spotlight/vulnerabilities/group-by/cve].
Vulnerability management - remediations	Schedule reports with remediation data from the **Vulnerabilities** page at Exposure management > Vulnerability management > Vulnerabilities [/spotlight/vulnerabilities/group-by/cve].
Vulnerability management - Installed Patches	Schedule reports with data from **Installed Patches** at Exposure management > Vulnerability management > Installed patches [/spotlight/patches].
Vulnerability management - vulnerabilities with evidence	Schedule reports with vulnerability evaluation test results from the **Vulnerabilities** page at Exposure management > Vulnerability management > Vulnerabilities [/spotlight/vulnerabilities/group-by/cve].
Cloud Security Posture - IOA	Schedule reports with indicators of attack (IOA) findings in your cloud environment at Cloud security > Cloud security > Cloud security posture > Assessment > Behavior [/cloud-security/cspm/assessment/behavior] .
Cloud Security Posture - IOM	Schedule reports with indicators of misconfiguration (IOM) findings in your cloud environment at Cloud security > Cloud security > Cloud security posture > Assessment > Configuration [/cloud-security/cspm/assessment/configuration] .
FileVantage monitored changes	Schedule reports with data from the **File Integrity Changes** page at FileVantage > Changes [/filevantage/changes].
Assets - applications	Schedule reports with data about applications that are installed or used in your environment at

	Exposure management > Assets > Applications > Applications [/discover/applications/inventory].
Data source type	**Description**
Configuration assessments	Schedule reports with data about configuration assessments in your environment at Exposure management > Configuration assessment > Assessments [/configuration-assessment/assessments/group-by/rule] •

Filters

Cloud Security Posture, FileVantage, configuration assessment, vulnerability management, and **Hosts** data sources provide additional filters that you can use to customize the report data that displays. Filter options vary by data source. If no filters are applied, your report contains all available data from the selected source.

Dashboard types

The **Dashboard** data source requires you to select a specific dashboard to report on. Dashboard reports include all data the selected dashboard and do not allow additional filtering.

Usage notes:

- You can only schedule reports for dashboards you have access to.
- The scheduled reporting feature does not support Legacy dashboards.

Data details

The asset applications data source requires additional data to determine the report data that displays. Select an existing **Application group** or click to create a new one. Then, apply one of these criteria:

- At least one app in group is installed or used
- All apps in group are installed or used
- No apps in group are installed or used
- At least one app in group is not installed or used

Then, apply the filters you want to the data, such as the host groups to include in the report. If you don't apply filters, your report contains all available data from the selected source. For info about application groups, see Create application groups [/documentation/page/ab0b6dc5/asset-management-applications#k6cf93f9].

Report details

In the **Report details** section, provide basic information that defines your report.

- **Name:** Provide a descriptive name for the scheduled report. The name identifies the report on the Scheduled reports page. It also appears in report notifications.
- **Description:** Enter an optional description to briefly define the report contents or purpose.
- **File format:** Choose a file format for generating your reports.
  - **Vulnerability management and host reports:** JSON (default) or CSV
  - **Dashboard reports:** PDF
  - **Cloud Security Posture reports:** JSON
  - **Asset applications reports:** JSON or CSV (default)
- **Shared with:** Specify the users to share your report with. Users on this list are your account users that are entered in Falcon. You can share the report with as many users as you'd like. Your scheduled report will appear on shared users' **Scheduled reports** page with options to view the report history and download generated reports.

- Email attachments are only available for accounts based in CrowdStrike's US-1, US-2, and EU-1 clouds.

Email

Send scheduled report notifications to a specified list of email addresses in your approved domains. You can designate up to 10 email notification recipients per scheduled report, including people who are not Falcon users.

Email attachments

When configuring an email notification, you can choose to include generated report files as attachments (US-1, US-2, and EU-1 cloud-based accounts only). All email attachments are Base64 encoded for safe transmission. In addition, attachments containing CSV and JSON data are compressed into a ZIP file prior to Base64 encoding.

The maximum individual file size for an email attachment is 6MB (after Base64 encoding). Note that because Base64 encoding enlarges a file by approximately 33%, there is a difference in size between files directly downloaded from Falcon and those sent as email attachments. You should consider this enlargement factor when configuring your report data and frequency to keep email attachments below the required size limit. Files that exceed 6MB aren't included as attachments; however, the email notification includes a link to access the report in Falcon.

Note:

- Attaching reports sends data out of Falcon to systems that might have different security standards or terms and conditions.
- The file size limit for email attachments is subject to change in accordance with CrowdStrike policies.

Calculating email attachment file size

You can use the size of a report you've downloaded from Falcon [/documentation/page/d31f69e2/scheduled-reports] to help determine whether the file meets the allowed 6MB limit for email attachments. To account for compression and Base64 encoding in attachments, your downloaded file size should not exceed the following:

- PDF report files: 4MB max download size
- CSV and JSON report files: 30MB max download size

If a file is too large, you can adjust the report filters or run the report more frequently to reduce the size.

Slack

Route notifications to one or more channels in your integrated Slack account. A Slack integration through the CrowdStrike Store [/store-v2/91f3206aa38a436a82bf81fd9b883f2a] is required. For information about setting up a Slack integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

PagerDuty

Configure notifications to automatically open an incident in PagerDuty and alert relevant user groups. Select the PagerDuty source and severity from your connected service to configure notification delivery. A PagerDuty integration through the CrowdStrike Store [/store-v2/bd2a30880a08479ea21f2b3211af0c78] is required. You can get more info about setting up your PagerDuty integration in CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

Microsoft Teams

Send notifications to one or more channels in your integrated Microsoft Teams account. A Microsoft Teams integration through the CrowdStrike Store is required. For info about setting up a Microsoft Teams integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

Webhook

Distribute notifications to other applications through a webhook. A webhook integration through the CrowdStrike Store is required. For info about setting up a webhook integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

Scheduled report limits

As you create your scheduled reports, be aware of the following limitations.

Run a scheduled report on demand

In addition to the scheduled generation of reports, use the **Run report** option to generate a current report on demand. Just like reports that run on a schedule, notifications are sent to recipients and the report is saved in the report history when processing is complete.

Usage Notes":"

- Reports that you run on demand include a timestamp based on your local system time and not UTC time.
- The **Last report status** does not update in real time and might show as **Processing** even after processing is complete. You can periodically refresh the page to get the current status, or check for the completed report in the report history. If you receive report notifications, you'll be alerted when the report is ready.

To run a report on demand:

1. Go to Dashboards and reports > Dashboards > Scheduled reporting [/dashboards-v2/scheduled-reports] .
2. Click the three-dot menu on the right of the report you want to run and select **Run report**. The report begins processing and notifies designated recipients when the **Last report status** shows **Completed**.

Download a generated scheduled report

Download generated reports to review the report content. You can download reports from the report history of scheduled reports created by you and those that other users have shared with you. Reports are downloaded in the file format specified in the scheduled report settings.

1. Go to Dashboards and reports > Dashboards > Scheduled reporting [/dashboards-v2/scheduled-reports] .
2. Click the three-dot menu on the right of the scheduled report in the list and select **View report history.**
3. Find the report you want to download. Click the three-dot menu and select **Download.**

Deactivate a scheduled report

To stop running a report, deactivate it. When a report is deactivated, its **Schedule status** changes to **Inactive** and all further report generation stops. A deactivated report cannot be reactivated. Deactivated reports are automatically deleted after 30 days.

1. Go to Dashboards and reports > Dashboards > Scheduled reporting [/dashboards-v2/scheduled-reports].
2. Click the three-dot menu on the right of the report you want to deactivate and select **Deactivate.**

Take ownership of a scheduled report

Admin users can use the **Take Ownership** option to replace the owner of a scheduled report and become its owner. This is useful for reports that were created by a user who was later deleted. You must have an admin role, such as Scheduled Reports Admin, Falcon Admin, or Intel Admin, to use **Take Ownership.**

1. Go to Dashboards and reports > Dashboards > Scheduled reporting [/dashboards-v2/scheduled-reports].
2. Click the three-dot menu on the right of the report whose owner you want to replace and select **Take Ownership.**

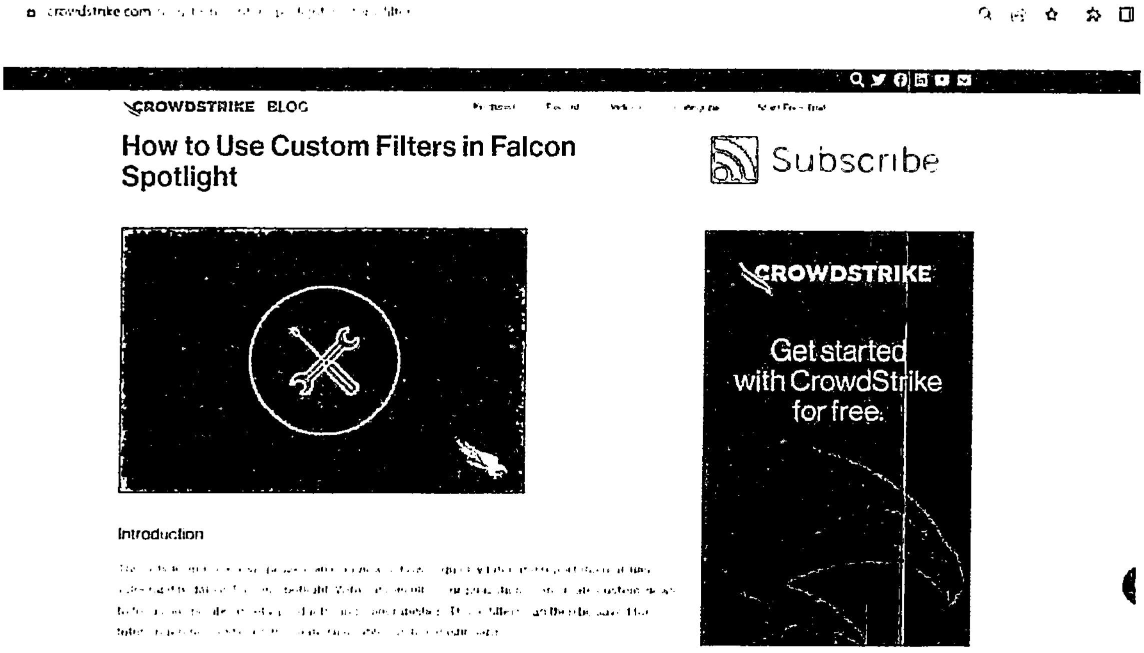
Delete a scheduled report

If you no longer need a scheduled report, you can delete it. Deleting a scheduled report permanently removes it from Falcon.

1. Go to Dashboards and reports > Dashboards > Scheduled reporting [/dashboards-v2/scheduled-reports] .
2. Click the three-dot menu on the right of the report you want to delete and select **Delete.**

Scheduled report notification configuration fields

When configuring a scheduled report, set up notifications if you want to alert others each time that the scheduled report runs. For more info about notifications and app integrations, see Notifications [/documentation/page/d31f69e2/scheduled-reports#d765d518].



crowdstrike.com [illegible]

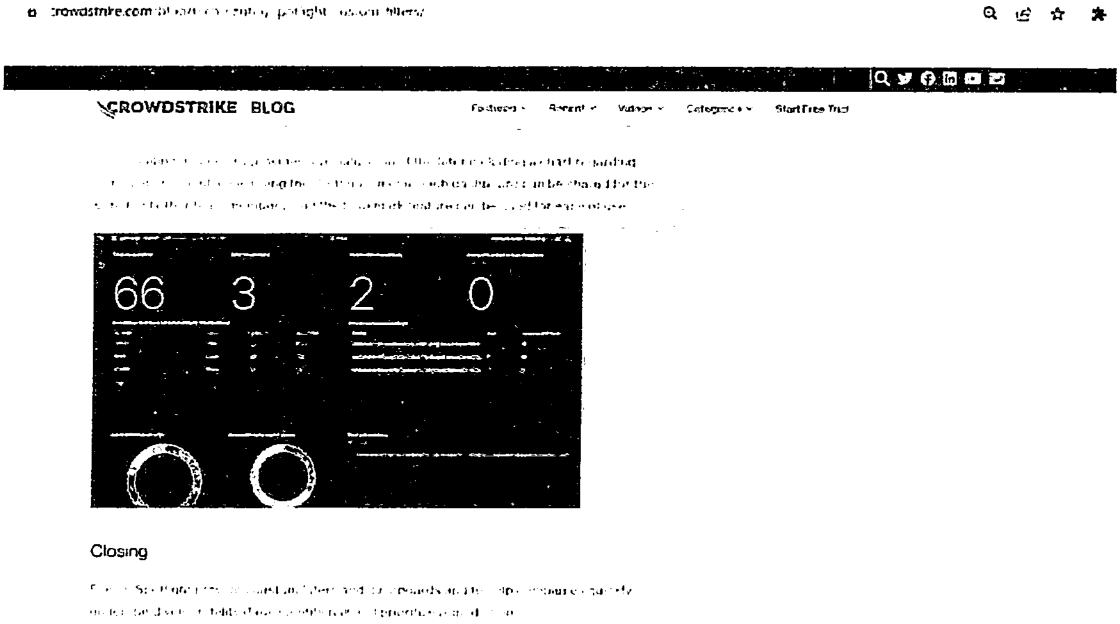
CROWDSTRIKE BLOG

How to Use Custom Filters in Falcon Spotlight

Subscribe

Introduction

[illegible]



crowdstrike.com [illegible]

CROWDSTRIKE BLOG

Start Free Trial

[illegible]

Closing

[illegible]

Vulnerability Management: Installed Patch Monitoring

Last updated: Aug. 29, 2023

Vulnerability Management: Installed Patch Monitoring

You now access Spotlight from a new console menu location: **Exposure management > Vulnerability management**.

You now access Spotlight's product documentation from **Support and resources > Documentation > Exposure Management > Vulnerability Management**.

For more info, see Release Notes, Updated Console Menu, Roles, and API Scopes [/support/news/release-notes-updates-to-console-menu-roles-and-api-scopes].

Overview

Monitor patches on Windows-based hosts in your environment within the Falcon console.

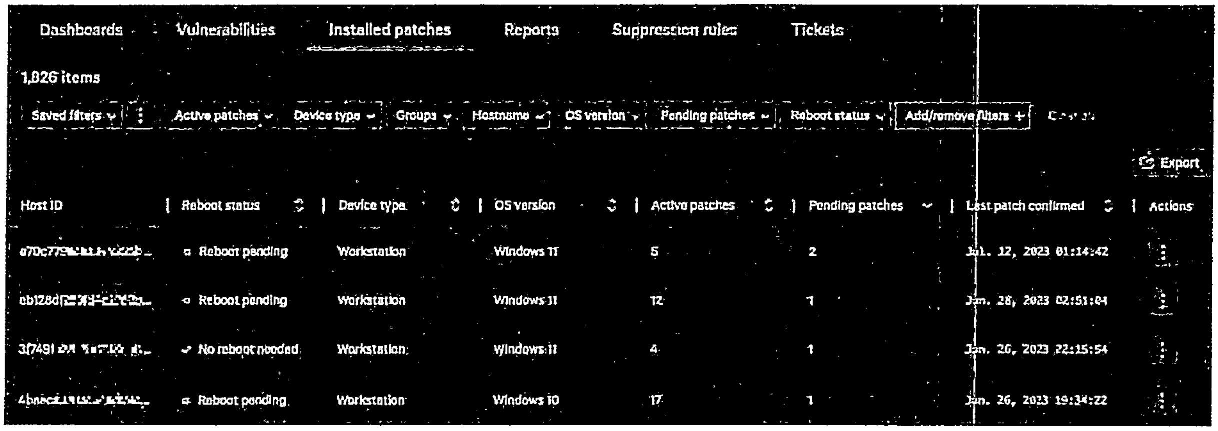
- Identify hosts with active Windows Update patches.
- Identify hosts with pending patches that require a reboot.
- View patch details for individual hosts.
- Export patching reports.

Requirements

- **Subscriptions supported:** Falcon Exposure Management and Falcon Spotlight (a Falcon Insight XDR add-on)
- **Default roles:** Falcon Administrator, Exposure Management Manager, and Vulnerability Manager

Installed patches page

Go to Exposure management > Vulnerability management > Installed patches [/spotlight/patches] to review Windows Update patching information for your organization's hosts. The **Installed patches** table reports on individual hosts.

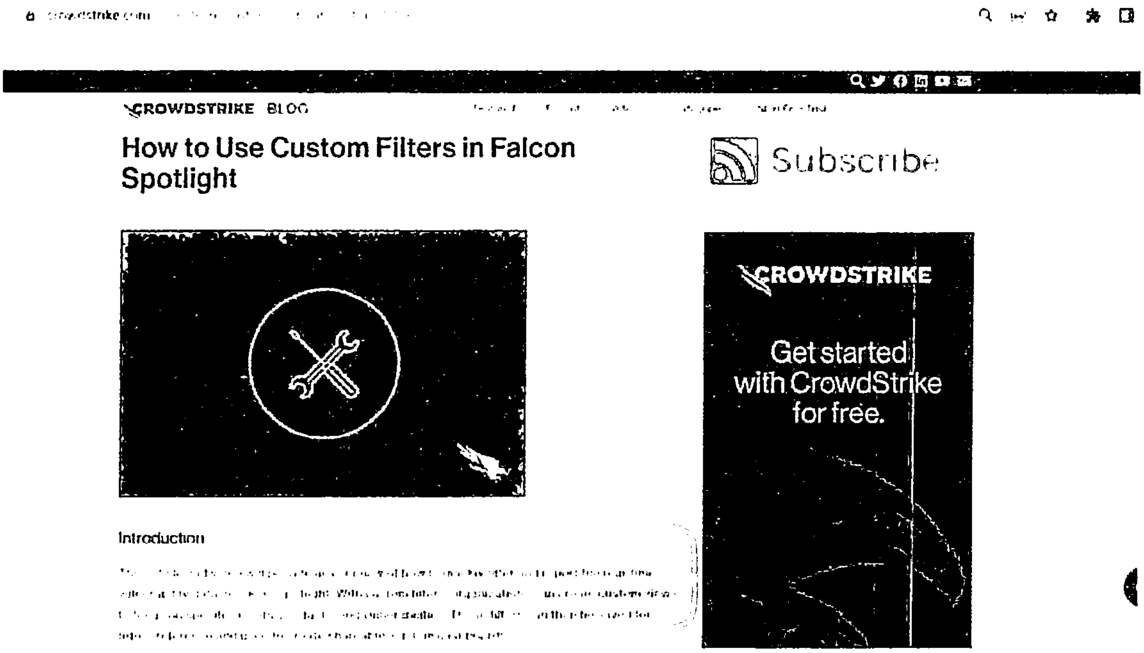


1,826 items

Host ID	Reboot status	Device type	OS version	Active patches	Pending patches	Last patch confirmed	Actions
a70c77[illegible]...	Reboot pending	Workstation	Windows 11	5	2	Jul. 12, 2023 01:14:42	⋮
cb128d[illegible]...	Reboot pending	Workstation	Windows 11	12	1	Jun. 28, 2023 02:51:04	⋮
3f7491[illegible]...	✓ No reboot needed	Workstation	Windows 11	4	1	Jun. 26, 2023 22:15:54	⋮
4b[illegible]...	Reboot pending	Workstation	Windows 10	17	1	Jun. 26, 2023 19:34:22	⋮

To view additional info, in the **Actions** column for a host, click **Open menu** ⋮ and select:

- **View host summary:** Open the host details panel.
- **View patch details** page: Open the **Patch details** page.
- **View in Host Management:** View host details on the **Host Management** page.



crowdstrike.com

CROWDSTRIKE BLOG

How to Use Custom Filters in Falcon Spotlight

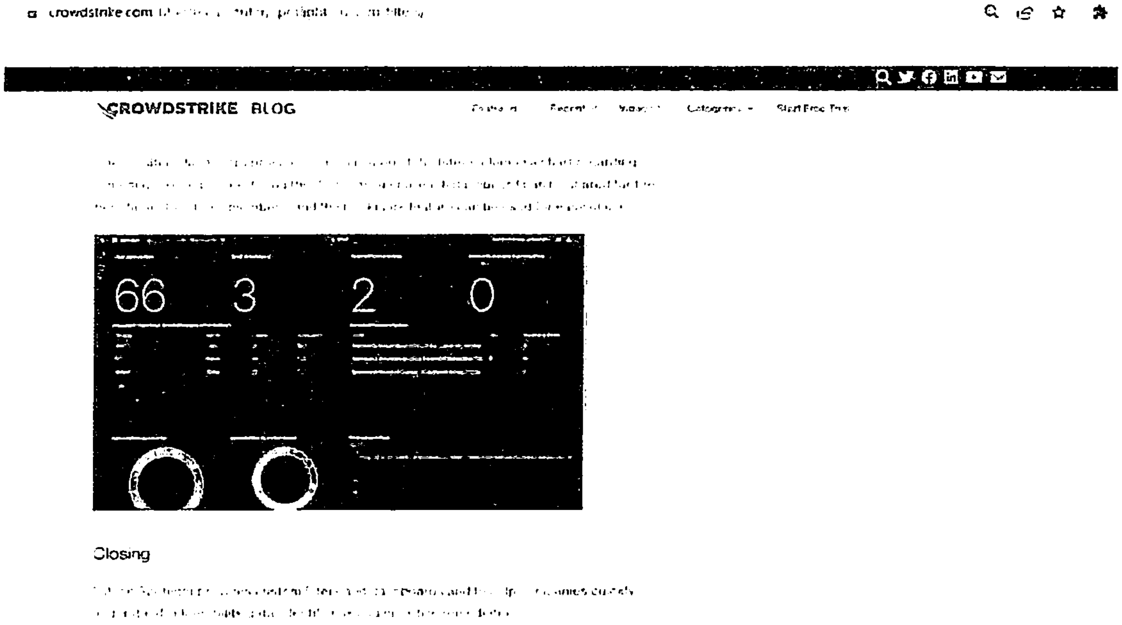
Subscribe

CROWDSTRIKE

Get started with CrowdStrike for free.

Introduction

[illegible]



crowdstrike.com

CROWDSTRIKE BLOG

[illegible]

Closing

[illegible]

KEY CAPABILITIES

REDUCE VULNERABILITY PRIORITIZATION EFFORT

Falcon Spotlight is a dynamic vulnerability management solution equipped with intuitive dashboards and powerful filtering capabilities, enabling you to improve your organization's security posture by serving up the most relevant information. Dashboard capabilities include:

- **ExPRT rating:** Immediately prioritize which vulnerabilities are truly relevant to your organization with a dynamic rating that more accurately shows risk levels. The rating is adjusted according to a vast database of source data.
- **Exploit status:** Using integrated vulnerability exploit and threat intelligence, you can easily identify which vulnerabilities in your environment represent the greatest risk, and build reports and dashboards that keep track of these vulnerabilities.
- **Recommended remediations:** Ensure that your remediation efforts are reducing the most risk. Falcon Spotlight intelligently recommends the highest-impact patches to deploy, reducing the chances of deploying a superseded patch.
- **Installed patches:** Use the Installed Patches page to identify which patches are active across your environment, or which patches have been installed but are pending a reboot.

AUTOMATE VULNERABILITY ASSESSMENT

Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.

IMPROVE SECURITY OPERATION EFFICIENCY

Streamline your vulnerability management program with custom dashboard features. Create and save custom filters so staff can quickly navigate and research critical issues. Use the custom team dashboards to share insights across your entire team, and set remediation timeframes to speed vulnerability resolution and increase your team's efficiency.

REDUCE OVERALL COMPLEXITY

Falcon Spotlight does not require an additional agent, and endpoints no longer need to use cumbersome hardware or weighty agents, or be on the network to be assessed. Falcon Spotlight is always on, seamlessly bridging the gap between vulnerability management and the rest of the Falcon platform, enriching threat detection and intelligence use cases. Simply select a vulnerability within the dashboard to see a wealth of data around threat actors, including threat intelligence reports and additional insights. Since all data is housed within the same console, analysts can pivot quickly to those vulnerabilities that show the most significant risk to resolve them first.

For hosts with critical vulnerabilities that need remediation instantly, IT staff can take advantage of emergency patching — it's a simple one-click action for Windows patch updates.

A SINGLE SOLUTION FOR CONTINUOUS VULNERABILITY ASSESSMENT AND MONITORING

Eliminate the need for cobbling together tools to get a complete vulnerability picture — Falcon Spotlight connects the dots, providing immediate visibility of your environment

Tap into the full power of contextual data by using threat intelligence in conjunction with Falcon Spotlight

Maintain business productivity with virtually no impact on any endpoint

Speed up your search results with custom saved searches or universal search to filter results across the entire Falcon console

Utilize the tight integration between the Falcon platform and other Falcon modules for additional in-depth research

CrowdStrike Products

CROWDSTRIKE

Data Sheet

FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

Initiate emergency patching for critical vulnerabilities with native Falcon integrations

KEY CAPABILITIES

REDUCE VULNERABILITY PRIORITIZATION EFFORT

Falcon Spotlight is a dynamic vulnerability management solution equipped with intuitive dashboards and powerful filtering capabilities, enabling you to improve your organization's security posture by serving up the most relevant information. Dashboard capabilities include:

- **ExPRT rating:** Immediately prioritize which vulnerabilities are truly relevant to your organization with a dynamic rating that more accurately shows risk levels. The rating is adjusted according to a vast database of source data.
- **Exploit status:** Using integrated vulnerability exploit and threat intelligence, you can easily identify which vulnerabilities in your environment represent the greatest risk, and build reports and dashboards that keep track of these vulnerabilities.
- **Recommended remediations:** Ensure that your remediation efforts are reducing the most risk. Falcon Spotlight intelligently recommends the highest-impact patches to deploy, reducing the chances of deploying a superseded patch.
- **Installed patches:** Use the Installed Patches page to identify which patches are active across your environment, or which patches have been installed but are pending a reboot.

AUTOMATE VULNERABILITY ASSESSMENT

Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.

IMPROVE SECURITY OPERATION EFFICIENCY

Streamline your vulnerability management program with custom dashboard features. Create and save custom filters so staff can quickly navigate and research critical issues. Use the custom team dashboards to share insights across your entire team, and set remediation timeframes to speed vulnerability resolution and increase your team's efficiency.

REDUCE OVERALL COMPLEXITY

Falcon Spotlight does not require an additional agent, and endpoints no longer need to use cumbersome hardware or weighty agents, or be on the network to be assessed. Falcon Spotlight is always on, seamlessly bridging the gap between vulnerability management and the rest of the Falcon platform, enriching threat detection and intelligence use cases. Simply select a vulnerability within the dashboard to see a wealth of data around threat actors, including threat intelligence reports and additional insights. Since all data is housed within the same console, analysts can pivot quickly to those vulnerabilities that show the most significant risk to resolve them first.

For hosts with critical vulnerabilities that need remediation instantly, IT staff can take advantage of emergency patching — it's a simple one-click action for Windows patch updates.

A SINGLE SOLUTION FOR CONTINUOUS VULNERABILITY ASSESSMENT AND MONITORING

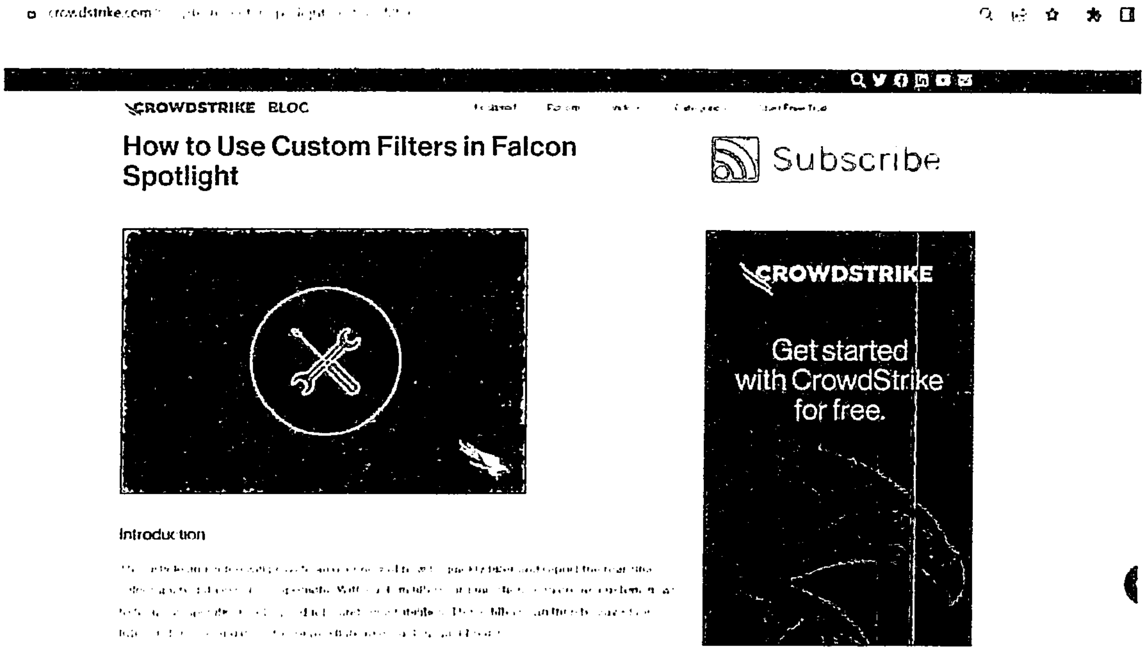
Eliminate the need for cobbling together tools to get a complete vulnerability picture — Falcon Spotlight connects the dots, providing immediate visibility of your environment

Tap into the full power of contextual data by using threat intelligence in conjunction with Falcon Spotlight

Maintain business productivity with virtually no impact on any endpoint

Speed up your search results with custom saved searches or universal search to filter results across the entire Falcon console

Utilize the tight integration between the Falcon platform and other Falcon modules for additional in-depth research



crowdstrike.com [illegible]

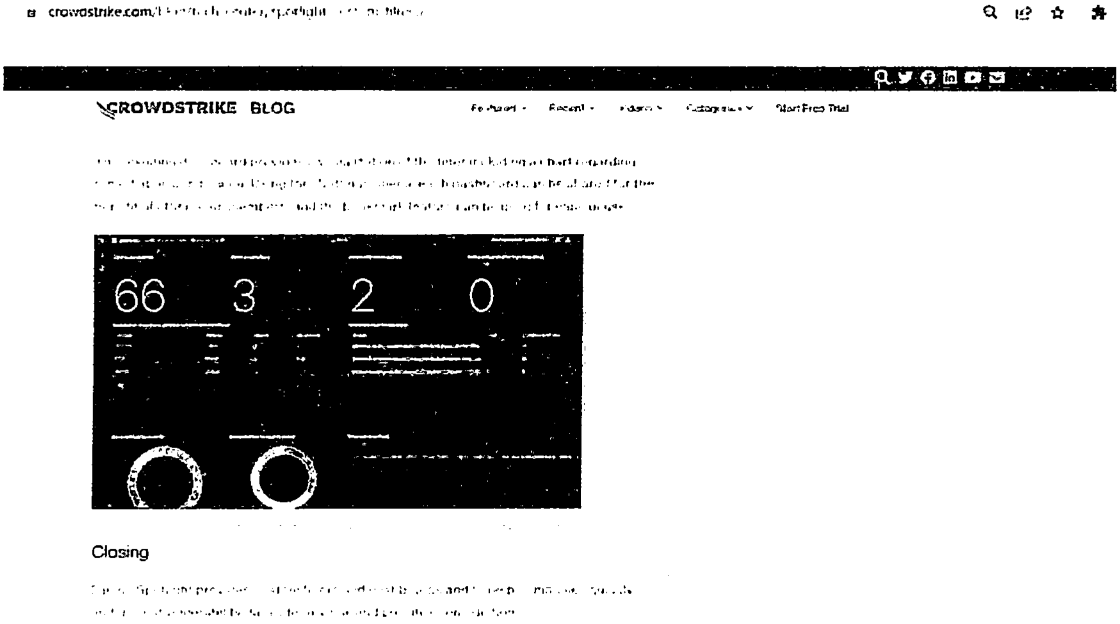
CROWDSTRIKE BLOG

How to Use Custom Filters in Falcon Spotlight

Subscribe

Introduction

[illegible]



crowdstrike.com/[illegible]

CROWDSTRIKE BLOG

Featured · Recent · Videos · Categories · Start Free Trial

[illegible]

Closing

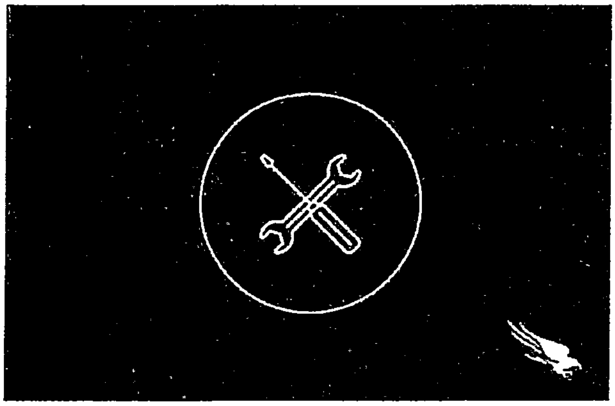
[illegible]

CROWDSTRIKE BLOG

BACK TO TECH CENTER

Using Falcon Spotlight for Vulnerability Management

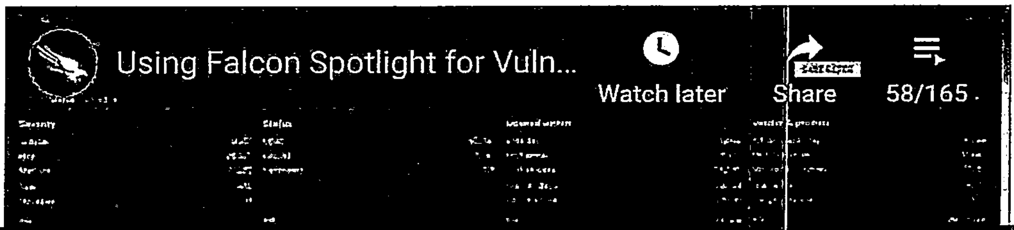
February 4, 2022   Rachel Scoboy   Tech Center

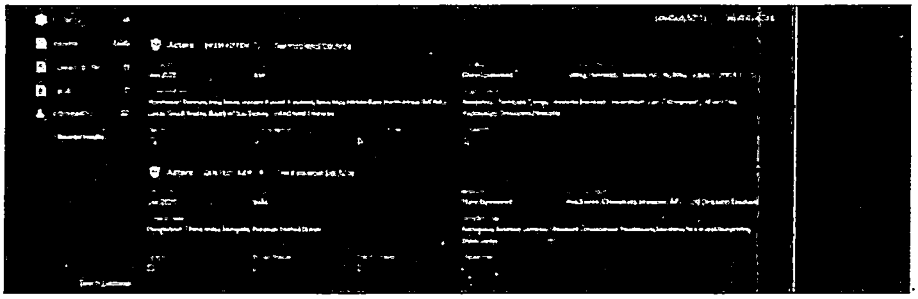


Introduction

This document and video will demonstrate how to use Falcon Spotlight to assess, report and research vulnerabilities in your environment while overcoming the challenges with traditional vulnerability management solutions.

Video

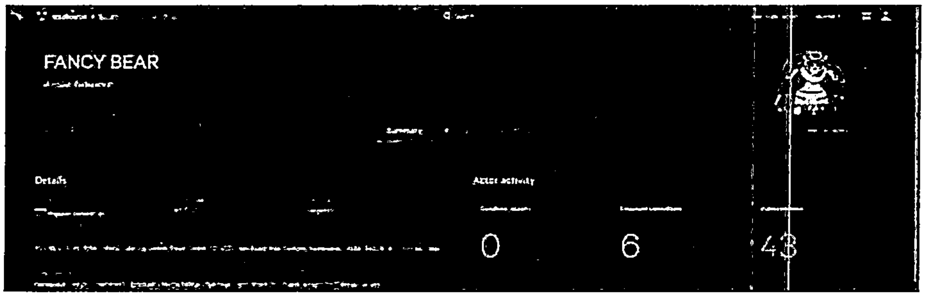




Spotlight for Investigations

In the situation of an incident or compromised system, Spotlight can also be used to assess the health of a given host. This host has a number of open vulnerabilities across multiple applications. Again, the export option can be used to share this information with the patch management team to prioritize the remediation.

The valuable vulnerability data can also be found in the actor profiles. When an actor is known to use a specific CVE, Falcon Spotlight provides additional context by showing the number of vulnerable hosts corresponding to each CVE.



B.2
Vulnerability Assessment and Penetration Testing (VAPT)

TRENDS | Managed ICT Services
Service Delivery with Flexibility

VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS

This document serves as the reference of the Vulnerability Assessment and Penetration Testing process.

DOCUMENT ID	
DOCUMENT OWNER	**TRENDS Vulnerability Assessment and Penetration Testing**
DOCUMENT CLASSIFICATION	TLP:GREEN INTERNAL
DOCUMENT STATUS	**RELEASE**
DOCUMENT VERSION	**1.0**
REVISION DATE	**2023 SEPTEMBER 01**

TABLE OF CONTENTS

1. Introduction

1.1 Overview

In today's digital age, cybercriminals use evolving tools, techniques, and processes to compromise organizations. Safeguarding sensitive information and critical systems is paramount. To fortify defenses against this, it is important to regularly test your organization's cybersecurity using a proactive approach.

The Vulnerability Assessment and Penetration Testing offers various benefits to the organization when it comes to cyber security like:

- This will give the organization a comprehensive evaluation of your application, system, or network.
- This will help the organization to understand the loopholes or errors that can lead to major cyber-attacks.
- It gives a more detailed view of the threats that your network, system, or application is facing.
- This helps the organization to protect their data and system from malicious attacks.
- This will help the organization to protect your business from data loss and unauthorized access.
- This also helps the organization in protecting the data from outside and insider threats.

1.2 Purpose of the Document

This document defines the methodologies and procedures for performing Vulnerability Assessment and Penetration Testing.

1.3 Target Readership

This document is prepared for the following:

- TRENDS, MICTS, Service Operations
- Any authorized person or entity requiring information and education about the subject matter at hand.

1.4 Document Definitions

Term	Definition
Vulnerability Assessment (VA)	refers to the process of identifying risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem.
Penetration Test (PT)	is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.
Vulnerability	is a weakness or opportunity in an information system that cybercriminals can exploit and gain unauthorized access to a computer system. Vulnerabilities weaken systems and open the door to malicious attacks.
Exploit	is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system, typically for malicious purposes such as installing malware. An exploit is not malware itself, but rather it is a method used by cybercriminals to deliver malware.
Threat	is something that can exploit a vulnerability.
Risk	is damage that could be caused by the open vulnerability being

	exploited by a threat
Privilege Escalation	is the exploitation of a programming error, vulnerability, design flaw, configuration oversight or access control in an operating system or application to gain unauthorized access to resources that are usually restricted from the application or user.
Cybersecurity	is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.
Cybercriminal	is a person who conducts some form of illegal activity using computers or other digital technology such as the Internet. The criminal may use computer expertise, knowledge of human behavior, and a variety of tools and services to achieve his or her goal.

1.5 Reference Documents and Bibliography

https://www.beyondtrust.com/resources/glossary/vulnerability-assessment
https://www.contrastsecurity.com/glossary/penetration-testing
https://www.simplilearn.com/vulnerability-in-security-article
https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html
https://www.upguard.com/blog/privilege-escalation
https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security
https://www.sciencedirect.com/topics/computer-science/cybercriminals
https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing

2. Purpose and Objective

2.1 Purpose

The purpose of the Vulnerability Assessment and Penetration Testing process is to establish methodologies and procedural frameworks that serve as a definitive guide for conducting the service. It ensures that all phases of the service are conducted systematically and consistently.

2.2 Objective

The objectives of having Vulnerability Assessment and Penetration Testing process are the following:

- To have a document that contains established methodologies and procedures in performing the service.
- To establish KPIs for measuring the effectiveness and efficiency of the methodologies and procedures.

3. Scope and Definition

This Vulnerability Assessment and Penetration Testing will be performed annually based on agreed schedules and scope with the agencies. The VAPT scope may include targets such as but not limited to network infrastructure, network devices, servers, workstations, applications, (e.g., public-facing web and mobile applications), and APIs, endpoints, hosts and database, including member service systems or kiosks, if any and among others.

4. Vulnerability Assessment and Penetration Testing Methodology

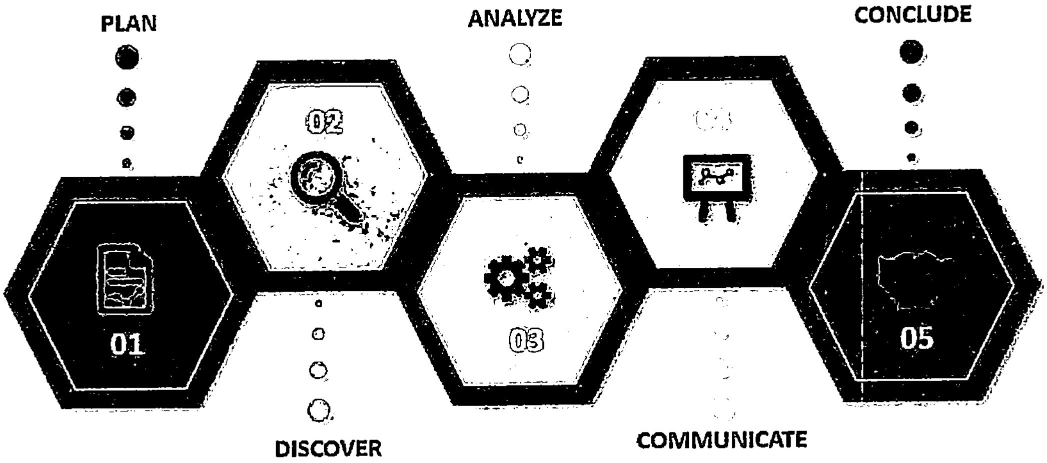


Figure 1 Vulnerability Assessment and Penetration Testing Methodology

4.1 Plan

This stage aims to complete the prerequisites of the activity: what's needed and how it is to be done.

4.1.1 Secure Pertinent Documentary Requirement

Prior to the actual activity, a Non-disclosure Agreement shall be signed by the involved persons/ parties to observe confidentiality of the client's assets and anything they will discover during the activity.

4.1.2 Planning the Execution

The project lead will prepare the necessary items for the kick-off and rules of engagement. This includes the project timeline, reiteration of scope, requirement settings, and authorization. The kick-off meeting will then be scheduled with the project team and client. Activity will proceed once Rules of Engagement are signed.

4.1.3 Prepare Necessary Requirements

The team will diligently collect all essential prerequisites needed to conduct a thorough Vulnerability Assessment and Penetration Testing on the designated target, in accordance with the established testing methodology. These requirements encompass a range of tasks, including but not limited to facilitating network or VPN access, verifying connectivity, deploying necessary tools, obtaining copies of APK or IPA files, providing API documentation or Postman collections, and furnishing test credentials.

4.2 Discover

This is the VAPT activity proper – discover the vulnerabilities and attempts to penetrate.

4.2.1 Perform the Manual and Automated Vulnerability Assessment on the Target

During the discovery stage, the engineer will commence the process of discovering, fingerprinting, and identifying vulnerabilities within the host, operating system (OS) and services for the following, but not limited to:

- Windows (all versions)
- Linux and other Unix flavors (all versions)
- Network and security-related equipment, whether software or hardware-based
- User profile settings
- Advanced password analysis

Furthermore, the engineer will perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:

- Application servers
- Authentication servers
- Backdoors and remote access services
- Backup applications/tools
- Database servers
- Active Directory, Lightweight Directory Access Protocol (LDAP)
- Domain Name Systems (DNS)
- Mail servers and Simple Mail Transfer Protocols (SMTP)
- Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS)
- Network Time Protocols (NTP)
- Remote Procedure Calls
- Routing protocols
- Simple Network Monitoring Protocol (SNMP)
- Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH)
- Virtual Private Network (VPN)
- Web and mobile applications
- Web servers

This can be achieved through either manual or automated methods. Automated Vulnerability Assessment employs different scanning tools and in-house scripts. Subsequently, the findings are validated using a manual approach by the engineers to minimize false positives.

4.2.2 Conduct the Penetration Testing on the Target

After listing down the vulnerabilities, engineers proceed to exploit them, delving as deeply as possible. This involves attempting to take advantage of the identified weaknesses to understand their potential impact and any further vulnerabilities they may expose. Additionally, engineers conduct manual testing on scenarios that automated tools may not cover. This helps in uncovering vulnerabilities that might go undetected by automated tools, ensuring a more comprehensive assessment of the system's security posture.

Additionally, throughout the testing phase, we establish a service level agreement with the client based on the severity of the findings. For instance, in the event that a critical vulnerability is discovered, we promptly notify the client within 1-2 business days following confirmation. This ensures a transparent and efficient communication process, enabling swift action to be taken for critical security issues.

4.3 Analyze

All acquired information, from raw outputs to manual checking is collated, discussed, studied, and analyzed by the engineer.

4.3.1 Data Collation, Processing, Analysis, Report Generation

In this stage, the engineer evaluates the severity of identified vulnerabilities using CVSS version 3.1, examines the penetration testing specifics, considers potential business impacts, and outlines possible remediation measures. Subsequently, this information is synthesized into a comprehensive report using the predefined templates containing an executive summary and technical report. Following the report's compilation, the engineer engages in a peer-to-peer discussion with their seniors, team lead, or the team to review the findings.

4.4 Communicate

This stage is focused on submitting the report and conducting a presentation.

Trends has predefined fields/ templates for the generation of reports, such as but not limited to:

- VAPT report (i.e., Executive Summary. Conclusion for Management Area, and Specific Action Plans)
- Security Profiling Results (including reports from automated scanning tools)
- Detailed observations and recommendations.

After the results have been meticulously documented in a comprehensive report, this information will be presented to all designated Points of Contact through a formal presentation. Additionally, copies of the reports, available in file formats including but not limited to PDF and Excel, will be submitted via our portal. The portal includes all historical test reports and trend analysis.

Furthermore, Trends will provide online reporting and metric capability. Trends will provide access to agencies to an online reporting portal that will include the VAPT results/ data (including risk, remediation status, and data compromised, if any) and access to historical test result and trends analysis delivered. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations.

4.5 Conclude

This stage is the project acceptance and closure.

After the client completes the remediation process and the engineer conducts the revalidation activity, the engineer will then send the project sign-off document along with a Customer Satisfaction survey. This step is crucial for formally accepting and officially closing the project. The sign-off document serves as a formal acknowledgment of the successful completion of the project, while the Customer Satisfaction survey allows us to gather feedback and ensure that the client's expectations and needs were met to their satisfaction.

5. Vulnerability Assessment and Penetration Testing Process

5.1 Committee Formation

This is to identify the key personnel that will be involved throughout the entire process and create the RACI table. These include (but not limited to) the following:

Committee	Description
Vulnerability Assessment and Penetration Testing Engineer	Responsible for the Kickoff meeting, Rules of Engagement, Vulnerability Assessment and Penetration Testing, Revalidation, report creation and technical report presentation.
Client	Responsible for the asset that will be subjected to the security services. They are the ultimate decision makers on actions to be taken against the identified risks.

5.2 RACI Matrix

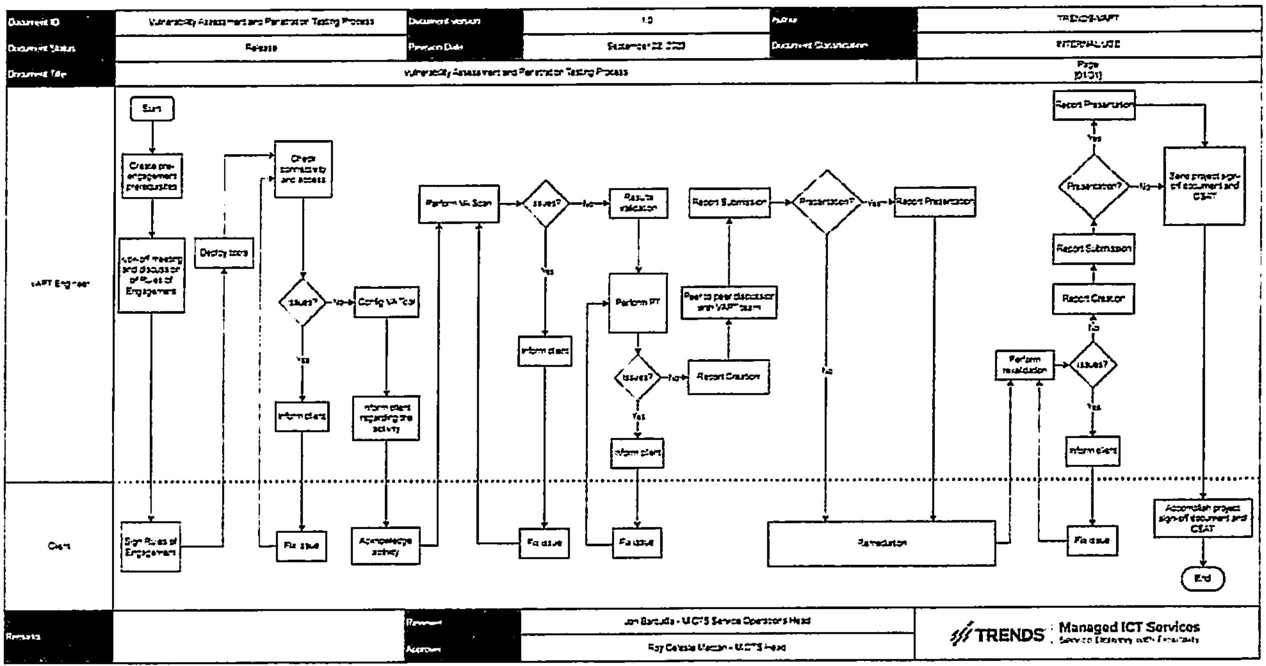
The RACI Matrix establishes the roles and responsibilities for the Pre-Engagement process. The designation are as follows:

Role	Description
Responsible	Responsible to perform the task assigned
Accountable	Owner of the process or activity. Accountable and ensures that the goals and objectives of the process or activity are being followed
Consulted	Consulted about how to perform task appropriately
Informed	Informed about key events regarding the task

Task	VAPT Engineer	Client
Creating pre-engagement prerequisites	R/A	I
Kickoff Meeting and discussion of Rules of Engagement	R/A	I
Sign Rules of Engagement	R/A	R/A
Deployment of Tools	R/A	I
Connectivity checking	R/A	I
Config Vulnerability Assessment tool	R/A	I
Inform client regarding the activity	R/A	I
Acknowledge activity	I	R/A
Perform Vulnerability Assessment scan	R/A	I
Monitor activity	R/A	I
Results validation	R/A	I
Perform Penetration Testing	R/A	I
Report creation	R/A	NA
Peer to peer discussion with VAPT Team	R/A	NA
Report submission	R/A	I
Report presentation	R/A	I
Remediation	C/I	R/A
Perform revalidation	R/A	I
Report creation	R/A	I

Report submission	R/A	I
Report presentation	R/A	I
Send Project sign-off document and CSAT	R/A	I
Accomplish project sign-off document and CSAT	I	R/A

5.3 Process Flow



Document ID	Vulnerability Assessment and Penetration Testing Process	Document Version	1.0	Author	TRENDS-VAPT
Document Status	Release	Revision Date	September 22, 2023	Document Classification	INTERNAL USE
Document Title	Vulnerability Assessment and Penetration Testing Process				Page [01:01]

Remarks		Reviewer	Jon Barcuta - MICTS Service Operations Head
		Approver	Ray Celeste Macan - MICTS Head

Figure 2 Vulnerability Assessment and Penetration Testing Process Flow

5.4 Procedure

1. The VAPT Engineer will prepare the following pre-engagement pre-requisites:
   a. Kick-off Slides
   b. Rules of Engagement
   c. Work Breakdown Structure
2. The VAPT Engineer will facilitate the kick-off meeting, discuss the Rules of Engagement, and send them to the Client once completed.
3. The Client will sign the Rules of Engagement and send them back to the VAPT Engineer once completed.
4. The VAPT Engineer will prepare and deploy all the tools needed.
5. The VAPT Engineer will check network connectivity and access. If any issues arise, they will promptly inform the client.
6. The VAPT Engineer will configure the Vulnerability Assessment tool, including scan policies and profiles.
7. The VAPT Engineer will monitor the scanning activity. If an issue arises, they will inform the client.
8. Once the scan is done, VAPT Engineer will perform results validation to remove false positives.
9. The VAPT Engineer will perform penetration testing, attempting to exploit vulnerabilities to determine their impact and potential damages, and gather evidence.
10. After the VAPT activity, the VAPT Engineer will analyze the data, including but not limited to:

   a. Impact and risk analysis
   b. Set prioritization and severity setting
   c. Remediation recommendations
   d. Over-all conclusion

11. The VAPT Engineer will create the executive and technical report.
12. Subsequently, the VAPT Engineer will conduct a peer-to-peer discussion with their seniors, team lead, or the team to review the findings once the report is complete.
13. The VAPT Engineer will submit the VAPT report in PDF and excel format via our portal.
14. The VAPT Engineer will perform a VAPT report presentation if needed.
15. The Client will now proceed with the remediation of the findings.
16. Once the remediation of the findings is complete, the VAPT Engineer will perform the revalidation activity. If an issue arises, they will inform the Client.
17. The VAPT Engineer will create the revalidation report.
18. The VAPT Engineer will submit the revalidation report in PDF and excel format via our portal.
19. The VAPT Engineer will perform a revalidation report presentation if needed.
20. The VAPT Engineer will prepare and send the project sign-off document along with the Customer Satisfaction survey.
21. The Client will complete and return the project sign-off document and provide feedback through the Customer Satisfaction survey.

6. Annex

ANNEX 1 – Severity Rating
ANNEX 2 – Vulnerability Assessment and Penetration Testing Report
ANNEX 3 – Revalidation Report
ANNEX 4 – Project Sign-off Document
ANNEX 5 – Scope of the Vulnerability Assessment and Penetration Testing

ANNEX 1. Severity Rating

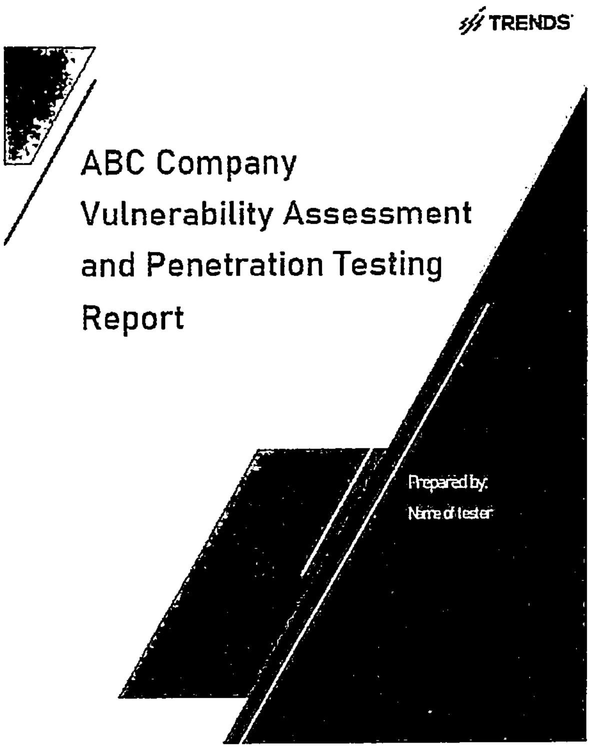
The severity rating for vulnerabilities is computed using the Common Vulnerability Scoring System 3.1 (CVSS v3.1) and the response time of findings will be based on the risk rating on each confirmed vulnerability.

Trends using Tenable can generate multi-format pre-built reports and can be exported using PDF, MS Excel, XML, CSV, and HTML.

Risk Rating	Description	Response Time
Critical	Vulnerabilities that can allow attackers to take complete control and fully compromise the system potentially causing massive impact/damage.	Within 1-2 business days of confirmation
High	Vulnerabilities that can allow attackers to compromise the system and possibly escalate the attack to critical severity.	Will be reflected on the report.
Medium	Vulnerabilities that can allow attackers to find further vulnerabilities and use them in conjunction to escalate the attack or gain further understanding to refine their attacks.	Will be reflected on the report.
Low	Vulnerabilities that do not have any significant impact and are not exploitable. These are reported as additional findings but does not require any action as immediate as medium severity.	Will be reflected on the report.

ANNEX 2. Vulnerability Assessment and Penetration Testing Report

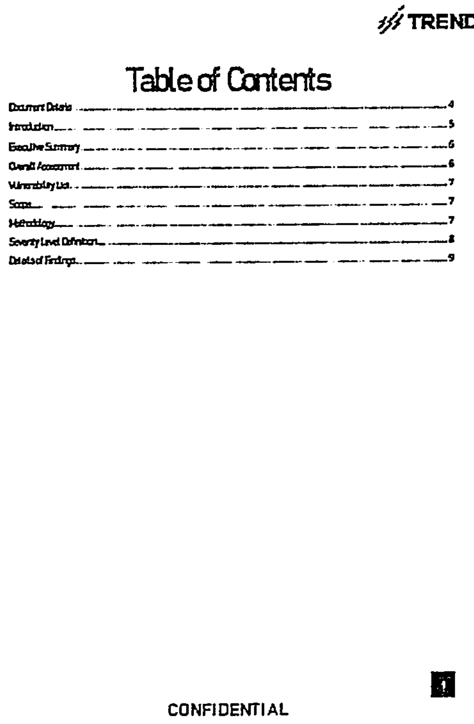
Executive Report:



TRENDS

ABC Company Vulnerability Assessment and Penetration Testing Report

Prepared by:
Name of tester



TRENDS

Table of Contents

CONFIDENTIAL

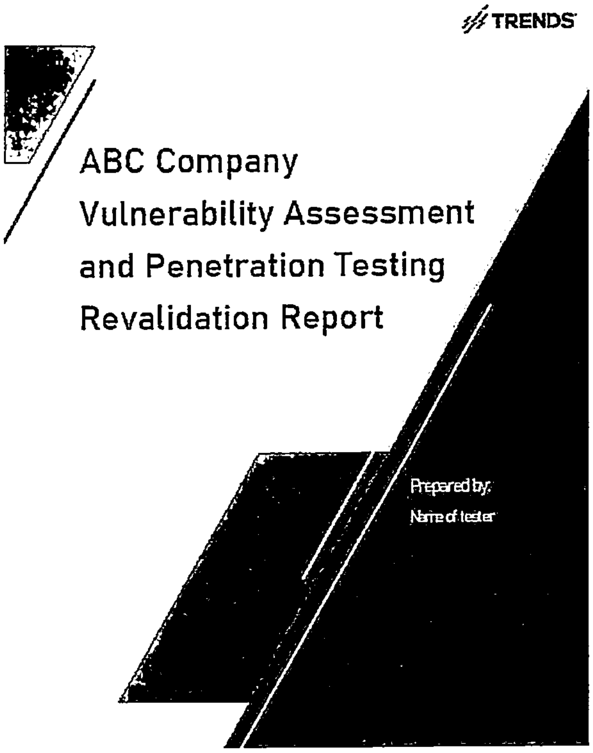
1

Technical Report:

Vulnerability Name	Severity	URL	Impact	Recommended Solution	References
Account Takeover	Critical	https://ABC.com.ph/api/user/reset_password_non_customer	Account takeover attacks can lead to the breach and exfiltration of vast amounts of sensitive, confidential, or protected classes of data like credit card numbers or personally identifiable information (PII).	Here are a few ways you can protect your organization against ATO. Multi-Factor Authentication At this point, ask your user to authenticate using something in addition to their password: •Something they know – a security question, such as their mother's maiden name, first pet's name, etc. •Something they possess – a token, dongle or other physical object. •Something they are – face ID, iris scan, fingerprint, or the	https://www.cloudflare.com/learning/access-management/account-takeover/#:~:text=Impact%20of%20account%20takeover%20attacks&text=Malware%20delivery%3A%20Account%20takeover%20attacks,to%20carry%20out%20further%20attacks. https://www.imperva.com/learn/application-security/account-takeover-ato/
Business Logic – Payment Bypass	Critical	https://ABC.com.ph/api/ordering	This vulnerability bypasses the payment method and marks the order as paid.	Make sure developers and testers understand the domain that the application serves. Avoid making implicit assumptions about user behavior or the behavior of other parts of the application. Maintain clear design documents and data flows for all transactions and workflows, noting any assumptions that are made at each stage. Write code as clearly as possible. If it's difficult to understand what is supposed to happen, it will be difficult to spot any logic flaws. Ideally, well-written code shouldn't need documentation to understand it. In unavoidably complex cases, producing clear documentation is crucial to ensure that other developers and testers know what assumptions are being made and exactly what the expected	https://portswigger.net/Web-security/logic-flaws#:~:text=What%20are%20business%20logic%20vulnerabilities,to%20achieve%20a%20malicious%20goal. https://brightsec.com/blog/business-logic-vulnerabilities/
User Enumeration	High	https://ABC.com.ph/api/user/noncustomers		Ensure don't use static token. Create a generic response for the server Make sure the HTTP response, and the time taken to respond are no different when a username does not exist, and an incorrect password is entered.	https://www.hacksplaining.com/prevention/user-enumeration https://www.virtuesecurity.com/kb/username-enumeration/
File Path Manipulation	Medium	https://ABC.com.ph/Contact-Center/Customer-Details	An attacker can modify the file path to access different resources, which may contain sensitive information. Even where an attack is constrained within the web root, it is often possible to retrieve items that are normally	The application should validate the user input before processing it. Ideally, the validation should compare against a whitelist of permitted values. If that isn't possible for the required functionality, then the validation should verify that the input contains only permitted content, such as purely alphanumeric characters.	https://portswigger.net/web-security/file-path-traversal https://portswigger.net/kb/issues/00100b00_file-path-manipulation

ANNEX 3. Revalidation Report

Executive Report:


TRENDS

ABC Company
Vulnerability Assessment
and Penetration Testing
Revalidation Report

Prepared by:
Name of tester

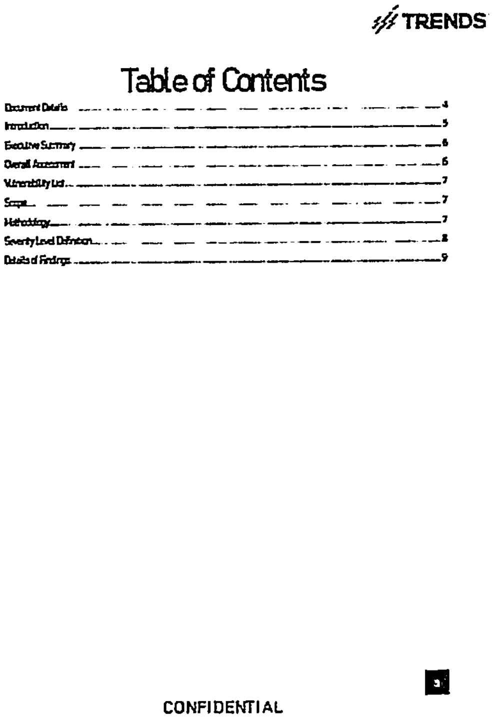
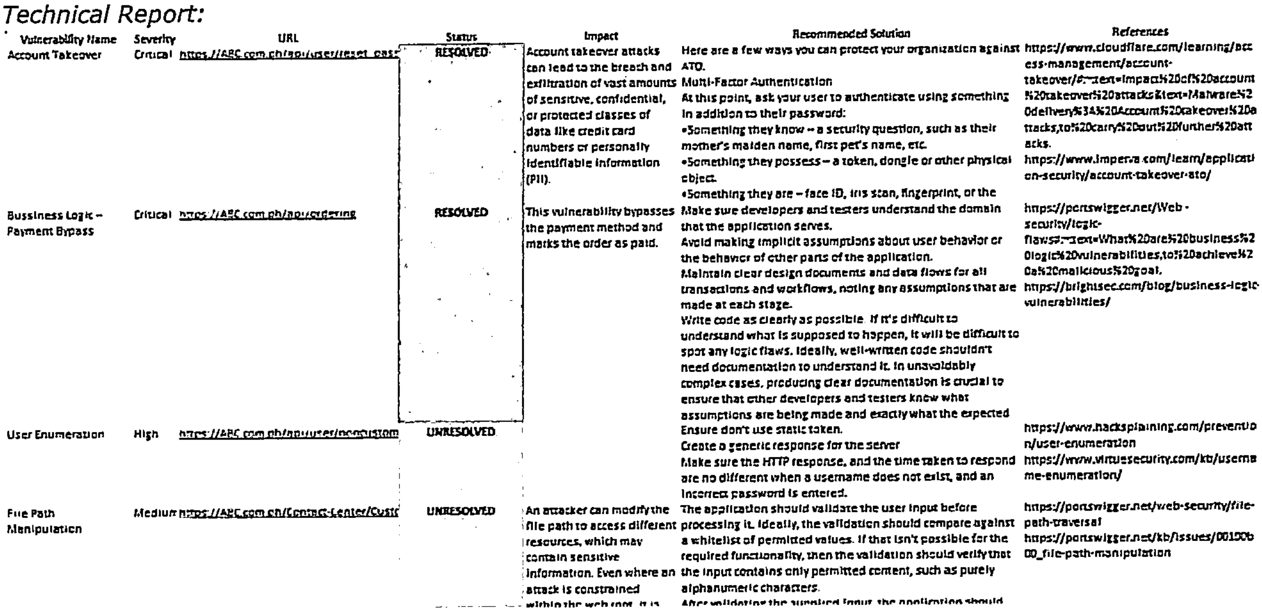

TRENDS

Table of Contents

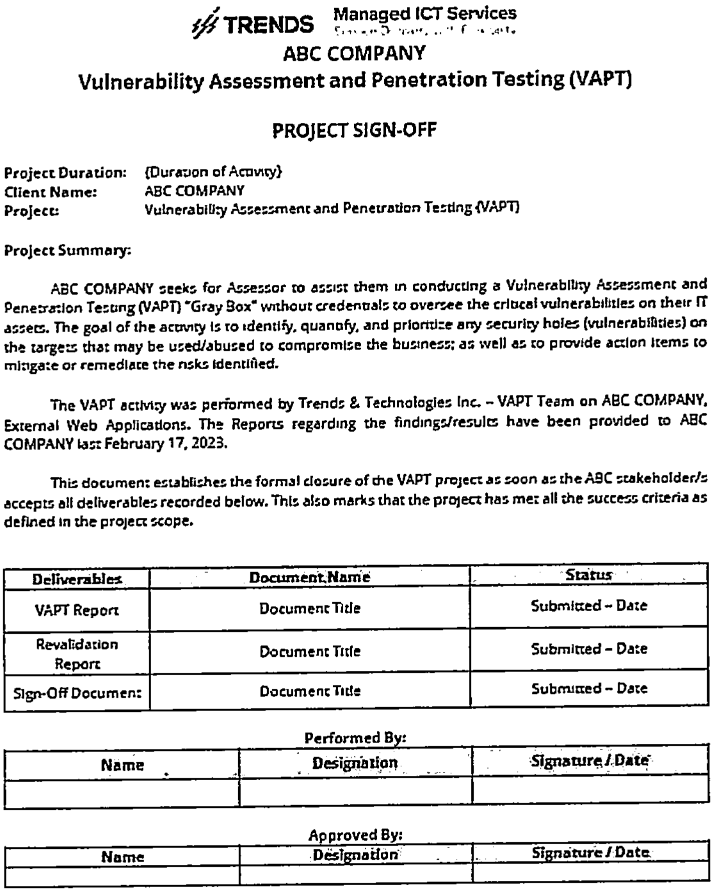
CONFIDENTIAL

Technical Report:



Vulnerability Name	Severity	URL	Status	Impact	Recommended Solution	References
Account Takeover	Critical	https://ABC.com.ph/api/user/reset_pass	RESOLVED	Account takeover attacks can lead to the breach and exfiltration of vast amounts of sensitive, confidential, or protected classes of data like credit card numbers or personally identifiable information (PII).	Here are a few ways you can protect your organization against ATO. Multi-Factor Authentication At this point, ask your user to authenticate using something in addition to their password: •Something they know – a security question, such as their mother's maiden name, first pet's name, etc. •Something they possess – a token, dongle or other physical object. •Something they are – face ID, iris scan, fingerprint, or the	https://www.cloudflare.com/learning/access-management/account-takeover/#:~:text=Impact%20of%20account%20takeover%20attacks&text=Malware%20delivery%3A%20Account%20takeover%20attacks,to%20carry%20out%20further%20attacks. https://www.imperva.com/learn/application-security/account-takeover-ato/
Bussiness Logic – Payment Bypass	Critical	https://ABC.com.ph/api/ordering	RESOLVED	This vulnerability bypasses the payment method and marks the order as paid.	Make sure developers and testers understand the domain that the application serves. Avoid making implicit assumptions about user behavior or the behavior of other parts of the application. Maintain clear design documents and data flows for all transactions and workflows, noting any assumptions that are made at each stage. Write code as clearly as possible. If it's difficult to understand what is supposed to happen, it will be difficult to spot any logic flaws. Ideally, well-written code shouldn't need documentation to understand it. In unavoidably complex cases, producing clear documentation is crucial to ensure that other developers and testers know what assumptions are being made and exactly what the expected	https://portswigger.net/Web-security/logic-flaws#:~:text=What%20are%20business%20logic%20vulnerabilities,to%20achieve%20a%20malicious%20goal. https://brightsec.com/blog/business-logic-vulnerabilities/
User Enumeration	High	https://ABC.com.ph/api/user/noncustom	UNRESOLVED		Ensure don't use static token. Create a generic response for the server Make sure the HTTP response, and the time taken to respond are no different when a username does not exist, and an Incorrect password is entered.	https://www.hacksplaining.com/prevention/user-enumeration https://www.virtuesecurity.com/kb/username-enumeration/
File Path Manipulation	Medium	https://ABC.com.ph/Contact-Center/Custo	UNRESOLVED	An attacker can modify the file path to access different resources, which may contain sensitive information. Even where an attack is constrained within the web root, it is	The application should validate the user input before processing it. Ideally, the validation should compare against a whitelist of permitted values. If that isn't possible for the required functionality, then the validation should verify that the input contains only permitted content, such as purely alphanumeric characters. After validating the supplied input, the application should	https://portswigger.net/web-security/file-path-traversal https://portswigger.net/kb/issues/00100b00_file-path-manipulation

ANNEX 4. Project Sign-off Document



TRENDS Managed ICT Services

ABC COMPANY

Vulnerability Assessment and Penetration Testing (VAPT)

PROJECT SIGN-OFF

Project Duration: (Duration of Activity)
Client Name: ABC COMPANY
Project: Vulnerability Assessment and Penetration Testing (VAPT)

Project Summary:

ABC COMPANY seeks for Assessor to assist them in conducting a Vulnerability Assessment and Penetration Testing (VAPT) "Gray Box" without credentials to oversee the critical vulnerabilities on their IT assets. The goal of the activity is to identify, quantify, and prioritize any security holes (vulnerabilities) on the targets that may be used/abused to compromise the business; as well as to provide action items to mitigate or remediate the risks identified.

The VAPT activity was performed by Trends & Technologies Inc. – VAPT Team on ABC COMPANY, External Web Applications. The Reports regarding the findings/results have been provided to ABC COMPANY last February 17, 2023.

This document establishes the formal closure of the VAPT project as soon as the ABC stakeholder/s accepts all deliverables recorded below. This also marks that the project has met all the success criteria as defined in the project scope.

Deliverables	Document Name	Status
VAPT Report	Document Title	Submitted – Date
Revalidation Report	Document Title	Submitted – Date
Sign-Off Document	Document Title	Submitted – Date

Performed By:

Name	Designation	Signature / Date

Approved By:

Name	Designation	Signature / Date

ANNEX 5. Scope of Vulnerability Assessment and Penetration Testing

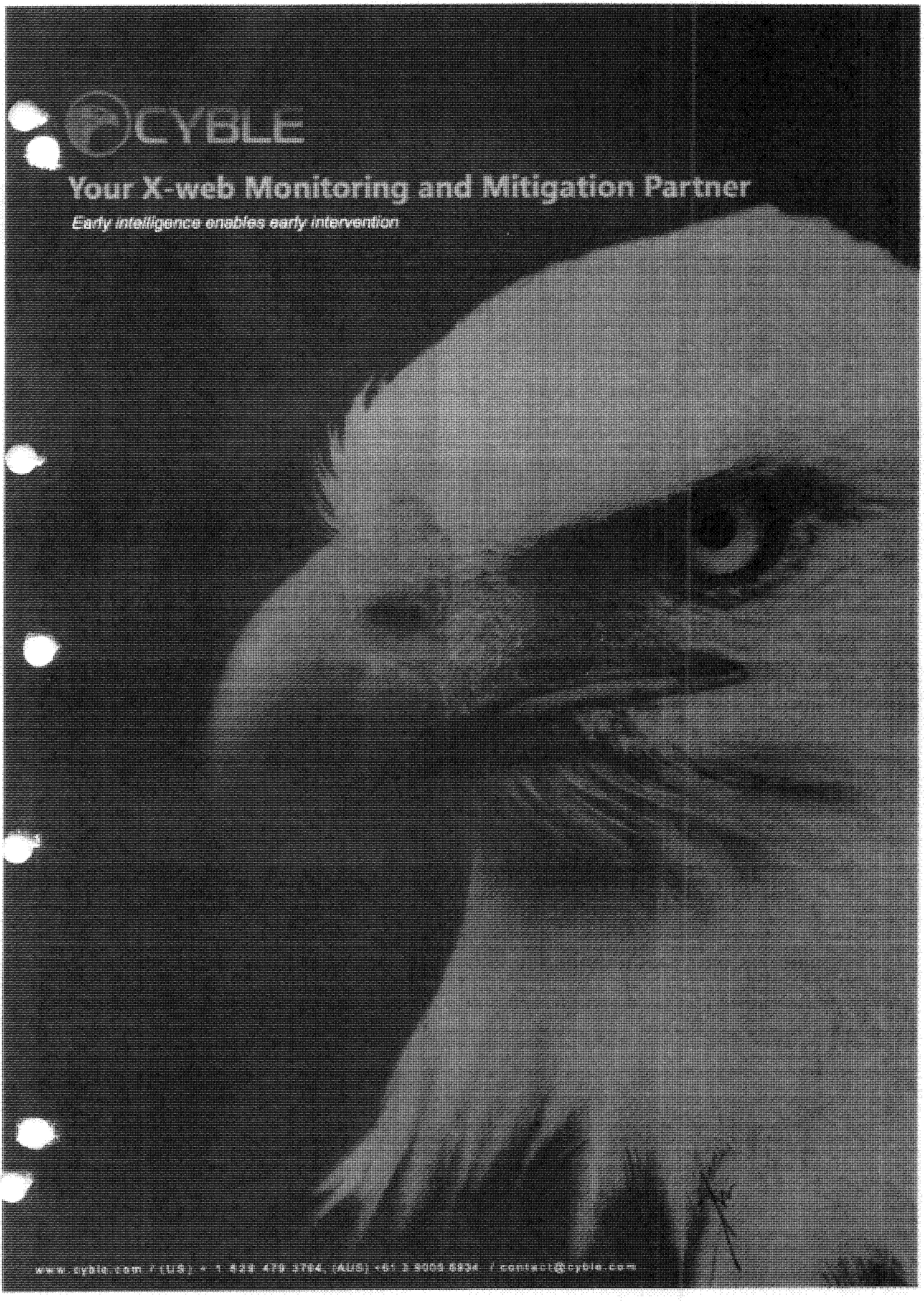
This Vulnerability Assessment and Penetration Testing will be performed annually based on agreed schedules and scope with the agencies. The VAPT scope may include targets such as but not limited to network infrastructure, network devices, servers, workstations, applications, (e.g., public-facing web and mobile applications), and APIs, endpoints, hosts and database, including member service systems or kiosks, if any and among others.

The scope of VAPT will be at least the following:

Agency	Scope
BTr	7 External resources, up to 80 IP addresses
GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses
SSS	25 External resources, 1 mobile app up to 150 IP addresses
PDIC	8 External resources, up to 80 IP addresses

Moreover, the VAPT team shall deliver and maintain a vulnerability database with relevant software version upgrade and security policy updates through various platforms and tools that shall be used to perform the vulnerability and penetration services. This vulnerability database shall be accessible upon request of the agencies.

C.Threat Intelligence



CYBLE

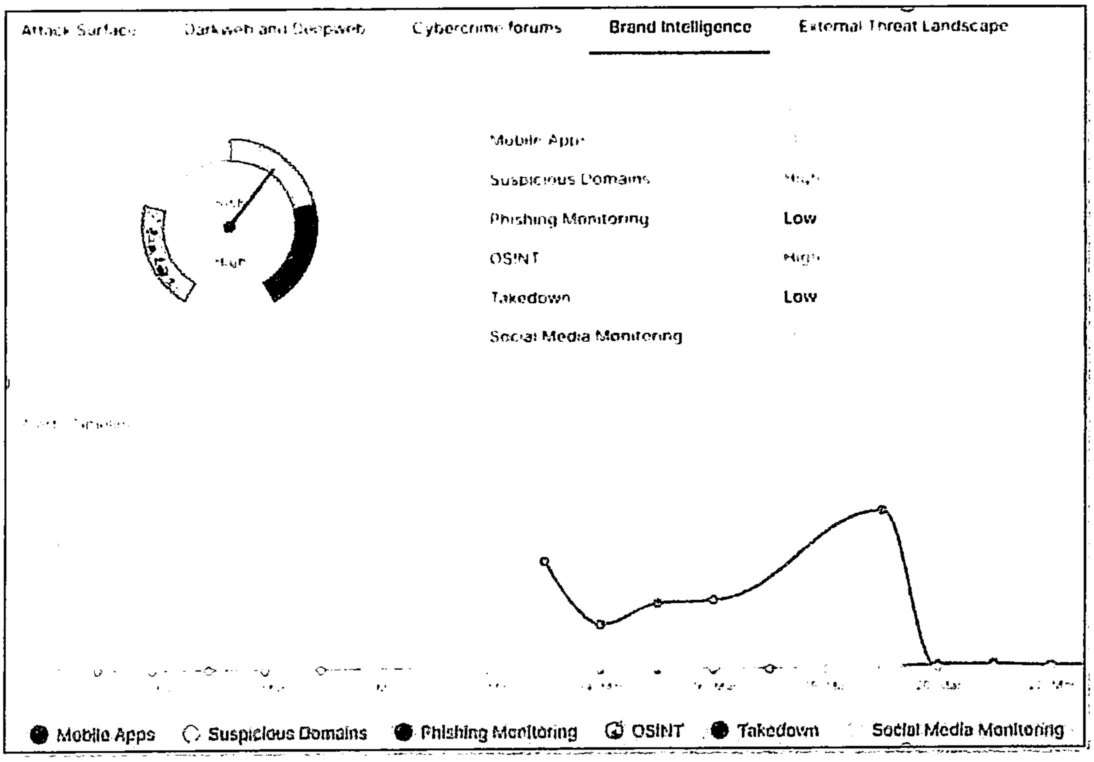
Your X-web Monitoring and Mitigation Partner

Early intelligence enables early intervention

www.cyble.com / (US) + 1 828 479 3794, (AUS) +61 3 9005 6834 / contact@cyble.com

Digital Brand Protection & Social Media Monitoring

Cyble's Brand Protection suite aims to provide comprehensive coverage of detecting various threat vectors and techniques that are used by cybercriminals to launch brand abuse and phishing attacks across multiple channels to target your brand. Cyble employs a holistic approach to detect digital brand abuse and social media abuse.



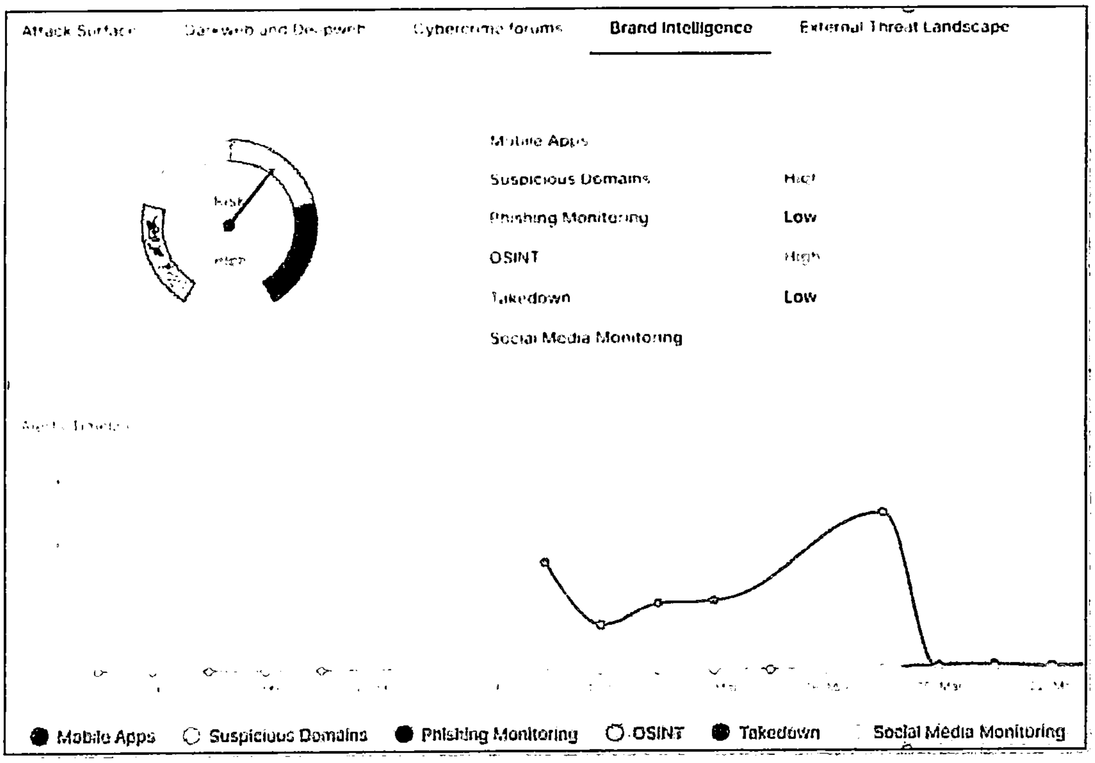
Mobile Apps	
Suspicious Domains	High
Phishing Monitoring	Low
OSINT	High
Takedown	Low
Social Media Monitoring	

Our suite of brand protection capabilities employs a combination of human security analysts and automated mechanisms to achieve the following –

1. Detection of phishing URLs hosted on fake or look-alike domains or on hacked websites
2. Domain name registration monitoring and search (newly registered domains) to detect suspicious domains or typo-squatted domains that are created to target your brand
3. Analysis of global SSL certificate transparency logs to identify suspicious or fake domains
4. Website watermarking and monitoring to notify you whenever a fraudster mirrors your website or copies your code to setup a look alike phishing website
5. Detection of false affiliation claims or trademark infringement
6. Detection of fake mobile apps that are hosted on legitimate as well as third party app stores
7. Detecting social media accounts/handles/profiles (Instagram, Facebook, YouTube, LinkedIn, Reddit) that are created to impersonate the official accounts of the organization

Digital Brand Protection & Social Media Monitoring

Cyble's Brand Protection suite aims to provide comprehensive coverage of detecting various threat vectors and techniques that are used by cybercriminals to launch brand abuse and phishing attacks across multiple channels to target your brand. Cyble employs a holistic approach to detect digital brand abuse and social media abuse.



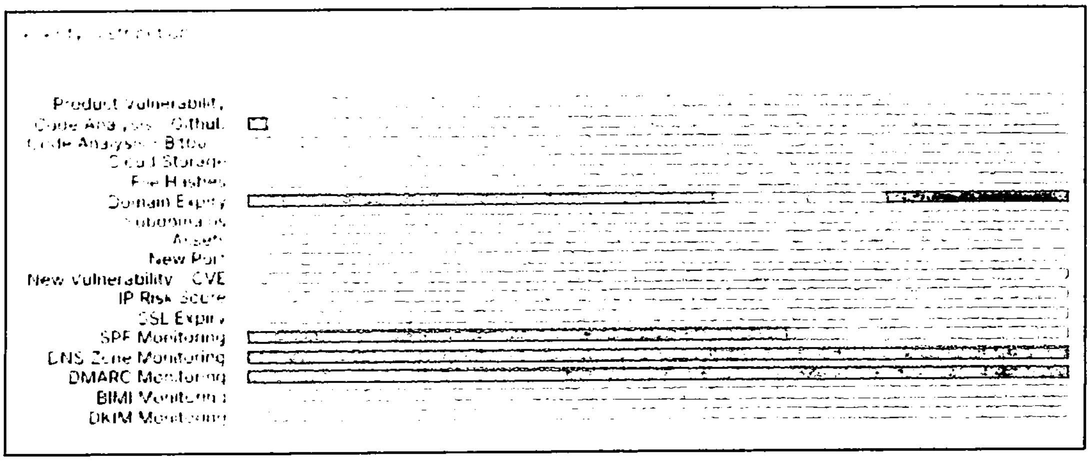
Mobile Apps	
Suspicious Domains	High
Phishing Monitoring	Low
OSINT	High
Takedown	Low
Social Media Monitoring	

Our suite of brand protection capabilities employs a combination of human security analysts and automated mechanisms to achieve the following –

1. Detection of phishing URLs hosted on fake or look-alike domains or on hacked websites
2. Domain name registration monitoring and search (newly registered domains) to detect suspicious domains or typo-squatted domains that are created to target your brand
3. Analysis of global SSL certificate transparency logs to identify suspicious or fake domains
4. Website watermarking and monitoring to notify you whenever a fraudster mirrors your website or copies your code to setup a look alike phishing website
5. Detection of false affiliation claims or trademark infringement
6. Detection of fake mobile apps that are hosted on legitimate as well as third party app stores
7. Detecting social media accounts/handles/profiles (Instagram, Facebook, YouTube, LinkedIn, Reddit) that are created to impersonate the official accounts of the organization

Attack Surface Management

Our attack surface management (ASM) capabilities allow you to enumerate and evaluate the risk of your internet-facing assets continuously.

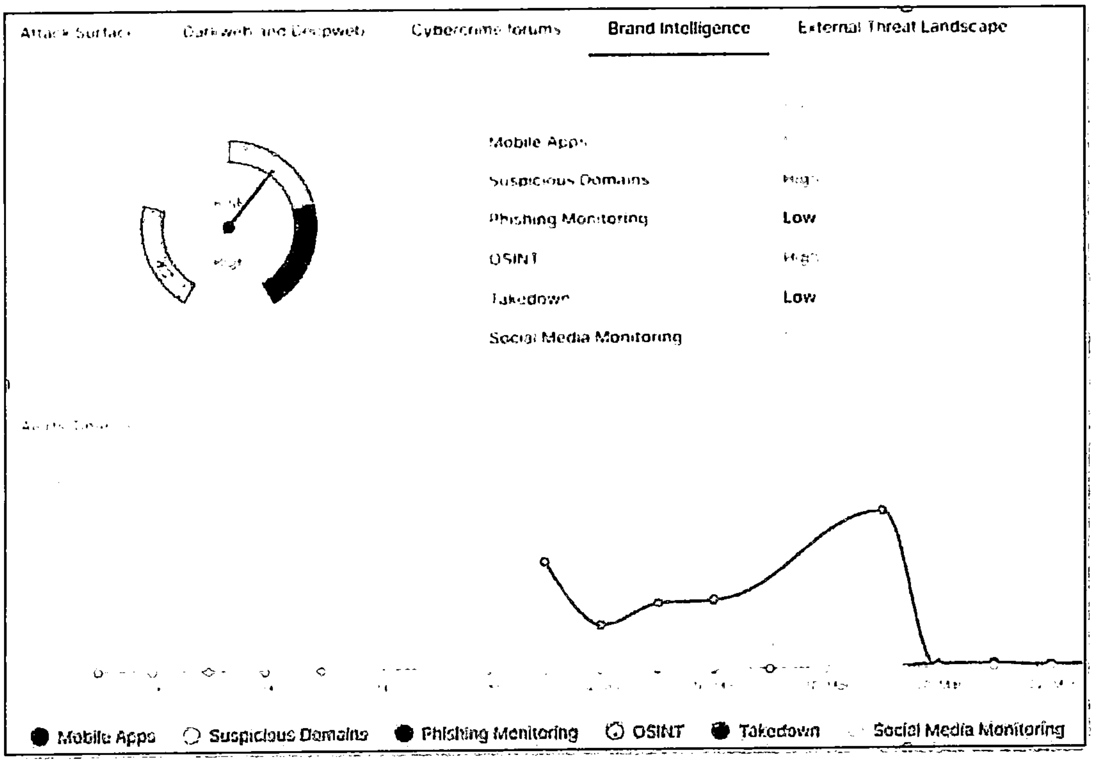


With our ASM feature, you can

1. discover your domains and sub-domains, their hosting infrastructure along with the details of their discoverability and the IP reputation of these assets.
2. Identify sensitive open ports in your internet-facing infrastructure (FTP, RDP etc) that should be closed or filtered
3. Validate the SSL certificates of your websites, to notify you about certificate expiry for appropriate remediation.
4. Visualize the dynamic risk score of every IP address to notify you whether there is any security risk or malicious activity reported for that asset to facilitate analysis and resolution of the issue.
5. With our vulnerability tracker, maintain an inventory of your technology stack that enables you to be notified whenever a new vulnerability is published that affects any of your listed components
6. DNS Zone Transfer Monitoring, SPF Monitoring, DMARC, DKIM monitoring & BIMI Monitoring
7. Understand the vulnerability posture of your internet-facing assets to become aware of critical unpatched vulnerabilities and thus improve the effectiveness of patch management and remediation efforts
8. Discover the exposure of your sensitive data (API keys, user accounts, access keys, passwords, sensitive IP addresses etc.) and software (application code and builds) via public insecure code repositories such as GitHub and Bitbucket etc.
9. Discover the exposure of your business confidential data or customer PII information in your own or third-party cloud data stores such as Amazon S3 or Azure Blob
10. Identify any network security misconfigurations leading to inadvertent exposure of internal databases or Elastic Servers over the internet.
11. Discover any active botnet infections in your network by our global honeypot network and our stealer log analysis base correlation capabilities.
12. Scan web applications vis a vis OWASP Top 10 Vulnerabilities

Digital Brand Protection & Social Media Monitoring

Cyble's Brand Protection suite aims to provide comprehensive coverage of detecting various threat vectors and techniques that are used by cybercriminals to launch brand abuse and phishing attacks across multiple channels to target your brand. Cyble employs a holistic approach to detect digital brand abuse and social media abuse.



Mobile Apps	
Suspicious Domains	High
Phishing Monitoring	Low
OSINT	High
Takedown	Low
Social Media Monitoring	

Our suite of brand protection capabilities employs a combination of human security analysts and automated mechanisms to achieve the following –

1. Detection of phishing URLs hosted on fake or look-alike domains or on hacked websites
2. Domain name registration monitoring and search (newly registered domains) to detect suspicious domains or typo-squatted domains that are created to target your brand
3. Analysis of global SSL certificate transparency logs to identify suspicious or fake domains
4. Website watermarking and monitoring to notify you whenever a fraudster mirrors your website or copies your code to setup a look alike phishing website
5. Detection of false affiliation claims or trademark infringement
6. Detection of fake mobile apps that are hosted on legitimate as well as third party app stores
7. Detecting social media accounts/handles/profiles (Instagram, Facebook, YouTube, LinkedIn, Reddit) that are created to impersonate the official accounts of the organization

8. Detecting social media posts that reference your brand and are designed to spread disinformation, fake news, affect your share price, scam your customers, or display fake affiliations
9. Website Monitoring to detect suspicious or malicious changes to the website such as insertion of malicious scripts or defacement
10. Referral Log Analysis, monitoring malicious redirecting URL
11. Detecting malware files (mobile and desktop) in the wild (sold on underground forums) or on app stores that are targeting client brand
12. DMARC monitoring- Detecting C2 or Phishing URLs by monitoring spam or phishing emails targeting client brands via spoofing

VIP/ Executive Monitoring

VIP/Executives in an organization are high-value targets as they have privileged access and authority which can be used to very good effect to achieve the nefarious motives of cyber criminals.

Cybercriminals tend to abuse the social presence of key executives so that they can target them for blackmail or their other high-value connections for phishing or fraud.

VIP executives also have access to troves of sensitive information of the organization that holds significant value for attackers as they offer the greatest return on malicious effort. As a result, securing their access and credentials to company infrastructure and applications becomes very critical.

Cyble offers VIP/ Executive monitoring spanning social media as well as the Dark web by detecting and notifying you about following suspicious activity –

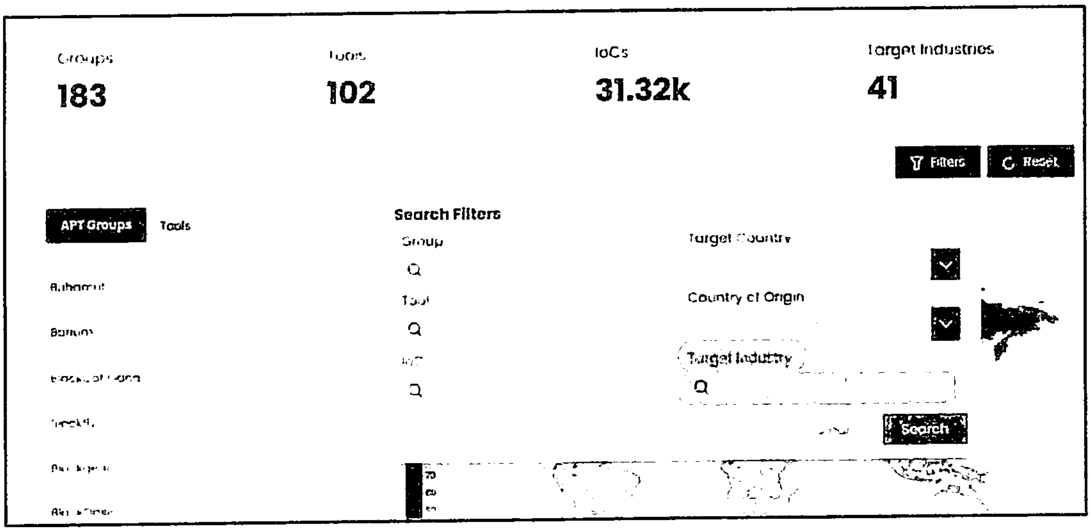
1. Creation of lookalike social media profiles (Twitter handles, Facebook pages, LinkedIn profiles, YouTube channels etc.)
2. Identifying the exposure of sensitive PII data (Personal details, government ID etc.) of key VIP executives on cyber-criminal forums or public or third-party data breaches on the dark web
3. Identifying and notifying you about the exposure of sensitive information of VIP executives such as compromised credentials of corporate as well as personal accounts

2.5.2 Threat Library

The Threat Library is the latest feature to be introduced in Cyble Vision. This feature is aimed at assisting threat researchers and threat intelligence analysts to enhance their understanding of Advanced Persistent Groups and their activities.

The Threat Library contains a catalogue of

- APT Groups and their Aliases
- Their native origins and nation-states backing them
- The countries and sectors that these APT systems have been known to actively target
- Indicators of Compromise associated with these APT groups and their campaigns



Groups 183

Tools 102

IoCs 31.32k

Target Industries 41

The Threat Library is being continuously updated by Cyble Researchers in near real-time, who closely track current and emerging APT groups and the threat information will help clients in staying up to date with the latest IOCs associated with these APT groups. Currently, the threat library contains information on –

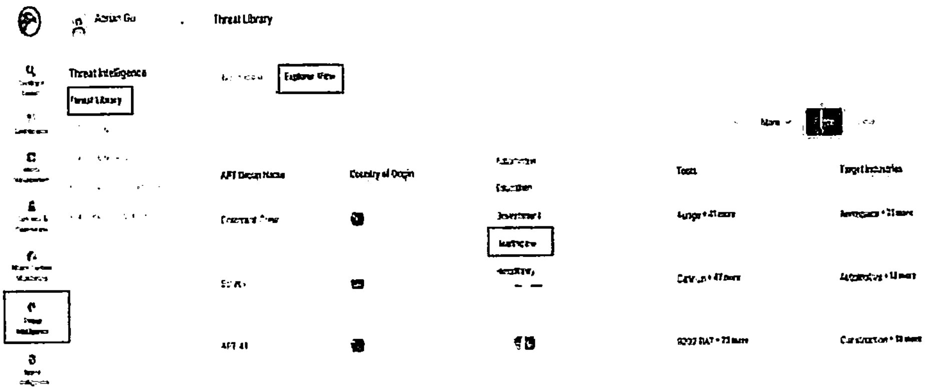
- 200+ APT Groups (including Aliases)
- 100+ unique tools
- 41 sectors and industries
- 13000+ unique Indicators of compromise associated with the APT activity

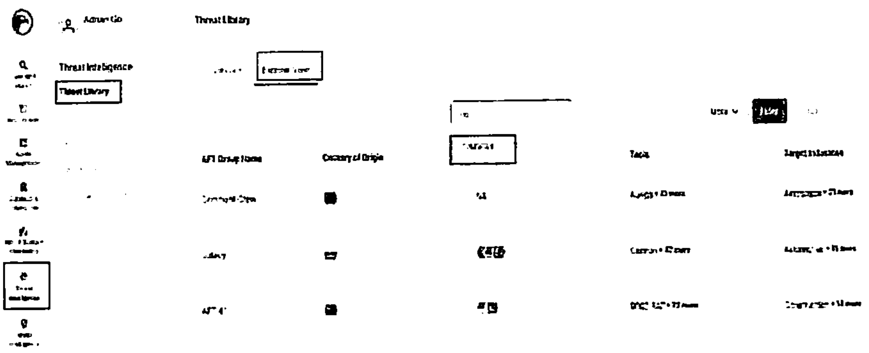
How threat analysts can use the Threat Library –

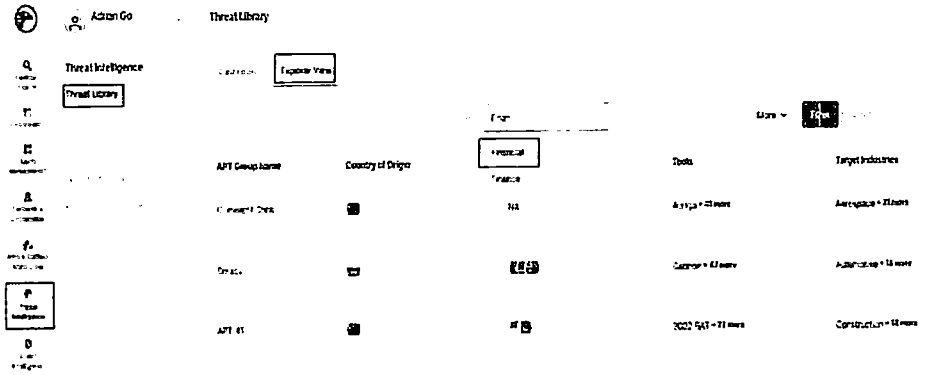
- Read more about an APT group and the tools that they are known to use
- As a part of their internal threat hunting exercises, search for an IOC in the Threat library to determine if it is associated with an APT group and the malware/hacking tools associated with the IOC
- lookup an APT group by its name and alias to learn more about their target geography, target business sectors, tools they have been known to use along with the curated Indicators of Compromise associated with these groups.

Cyble is currently catering to 100+ global BFSI customers, we do extensive research on DW & Open internet to identify issues in BFSI sector. Cyble provides sector & region-specific Threat Intel in the form of Advisories, News Flashes & Ransomware updates.

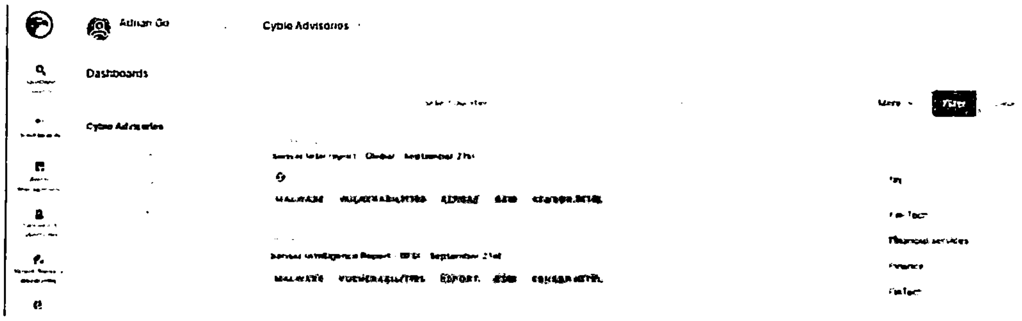
Sector monitoring Financial, Government, Insurance, and Healthcare can be search it in Vision Portal under Threat Intelligence>Threat Library>Search Target Industry

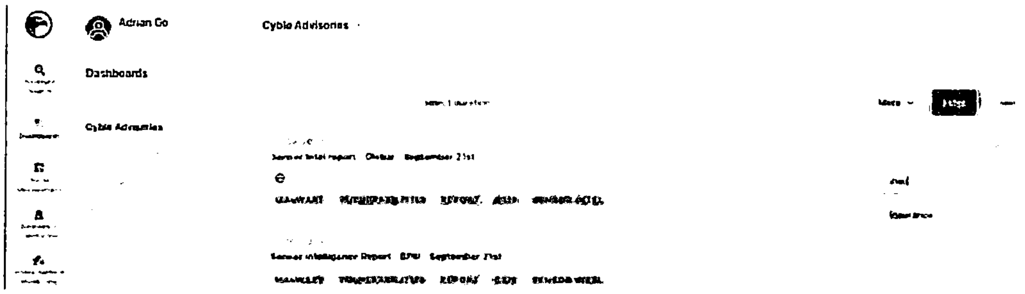


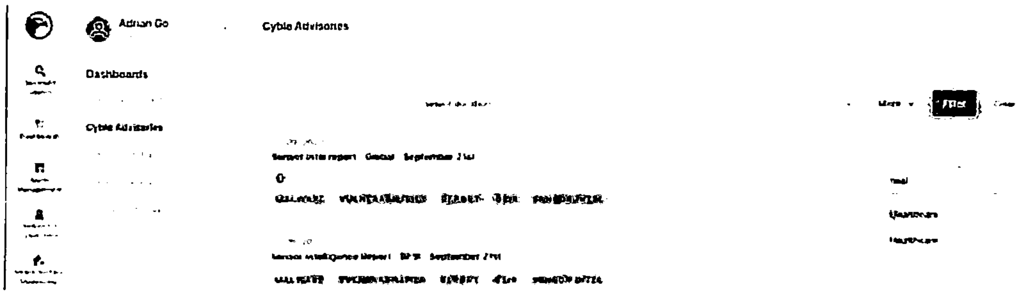




You may also search it thru advisories under **Dashboards>Cyble Advisories**



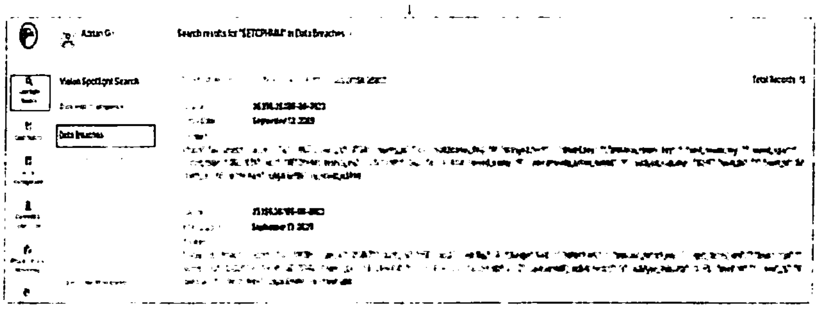




SWIFT Codes can be considered as keyword in Cycle for any exposure on the DarkWeb or Open Internet will be indexed on the Cyble Vision dashboard.

For this case, we used a sample SWIFT code from one of our local banks here in Philippines. We used the "Cyble Spotlight Search" and we used "SETCPHMM" SWIFT Codes keyword for search results.

1. SWIFT code exposure in data breach

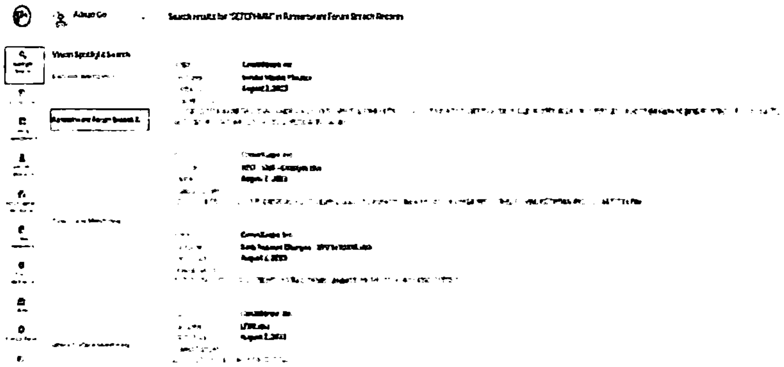


Search results for "SETCPHMM" in Data Breaches

Vision Spotlight Search

Data Breaches

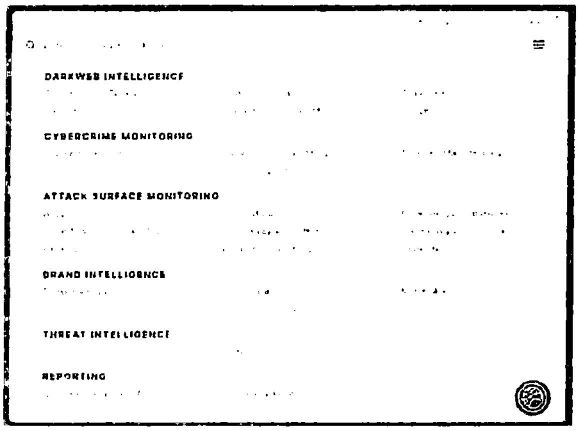
2. SWIFT code exposure in ransomware forum



Search results for "SETCPHMM" in Ransomware Forum Breach Records

Vision Spotlight Search

Using **Cyble Spotlight Search**, it can use and select the different services available that capture in terms of search results.



DARKWEB INTELLIGENCE

CYBERCRIME MONITORING

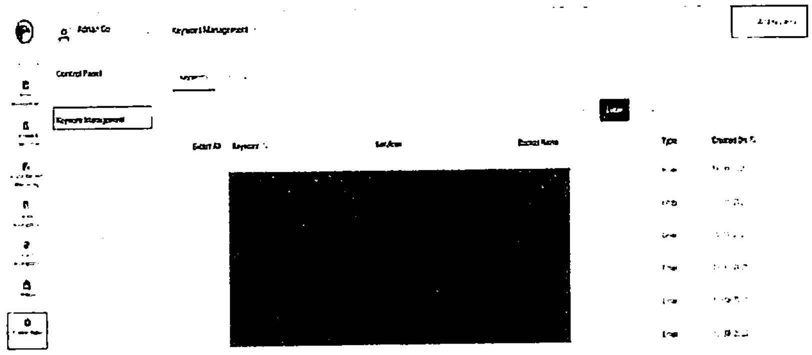
ATTACK SURFACE MONITORING

BRAND INTELLIGENCE

THREAT INTELLIGENCE

REPORTING

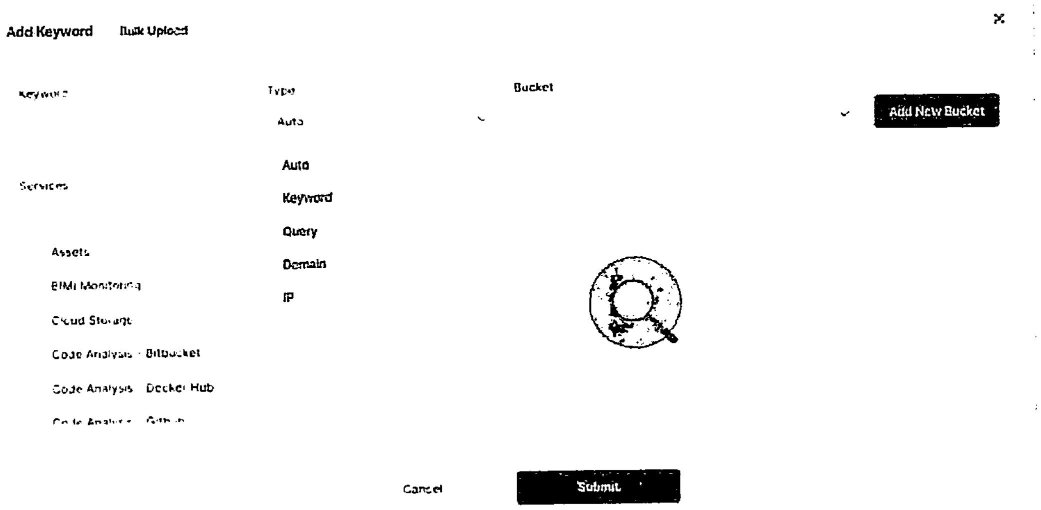
Another option aside from using the Cyble Spotlight Search, it can configure any specific SWIFT Codes that the agencies will be required under Control Panel>Keyword Management the +Add Keyword.



[redacted]

After clicking "+Add Keyword".

1. Enter the Keyword
2. Choose "Keyword" as type
3. Select the Bucket
4. Select the Services
5. Then click Submit



Comprehensive digital risk protection with Cyble vision

Reduce your Cyber Attack Surface

- Critical Vulnerabilities and Open Ports
- Misconfigured Cloud Storage Buckets (AWS, Azure)
- Source Code Leaks
- Exposed Secrets/API Keys/Access Tokens in GitHub

Manage your Brand Reputation Risk

- Phishing and Typo-squatted Domains
- Social Media and Mobile App Store Monitoring
- Executive Profile Monitoring
- Malware Campaign Monitoring
- Website Watermarking

Determine your Data Security and Privacy Risk on the Darkweb

- Personally Identifiable Information (PII) Leaks
- Protected Health information (PHI) Leaks
- Exposed Card Holder Data (PAN, CVV, PIN) in Data Breaches

Detect and Prevent Fraud

- Compromised Credit and Debit Cards
- Vouchers and Coupons
- Gift Cards

Manage your Supply Chain Cyber Risk

- Vendor Risk Scoring
- Critical Vulnerabilities in Third Party Assets
- Compromised Vendor Credentials on the Dark Web
- Sensitive Company Data exposed in Third Party Data Breaches and Ransomware Attacks
- Corporate Data exposed in Third Party Cloud Storage

Hunt for Threats with Cyber Threat Intelligence

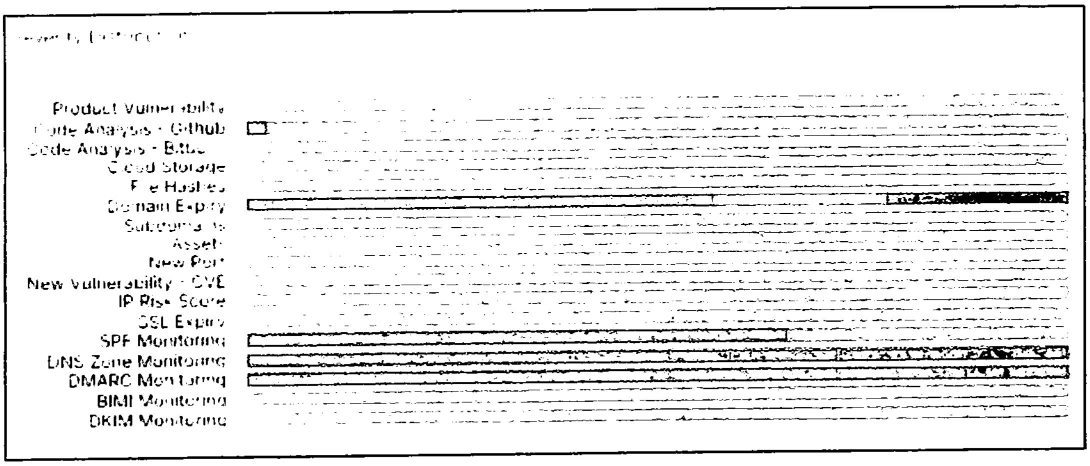
- Global Sensor Intelligence
- 400+ Threat Actors, 700+ malware operators, APT Groups, Cybercrime marketplaces
- Open Source (OSINT) and Premium Threat Intelligence Feed (IOC) Integration with SIEM and SOAR solutions
- Threat Intelligence Advisories

Enhance your Incident Response Capability

- Bespoke Ransomware Response and Mitigation
- Forensic Analysis/Malware Analysis and Investigation support
- Threat Actor Profiling and Reconnaissance

Attack Surface Management

Our attack surface management (ASM) capabilities allow you to enumerate and evaluate the risk of your internet-facing assets continuously.



With our ASM feature, you can

1. discover your domains and sub-domains, their hosting infrastructure along with the details of their discoverability and the IP reputation of these assets.
2. Identify sensitive open ports in your internet-facing infrastructure (FTP, RDP etc) that should be closed or filtered
3. Validate the SSL certificates of your websites, to notify you about certificate expiry for appropriate remediation.
4. Visualize the dynamic risk score of every IP address to notify you whether there is any security risk or malicious activity reported for that asset to facilitate analysis and resolution of the issue.
5. With our vulnerability tracker, maintain an inventory of your technology stack that enables you to be notified whenever a new vulnerability is published that affects any of your listed components
6. DNS Zone Transfer Monitoring, SPF Monitoring, DMARC, DKIM monitoring & BIMI Monitoring
7. Understand the vulnerability posture of your internet-facing assets to become aware of critical unpatched vulnerabilities and thus improve the effectiveness of patch management and remediation efforts
8. Discover the exposure of your sensitive data (API keys, user accounts, access keys, passwords, sensitive IP addresses etc.) and software (application code and builds) via public insecure code repositories such as GitHub and Bitbucket etc.
9. Discover the exposure of your business confidential data or customer PII information in your own or third-party cloud data stores such as Amazon S3 or Azure Blob
10. Identify any network security misconfigurations leading to inadvertent exposure of internal databases or Elastic Servers over the internet.
11. Discover any active botnet infections in your network by our global honeypot network and our stealer log analysis base correlation capabilities.
12. Scan web applications vis a vis OWASP Top 10 Vulnerabilities

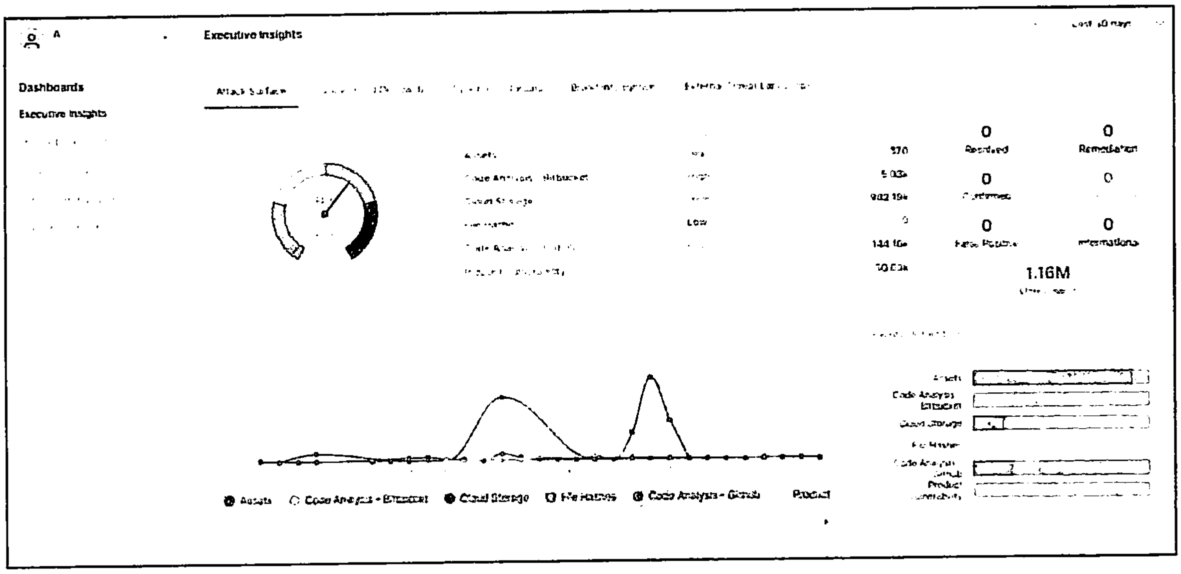
Configuration, Dashboards, Alerts, and Incident Management

The Master Dashboard module in Cyble Vision provides an easy-to-use interface for clients to configure their search keywords, domains, assets and define the alerting rules for events of their interest.

The Cyble Vision platform includes an Executive Dashboard that provides a centralized graphical visualization of various threat events generated for each service within Cyble Vision along with their severity rating.

The intuitive graphs and trend analysis charts can help the client managers and executives in gaining a quick high-level insight into their evolving digital risk posture across multiple domains within a single pane of glass.

Cyble Vision can be configured to generate alerts for specific events based on their severity rating and service. All such alerts can be viewed in the central "My Events" tab within the user interface. A provision for exporting the alerts in the "My Events" option to a CSV format for more detailed analysis, is also present.



Executive Dashboard

SLA for Brand Monitoring and take down services

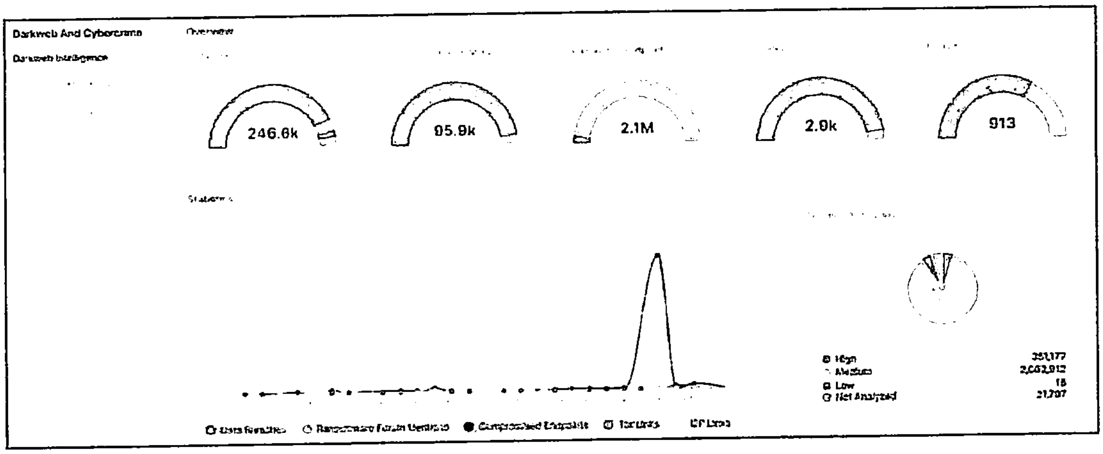
Cyble offers the following Service Levels on a best effort basis for Detection and Takedown of web content/ properties targeting our client brands contingent on the dependencies listed below–

Sr No	Description	Type of Incident	SLA for takedown initiation	*Estimated time for completion of complaint
1	Phishing website	Website cloning Phishing email	Upon confirmation by client, the Cyble incident response team will initiate enforcement process within 2 hours	Within 3 business days Within 5 business days
2	Website	Trademark / Copyright infringement		Within 10 business days
3	Social Media	Brand impersonation/ Trademark infringement / Copyright infringement		Within 3 business days
4	Mobile Apps	Apps hosted on 3rd party platforms Trademark infringement- Play store/Apple App store		Within 5 business days
5	Public Code Repositories	Code leaks on public code repositories (GitHub, Bitbucket etc)		Within 10 business days
6	Professional Network/social media	Fake profiles of the company brand or employees on professional network sites or social media		Within 10 business days
7	Anonymous Public Cloud Storage	Breach data containing your company information hosted on a public cloud storage link in a "ready to download" format		Within 10 business days

Dark Web and Cyber Crime Intelligence

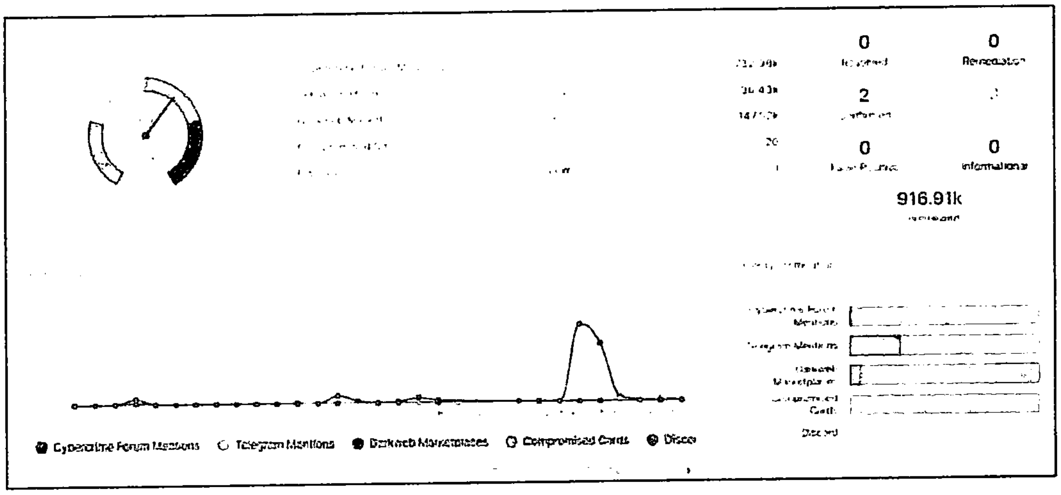
Our dark web and cybercrime intelligence module combine the technical expertise of our global threat research and dark web monitoring team with the power of big data to bring in early warning threat intelligence signals and cybercrime insights of relevance and interest to you from across the deep and dark web.

Through our big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.



The Cyble Threat Research team also stays at the forefront of cutting-edge threat research by continuously discovering, analyzing, and reporting on emerging threat actors, the tools of their trade that includes zero-day malware and then publishing detailed analytical advisories and reports that includes the exclusive IOCs and TTP to help clients prepare for and pre-empt a future attack.

Our dark web monitoring and intelligence team continuously monitors the activities across various open as well as invite-only invite-only/private forums to gain early warning intelligence about a potential cyber-attack on a victim, any posts or chatter or messages on dark web forums that could indicate an access or data compromise involving the client organization, its employees, or its vendors. This allows our clients to initiate an appropriate response or conduct an internal investigation to identify the source of the incident.



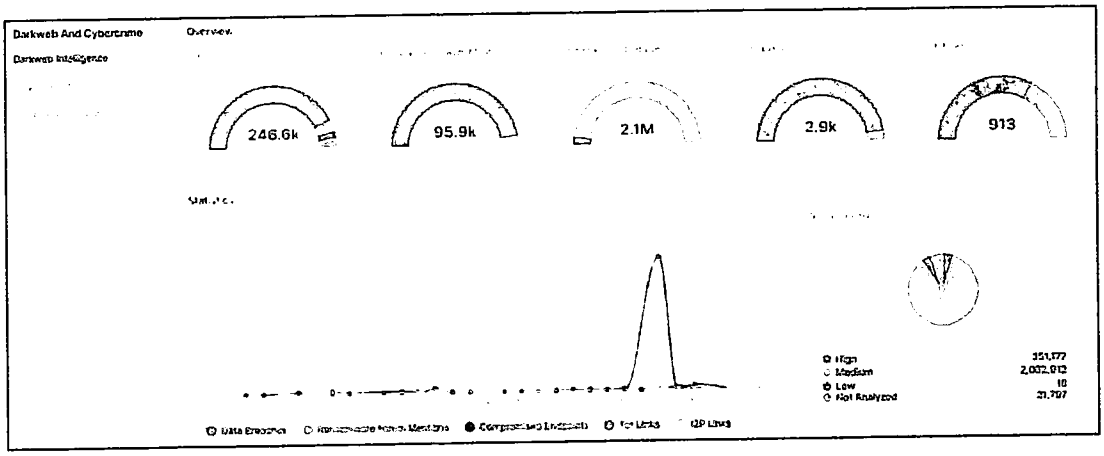
Our dark web and cyber-crime intelligence services enable you to

1. Identify compromised user accounts of your organization, and their credentials with their system information that can be used to trace the compromised/infected systems for detailed forensic analysis and mitigation.
2. The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following:
   - Employee compromised credentials.
   - Sensitive information Leakage such as Username Password Secret token access keys
   - Compromised PII such as Email ID, Phone number and Address.
   - information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation.
   - Exposed Cloud Buckets
   - Malware and Malicious Infrastructure related to Customer domain.
   - Private / Sensitive Documents relating to the business.
   - Hacking documents/tools specifically targeting client; -Leaked Source Code.
   - Intellectual property exposed or leaked.
   - Copyright / Trademark infringement.
   - Technical Information / Data that could be used to compromise corporate systems.
   - -Mentions of IP Addresses and Infrastructure
   - Stolen / Compromised Login Credentials and Customer Account Information.
3. Become aware of prominent data leaks, breaches, or ransomware-related breaches across the globe along with any organizational data or customer PII exposed in the breach/leak at a third party (business partner, vendor, consulting firm or service provider etc.) to assess its impact to your business; all these through our updated threat advisories and quick reports.
4. Become aware of any communication between threat actors that could point to any malicious activity associated with your organization.
5. Search for specific threat actors, review their posts and chatter that refer to your organization, across prominent cyber-crime forums.
6. In special circumstances or situations, engage with the threat research team to gather more information or intelligence through direct engagement with the cyber-criminal or threat actors.

Dark Web and Cyber Crime Intelligence

Our dark web and cybercrime intelligence module combine the technical expertise of our global threat research and dark web monitoring team with the power of big data to bring in early warning threat intelligence signals and cybercrime insights of relevance and interest to you from across the deep and dark web.

Through our big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.



The Cyble Threat Research team also stays at the forefront of cutting-edge threat research by continuously discovering, analyzing, and reporting on emerging threat actors, the tools of their trade that includes zero-day malware and then publishing detailed analytical advisories and reports that includes the exclusive IOCs and TTP to help clients prepare for and pre-empt a future attack.

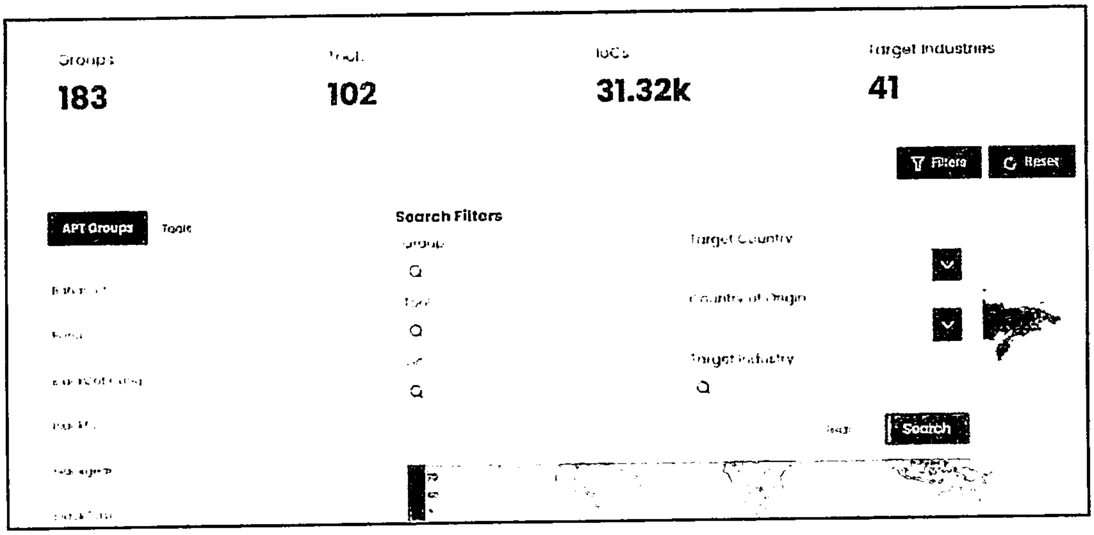
Our dark web monitoring and intelligence team continuously monitors the activities across various open as well as invite-only invite-only/private forums to gain early warning intelligence about a potential cyber-attack on a victim, any posts or chatter or messages on dark web forums that could indicate an access or data compromise involving the client organization, its employees, or its vendors. This allows our clients to initiate an appropriate response or conduct an internal investigation to identify the source of the incident.

2.5.2 Threat Library

The Threat Library is the latest feature to be introduced in Cyble Vision. This feature is aimed at assisting threat researchers and threat intelligence analysts to enhance their understanding of Advanced Persistent Groups and their activities.

The Threat Library contains a catalogue of

- APT Groups and their Aliases
- Their native origins and nation-states backing them
- The countries and sectors that these APT systems have been known to actively target
- Indicators of Compromise associated with these APT groups and their campaigns



The Threat Library is being continuously updated by Cyble Researchers in near real-time, who closely track current and emerging APT groups and the threat information will help clients in staying up to date with the latest IOCs associated with these APT groups. Currently, the threat library contains information on –

- 200+ APT Groups (including Aliases)
- 100+ unique tools
- 41 sectors and industries
- 13000+ unique Indicators of compromise associated with the APT activity

How threat analysts can use the Threat Library –

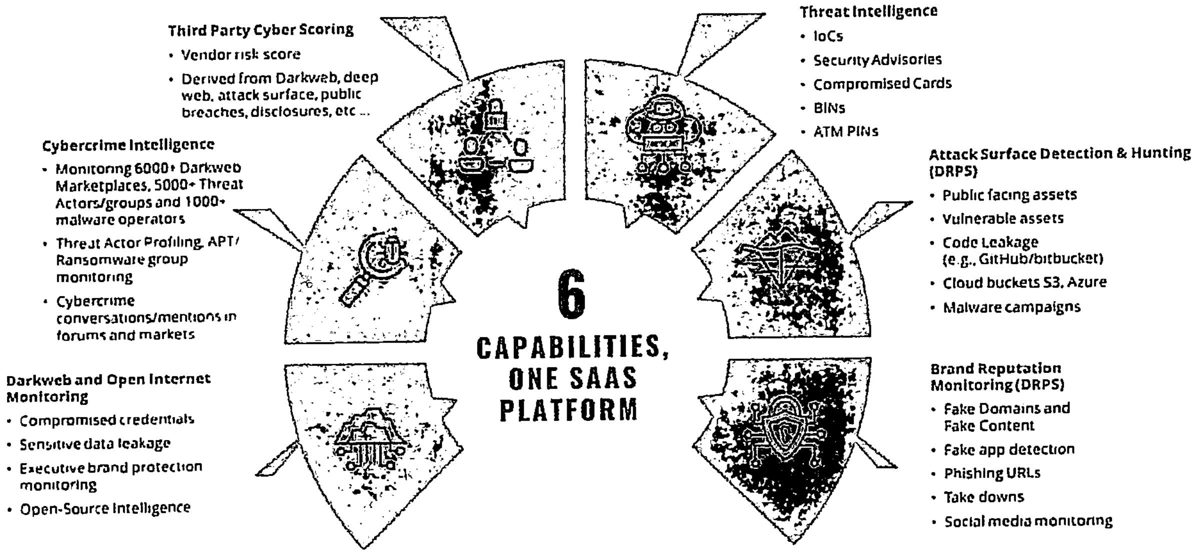
- Read more about an APT group and the tools that they are known to use
- As a part of their internal threat hunting exercises, search for an IOC in the Threat library to determine if it is associated with an APT group and the malware/hacking tools associated with the IOC
- lookup an APT group by its name and alias to learn more about their target geography, target business sectors, tools they have been known to use along with the curated Indicators of Compromise associated with these groups.

Cyble Vision – Solution and Services Overview

Our flagship Cloud-based SaaS platform - Cyble Vision unifies several different threat detection services into a single platform that provides our clients with a unified view of their digital risk footprint across the surface web, the deep web and the dark web. Through our unified digital risk platform, Cyble offers 5 distinct cyber threat detection and mitigation capabilities as below –

- Attack Surface Management
- Dark Web and Cyber Crime Monitoring and Intelligence
- Brand Protection and Social Media Monitoring
- VIP/Executive Monitoring
- Cyber Threat Intelligence
- Incident Response

The below sections cover each of these capabilities in a little more detail.



Third Party Cyber Scoring

- Vendor risk score
- Derived from Darkweb, deep web, attack surface, public breaches, disclosures, etc ...

Cybercrime Intelligence

- Monitoring 6000+ Darkweb Marketplaces, 5000+ Threat Actors/groups and 1000+ malware operators
- Threat Actor Profiling, APT/ Ransomware group monitoring
- Cybercrime conversations/mentions in forums and markets

Darkweb and Open Internet Monitoring

- Compromised credentials
- Sensitive data leakage
- Executive brand protection monitoring
- Open-Source Intelligence

6 CAPABILITIES, ONE SAAS PLATFORM

Threat Intelligence

- IoCs
- Security Advisories
- Compromised Cards
- BINs
- ATM PINs

Attack Surface Detection & Hunting (DRPS)

- Public facing assets
- Vulnerable assets
- Code Leakage (e.g., GitHub/bitbucket)
- Cloud buckets S3, Azure
- Malware campaigns

Brand Reputation Monitoring (DRPS)

- Fake Domains and Fake Content
- Fake app detection
- Phishing URLs
- Take downs
- Social media monitoring

Reference: https://thecyberexpress.com/firewall-daily/

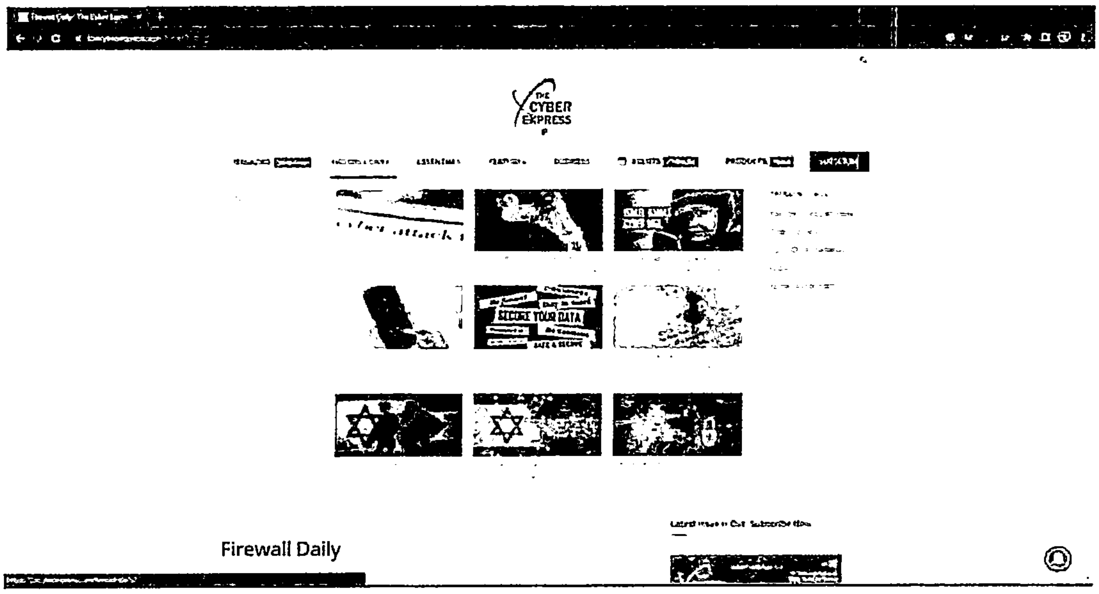
The Cyber Express, No. 1 Trusted Cybersecurity News Site

Through Cyble big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.

Harvest data from the mainstream media (including news, information security sites, vendor research, blogs, vulnerability disclosures) are being published in The Cyber Express.

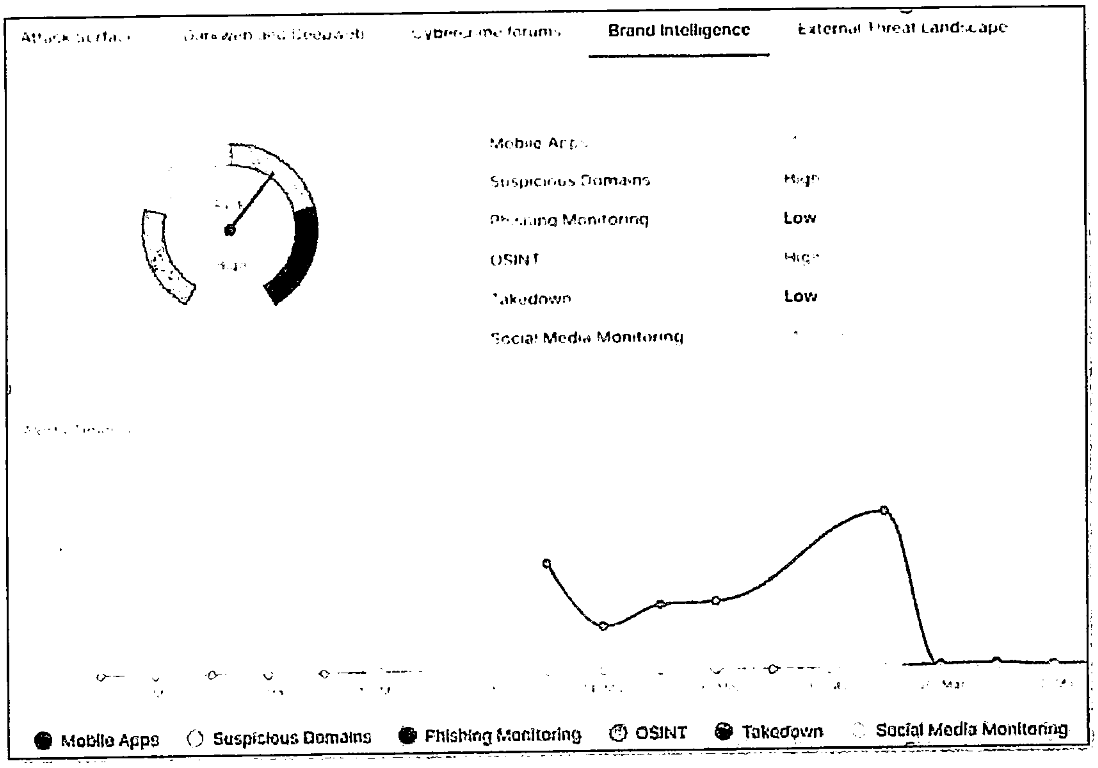
The Cyber Express by Cyble is a cybersecurity news publication that provides the latest news and analysis about the information security industry.

Cyble experienced journalists and researchers works diligently to bring you the most important and relevant news and information about cybersecurity. We cover a wide range of topics, including cyber threats and vulnerabilities, data breaches, cybercrime, cyber defense and security, and the latest technologies and tools for protecting against cyber-attacks.



Digital Brand Protection & Social Media Monitoring

Cyble's Brand Protection suite aims to provide comprehensive coverage of detecting various threat vectors and techniques that are used by cybercriminals to launch brand abuse and phishing attacks across multiple channels to target your brand. Cyble employs a holistic approach to detect digital brand abuse and social media abuse.



Mobile Apps	
Suspicious Domains	High
Phishing Monitoring	Low
OSINT	High
Takedown	Low
Social Media Monitoring	

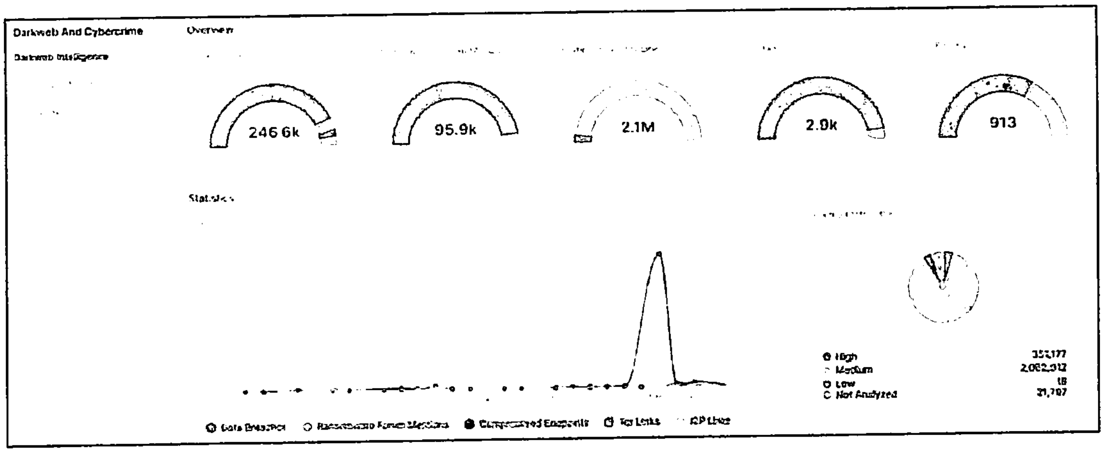
Our suite of brand protection capabilities employs a combination of human security analysts and automated mechanisms to achieve the following –

1. Detection of phishing URLs hosted on fake or look-alike domains or on hacked websites
2. Domain name registration monitoring and search (newly registered domains) to detect suspicious domains or typo-squatted domains that are created to target your brand
3. Analysis of global SSL certificate transparency logs to identify suspicious or fake domains
4. Website watermarking and monitoring to notify you whenever a fraudster mirrors your website or copies your code to setup a look alike phishing website
5. Detection of false affiliation claims or trademark infringement
6. Detection of fake mobile apps that are hosted on legitimate as well as third party app stores
7. Detecting social media accounts/handles/profiles (Instagram, Facebook, YouTube, LinkedIn, Reddit) that are created to impersonate the official accounts of the organization

Dark Web and Cyber Crime Intelligence

Our dark web and cybercrime intelligence module combine the technical expertise of our global threat research and dark web monitoring team with the power of big data to bring in early warning threat intelligence signals and cybercrime insights of relevance and interest to you from across the deep and dark web.

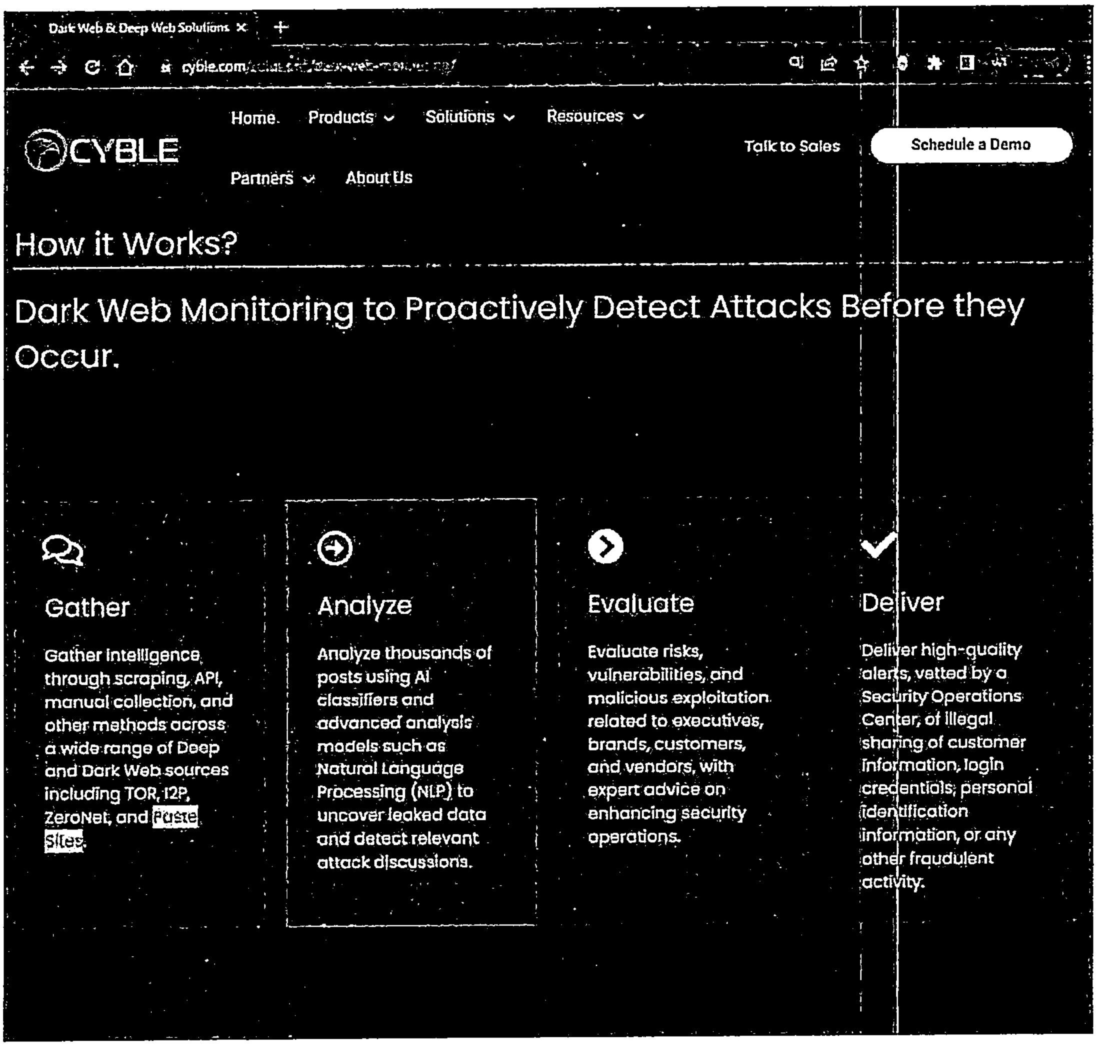
Through our big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.



The Cyble Threat Research team also stays at the forefront of cutting-edge threat research by continuously discovering, analyzing, and reporting on emerging threat actors, the tools of their trade that includes zero-day malware and then publishing detailed analytical advisories and reports that includes the exclusive IOCs and TTP to help clients prepare for and pre-empt a future attack.

Our dark web monitoring and intelligence team continuously monitors the activities across various open as well as invite-only invite-only/private forums to gain early warning intelligence about a potential cyber-attack on a victim, any posts or chatter or messages on dark web forums that could indicate an access or data compromise involving the client organization, its employees, or its vendors. This allows our clients to initiate an appropriate response or conduct an internal investigation to identify the source of the incident.

Reference: Dark Web & Deep Web Monitoring https://cyble.com/solutions/dark-web-monitoring/



How it Works?

Dark Web Monitoring to Proactively Detect Attacks Before they Occur.

Gather

Gather intelligence through scraping, API, manual collection, and other methods across a wide range of Deep and Dark Web sources including TOR, I2P, ZeroNet, and Paste Sites.

Analyze

Analyze thousands of posts using AI classifiers and advanced analysis models such as Natural Language Processing (NLP) to uncover leaked data and detect relevant attack discussions.

Evaluate

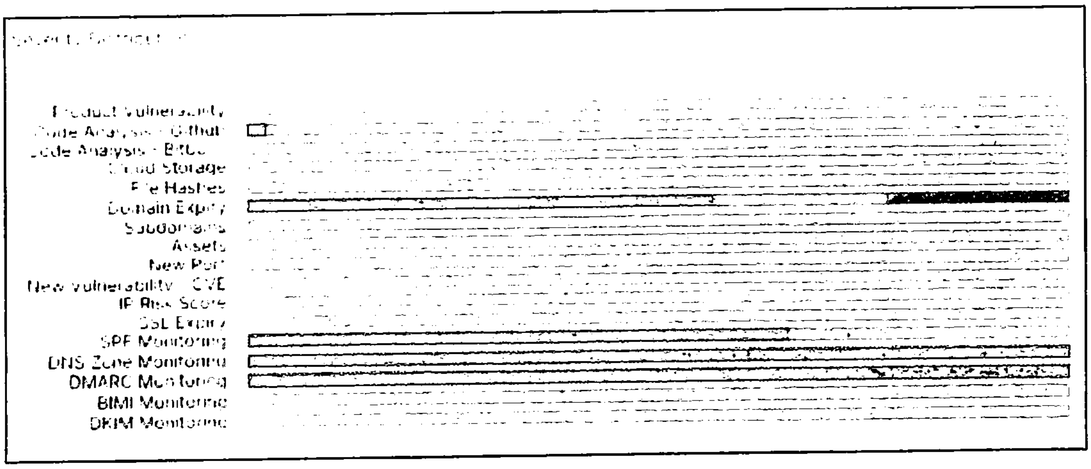
Evaluate risks, vulnerabilities, and malicious exploitation related to executives, brands, customers, and vendors, with expert advice on enhancing security operations.

Deliver

Deliver high-quality alerts, vetted by a Security Operations Center, of illegal sharing of customer information, login credentials, personal identification information, or any other fraudulent activity.

Attack Surface Management

Our attack surface management (ASM) capabilities allow you to enumerate and evaluate the risk of your internet-facing assets continuously.



With our ASM feature, you can

1. discover your domains and sub-domains, their hosting infrastructure along with the details of their discoverability and the IP reputation of these assets.
2. Identify sensitive open ports in your internet-facing infrastructure (FTP, RDP etc) that should be closed or filtered
3. Validate the SSL certificates of your websites, to notify you about certificate expiry for appropriate remediation.
4. Visualize the dynamic risk score of every IP address to notify you whether there is any security risk or malicious activity reported for that asset to facilitate analysis and resolution of the issue.
5. With our vulnerability tracker, maintain an inventory of your technology stack that enables you to be notified whenever a new vulnerability is published that affects any of your listed components
6. DNS Zone Transfer Monitoring, SPF Monitoring, DMARC, DKIM monitoring & BIMI Monitoring
7. Understand the vulnerability posture of your internet-facing assets to become aware of critical unpatched vulnerabilities and thus improve the effectiveness of patch management and remediation efforts
8. Discover the exposure of your sensitive data (API keys, user accounts, access keys, passwords, sensitive IP addresses etc.) and software (application code and builds) via public insecure code repositories such as GitHub and Bitbucket etc.
9. Discover the exposure of your business confidential data or customer PII information in your own or third-party cloud data stores such as Amazon S3 or Azure Blob
10. Identify any network security misconfigurations leading to inadvertent exposure of internal databases or Elastic Servers over the internet.
11. Discover any active botnet infections in your network by our global honeypot network and our stealer log analysis base correlation capabilities.
12. Scan web applications vis a vis OWASP Top 10 Vulnerabilities

8. Detecting social media posts that reference your brand and are designed to spread disinformation, fake news, affect your share price, scam your customers, or display fake affiliations
9. Website Monitoring to detect suspicious or malicious changes to the website such as insertion of malicious scripts or defacement
10. Referral Log Analysis, monitoring malicious redirecting URL
11. Detecting malware files (mobile and desktop) in the wild (sold on underground forums) or on app stores that are targeting client brand
12. DMARC monitoring- Detecting C2 or Phishing URLs by monitoring spam or phishing emails targeting client brands via spoofing

VIP/ Executive Monitoring

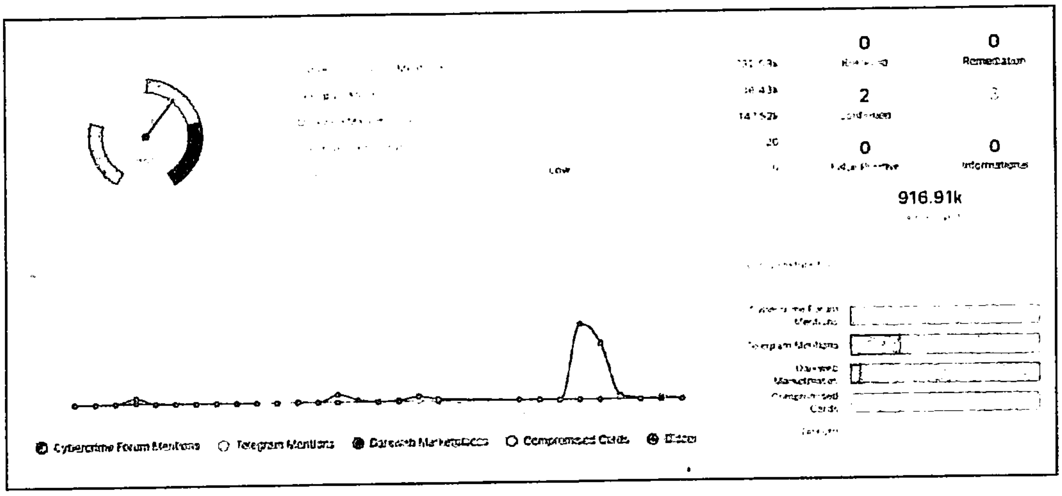
VIP/Executives in an organization are high-value targets as they have privileged access and authority which can be used to very good effect to achieve the nefarious motives of cyber criminals.

Cybercriminals tend to abuse the social presence of key executives so that they can target them for blackmail or their other high-value connections for phishing or fraud.

VIP executives also have access to troves of sensitive information of the organization that holds significant value for attackers as they offer the greatest return on malicious effort. As a result, securing their access and credentials to company infrastructure and applications becomes very critical.

Cyble offers VIP/ Executive monitoring spanning social media as well as the Dark web by detecting and notifying you about following suspicious activity –

1. Creation of lookalike social media profiles (Twitter handles, Facebook pages, LinkedIn profiles, YouTube channels etc.)
2. Identifying the exposure of sensitive PII data (Personal details, government ID etc.) of key VIP executives on cyber-criminal forums or public or third-party data breaches on the dark web
3. Identifying and notifying you about the exposure of sensitive information of VIP executives such as compromised credentials of corporate as well as personal accounts



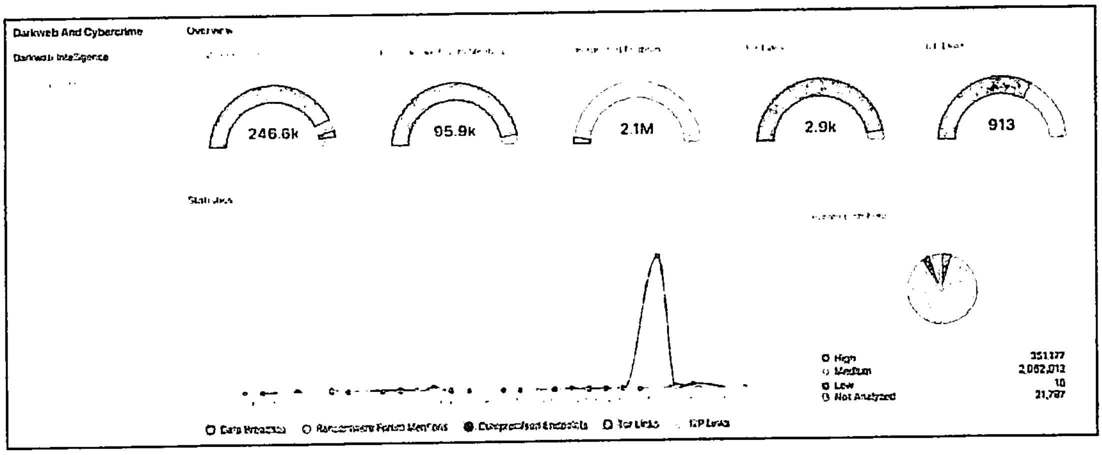
Our dark web and cyber-crime intelligence services enable you to

1. Identify compromised user accounts of your organization, and their credentials with their system information that can be used to trace the compromised/infected systems for detailed forensic analysis and mitigation.
2. The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following:
   - Employee compromised credentials.
   - Sensitive information Leakage such as Username Password Secret token access keys
   - Compromised PII such as Email ID, Phone number and Address.
   - information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation.
   - Exposed Cloud Buckets
   - Malware and Malicious Infrastructure related to Customer domain.
   - Private / Sensitive Documents relating to the business.
   - Hacking documents/tools specifically targeting client; -Leaked Source Code.
   - Intellectual property exposed or leaked.
   - Copyright / Trademark infringement.
   - Technical Information / Data that could be used to compromise corporate systems.
   - -Mentions of IP Addresses and Infrastructure
   - Stolen / Compromised Login Credentials and Customer Account Information.
3. Become aware of prominent data leaks, breaches, or ransomware-related breaches across the globe along with any organizational data or customer PII exposed in the breach/leak at a third party (business partner, vendor, consulting firm or service provider etc.) to assess its impact to your business; all these through our updated threat advisories and quick reports.
4. Become aware of any communication between threat actors that could point to any malicious activity associated with your organization.
5. Search for specific threat actors, review their posts and chatter that refer to your organization, across prominent cyber-crime forums.
6. In special circumstances or situations, engage with the threat research team to gather more information or intelligence through direct engagement with the cyber-criminal or threat actors.

Dark Web and Cyber Crime Intelligence

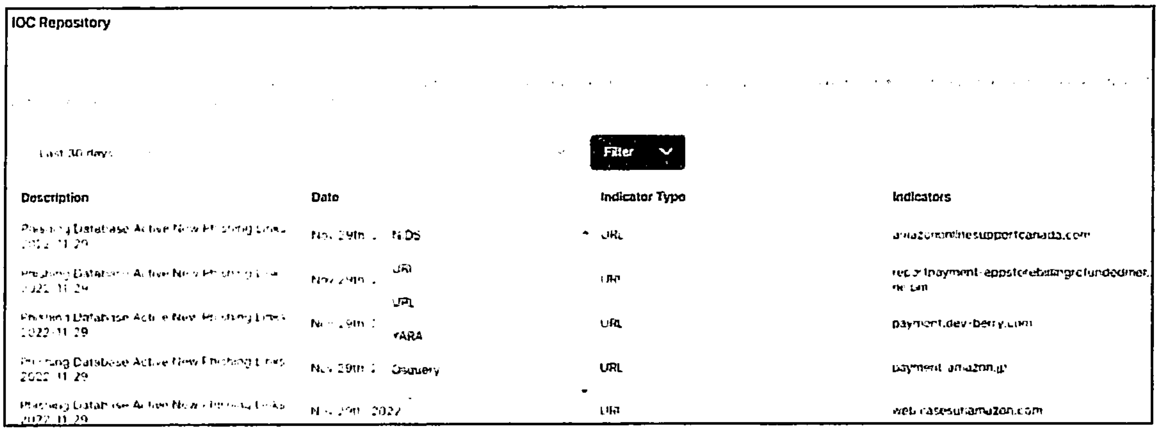
Our dark web and cybercrime intelligence module combine the technical expertise of our global threat research and dark web monitoring team with the power of big data to bring in early warning threat intelligence signals and cybercrime insights of relevance and interest to you from across the deep and dark web.

Through our big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.



The Cyble Threat Research team also stays at the forefront of cutting-edge threat research by continuously discovering, analyzing, and reporting on emerging threat actors, the tools of their trade that includes zero-day malware and then publishing detailed analytical advisories and reports that includes the exclusive IOCs and TTP to help clients prepare for and pre-empt a future attack.

Our dark web monitoring and intelligence team continuously monitors the activities across various open as well as invite-only invite-only/private forums to gain early warning intelligence about a potential cyber-attack on a victim, any posts or chatter or messages on dark web forums that could indicate an access or data compromise involving the client organization, its employees, or its vendors. This allows our clients to initiate an appropriate response or conduct an internal investigation to identify the source of the incident.



IOC Repository

Last 30 days

Description	Date	Indicator Type	Indicators
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th	URL	amazononlinesupportcanada.com
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th	URI	[illegible]payment-appstorebillingrefunddomer.[illegible]
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th	URL	payment.dev-berry.com
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th	URL	payment.amazon.jp
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th 2022	URI	web.casesuramazon.com

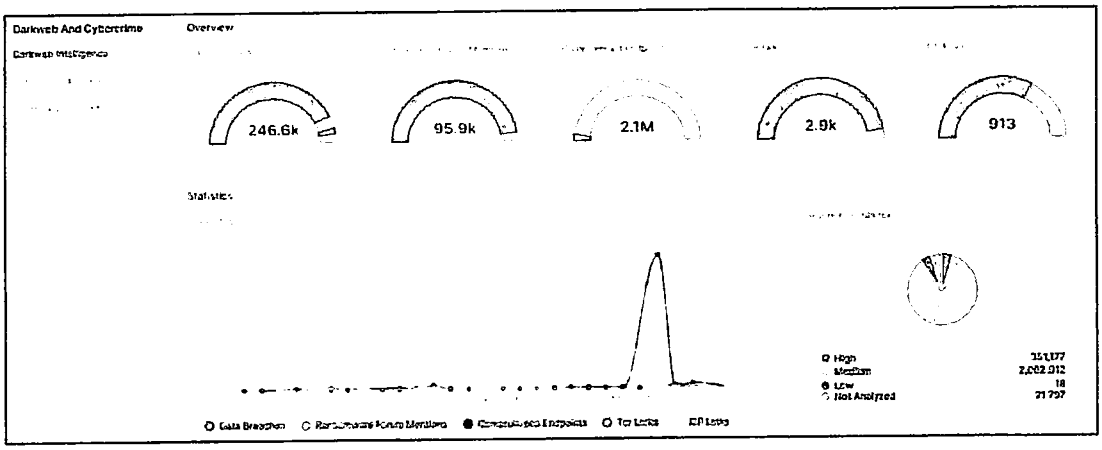
Clients can search for an Indicator of Compromise and get contextual information about any malicious activity associated with the indicator. The IOC is also enriched with information from reputed global third-party intelligence aggregators and providers such as VirusTotal to provide a confidence rating for that IOC.

1. Threat Intelligence gathered from various sources, ranging from public sources, technical sources, dark web & deep web, Underground forums, special access sites, Code Repositories, Paste bin and human analyst
2. The threat intelligence solution can collect data in all major global languages, including, but not limited to Urdu, Arabic, Chinese, Russian, Korean etc.
3. Threat intelligence feed identify new global threats like Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc.
4. Collection of Threat intelligence from the various sources should be automated, using technologies such as machine learning and Deep Language Processing, which allows mass collection of intelligence with low false positives, in real-time.
5. Threat Intelligence of IOCs delivered with full context of related entities, such as related hashes, IPs, CVEs and Threat Actors, Threat Vectors, Malwares, Product impacted etc. The contextualized threat information should be delivered in a simple and easy to digest format.
6. Cyble's global IOC repository contains over 2.5 billion + Indicators of compromise across **23 categories (CIDR, Domain, CVE, File hashes of various types, IP V4, IP V6, Email, File Path, Hostnames, Mutex, NIDS, URI, URL, YARA, OSquery, Ja3, Bitcoin Addresses, SSLCertFingerprint** etc) that is updated daily.
7. The service should support malware sandboxing by allowing users to-
   - Upload suspicious files to the platform and download a detailed file behaviour analysis report and network analysis report for each uploaded file
   - The analysis report should contain risk score of the file, relevant indicators of compromise such as IP addresses, domains or C2 URLs, suspicious network connections, usage of potentially malicious API and files downloaded or dropped on the disk upon successful execution.
   - The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party.
   - The sandboxing should support common operating systems such as Android, Linux and Windows at a minimum.
   - The service should support automated analysis of at-least 5 samples per day.
   - The service provider should provide analyst support for report interpretation and explanation as and when required.

Dark Web and Cyber Crime Intelligence

Our dark web and cybercrime intelligence module combine the technical expertise of our global threat research and dark web monitoring team with the power of big data to bring in early warning threat intelligence signals and cybercrime insights of relevance and interest to you from across the deep and dark web.

Through our big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.



Darkweb And Cybercrime

Darkweb Intelligence

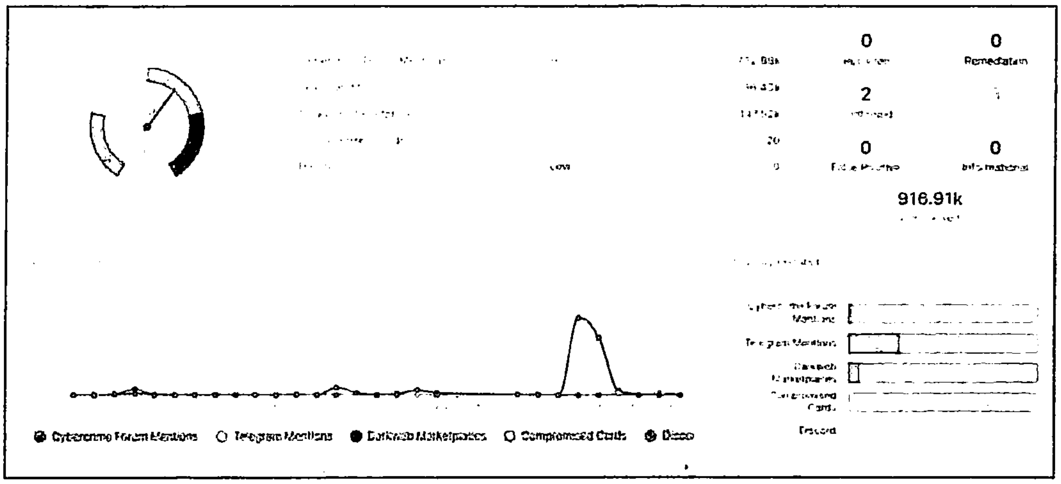
The Cyble Threat Research team also stays at the forefront of cutting-edge threat research by continuously discovering, analyzing, and reporting on emerging threat actors, the tools of their trade that includes zero-day malware and then publishing detailed analytical advisories and reports that includes the exclusive IOCs and TTP to help clients prepare for and pre-empt a future attack.

Our dark web monitoring and intelligence team continuously monitors the activities across various open as well as invite-only invite-only/private forums to gain early warning intelligence about a potential cyber-attack on a victim, any posts or chatter or messages on dark web forums that could indicate an access or data compromise involving the client organization, its employees, or its vendors. This allows our clients to initiate an appropriate response or conduct an internal investigation to identify the source of the incident.

SLA for Brand Monitoring and take down services

Cyble offers the following Service Levels on a best effort basis for Detection and Takedown of web content/ properties targeting our client brands contingent on the dependencies listed below–

Sr No	Description	Type of Incident	SLA for takedown initiation	*Estimated time for completion of complaint
1	Phishing website	Website cloning Phishing email	Upon confirmation by client, the Cyble incident response team will initiate enforcement process within 2 hours	Within 3 business days Within 5 business days
2	Website	Trademark / Copyright infringement		Within 10 business days
3	Social Media	Brand impersonation/ Trademark infringement / Copyright infringement		Within 3 business days
4	Mobile Apps	Apps hosted on 3rd party platforms Trademark infringement- Play store/Apple App store		Within 5 business days
5	Public Code Repositories	Code leaks on public code repositories (GitHub, Bitbucket etc)		Within 10 business days
6	Professional Network/social media	Fake profiles of the company brand or employees on professional network sites or social media		Within 10 business days
7	Anonymous Public Cloud Storage	Breach data containing your company information hosted on a public cloud storage link in a "ready to download" format		Within 10 business days



Our dark web and cyber-crime intelligence services enable you to

1. Identify compromised user accounts of your organization, and their credentials with their system information that can be used to trace the compromised/infected systems for detailed forensic analysis and mitigation.
2. The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following:
   - Employee compromised credentials.
   - Sensitive information Leakage such as Username Password Secret token access keys
   - Compromised PII such as Email ID, Phone number and Address.
   - information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation.
   - Exposed Cloud Buckets
   - Malware and Malicious Infrastructure related to Customer domain.
   - Private / Sensitive Documents relating to the business.
   - Hacking documents/tools specifically targeting client; -Leaked Source Code.
   - Intellectual property exposed or leaked.
   - Copyright / Trademark infringement.
   - Technical Information / Data that could be used to compromise corporate systems.
   - -Mentions of IP Addresses and Infrastructure
   - Stolen / Compromised Login Credentials and Customer Account Information.
3. Become aware of prominent data leaks, breaches, or ransomware-related breaches across the globe along with any organizational data or customer PII exposed in the breach/leak at a third party (business partner, vendor, consulting firm or service provider etc.) to assess its impact to your business; all these through our updated threat advisories and quick reports.
4. Become aware of any communication between threat actors that could point to any malicious activity associated with your organization.
5. Search for specific threat actors, review their posts and chatter that refer to your organization, across prominent cyber-crime forums.
6. In special circumstances or situations, engage with the threat research team to gather more information or intelligence through direct engagement with the cyber-criminal or threat actors.

8. Detecting social media posts that reference your brand and are designed to spread disinformation, fake news, affect your share price, scam your customers, or display fake affiliations
9. Website Monitoring to detect suspicious or malicious changes to the website such as insertion of malicious scripts or defacement
10. Referral Log Analysis, monitoring malicious redirecting URL
11. Detecting malware files (mobile and desktop) in the wild (sold on underground forums) or on app stores that are targeting client brand
12. DMARC monitoring- Detecting C2 or Phishing URLs by monitoring spam or phishing emails targeting client brands via spoofing

VIP/ Executive Monitoring

VIP/Executives in an organization are high-value targets as they have privileged access and authority which can be used to very good effect to achieve the nefarious motives of cyber criminals.

Cybercriminals tend to abuse the social presence of key executives so that they can target them for blackmail or their other high-value connections for phishing or fraud.

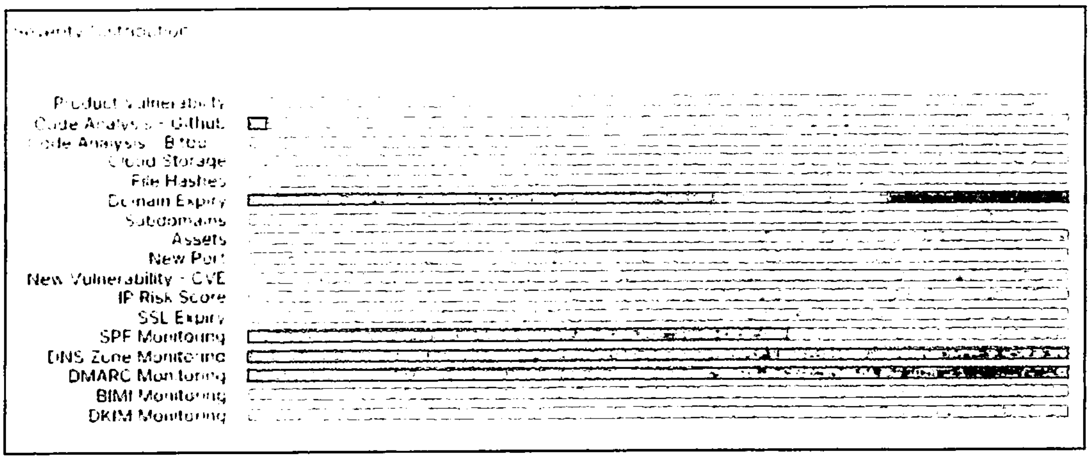
VIP executives also have access to troves of sensitive information of the organization that holds significant value for attackers as they offer the greatest return on malicious effort. As a result, securing their access and credentials to company infrastructure and applications becomes very critical.

Cyble offers VIP/ Executive monitoring spanning social media as well as the Dark web by detecting and notifying you about following suspicious activity –

1. Creation of lookalike social media profiles (Twitter handles, Facebook pages, LinkedIn profiles, YouTube channels etc.)
2. Identifying the exposure of sensitive PII data (Personal details, government ID etc.) of key VIP executives on cyber-criminal forums or public or third-party data breaches on the dark web
3. Identifying and notifying you about the exposure of sensitive information of VIP executives such as compromised credentials of corporate as well as personal accounts

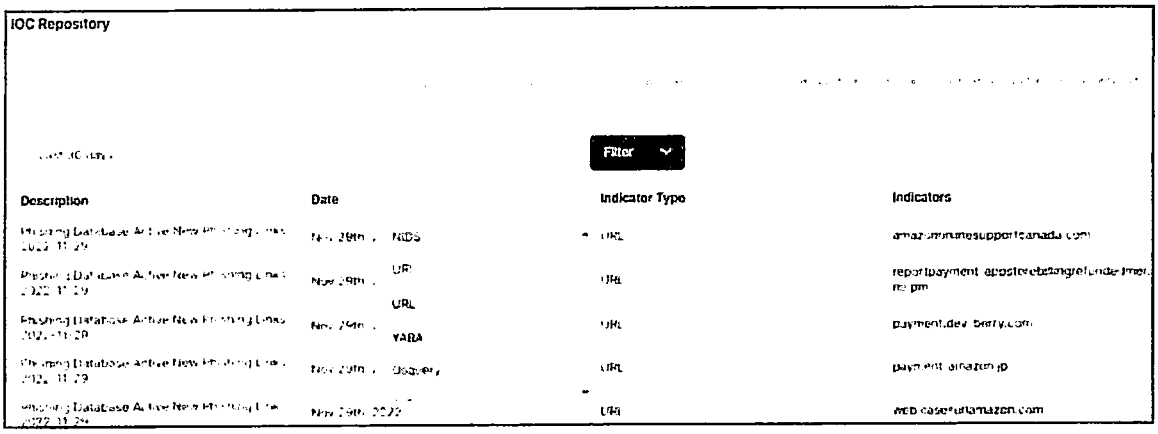
Attack Surface Management

Our attack surface management (ASM) capabilities allow you to enumerate and evaluate the risk of your internet-facing assets continuously.



With our ASM feature, you can

1. discover your domains and sub-domains, their hosting infrastructure along with the details of their discoverability and the IP reputation of these assets.
2. Identify sensitive open ports in your internet-facing infrastructure (FTP, RDP etc) that should be closed or filtered
3. Validate the SSL certificates of your websites, to notify you about certificate expiry for appropriate remediation.
4. Visualize the dynamic risk score of every IP address to notify you whether there is any security risk or malicious activity reported for that asset to facilitate analysis and resolution of the issue.
5. With our vulnerability tracker, maintain an inventory of your technology stack that enables you to be notified whenever a new vulnerability is published that affects any of your listed components
6. DNS Zone Transfer Monitoring, SPF Monitoring, DMARC, DKIM monitoring & BIMI Monitoring
7. Understand the vulnerability posture of your internet-facing assets to become aware of critical unpatched vulnerabilities and thus improve the effectiveness of patch management and remediation efforts
8. Discover the exposure of your sensitive data (API keys, user accounts, access keys, passwords, sensitive IP addresses etc.) and software (application code and builds) via public insecure code repositories such as GitHub and Bitbucket etc.
9. Discover the exposure of your business confidential data or customer PII information in your own or third-party cloud data stores such as Amazon S3 or Azure Blob
10. Identify any network security misconfigurations leading to inadvertent exposure of internal databases or Elastic Servers over the internet.
11. Discover any active botnet infections in your network by our global honeypot network and our stealer log analysis base correlation capabilities.
12. Scan web applications vis a vis OWASP Top 10 Vulnerabilities



IOC Repository

Description	Date	Indicator Type	Indicators
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th , NIDS	URL	amazonmunesupportcanada.com
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th , URI	URL	reportpayment [illegible] .pm
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th , URL YARA	URL	payment.dev [illegible] .com
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th , OSquery	URL	payment amazon.jp
Phishing Database Active New Phishing Links 2022-11-29	Nov 29th, 2022	URL	web.casefullamazon.com

Clients can search for an Indicator of Compromise and get contextual information about any malicious activity associated with the indicator. The IOC is also enriched with information from reputed global third-party intelligence aggregators and providers such as VirusTotal to provide a confidence rating for that IOC.

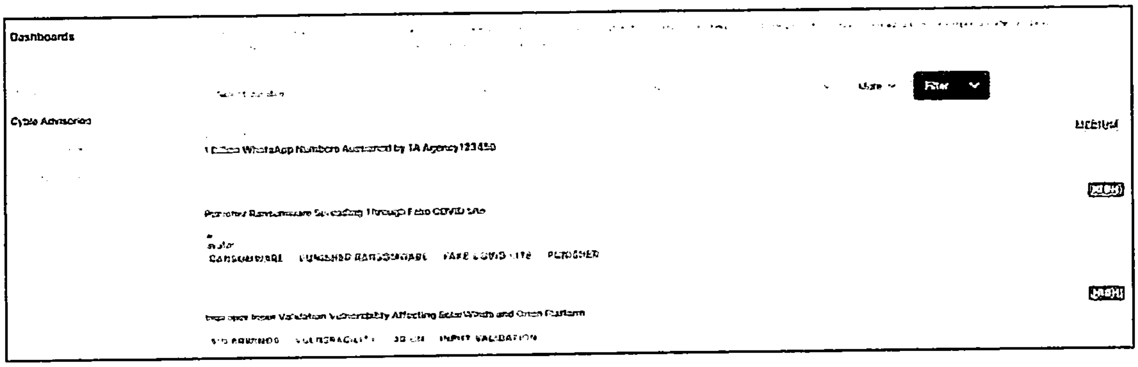
1. Threat Intelligence gathered from various sources, ranging from public sources, technical sources, dark web & deep web, Underground forums, special access sites, Code Repositories, Paste bin and human analyst
2. The threat intelligence solution can collect data in all major global languages, including, but not limited to Urdu, Arabic, Chinese, Russian, Korean etc.
3. Threat intelligence feed identify new global threats like Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc.
4. Collection of Threat intelligence from the various sources should be automated, using technologies such as machine learning and Deep Language Processing, which allows mass collection of intelligence with low false positives, in real-time.
5. Threat Intelligence of IOCs delivered with full context of related entities, such as related hashes, IPs, CVEs and Threat Actors, Threat Vectors, Malwares, Product impacted etc. The contextualized threat information should be delivered in a simple and easy to digest format.
6. Cyble's global IOC repository contains over 2.5 billion + Indicators of compromise across **23 categories (CIDR, Domain, CVE, File hashes of various types, IP V4, IP V6, Email, File Path, Hostnames, Mutex, NIDS, URI, URL, YARA, OSquery, Ja3, Bitcoin Addresses, SSLCertFingerprint** etc) that is updated daily.
7. The service should support malware sandboxing by allowing users to-
   - Upload suspicious files to the platform and download a detailed file behaviour analysis report and network analysis report for each uploaded file
   - The analysis report should contain risk score of the file, relevant indicators of compromise such as IP addresses, domains or C2 URLs, suspicious network connections, usage of potentially malicious API and files downloaded or dropped on the disk upon successful execution.
   - The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party.
   - The sandboxing should support common operating systems such as Android, Linux and Windows at a minimum.
   - The service should support automated analysis of at-least 5 samples per day.
   - The service provider should provide analyst support for report interpretation and explanation as and when required.

Cyber Threat Intelligence

Cyble's Threat Intelligence module is powered by a vast global big data repository of Indicators of Compromise gleaned from several different sources such as

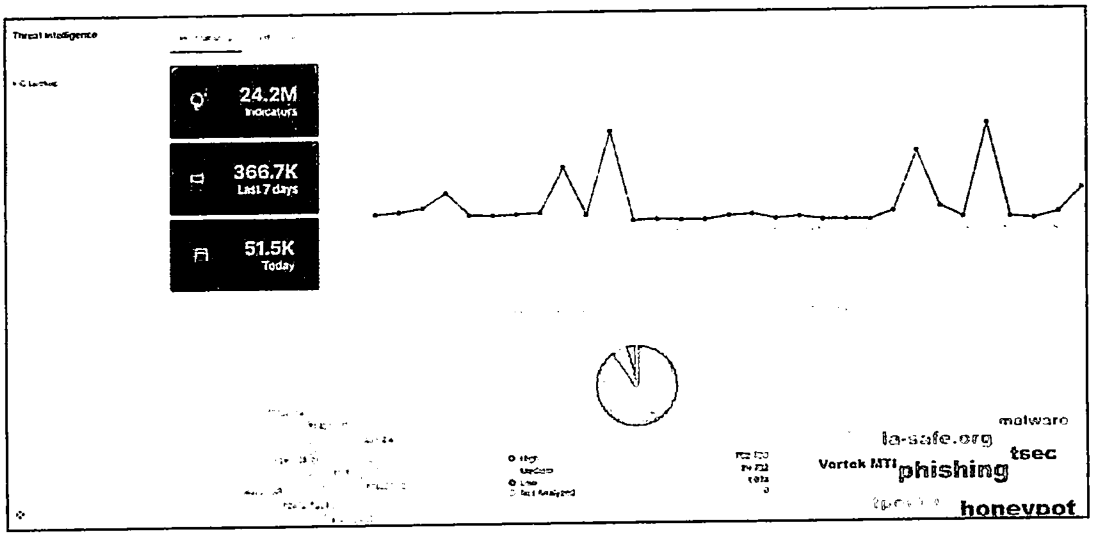
- our own and managed global honeypot sensor intelligence network
- the open internet,
- open-source public threat intelligence sources
- premium commercial threat intelligence provider feeds.

Further, Cyble has recently entered a threat intelligence partnership with Google, to provide its threat indicators to Virus Total to increase the situational awareness and enhance the collective security intelligence capabilities of the cyber security community globally.


Dashboards
Filter
Cyble Advisories
WhatsApp Numbers ... by TA Agency123450
... Ransomware Spreading Through Fake COVID Site
FAKE COVID SITE
... Input Validation Vulnerability Affecting SolarWinds and Orion Platform
INPUT VALIDATION

Cyble Advisories

2.5.1 Global IOC Repository



Cyble's global IOC repository contains over 80 billion + Indicators of compromise across **various categories (CIDR, Domain, CVE, File hashes of various types, IP V4, IP V6,Hostnames, URI, URL, YARA, Bitcoin Addresses, SSLCertFingerprint etc)** that is updated daily.