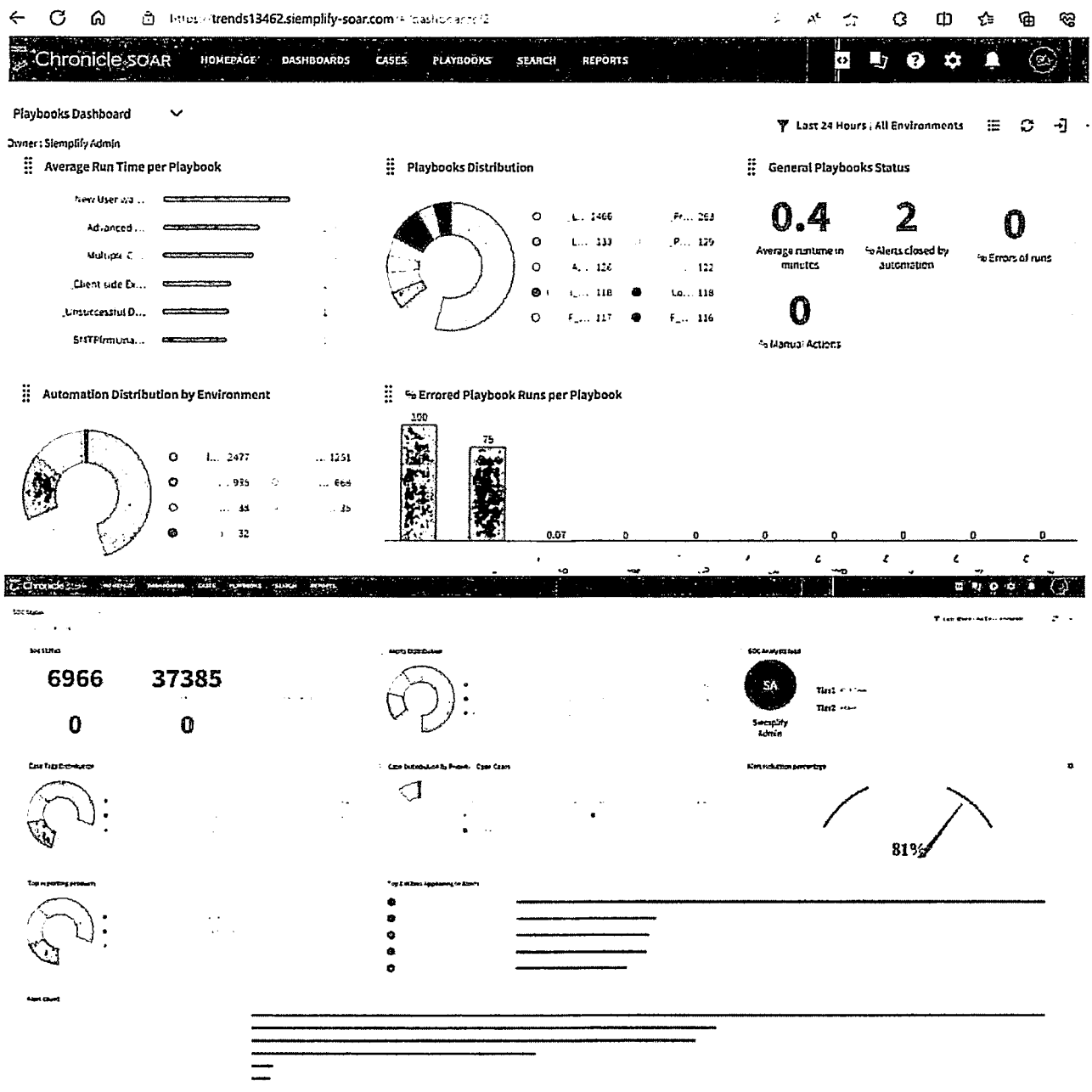


TRENDS | Managed ICT Services
Service Delivery with Flexibility

# INCIDENT MANAGEMENT
## POLICIES, STANDARDS, PROCEDURES & GUIDELINES

This document defines the policies, standards, procedures and guidelines for the effective handling and managing of service incidents.

| | |
|---|---|
| DOCUMENT ID | |
| DOCUMENT OWNER | **TRENDS Cyber Security Intelligence** |
| 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

TRENDS Managed ICT Services (MICTS) is aligned to the ITIL 4 framework as it operates and provides IT services to its clients, both internally and externally. Two of the most important practices of IT Service Management concepts are incident and problem management, whereas incident management is defined as restoring to normal service.

It is with this premise that the Incident Management Policies, Standards, Procedures, and Guidelines is written, such, to provide clear understanding on how to identify, categorize, prioritize and handle IT incidents from the moment its occurrence up to its resolution thus ensuring that agreed levels of service quality are maintained.

These policies, standards, and procedures will be used the SOC operations team. The SOC operations team, through the SIEM, shall detect and monitor threats, correlate with threat intelligence sources, generate alerts, conduct investigation, and escalate tickets on a 24x7 basis using the Security Operations Center (SOC) platforms.

## 1.2 Purpose of the Document

This document is written to provide the policies, standards, procedures, and guidelines to handle and manage IT incidents effectively and efficiently.

## 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

| | |
|---|---|
| Information Security | The preservation of confidentiality, integrity, and availability of information. |
| Information Security Management System | Part of overall management process that takes care of planning, implementing, maintaining, reviewing, and improving the information security. [1] |
| ISGAB | Information Security Governance and Advisory Board |
| CI | Configuration Item |
| Incident | An unplanned interruption to an IT service, reduction in the quality of a service.[2] |
| Configuration Item | Any component that needs to be managed in order to deliver an IT service. Components that make up a service in which a configuration item is an item that will assist in facilitating outcomes. CIs may be any of the following:<br>• Software (e.g.: Applications, Internet Services)<br>• Hardware (e.g.: Laptops)<br>• Environment (e.g.: Location, Power)<br>• People (e.g.: Person or Role) |

[1] ISO Consultants Toolkit
[2] ITIL Foundation – ITIL 4 Edition, Axelos, 2019

| | |
|---|---|
| | ◦ Infrastructure (e.g.: Network)<br>◦ Documentation (e.g.: Licenses, Contracts, Training) |
| Event | Any change of state that has significance for the management of a configuration item (CI) or IT service. |
| Availability | The ability of an IT service or other configuration item to perform its agreed function when required. |
| Service | A means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks. |

### 1.5 Reference Documents & Bibliography

In relation to this document, the following documents are key references:

- MICTS-SO-Documentation Standards_v1.0_TLPAMBER.docx
- ITIL Foundation - ITIL 4 Edition, Axelos, 2019
- ITIL Intermediate Certification Companion, Sybex, 2017
- NIST Special Publication 800-61 Rev. 2

# 2 Purpose and Objective

## 2.1 Purpose

The purpose of incident management practice is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. Normal service operation is defined as an operational state where services and Configuration Items are performing within their agreed service and operational levels.[3]

## 2.2 Objective

The objectives of having documented Incident Management Standards, Procedures and Guidelines are the following:

- To have a unified document that contains all information that pertains to Incident Management of the ITIL 4 Framework.
- To establish standardized methods and models for managing incidents. This means that incidents should be handled in a consistent way regardless of service, technology or support group. This enables MICTS and its clients to have clear expectations of how any particular incident will be handled.
- To increase visibility and communications of incidents. This allows the business to track the progress of the incidents they report and ensures that all MICTS staff have access to the information relating to the incident.
- Align activities with business needs by ensuring that incidents are prioritized based on their importance to the business.
- Maintain client satisfaction.
- To establish KPIs for measuring the effectivity and efficiency of the standards and procedures.

[3] ITIL Intermediate Certification Companion, Sybex, 2017

# 3 Scope and Definition

The Incident Management Standards, Procedures, and Guidelines encompasses all incidents. This means all events that have a real or potential impact to the quality of service of the Service Operations Group under MICTS and the services being offered by TRENDS to its clients.

The Incident Management Policies, Standards, Procedures and Guidelines uses ITIL 4 Incident Management practice and NIST Special Publication 800-61 revision 2 as references in establishing the standardized methods and models in managing incidents.

## 4 Compliance

These standards shall take effect upon publication. Compliance is expected with all enterprise policies and standards and procedures. Policies, standards, and procedures maybe amended at any time.

If compliance with the standards stipulated in this document is not feasible or technically possible, or if deviation from these standards is necessary to support a business function, entities shall request an exception through the ISGAB's deviation process.

## 5 Awareness

It is the responsibility of the Compliance and Continual Improvement department to establish informational training regarding the Incident Management Policies, Standards, Procedures & Guidelines.

Awareness to these policies, standards, procedures, and guidelines must be included in the Personnel On-Boarding Procedure.

Each personnel affected by these policies, standards, procedures, and guidelines must sign in the collective sign-off sheet after going through the informational training on Incident Management Policies, Standards, Procedures & Guidelines.

# 6 Incident Management

## 6.1 Policy

Below are the policies to ensure efficient and effective incident management practice.

1. All incidents must be stored and managed in a single management system.
2. All incidents must be categorized and prioritized in a standard way and agreed upon.
3. All incidents must use a common format.
4. Incidents and their status must be communicated in a timely and effective manner.
5. Incidents must be resolved within timeframes that are acceptable to the business.
6. Customer satisfaction must be maintained at all times.
7. Incident processing and handling should be aligned with the overall service levels and objectives.
8. Escalation conditions and channels must be agreed upon.
9. Incident records must be audited on a regular basis.

## 6.2 Classification of Incident

TRENDS MICTS classifies an incident into either Information Security (IS) Incident or Quality-of-Service (QoS) Incident.

Information Security Incident is defined as a violation or imminent threat of violation of information security policies, acceptable use policy, or standard security practices.

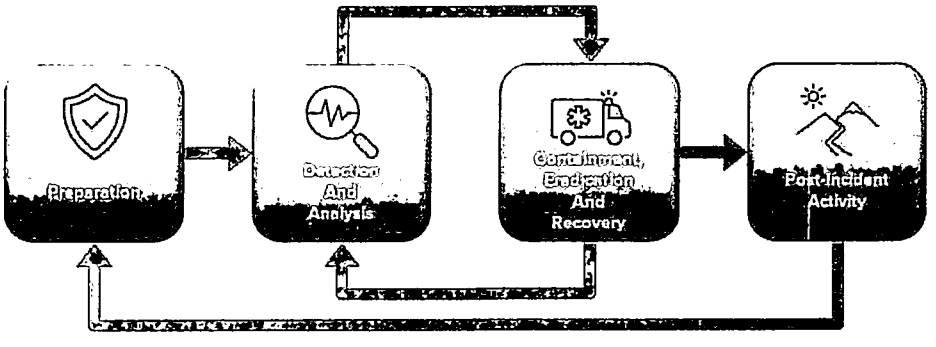
On the other hand, Quality-of-Service Incident relates to degradation, unavailability, or inability of an IT service to deliver the intended outcome a client wants to achieve.

## 6.3 Incident Response Life Cycle

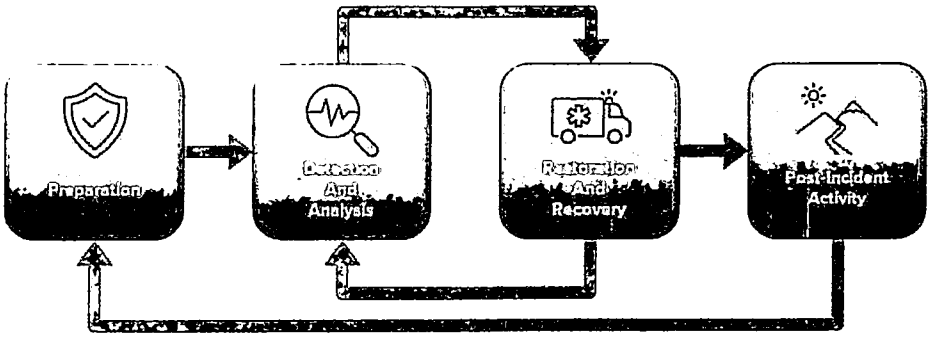
The Incident Response Life Cycle that the MICTS Service Operations follows is based on the NIST SP 800-61 revision 2 (Computer Security Incident Handling Guide) which is a 4-step process as follows:

1. Preparation
2. Detection & Analysis
3. Recovery
4. Post-incident Activity

**Information Security Incident Response Life Cycle**



**Quality-of -Service Incident Response Life Cycle**




### 6.4 Identification of Incident

The manners in which awareness to an incident may be achieved are as follows:

- Monitoring of SOAR, SIEM or NMS by TOC personnel on duty
- Reports from client on experienced incidents
- Monitoring of information feeds from the internet

### 6.5 Incident Prioritization

The priority level assigned to an incident indicates the relative impact to be business. Assigning a priority level to an incident ensures that proper actions are taken timely and accordingly.

Incidents' priority level can be assigned from the 5 levels of prioritization as presented below.

| | | IMPACT | | |
|---|---|---|---|---|
| | | HIGH | MEDIUM | LOW |
| URGENCY | HIGH | 1 | 2 | 3 |
| | MEDIUM | 2 | 3 | 4 |
| | LOW | 3 | 4 | 5 |

Priority levels for incidents internal to TRENDS can be found as ANNEX 1 – TRENDS Operations Center Incident Impact Criteria, Urgency Criteria and Priority Matrix. For client priority matrix, refer to client contract/SLA.

### 6.6 Logging of Incidents

All incidents shall be logged into the Incident Registry. The IVANTI Service Management system serves as the Incident Registry.

### 6.7 Incident Response Updating, Restoration, Resolution and Root Cause Analysis Time

Response Time is the target duration for TRENDS Operations Center to respond to a reported or detected incident. For incidents internal to TRENDS, the response timetable is indicated as ANNEX 2 – TRENDS Operations Center Incident Response & Update Time. For client incidents' response timetable, refer to client SLA.

Update Time is the target frequency for TRENDS Operations Center to update a reported or detected incident. For incidents internal to TRENDS, the update timetable is indicated as ANNEX 2 – TRENDS Operations Center Incident Response & Update Time. For client incidents' response timetable, refer to client SLA.

Restoration Time is the target duration for TRENDS Operations Center to restore the service to normal service operations. For incidents internal to TRENDS, the restoration timetable is indicated as ANNEX 3 – TRENDS Operations Center Quality-of-Service Incident Restoration Time. For client incidents' restoration timetable, refer to client SLA.

Resolution Time is the target duration for TRENDS Operations Center to resolve a security incident. For incidents internal to TRENDS, the resolution timetable is indicated as ANNEX 4 – TRENDS Operations Center Information Security Incident Resolution Time. For client incidents' resolution timetable, refer to client SLA.

Root Cause Analysis (RCA) Time is the target duration for TRENDS Operations Center to publish the Root Cause Analysis of an incident. For incidents internal to TRENDS, the RCA timetable is indicated as ANNEX 5 – TRENDS Operations Center Root Cause Analysis Response Time. For client incidents' RCA timetable, refer to client SLA.

## 6.8 Incident Monitoring

To ensure that incidents are properly handled, incident monitoring shall regularly be conducted. After a shift has concluded, any open incident tickets shall be endorsed and turned over to the next shift until the incident resolved.

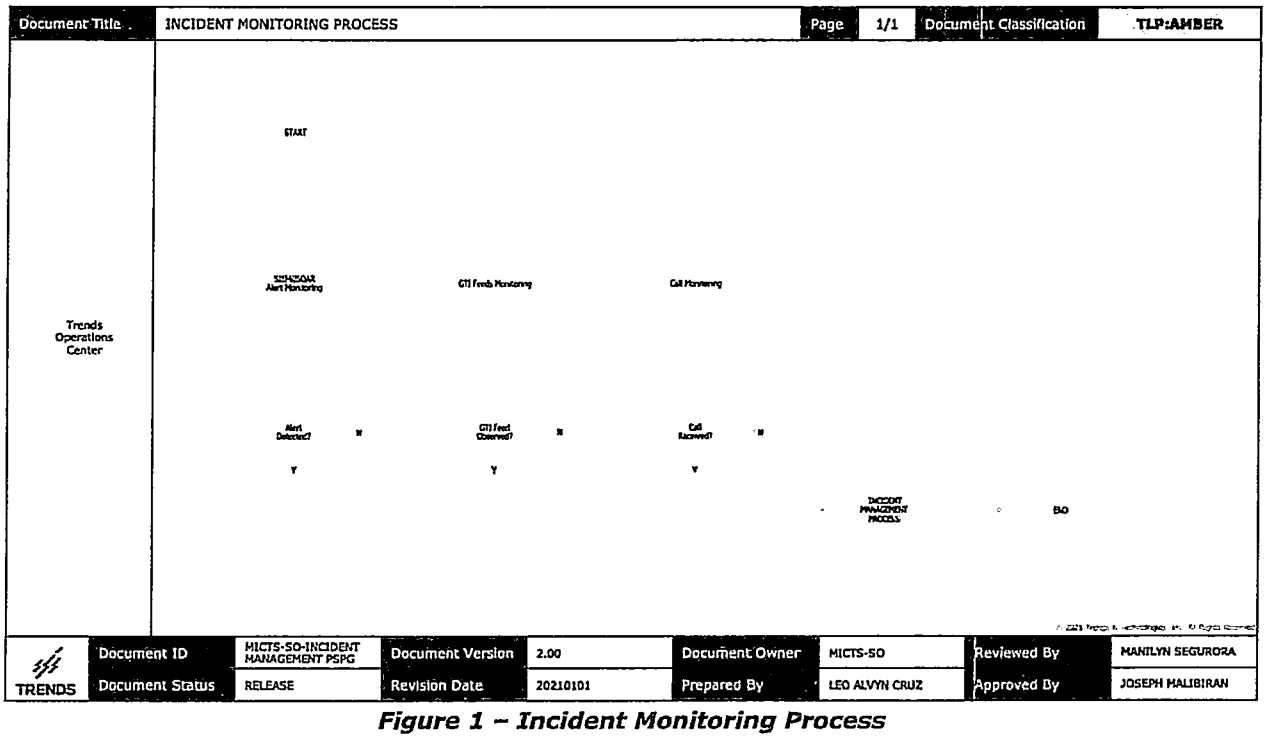



***Figure 1 – Incident Monitoring Process***

## 6.9 Incident Manager

Since the Incident Manager is responsible for maintaining the Incident Management Process, the Incident Manager is also responsible for monitoring of incident tickets and ensuring incidents have been properly logged in the Incident Registry. Other responsibilities of the Incident Manager include:

- Monitoring the effectiveness of the Incident Management procedure and coordinating recommendations for improvement with the Compliance and Continual Improvement (CCI) Manager.
- Leading the communications between teams/clients during a major incident.
- Planning and managing support for the Incident Management Procedure.
- Regularly reviewing similar and recurring incidents with the Problem Manager to address identified problems and leading them to closure.
- Facilitating the six (6) phases of IR

The Incident Manager role shall be assigned to the SOC Manager for Information Security related incidents and the NOC Manager for Quality-of-Service related incidents.

The Cyber Security Intelligence (CSI) Manager shall take upon the responsibilities of the Incident Manager in the absence of a SOC Manager, while the SO Head shall take upon the responsibilities of Incident Manager in the absence of a NOC Manager.

## 6.10 Common Procedures

### Incident Reporting

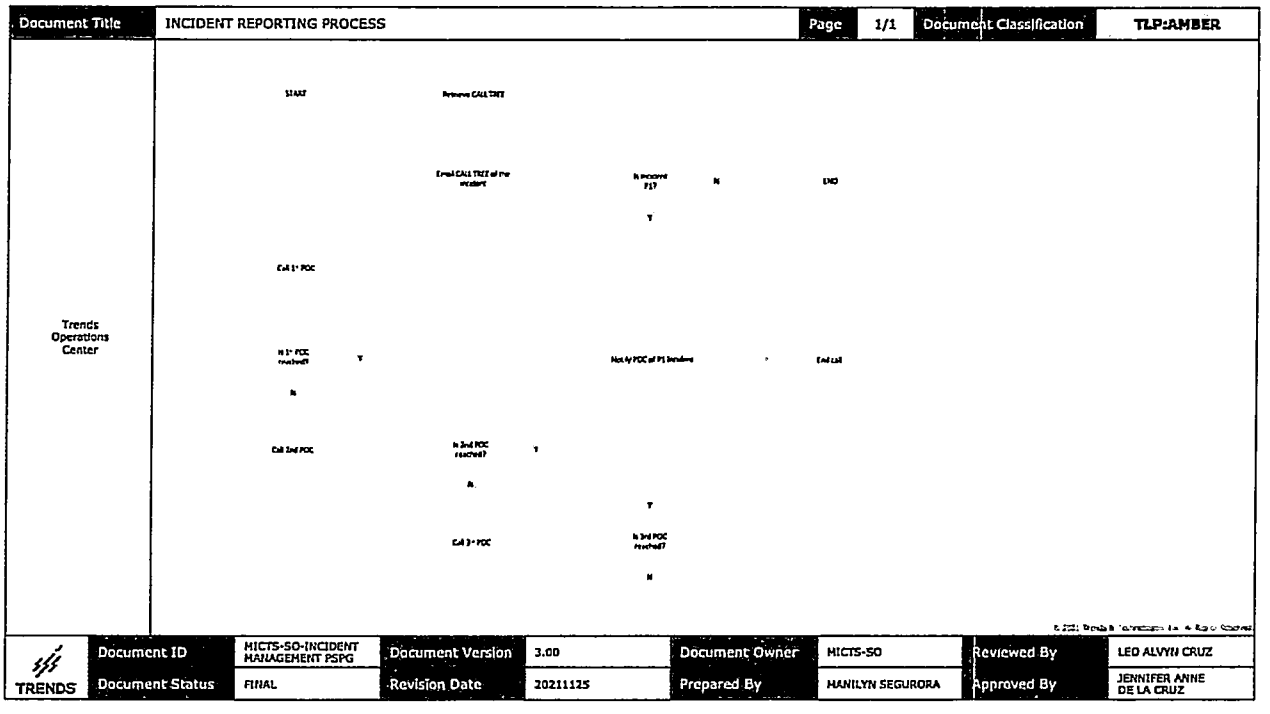



***Figure 2 – Incident Reporting Process***

1. TRENDS Operations Center Incident Responder (L2) retrieves call tree reference.
2. TRENDS Operations Center Incident Responder (L2) sends email notification about incident.
3. If incident priority is P1, TRENDS Operations Center Incident Responder (L2) initiates a call to the 1st-level POC. If 1st-level Client POC does not pick-up/answer the call after 3 call attempts with 3 rings each call, next level Client POC will be called upon. If after the 3rd-level Client POC, TRENDS Operations Center Incident Responder (L2) haven't reached or communicated with the client, the cycle goes back to calling the 1st-level Client POC.
4. Once the Client POC has been reached, inform Client POC of the incident and share pertinent details. Likewise, inform Client POC to check further details over sent email. After Client POC has been informed, TRENDS Operations Center Incident Responder (L2) ends the call. The email/ call should provide the following details:
    a. Impact: Severity of the security event to critical assets
    b. Priority: Based on the impact and severity
    c. Nature of threat
    d. Potential business impact
    e. If available, remediation recommendations

### Chronological Escalation

1. Retrieve priority SLA. Refer to:
   - ANNEX 2 – TRENDS Operations Center Incident Response & Update Time; for client incidents' response timetable, refer to client SLA.
   - ANNEX 3 – TRENDS Operations Center Quality-of-Service Incident Restoration Time; for client incidents' restoration timetable, refer to client SLA.
   - ANNEX 4 – TRENDS Operations Center Information Security Incident Resolution Time; for client incidents' resolution timetable, refer to client SLA.
2. Divide the SLA time of the incident by 4 which is the levels of support.
3. Determine allowed time for each support level.
4. Escalate to next level support when time for the support level is reached.

**Priority Escalation & De-escalation**

Incidents may be reassessed for its priority categorization. Assessment shall be made by the Incident Manager in accordance with the Update SLA. Refer to: ANNEX 2 – TRENDS Operations Center Incident Response & Update Time.

Below are the criteria for Priority Escalation & De-escalation:

- Incident Priority shall be escalated when the SLA has already been breached.
- Incident Priority may be escalated depending on the sensitivity of the incident.
- Incident Priority may be escalated or de-escalated depending on the severity of the incident and/or criticality of the involved asset.
- Incident Priority may be escalated or de-escalated upon the request of the client.

### 6.11 Information Security Incident Management

**Attack Vectors**

Incidents can occur in countless various ways. However, these incidents can be further categorized into the methods of attack vectors. Below are the common attack vectors which a security incident may be further categorized.

- **External/Removable media**: An attack executed from removable media or a peripheral device. *Examples are: malicious code spreading onto a system from an infected USB flash drive.*
- **Attrition**: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks or services. *Examples are: DDoS, brute force attack against an authentication mechanism.*
- **Web**: An attack executed from a website or web-based applications. *Examples are: Cross-site scripting (XSS) attack.*
- **Email**: An attack executed via an email message or attachment. *Examples are: Exploit code designed as an attached document or a link to a malicious website in the body of an email message.*
- **Impersonation**: An attack involving replacement of something benign with something malicious. *Examples are: Spoofing, Man-in-the-middle (MITM) attacks, rogue wireless access points, SQL injection attacks.*
- **Improper Usage**: Any incident resulting from the violation of an organization's acceptable use policies by an authorized user.
- **Loss or Theft of Equipment**: Loss or theft of a computing device or media used by the organization.
- **Other**: An attack the does not fit into any of the other categories.

These attack vectors are the references for the Security Incident playbooks.

## Typical Incident Handling Procedure for Information Security Incident

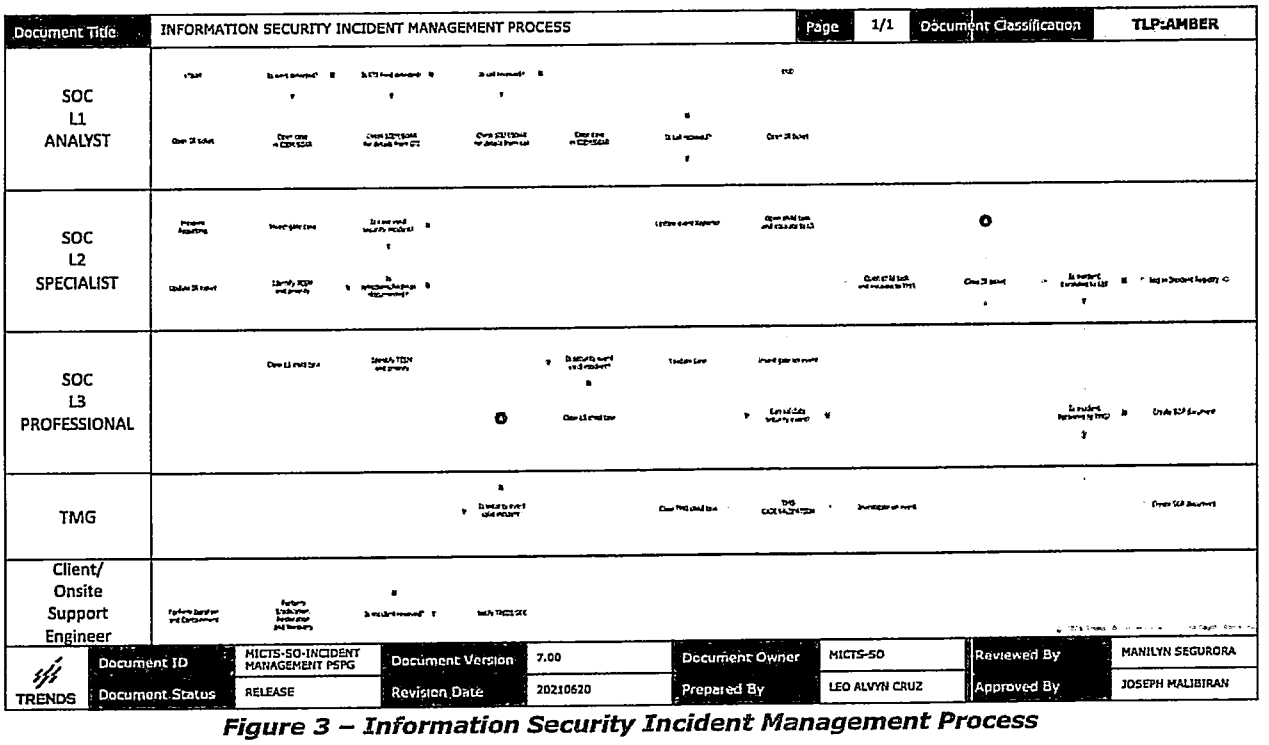



***Figure 3 – Information Security Incident Management Process***

1. TRENDS Operations Center Analyst (L1) detects a security incident alert or information from GTI feeds or a call about a security incident is received.
2. TRENDS Operations Center Analyst (L1) creates an incident case in the SIEM.
3. TRENDS Operations Center Incident Responder (L2) investigates the case and validates if the case is a security incident.
4. If incident is valid, TRENDS Operations Center Incident Responder (L2) identifies the use-case and incident priority based on the incident prioritization matrix. Otherwise, process is ended.
5. Following a valid incident, TRENDS Operations Center Analyst (L1) creates IR ticket per instructions and details from TRENDS Operations Center Incident Responder (L2).
6. TRENDS Operations Center Specialist (L2) performs incident reporting and notifies the corresponding call-tree.
7. TRENDS Operations Center Incident Responder (L2) updates the IR ticket status.
8. ONSITE SUPPORT ENGINEER performs isolation, containment, eradication, and remediation based on the recommendation from TRENDS Operations Center. If the incident observed is in the environment managed by the Client, the Client performs the isolation, containment, eradication, and remediation based on the recommendation from TRENDS Operations Center.
9. Once the incident is resolved, ONSITE SUPPORT ENGINEER or the Client notifies TRENDS Operations Center.
10. TRENDS Operations Center Analyst (L1) updates IR Ticket status to resolved.
11. TRENDS Operations Center Incident Responder (L2) logs Incident Report to Incident Registry.

**Guidelines on Handling of certain specific Information Security Incidents**

Certain Information Security Incidents require specific methods in handling and managing the incident. The guidelines and references for handling Malware Incidents are in Annex 6 - Guidelines on Handling of Specific Information Security Incidents.

**Invocation of Computer Security Incident Response Team (CSIRT)**

Any information security incident having a P1 priority level automatically invokes the CSIRT. The CSI Manager is responsible in mobilizing the CSIRT. The CSI Manager is also responsible for providing technical assistance to the agencies' CSIRTs during emergencies or successful breach responses.

TRENDS CSIRT is comprised of the following members:

- Chief Information Security Officer (CISO)
- MICTS Head
- Service Operations (SO) Head
- Managed Security Services (MSS) Head
- Infrastructure and Security Solutions Support and Engineering (ISSE) Head
- Security Operations Center (SOC) Manager
- Digital Forensics & Incident Response (DFIR) Manager
- Threat Hunting and Threat Intelligence (THTI) Manager
- Service Delivery Manager (SDM)

## 6.12 Quality-of-Service Incident Management

**Typical Incident Handling Procedure for Quality-of-Service Incident**

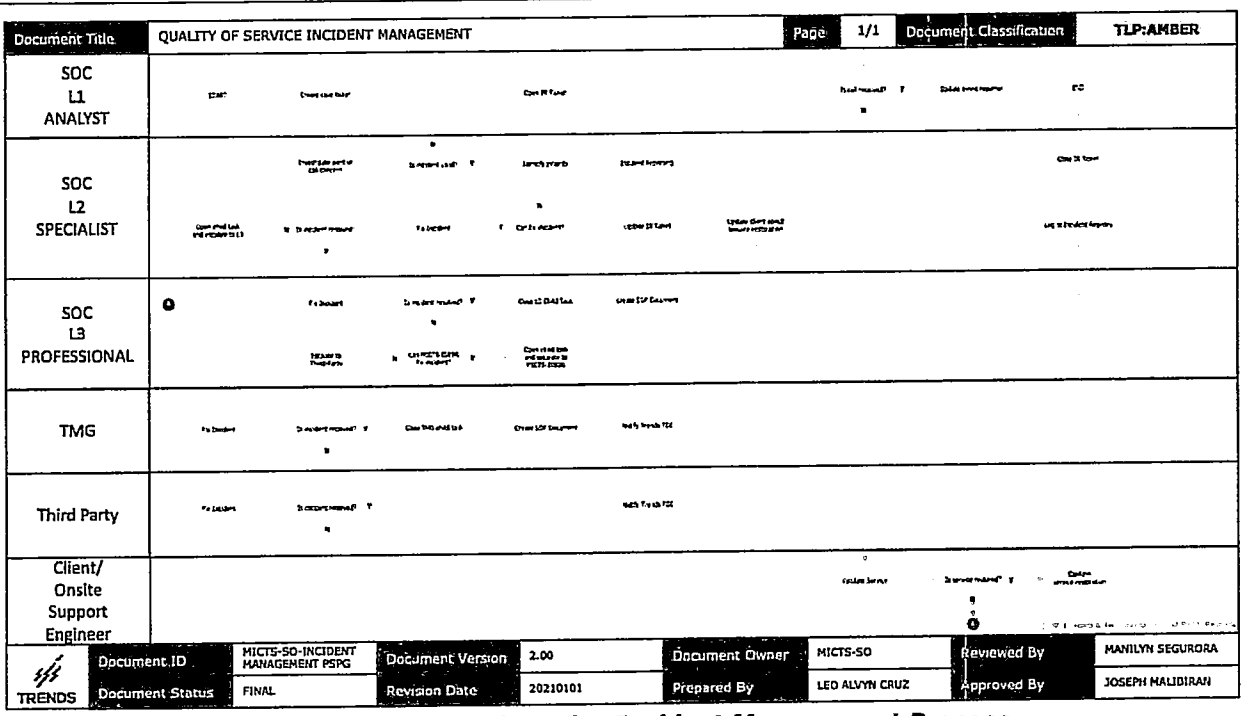



***Figure 4 – Quality of Service Incident Management Process***

1. Trends Operations Center Analyst (L1) detects an incident alert or a call for service disruption is received.
2. Trends Operations Center Analyst (L1) performs incident validation.
3. If incident is valid, Trends Operations Center Analyst (L1) escalates to Trends Operations Center Incident Responder (L2), identifies the incident priority based on the incident prioritization matrix. Otherwise, process is ended.
4. Following a valid incident, Trends Operations Center Analyst (L1) creates IR ticket per details validated.
5. Trends Operations Center Incident Responder (L2) performs incident reporting and notifies the corresponding call-tree.
6. Trends Operations Center Incident Responder (L2) updates the IR ticket status.
7. If incident can be fixed by Trends Operations Center Incident Responder (L2), Trends Operations Center Incident Responder (L2) performs fixes based on SOP.
8. If incident cannot be fixed by Trends Operations Center Incident Responder (L2), Trends Operations Center Incident Responder (L2) escalates to Trends Operations Center Specialist (L3).
9. Trends Operations Center Specialist (L3) attempts to fix the incident.
10. If incident cannot be fixed by Trends Operations Center Specialist (L3), Trends Operations Center Specialist (L3) determines whether to escalate to TMG or to Third Party.
11. Once Technology Management Group (TMG) or Third party receives the escalation, either TMG or Third party performs the fixes to the incident and reports to Trends Operations Center Incident Responder (L2) once incident is resolved.
12. If incident is resolved, Trends Operations Center Incident Responder (L2) notifies client about service resumption.
13. Client validates service status and confirms resumption of service.
14. Trends Operations Center Incident Responder (L2) updates IR Ticket status to resolved.

15. Trends Operations Center Incident Responder (L2) creates a formal Incident Report and sends to client.
16. Trends Operations Center Incident Responder (L2) logs Incident Report to Incident Registry.

**Fix Incident Procedure**

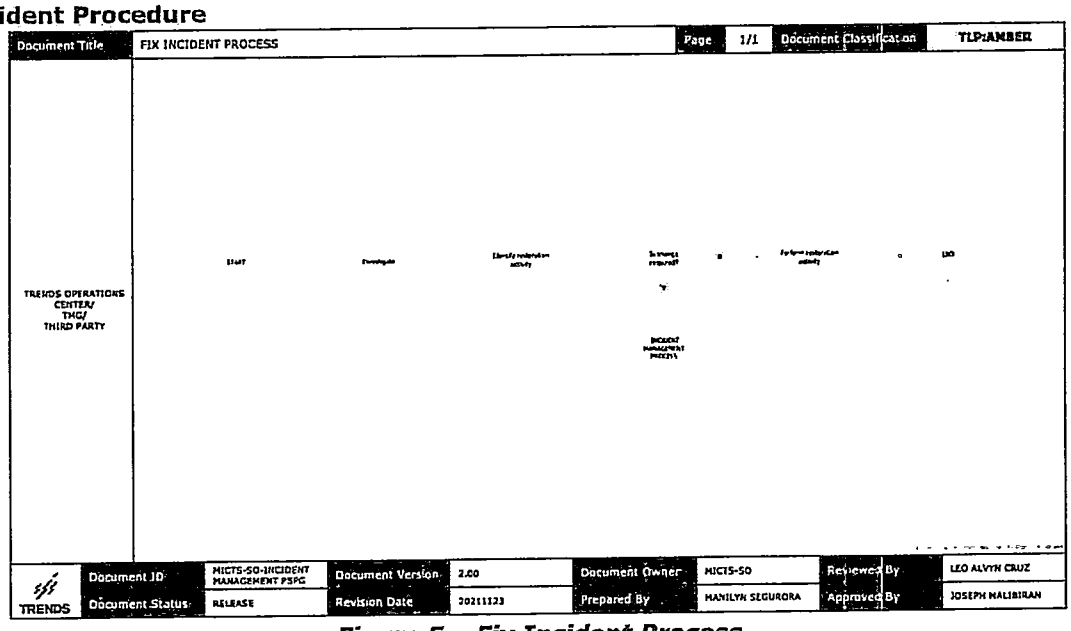



***Figure 5 – Fix Incident Process***

1. Process actor may be Trends Operations Center, or TMG, or THIRD-PARTY.
2. Process actor initiates the investigation and identifies restoration activity.
3. If the restoration activity does not require any change, the process actor performs the activity and ends the process. Otherwise, the process triggers the Service Request (SR) Process.

## 6.13 Call Tree

An incident call tree is a hierarchical notification chain detailing the point-of-contact that needs to be informed depending on the severity of the incident. The incident call tree for MICTS-SO is being maintained by the CCI team while the incident call tree for clients is with the Service Management Team.

## 6.14 Digital Forensics Overarching Process

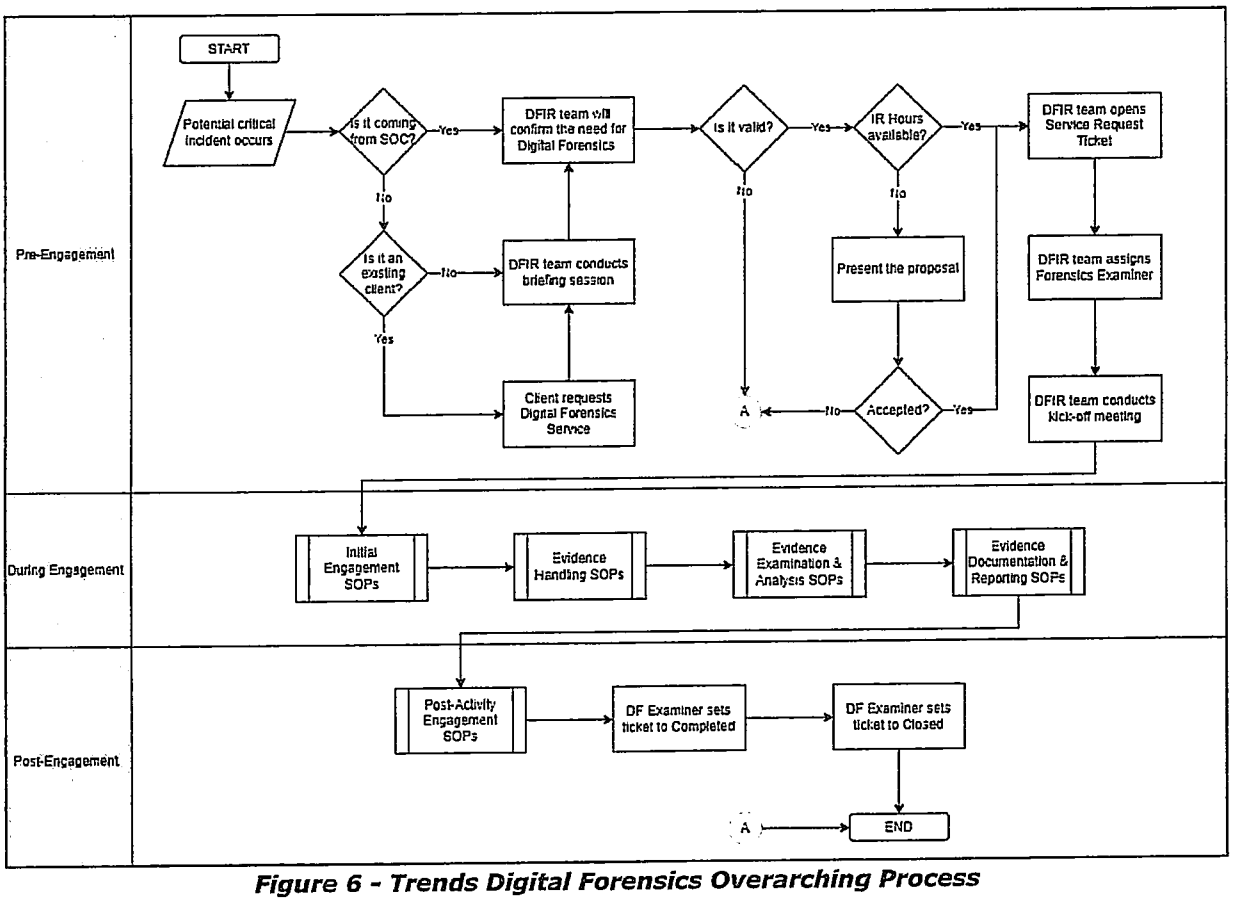



***Figure 6 - Trends Digital Forensics Overarching Process***

### A. Pre-Engagement

1. There is an identified occurrence of a potential critical incident.

2. If the notification is coming from Security Operations Center (SOC), the following steps will be taken:
    a) The Trends Digital Forensics and Incident Response (DFIR) Team shall confirm the necessity for conducting Digital Forensic services based on the escalated Incident Ticket. If upon confirmation the incident is not a valid case, the DFIR team will not proceed to the next steps.
    b) On the other hand, the client can request an assessment during the incident to extend the investigation and potentially confirm the root cause of it. There will be a briefing session to grasp the full context of the incident. However, if upon confirmation it is not a valid case, the DFIR team will not proceed to the next steps.
    c) The Laboratory Director shall review the remaining Incident Response hour of the client.
        i. If the client has remaining incident response hour, the client shall issue a Service Request (SR) ticket. The DFIR Team can create the SR ticket on behalf of the client in case of urgency and/or unavailability of the ticketing platform.

ii. Otherwise, the DFIR Team will start discussion with the Business Unit Group about the cost implications. If the client accepts the proposal, please refer to the previous bullet. Otherwise, the DFIR team will not proceed to the next steps.

3. The DFIR team sets a kick-off meeting with the client to provide a comprehensive overview of the activity and discuss the total incident response hour to spend.

**B. During Engagement**

1. The assigned Forensics Examiner will execute the various Standard Operating Procedures (SOPs) to ensure the successful completion of the activity.

2. Firstly, the Forensics Examiner shall do the Initial Engagement SOPs. The Initial Engagement phase serves as the starting point for conducting a thorough and effective investigation into digital evidence. This phase sets the foundation for the entire examination process, helping ensure that the investigation is well-planned, aligned with client's expectations, and conducted in a systematic and legally sound manner.

3. Next, Evidence Handling SOPs will be executed. Evidence handling is a critical component of digital forensic examination. It encompasses a set of procedures and protocols designed to ensure the integrity, security, and admissibility of digital evidence throughout the investigation process. There are two stages in this phase:

   - Evidence Intake SOPs – It outlines the systematic process for receiving and documenting physical evidence collected during investigations.

   - Evidence Acquisition SOPs – It ensures that evidence is properly preserved, documented, and protected throughout the investigation process.

4. Next, Evidence Examinations and Analysis SOP will be executed. This SOP outlines the systematic process for conducting thorough examinations, testing, and analysis pf physical evidence collected during investigations. This procedure ensures that evidence is subjected to scientific analysis using standardized methods, maintaining its integrity and reliability.

5. Finally, Evidence Documentation and Reporting SOP will be executed. This SOP outlines the systematic process for accurately documenting and reporting on the collection, analysis, and handling of evidence during investigations. This procedure ensures that all pertinent information is recorded, maintained, and presented in a clear and organized manner, facilitating transparency, accountability, and legal admissibility. The report shall include the root cause analysis which identified the intrusion vector and mitigating procedures conducted to address network and system vulnerabilities.

**C. Post-Engagement**

1. Once everything is set, the DFIR team shall execute the SOPs related to the Post-Engagement Activity:

   i. Post-Activity Engagement SOP outlines the systematic process for interacting with stakeholders and addressing key considerations after completing a digital forensic investigation. This procedure aims to gather insights, provide updates, and ensure effective collaboration, while also documenting findings for legal and reporting purposes.

ii. Sanitization of Digital Media SOP outlines a systematic process to securely erase or destroy digital data from various types of media to prevent unauthorized access, maintain data privacy, and comply with data protection regulations. This procedure ensures that sensitive information is effectively removed, making the media suitable for reuse, disposal, or repurposing.
iii. Return of Evidence SOP outlines a systematic process for returning digital evidence to clients after the completion of forensic analysis. This procedure ensures that evidence is returned securely, maintaining the chain of custody, and preserving its integrity for potential legal proceedings.

2. Once the client accepts the final document, the Digital Forensics Examiner will set the SR ticket to Completed then eventually change it to Closed.

# 7 Key Performance Indicators

To ensure the effectiveness of the aforementioned policies, standards, procedures, and guidelines, KPIs must be set and regularly monitored for compliance. KPI setting must be conducted every first month of the year. Review must be conducted at the last month of every quarter. This section enumerates the baseline KPIs that need to be measured. Other material KPIs must be set and recommended by the ISGAB, approved by the MICTS head, documented, and cascaded to all affected MICTS personnel.

Below are the baseline KPIs that need to be measured:

- Turn-around Time (time to send initial advisory) is within 15 minutes from the time the SIEM/SOAR generated the alert.
- Overall Turn-around Time (time to send complete details of incident) is within 60mins from the time an event was logged in a data-source.

## ANNEX

## Annex 1 – TRENDS Operations Center Impact Criteria, Urgency Criteria and Priority Matrix

### Impact Criteria

The following table lists the criteria for determining the impact of an incident.

| Impact | Description |
|---|---|
| High | • A large number of staff are affected and/or not able to do their job.<br>• A large number of customers are affected and/or acutely disadvantaged in some way.<br>• Involving IT Assets with Category 1.<br>• The damage to the reputation of the business is likely to be high. |
| Medium | • A moderate number of staff are affected and/or not able to do their job properly.<br>• A moderate number of customers are affected and/or inconvenienced in some way.<br>• Involving IT Assets with Category 2.<br>• The damage to the reputation of the business is likely to be moderate. |
| Low | • A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort.<br>• A minimal number of customers are affected and/or inconvenienced but not in a significant way.<br>• Involving IT Assets with Category 3.<br>• The damage to the reputation of the business is likely to be minimal. |

### Urgency Criteria

The following table lists the criteria for determining the urgency of an incident:

| Urgency | Description |
|---|---|
| High | • The damage caused by the Incident increases rapidly.<br>• Work that cannot be completed by staff is highly time sensitive<br>• A minor Incident can be prevented from becoming a major Incident by acting immediately.<br>• Several users with VIP status are affected. |
| Medium | • The damage caused by the Incident increases considerably over time.<br>• A single user with VIP status is affected |
| Low | • The damage caused by the Incident only marginally increases over time.<br>• Work that cannot be completed by staff is not time sensitive. |

### Priority Criteria

The following table lists the criteria for determining the priority of an incident by correlating impact and urgency.

| | | IMPACT | | |
|---|---|---|---|---|
| | | HIGH | MEDIUM | LOW |
| URGENCY | HIGH | 1 | 2 | 3 |
| | MEDIUM | 2 | 3 | 4 |
| | LOW | 3 | 4 | 5 |

**Annex 2 – TRENDS Operations Center Incident Response & Update Time**

| Priority Level | Description | Trends Acknowledgement Time SLA | Reference |
|---|---|---|---|
| 1 | Critical | Within 15 minutes | Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket. |
| 2 | High | Within 15 minutes | |
| 3 | Medium | Within 15 minutes | |
| 4 | Low | Within 15 minutes | |
| 5 | Baseline | Within 15 minutes | |

| Priority Level | Description | Service Level Target | Reference |
|---|---|---|---|
| 1 | Critical | 98% | Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket. |
| 2 | High | | |
| 3 | Medium | | |
| 4 | Low | | |
| 5 | Baseline | Not Computed | |

| Priority Level | Description | Trends Response Time SLA | Reference |
|---|---|---|---|
| 1 | Critical | Within 60 minutes | From the creation of service ticket up to triage. Triage is when the SOC L2 Incident Responder communicates with the client to further investigate and provide recommendation on how to contain, remediate, and recover from the security incident. |
| 2 | High | Within 90 minutes | |
| 3 | Medium | Within 120 minutes | |
| 4 | Low | Within 160 minutes | |
| 5 | Baseline | Within 160 minutes | |

| Priority Level | Description | Trends Update Time SLA | Reference |
|---|---|---|---|
| 1 | Critical | Every 10 minutes | From the time first response was executed. |
| 2 | High | Every 15 minutes | |
| 3 | Medium | Every 30 minutes | |
| 4 | Low | Every 30 minutes | |
| 5 | Baseline | Every 30 minutes | |

Measurement of Monthly SLA is computed as follows:

| Priority Level | Description | Trends Monthly SLA Computation | Reference |
|---|---|---|---|
| 1 | Critical | > 90% | Sum of the number of P1 and P2 incidents meeting the required Response Time for all days in the month |
| 2 | High | | |
| 3 | Medium | > 80% | Sum of the number of P1 and P2 incidents meeting the required Response Time for all days in the month |
| 4 | Low | | |
| 5 | Baseline | Not Computed | |

**Annex 3 – TRENDS Operations Center Quality-of-Service Restoration Time**

| Priority Level | Description | Trends Restoration Time SLA | Reference |
|---|---|---|---|
| 1 | Critical | Within 2 hours | From the time incident is detected by NMS or from the time CLIENT POC reports the incident (whichever comes first) |
| 2 | High | Within 4 hours | |
| 3 | Medium | Within 24 hours | |
| 4 | Low | Within 48 hours | |
| 5 | Baseline | Within 72 hours | |

**Annex 4 – TRENDS Operations Center Information Security Resolution Time**

| Priority Level | Description | Trends Resolution Time SLA | Reference |
|---|---|---|---|
| 1 | Critical | Within 2 hours | From the time incident is detected by SIEM or from the time CLIENT POC reports the incident (whichever comes first) |
| 2 | High | Within 4 hours | |
| 3 | Medium | Within 24 hours | |
| 4 | Low | Within 48 hours | |
| 5 | Baseline | Within 72 hours | |

**Annex 5 – TRENDS Operations Center Root Cause Analysis Response Time**

| Priority Level | Description | Trends RCA Release Time SLA | Reference |
|---|---|---|---|
| 1 | Critical | Within 3 business days | From the time incident is detected by SIEM or from the time CLIENT POC reports the incident (whichever comes first) |
| 2 | High | Within 3 business days | |
| 3 | Medium | Within 5 business days | |
| 4 | Low | Within 5 business days | |
| 5 | Baseline | Within 5 business days | |

## Annex 6 – Guidelines in Handling of Specific Security Incidents

### Malware Incident Response Guidelines

**Definition**
Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems, including malicious code, spyware, and system file hacks.

**Purpose**
This Incident Response Methodology is a guide for investigating a precise security issue. It is intended for:

- Security Operations Center (SOC) Management
- SOC Analysts
- Incident Responders
- Threat Hunters

**Scope**
This document is aligned to NIST Special Publication 800-83 Rev. 1 on "Guide to Malware Incident Prevention and Handling for Desktops and Laptops" and covers the 6 incident response process in handling malware infections:

- Preparation – getting ready to handle the incident
- Identification – detecting the incident
- Containment – limiting the impact of the incident
- Remediation – removing the threat
- Recovery – removing the threat
- Aftermath – drawing up and improving the process

**Preparation**
Build and maintain malware-related skills on Analysts.

- Has solid understanding of how each category of malware infects and spreads.
- Should be familiar with the organization's implementations and configurations of malware detection tools.
- For in-depth malware analysis, one should have strong skillset on malware reversing and familiar with numerous tools such as debuggers for example.
- Keeps abreast of ever-evolving landscape of malware threats and technology.

Establish an organized designation of tasks and responsibilities

- Should have complete contacts of POC for escalation and communication.
- Ensure proper communication and coordination with other teams.

Acquire tools and resources for malware detection and investigation.

- Ensure functional and updated Analysis tools (Antivirus, logs analyzers).

Has the capability to detect advance threat tactics and techniques.

**Identification**
*Detect the infection*

1. Monitor and inspect the following critical domains to observe any suspicious activities:
    - Endpoint security logs e.g. malware alerts and suspicious connection attempts.
    - User-behavior analytics e.g. insider threat and fraud.
    - Network threat analytics using WAF, IDS, and SIEM logs.
    - Application threat analytics e.g. vulnerability intelligence from vendors and data flow analysis of high-risk applications.
2. Using different security tools and platforms, SOC analyst shall identify indicators of compromise. Analyze and validate suspected malware activity by examining the detection sources. It helps to

understand the malicious activity's characteristics and assign appropriate priority and shall be handled as reflected in the Incident Management Process.

*Identify the infection*

- Analyze the symptoms to identify the malware, its propagation, vectors, and countermeasures.
- Leads can be found from:
  - Antivirus vendor's Virus Report (upon submission of the malware sample)
  - External support contacts (Antivirus companies, etc.)
  - Open-Source Tools (Threat Wikis)

*Assess the perimeter of the infection*

- Define the boundaries of the infection (i.e.: global infection, bounded to a subsidiary, etc.). If possible, identify the business impact of the infection.
- To scope and identify other infected endpoints from the network, use the malware's Indicators of Compromise (IOC) and create detection and blocking with logging for all available and capable security platforms and monitor the alarms and logs.

**Containment**

The primary goal of the containment process is to stop the spread of the malware and prevent it from causing further damage to host. It may vary depending on the assessment of the incident handlers. The following process and methods are currently implemented in TOC:

*Containment Process*

- The following actions should be performed and monitored by the crisis management cell/incident handlers:
  1. Isolate the infected area and disconnect it from any network (Incident handlers must perform risk assessment before disconnecting it depending on the impact).
  2. Block all IOCs and the infection vector. If it came from an email, retrieve the email from all user's mailbox from the email server and perform the purging of the copies.
  3. Do a password reset of all accounts that had access to the infected endpoint(s).
  4. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumvention techniques.
  5. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures have to be applied (patch, traffic blocking, disable devices, etc.). For example, the following techniques can be used:
     - Patch deployment tools (WSUS)
     - Windows GPO
     - Firewall rules
  6. Repeat steps 2 to 5 on each sub-area of the infected area until the propagation technique of the malware stops. If possible, monitor the infection using analysis tools (antivirus console, server logs, support calls).
- The spreading of the malware must be strictly monitored.

*Containment through user participation*

Each method will perform key role in the containment of the malware. In addition to the process, TOC exercises extra measure when it comes to containment and must keep in mind the continuous improvement.

User participation is still valuable since it guides the organization on how to respond to malware incident. To enable this, the following things must be maintained and observed:

1. Established communication between POC, incident handlers, and end-users – It ensures that every suspicious observation coming from SOC are investigated and disseminated with due diligence. Necessary actions are executed properly and on-time.

2. Awareness about Malware and Containment Process on Organization – Emails the organization about basic malware handling, the contact of incident handlers, and safety measures to prevent the infection at the first place.

*Containment through automated detection*

TOC, specifically, is a managed environment that applies automated detection using AV and end-point protection however, there are instances that advanced threats can evade these which will be the highlight of this method:

1. Ensures that unknown/undetected malwares are submitted immediately to the AV vendor for signatures. Further details about deployment are discussed in Remediation Section.
2. Maintains other tools for automated detection such as content filters (email servers and clients that contains anti-spam software), network-based IPS software, and end-point user protection software up to date.

Containment through disabling services

Disabling Services must be considered properly since it will not only affect the organization's function but as well as the other dependent application. Therefore, it's very crucial to maintain lists of the services the organization uses and the TCP and UDP ports used by each service. In case of infection, the organization can properly assess and shut down the affected service to achieve its goal to disable as little functionality of the malware as possible while containing the incident effectively.

Containment through disabling connectivity

This is an addition to the step 1 of the Containment process. If infected hosts within the organization attempt to spread its malware, the organization might block network traffic from the hosts' IP addresses to control the situation while the infected hosts are physically located and disinfected or disconnect the infected hosts from the network, which could be accomplished by reconfiguring network devices to deny network access or physically disconnecting network cables from infected hosts.

**Remediation**

*Identify*

Identify tools and remediation methods. The following resources should be considered:

- Vendor fixes (Microsoft, Oracle, etc.)
- Antivirus vendor's Virus Report (upon submission of the malware sample)
- Antivirus signature database
- External support contacts
- Security websites

*Test*

Apply the disinfection process in a testing machine first before deploying to all endpoints so that the organization can make sure that it properly works without damaging any services.

*Deploy*

Deploy the disinfection tools. Several options can be used:

- Windows WSUS (Windows Server Update Services)
- GPO (Group Policy)
- Antivirus signature deployment
- Manual disinfection and Artifact removal
- Re-image or reformat the endpoint
- Remediation progress should be monitored by the incident handlers.

*Rebuilding*

There are situations where simple disinfection doesn't work. Some types of malware are extremely difficult to remove from hosts; even if they can be removed, each host's OS may be damaged, possibly to the point where the hosts cannot boot. Then, rebuilding all infected hosts is the only option. It includes the reinstallation and securing of the OS and applications (or restoration of known

good OS and application backups, including the use of built-in OS rollback capabilities), and the restoration of data from known good backups.

The following characteristics must be seen to consider rebuilding the host:

- One or more attackers gained administrator-level access to the host.
- Unauthorized administrator-level access to the host was available to anyone through a backdoor, an unprotected share created by a worm, or other means.
- System files were replaced by a Trojan horse, backdoor, rootkit, attacker tools, or other means.
- The host is unstable or does not function properly after the malware has been eradicated by antivirus software or other programs or techniques. This indicates that either the malware has not been eradicated completely or that it has caused damage to important system or application files or settings.
- There is doubt about the nature of and extent of the infection or any unauthorized access gained because of the infection.

If none of the characteristics are observed, it's better to eradicate the malware from the host rather than rebuilding it.

**Recovery**

Verify all previous steps have been done correctly and get a management approval before doing the next steps:

- Reopen the network traffic that was used as a propagation method by the worm.
- Reconnect sub-areas together.
- Reconnect the area to your local network.
- Reconnect the area to the internet.

Identify who would perform the recovery tasks, estimate how many hours of labor would be needed and how much calendar time would elapse, and determine how the recovery efforts should be prioritized. All of these steps shall be made in a step-by-step manner and a technical monitoring shall be enforced by the crisis team.

**Aftermath**

*Report*

An Incident Report should be written and made available to all the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection.
- Actions and timelines of every important event.
- What went right?
- What went wrong?

*Lessons Learned*

Actions to improve the malware infection management processes should be defined to capitalize on this experience. The following can be the possible outcomes of lessons learned activities for malware incident are as follows:

- Security Policy Changes – Security policies might be modified to prevent similar incidents.
- Awareness Program Changes – Security awareness training for users might be changed to reduce the number of infections or to improve users' actions in reporting incidents and assisting with handling incidents on their own hosts.
- Software Reconfiguration – OS or application settings might need to be changed to support security policy changes or to achieve compliance with existing policy.
- Malware Detection Software Deployment – If hosts were infected through a transmission mechanism that was unprotected by antivirus software or other malware detection tools, an incident might provide sufficient justification to purchase and deploy additional software.

- Malware Detection Software Reconfiguration. Detection software might need to be reconfigured in various ways, such as the following:
  - Increasing the frequency of software and signature updates
  - Improving the accuracy of detection (e.g., fewer false positives, fewer false negatives)
  - Increasing the scope of monitoring (e.g., monitoring additional transmission mechanisms, monitoring additional files or file systems)
  - Changing the action automatically performed in response to detected malware.
- Improving the efficiency of update distribution.

## Annex 7 – Sample measurement of Acknowledgement SLA

| Type | Category | Subject | Created By | Created On |
|---|---|---|---|---|
| Notes | Status Update | Incident changed from Reported to Client to Pending with Customer | rbayuban | 17/02/2022 17:28 |
| Email | Outgoing Email | Incident 66272 - Security / Inbound Traffic from GTI Known Malicious Source - Not Blocked ... | rbayuban | 17/02/2022 17:23 |
| Notes | Log | Incident was created | rbayuban | 17/02/2022 17:23 |

**Annex 8 – Coverage of IR hours**

There shall be an allocation of 200 hours of Incident Response per agency. Unconsumed hours allocated for Incident Response can be converted to other services such as training or workshops.

**Annex 9 – Scope of Incident Response**

Trends shall assist the Government Insurance Cluster in the following:

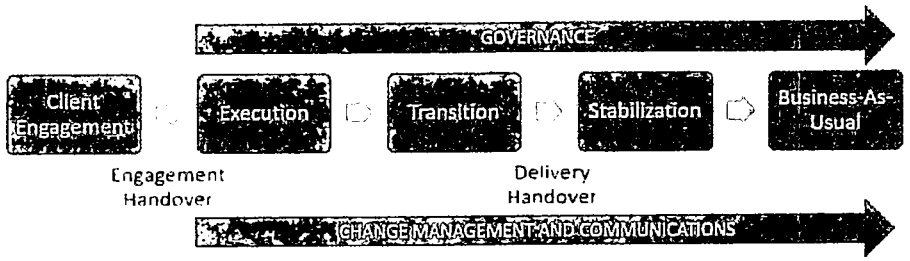
- Incident handling preparation and execution
- Crisis management
- Breach communication
- Forensic analysis including preservation of evidence for chain custody requirements
- Remediation

TRENDS®
*Technology To Transcend*

# PROJECT MANAGEMENT PROGRAM PLAN FOR GOVERNMENT INSURANCE CLUSTER

To ensure the compliance and delivery of the requirements by the Government Insurance Cluster, **TRENDS** will provide a Project Management Program below:

Trends will use a two-pronged approach for project management. The project phases are planned to use the Waterfall Project Management methodology while the actual tasks execution utilizes Agile Methodology.




***1. Client Engagement.***

During the Post Qualification Evaluation, Trends will demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.

Trends will assign the needed Project Manager and technical resources and will conduct kickoff activity to ensure that every team member understands the engagement approach. All facets of the project including manner of implementation, scope, requirements, and acceptance criteria will be discussed during the kickoff activity.

***2. Execution.***

Trends will implement the proposed solution in accordance with the scope of work. All throughout, monitoring of implementation activities will be done by Trend's Project Manager. Weekly project meetings will be conducted to ensure that all issues that may arise will be addressed. Project status updates and reports will be provided to the client in a timely manner. The monthly project monitoring report will be discussed by the Project Manager until the completion of the Phase I

**Trends & Technologies, Inc.**
6th Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines

Phone: +63 2 8811 8181 Fax: +63 2 8814 0130
www.trends.com.ph

and Phase II of the project, as defined in the Delivery Time/ Completion Schedule. The Project Manager shall be required to be onsite in any agency, by schedule, if necessary.

***3. Transition.***

Client onboarding will be done by Trends Service Transition Team to establish the service delivery processes and to ensure completeness of SOC visibility and familiarization with clients' processes and network behaviors.

Guided by the CIS Controls Framework, Trends will conduct Information Security Maturity Assessment which is a comprehensive gap analysis and risk assessment of an organization's readiness to detect, prevent, contain, and respond to threats to information systems. This takes on a holistic look on the organization's people, process, and technology to provide insights and understand vulnerabilities, identify, and prioritize remediation activities and demonstrate compliance.

Under CSC Control 17. Incident Response Management for Information Security Maturity Assessment, Trends will review agencies Incident Response Plan (IRP) which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines such as, but not limited to:

- Escalation process
- Incident containment process
- Incident eradication process
- Incident recovery process
- Incident identification process
- Process flow

Once the solution has been implemented, Trends will conduct process discovery and workshop, develop use cases, create playbooks and runbooks, and conduct tabletop exercises with the client. Trends will map security playbook and runbooks for applicable security use cases to guide client on their incident response. The playbooks and runbooks shall be signed off by the client and a signed Certificate of Completion and Acceptance (COCA) shall be issued to Trends by the client.

***4. Stabilization.***

Trends will validate that the systems are able to detect and respond to potential threats. Trends will perform fine tuning and comprehensive testing to verify the effectiveness of the security measures put in place. During the stabilization period, the SLA will not be in effect. The SLA will become mandatory during the Business-As-Usual (BAU) period.

Once the Stabilization period ends, there should be a signed Certificate of Completion of Stabilization Period issued to Trends by the client.

***5. Business-As-Usual.***

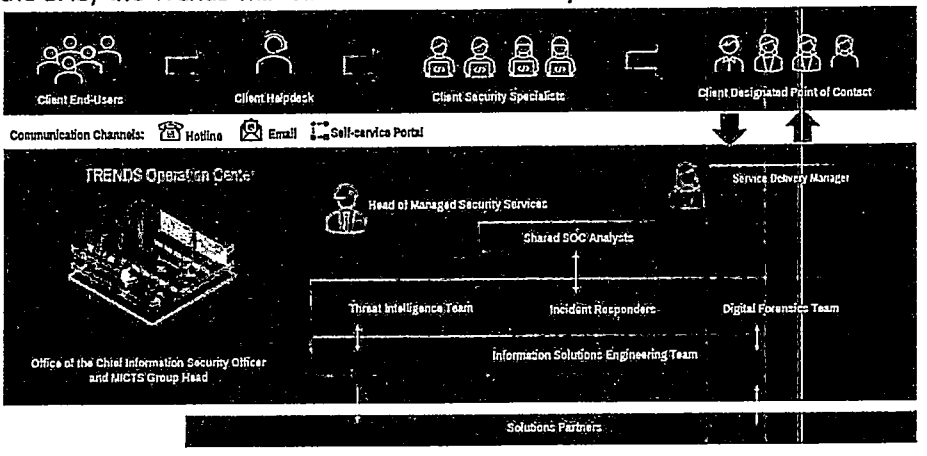
Once tools and technologies are installed and relevant stakeholders signed off the Certificate of Completion of Stabilization Period, Trends Operation Center will provide proactive monitoring, detection, and response to security incidents and cyber threats of Government Insurance Cluster.

Trends will provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a period of time.

Moreover, Trends, through its cloud SIEM platform, will ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidence of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required. The logs beyond the retention period shall be archived and given monthly to the agencies in an agreed format. Agencies will provide a storage repository for the archived logs.

*Service Delivery Architecture*

During the BAU, the Trends will follow the Service Delivery Architecture below:




Trends Security Operation Center (SOC) team will perform 24x7x365 monitoring services performed remotely at Trends Operations Center (TOC) located in Trends-MICTS Head Office Makati City, Philippines.

Trends will assign a Service Delivery Manager (SDM) to facilitate the delivery of the managed services and serve as the initial point of contact for any escalation. On the other hand, the agencies will also assign their respective SDM as the initial point of contact including tracking and validating of requests.

The agencies can report incidents to their helpdesk support. Only their helpdesk support is allowed to report the incidents to Trends SOC team for verification and authentication purposes.

Should there be any incidents not captured on the monitoring tool, the agency can report the incident through their SDM or helpdesk support, and contact Trends with the following details:

- Hotline: 8811-8181 extn: 8703, 8708, 8710 8715, 8716 and 8727
- Trends-SOC Email: soc@trends.com.ph

- Ivanti ticket: https://mictsv2-ism.trends.com.ph/HEAT/

*Manpower Resources*

Trends will have a dedicated 24x7x365 team assigned to the Government Insurance Cluster, composed of the following with their respective roles and responsibilities:

| Personnel | Roles and Responsibilities |
|---|---|
| SOC Manager or Tier 4 Analyst (1) | In charge of strategy, priorities and the direct management of SOC staff when major security incidents occur.<br><br>Responsible for the management of the MSOC operations for the agency and cluster. |
| Tier 3 Analyst (1) | Responsible for managing critical incidents.<br>Responsible for actively hunting for threats and assessing the vulnerability of the business.<br>1. Manage High Severity Triage<br>2. Incident Response and Forensics Capabilities<br>3. Threat Containment (Using Existing EDR or agreed process)<br>4. Reporting and Post Incident Review<br>5. Use Case Development<br>6. Threat Searches<br>7. New Correlation Rules |
| Tier 2 Analyst (1) | Responsible for conducting further analysis and deciding on a strategy for containment.<br>1. Proactive Searches/ Threat Hunting<br>2. Qualification of Incident Priority/Severity<br>3. Investigation via SIEM/Analytics Platform and other accessible sources<br>4. Rule Tuning<br>5. Ad hoc Vulnerability Advisory & Research<br>6. Threat Containment (Using Existing EDR or agreed process)<br>7. Incident Response/Recommendations |
| Tier 1 Analysts (2) | Responsible for the following tasks:<br>1. Monitoring via existing SIEM/Analytics Platform<br>2. Funneling of alerts (noise elimination)<br>3. Incident Validation<br>4. Case Management<br>5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up<br>6. General Communication<br>7. Weekly Summary Reports |

Furthermore, Trends will also ensure that there will be alternate personnel deployed to the Insurance Cluster should the primary personnel be unavailable for whatever reason.

*Reports and Meetings*

- **Monthly Service Performance Report.**

  The assigned dedicated local SOC Manager that will oversee that SOC and conduct regular monthly service performance review and reporting to client's management. The monthly service performance report which contains the status of cases and the assistance needed from the client, will be submitted and discussed by the SOC Manager. The monthly service performance report will include the following:

  - SLA Performance
  - Correlated Events Overview
  - Correlated Events Graph Distribution Overtime
  - Correlated Events and Rules Triggered Summary
  - Summary of Incident Ticker per Use Cases Incident Management

- **Regular Email Advisory and Intelligence Summary Reports**

  Trends will also provide regular email advisory and intelligence summary reports on the latest local and international news, latest cyber threats, and updates in Cyber security space, including detected information on the intention to target agencies or other government industries, major activist campaigns, and indications of activism against the agencies, financial and health sector, and the government.

  However, a **special report or notice to the agencies** immediately, should there be any information or detection of targeted attacks against the agencies, the government or the sectors of the concerned agencies.

- **Monthly Service Performance Review Meeting.**

  Led by the SOC Manager, Trends shall conduct monthly meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement.

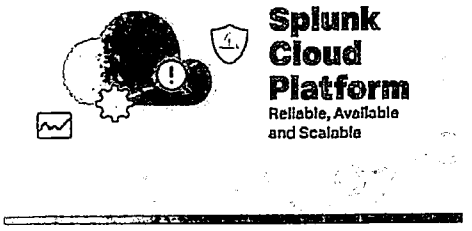
  Furthermore, Trends will also facilitate SOC security briefings to IT and CxOs and key decision-makers to discuss the intelligence summary reports and to share emerging technology trends and the risks associated with it, new regulations, complexity and sophistication of threats, requirement for companies to cyber-resilient among others.

PLATFORM

# Face the Unexpected with the Stability and Resiliency of Splunk Cloud Platform

By Splunk January 27, 2022

Stability and resiliency of cloud services are top of mind for organizations today. Whether rising to the challenge of a surge in pandemic-driven demand, or fire fighting an unexpected outage, you still have to support your own customers. With the Splunk Cloud Platform service, you have a dependable partner focused on stability and resiliency that can help to quickly investigate, troubleshoot and resolve impacts caused by massive industry-wide outages, internal security vulnerabilities, or user error.




The ongoing pandemic is accelerating an already fast-paced move to the cloud, and growing complexities in the security landscape continue to push stability, resilience and recovery to top of mind. At Splunk, we're laser-focused on helping customers mitigate the risk that future incidents hold. It's in our DNA to prioritize the stability and reliability of the service in order to help customers investigate and solve problems fast.

## Splunk Cloud Platform Reliable, Available and Scalable

Splunk Cloud Platform has an "always on," high availability commitment. From infrastructure management to data compliance, Splunk Cloud Platform is built to scale to your data analytics needs, ranging from GBs to PBs and beyond. Designed to facilitate sudden bursts in data volume, Splunk Cloud Platform allows you to incrementally upgrade capacity while retaining security by design. We provide dedicated cloud environments available in AWS and GCP for each customer as well as encryption in-transit and optional encryption at-rest. We are continuously evaluating and adding new international standards.

## How?

Splunk Cloud Platform offers impressive resilience, high availability and disaster recovery. Splunk Cloud Platform is built to be ready when things go wrong – and help fix them as fast as possible. The product team at Splunk has built-in innovations to provide business continuity for our customers.

## Stability and Resiliency for Our Customers

Customers expect reliable, highly available service – what Splunk provides. Splunk Cloud Platform is designed for:

**1. Reliable data-in-transit by using multiple queuing strategies including:**

- Separation of ingest and index (persistent queueing) in the Splunk Cloud Platform boundary, as part of the reimagined Splunk architecture in Victoria Experience
- Forwarder queueing to prevent data loss by persistently queuing data at its source and retrying if the indexer is down or there are network issues.

**2. Reliable data-at-rest and track availability using several key strategies:**

- Replication across availability zones (AZs) helps to prevent data loss by reducing the possibility of a single point of failure during ingest
- Load balancer indexer randomization helps to prevent high impact data loss scenarios in case one of many indexers goes down. The load balancer also helps to decrease indexer overload, facilitates resilient randomization, and improves ingest scalability, as part of the reimagined Splunk architecture in Victoria Experience
- Triple data replication for redundancy in the indexer layer.

**3. High search availability through:**

- Auto-duplication of indexers and replacement in case of failure reducing the opportunity for a single point of failure
- Load-balanced access to search tier via Search Head Cluster
- Nightly configuration backups.

**4. Prioritized availability for mission and business critical needs through:**

- Scalable, flexible indexing providing high resiliency to spikes in ingest and search patterns, helping to ensure that high priority, business critical searches are not skipped and do not fail, as part of the reimagined Splunk architecture in Victoria Experience
- Replication factors in indexing designed to produce high data availability and prevent skipped searches
- Search head clustering at the platform layer to prioritize search availability in case a search head goes down.

## Use Splunk to be Proactive About Downtime

**Detect problems before they happen, in real time.**
With Splunk Cloud Platform, stream, analyze, monitor and search any kind of data in real time to detect and prevent issues before they happen. Plus, respond anytime and anywhere with Splunk's mobile apps and augmented reality capabilities.

**Get to the root of the issue – FAST.**
With unified access to all your data sources in the Splunk Cloud Platform, you can investigate the root cause of issues across all your data and uncover previously inaccessible business insights.

**Problem solve in a jiffy.**
Splunk Cloud Platform allows you to maximize your team's efficiency by getting the most value from limited resources. Go live in as few as two days and minimize delays in change management processes for upgrades. When you're ready, expand your Splunk deployment quickly — multiple TBs of incremental capacity are typically available within two days. Let Splunk take care of the infrastructure management and administration.

## At Splunk – We Use Splunk

We trust the operational excellence of Splunk and use it to detect problems before they happen, in real time. We currently use Splunk Cloud Platform, IT Service Intelligence Cloud, Splunk On-Call and an in-house integration with our in-company communication channels to make sure the right teams are ready to tackle incident response and management. We learn fast through iteration, reviewing data to ensure things are running smoothly

> "Here at the Splunk NOC, we currently use Splunk on Splunk to track, maintain, and troubleshoot Splunk SaaS logins, scheduled and ad hoc search success, data ingestion and index success, and API function and availability - all to deliver the best possible experience to our Splunk customers."
> — **Brenden Reeves, Splunk NOC**

**Here are some ways we currently use Splunk Cloud Platform:**

- To track complete, valid Splunk SaaS logins. We use Splunk to monitor Splunk Cloud Platform logins and authentication success rates and investigate when things go wrong. For example, we have alerts for any unusual geography or multiple failed attempts.
- To monitor scheduled or ad hoc searches. We use Splunk to monitor search success rates and do deep-dive investigations when failures are beyond a set threshold. We actively and proactively monitor if a variety of Service Level Indicators (SLI) drop below a threshold.

- To monitor data ingestion and indexing. We monitor Indexers to track whether they're in the desired customer state, typically alerting customers only in outlier scenarios using machine learning to proactively identify unusual spikes and to keep from inundating customers with unnecessary alerts. If a customer requests support, we're ready to dive into the performance and resolve the problem quickly.
- To track availability and functioning of APIs. We monitor API services to help make sure they remain available to customers and are functioning properly. We monitor availability of the index tier to ingest (ex: HTTP Event Collector's sourced ingest and internal Splunk-to-Splunk 9997 ports), and the availability of the search tier (ex: availability of the login page, Hybrid Search API's ability to search cloud indexers, or the availability of search service itself via compute-negligible test searches).

The Splunk NOC monitors for suspicious or unexpected activity in any of these four areas, allowing Splunk to proactively reach out to customers when a potential issue is raised. The Splunk Dashboard Studio provides the visualizations that bring this all together for our NOC team allowing multiple team members to identify and quickly communicate potential issues.

> "The stack overview dashboards we have in our Splunk NOC allow us to get a fast overview of the entire cluster of servers and services per customer, so that we can quickly identify and work to resolve any customer problems"
> — **Brenden Reeves, Splunk NOC**

## So What?

Outages happen, security incidents happen. Splunk capabilities can help you thrive amidst uncertainty. The Splunk Cloud Platform is critical to helping our customers drive stability across their ecosystems from a security, infrastructure and application perspective. Here at Splunk, we depend on Splunk Cloud Platform's availability and resiliency as the bedrock of our own NOC. Splunk is dedicated to helping customers deliver business resilience and mitigate future risks. Our Splunk DNA drives us to innovate to make our service accessible as a stable, reliable service that enables customers to investigate and solve problems fast.

---

Thanks!
Garth Fort

POSTED BY
Splunk

TAGS
Cloud Splunk Cloud

## Related Posts

PLATFORM

**New Year, New Dashboard Studio Features: What's New in 8.2.2201**

By Lizzy Li March 17, 2022

PLATFORM

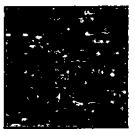
## AWS Operational, Security and Cost Management Insights Starting at $3/day

By Splunk November 30, 2016

PLATFORM

## The Insider's Guide to Splunk Enterprise Upgrades: Before, During, and After

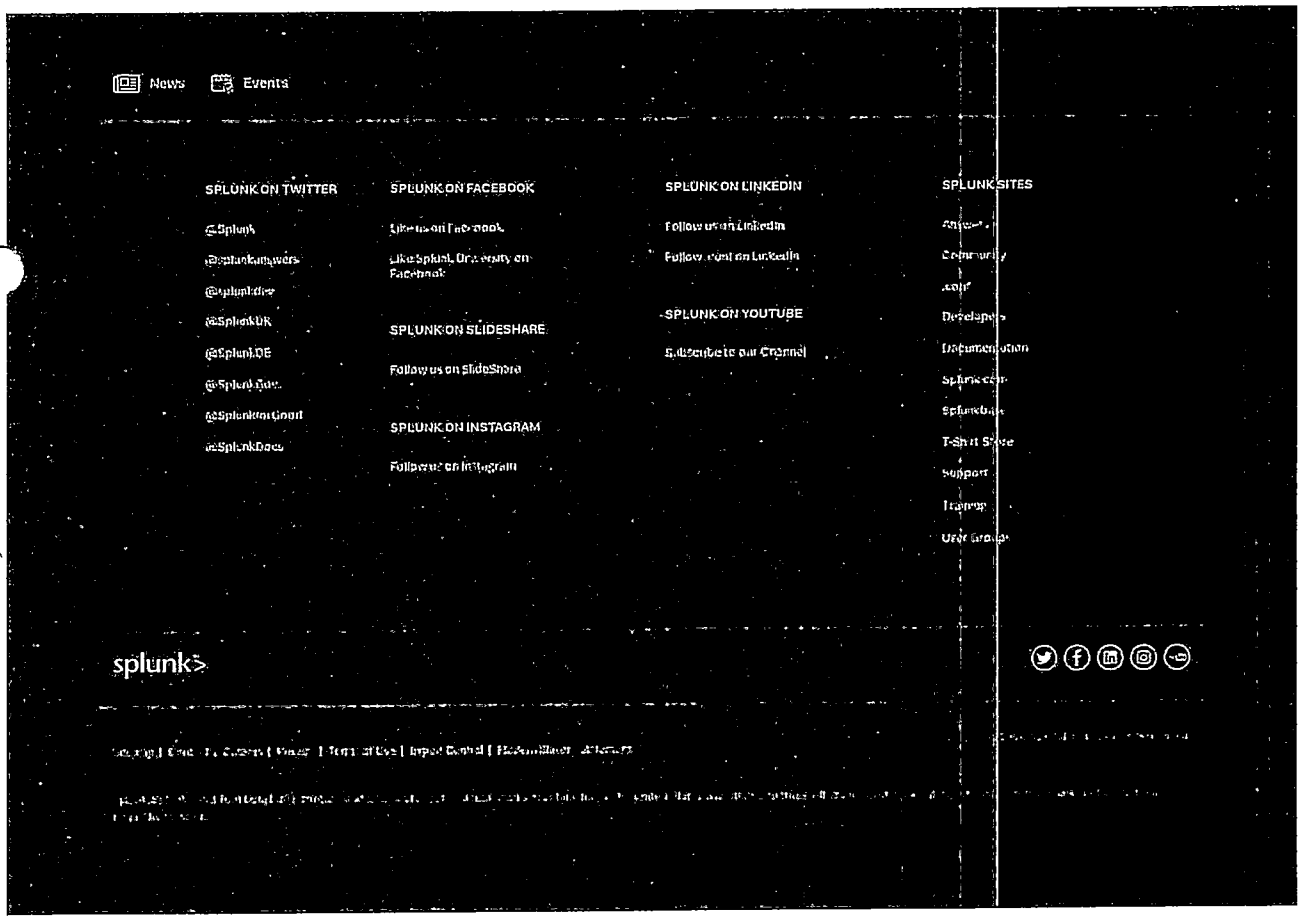
By Splunk September 24, 2019



PLATFORM

## Introducing New Deep Learning NLP Assistants for DSDL

By Tatsu Murata July 12, 2023



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.

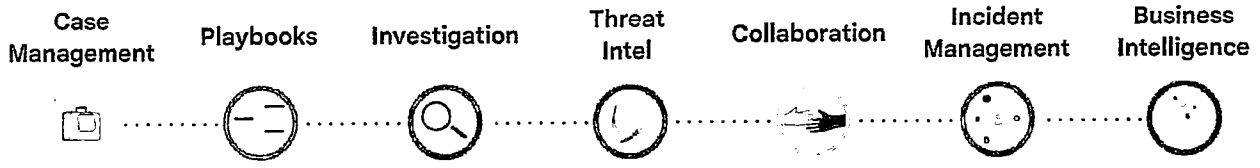
### Capture security operations insights consistently

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.

Google Cloud

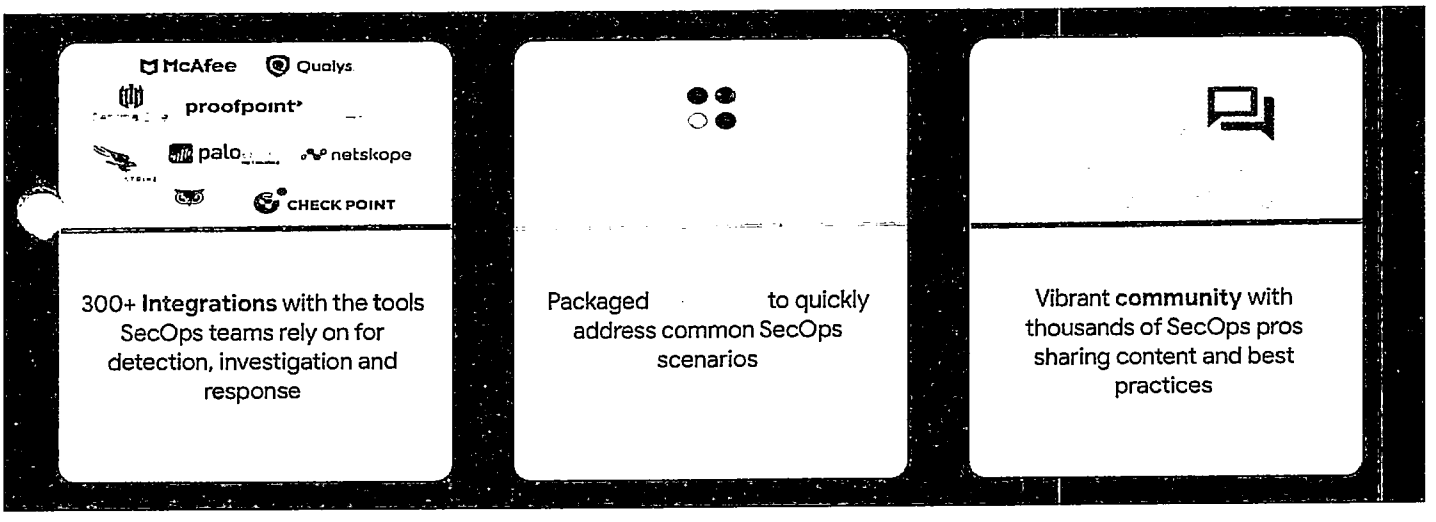
## What you get

Chronicle delivers well beyond customary SOAR offerings to help your security team move beyond the daily cyber grind and concentrate on what matters most: building resiliency and investigating and remediating real threats, fast.




> Chronicle SOAR has been a game-changer for our SOC! It has improved our tool integrations and capabilities during a period of significant growth in our SOC.

*SOC Director, IT Services Industry*



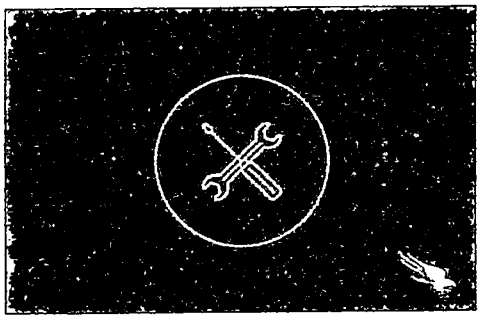

**Get started with our free Community SOAR Edition**
Experience Chronicle SOAR with our free Community Edition that comes complete with ready-to-deploy use cases.
Visit us at https://chronicle.security for more information.

# A.2
# Managed Detection and Response

CROWDSTRIKE BLOG

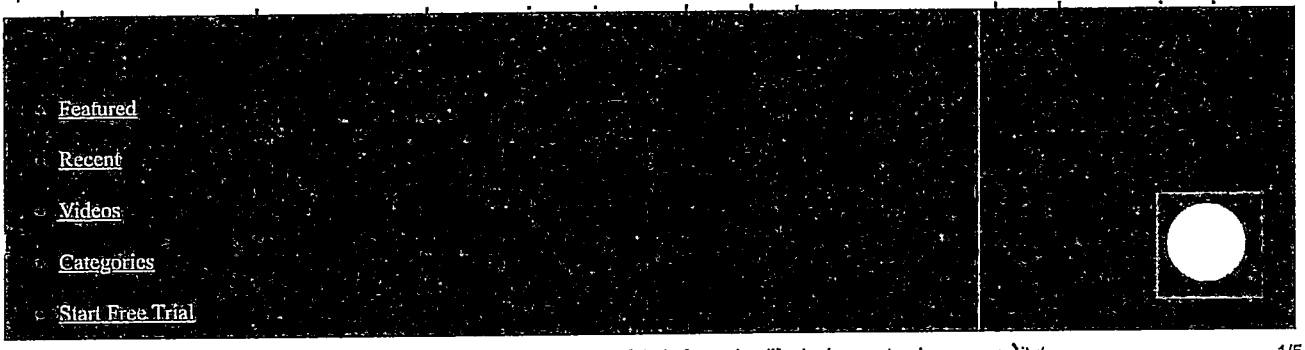
BACK TO TECH CENTER

# How the Falcon Platform Simplifies Deployment and Enhances Security



## Introduction

Traditional requirements for security are overly complicated and brittle. The large number of pieces that are required not only complicate the deployment but make getting the promised value of the solution challenging at best. CrowdStrike has developed a powerful platform that takes the hassle out of deployment. This means that not



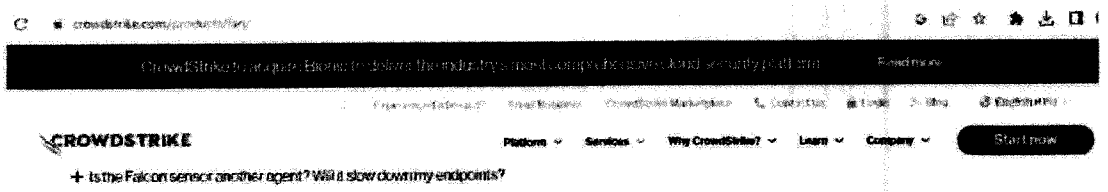
CROWDSTRIKE BLOG

## Deployment

The CrowdStrike solution is cloud native with a single user interface that delivers all of the functionality including management, configuration and policy.

The single, lightweight agent can be downloaded and installed for Windows, Mac and Linux to deliver complete protection without impacting resources or productivity. The install is fast and easy. For larger deployments, most companies prefer to use their existing software distribution process. The CrowdStrike agent can be deployed with all common deployment tools including SCCM, intune and JAMF. You can also build the agent into gold images or templates for cloud systems to ensure new hosts are protected from the beginning.

The CrowdStrike solution does not require any complex tuning, managed services or even signature updates to be effective. Instead, it delivers immediate value as systems are protected as soon as the agent is installed.




+ Is the Falcon sensor another agent? Will it slow down my endpoints?

— What Windows versions does the Falcon agent support?

Only these operating systems are supported for use with the Falcon sensor for Windows. Note: For identity protection functionality, you must install the sensor on your domain controllers, which must be running a 64-bit server OS.

64-bit Server OSes:

- Server 2022
- Server Core 2022
- Server 2019
- Server Core 2019
- Server 2016
- Server Core 2016
- Server 2012 R2
- Storage Server 2012 R2
- Server 2012
- Server 2008 R2 SP1

Microsoft ARM64:

- Windows 11
- Windows 10

Desktop OSes:

- Windows 11 22H2
- Windows 11 21H2
- Windows 10 22H2
- Windows 10 21H2
- Windows 10 21H1
- Windows 10 20H2
- Windows 10 1909
- Windows 10 1607
- Windows 10 1507
- Windows 7 SP1
- Windows 7 Embedded POS Ready

+ What Linux versions does the Falcon agent support?

+ What macOS versions does the Falcon agent support?

+ What Windows versions does the Falcon agent support?

— What Linux versions does the Falcon agent support?

We support x86_64, Graviton 64, and s390x zLinux versions of these Linux server OSes:

x86_64

- Alma Linux
  - 9.1 sensor version 7.01.5604 and later
  - 9.0 sensor version 6.41.13804 and later
  - 8.6 sensor version 6.41.13803 and later
  - 8.5 sensor version 6.23.13003 and later
  - 8.4 sensor version 6.20.12606 and later
- Amazon Linux 2
- Amazon Linux AMI
  - 2018.03
  - 2017.09
- CentOS
  - 8.5 sensor version 6.33.13003 and later
  - 8.4 sensor version 6.24.12104 and later
  - 8.3
  - 8.2 sensor version 5.34.9817 and later
  - 8.1 sensor version 5.27.9101 and later
  - 8.0
  - 7.9 sensor version 5.43.10503 and later
  - 7.8 sensor version 5.30.9510 and later
  - 7.4 - 7.7
  - 6.7 - 6.10
- Debian
  - 11 sensor version 6.34.13108 and later
  - 10 sensor version 6.20.11711 and later
  - 9.0-9.4 sensor version 6.33.9904 and later
- Oracle Linux
  - Oracle Linux 9 - UEK 7
  - Oracle Linux 8 - UEK 7

- Oracle Linux 8 - UEK 6
- Oracle Linux 7 - UEK 6, sensor version 6.39.18610 and later
- Oracle Linux 7 - UEK 3, 4, 5
- Oracle Linux 6 - UEK 3, 4
- Red Hat Compatible Kernels (supported RHCK kernels are the same as for RHEL)

- Red Hat Enterprise Linux CoreOS (RHCOS) **Note:** For DaemonSet deployment only.
  - 4.11: sensor version 6.46.14308 and later
  - 4.10: sensor version 6.40.14308 and later
  - 4.9: sensor version 6.39.13601 and later
  - 4.8: sensor version 6.39.13601 and later
  - 4.7: sensor version 6.39.13601 and later
- Red Hat Enterprise Linux (RHEL)
  - 9.1: sensor version 7.01.15604 and later
  - 9.0: sensor version 6.41.13804 and later
  - 8.7: sensor version 6.43.14604 and later
  - 8.6: sensor version 6.41.13803 and later
  - 8.5: sensor version 6.33.13003 and later
  - 8.4: sensor version 6.24.12104 and later
  - 8.3
  - 8.2: sensor version 5.34.09117 and later
  - 8.1: sensor version 5.27.9101 and later
  - 8.0
  - 7.9: sensor version 5.43.18303 and later
  - 7.8: sensor version 5.30.9810 and later
  - 7.4 - 7.7
  - 6.7 - 6.10
- Rocky Linux
  - 9.1: sensor version 7.01.15604 and later
  - 9.0: sensor version 6.41.13804 and later
  - 8.6: sensor version 6.41.13803 and later
  - 8.5: sensor version 6.33.13003 and later
  - 8.4: sensor version 6.29.12506 and later
- SUSE Linux Enterprise (SLES)
  - 15 - 15.4, SLES 15 SP4: sensor version 6.47.14408 and later
  - 12.2 - 12.5, SLES 12 SP5: sensor version 5.27.9101 and later
  - 11.4: you must also install OpenSSL version 1.0.1e or later
- OpenSuse LEAP
  - 15.4: sensor version 6.47.14408 and later
  - 15.3: sensor version 6.39.13601 and later
  - **Note:** Supported kernels are the same as SLES 15 SP3 and SLES 15 SP4

- Ubuntu
  - 22.04 LTS: sensor version 6.41.13803 and later
  - 20.04 LTS: sensor version 5.4.2.10807 and later
  - 18 AWS
  - 18.04 LTS
  - 16 AWS
  - 16.04 LTS and 16.04.6 LTS
  - 14.04 LTS

**Graviton**

- Alma Linux ARM64
  - 9.1: sensor version 7.02.15705 and later
  - 9.0 ARM64: sensor version 6.51.14810 and later
  - 8.7 ARM64: sensor version 6.48.14504 and later
  - 8.6 ARM64: sensor version 6.43.14005 and later
  - 8.5 ARM64: sensor version 6.41.13803 and later
- Amazon Linux 2
- CentOS ARM64
  - 8.5 ARM64: sensor version 6.41.13803 and later
- Red Hat Enterprise Linux (RHEL) ARM64
  - 9.1: sensor version 7.02.15705 and later
  - 9.0 ARM64: sensor version 6.51.14810 and later
  - 8.7 ARM64: sensor version 6.48.14504 and later

**s390x zLinux**

- Red Hat Enterprise Linux (RHEL)
  - RedHat 7.7, 7.8, 7.9
  - RedHat 8.0, 8.1, 8.2, 8.3, 8.4, 8.5
- Suse Linux Enterprise Server (SLES)
  - SLES 15 SP1, SP2, SP3, SP4
  - SLES 12 SP1, SP2, SP3, SP4, SP5
- Ubuntu
  - 22.04 LTS
  - 20.04 LTS
  - 18.04 LTS

    - 8.6 ARM64: sensor version 6.43.140015 and later
    - 8.5 ARM64: sensor version 6.41.138013 and later
- Rocky Linux ARM64
    - 9.1: sensor version 7.02.15705 and later
    - 9.0 ARM64: sensor version 6.51.14810 and later
    - 8.7 ARM64: sensor version 6.48.14504 and later
    - 8.6 ARM64: sensor version 6.43.14036 and later
    - 8.5 ARM64: sensor version 6.41.13803 and later
- Ubuntu
    - 20.04 AWS: sensor version 6.47.14409 and later
    - 20.04 LTS: sensor version 6.44.14107 and later
    - 18.04 LTS: sensor version 6.44.14107 and later

+ Can Falcon Prevent block attacks?

+ Can CrowdStrike Falcon® protect endpoints if they are not connected to the cloud?

## IN GRATION

+ Do I need a large staff to maintain my CrowdStrike Falcon® environment?

+ Does the Falcon sensor interfere with other endpoint software?

+ How do I integrate with the Falcon platform?

+ Does CrowdStrike Falcon® integrate with my SIEM?

## DEPLOYMENT

+ How long does it take to get started with CrowdStrike Falcon®?

+ Is the Falcon sensor another agent? Will it slow down my endpoints?

+ What Windows versions does the Falcon agent support?

+ What Linux versions does the Falcon agent support?

— What macOS versions does the Falcon agent support?

The Falcon sensor for Mac is currently supported on these macOS versions:

- Ventura 13: Sensor version 6.45.15801 and later
- Monterey 12: All supported versions

+ What ChromeOS versions does the Falcon platform support?

+ Can CrowdStrike Falcon® scale to protect large environments with 100,000-plus endpoints?

+ What AWS Compute Services does CrowdStrike support today?

## CLOUD

CrowdStrike Falcon® cloud-based or on-premises?

Is Falcon SOC2 compliant?

+ How does the Falcon sensor talk to the cloud and how much data does it send?

CROWDSTRIKE

# FALCON FOR MOBILE

Providing mobile endpoint detection and response (EDR) for iOS and Android

## THE INDUSTRY'S LEADING ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION FOR iOS AND ANDROID

Mobile devices have completely changed the way employees work — providing instant access to business-critical applications any time and anywhere. The increasing volume of business data stored or remotely accessed by enterprise mobile apps greatly elevates the risk of malicious activity and accidental data exposure by trusted employees.

Security and IT teams are not equipped with the tools they need to keep business data safe and personal information private. Unified endpoint management (UEM) solutions have been available for years, but they don't address core security concerns, and mobile threat defense (MTD) solutions have been slow to catch on — that's why a blended approach is needed in today's work-from-anywhere world.

CrowdStrike Falcon for Mobile™ builds on CrowdStrike's proven endpoint detection and response (EDR) technology, enabling security teams to detect malicious activity as well as unwanted access to sensitive corporate data. Real-time detection capabilities eliminate the time and complexity required to identify mobile threats, such as communication to known malicious servers, high-risk device configurations, unauthorized apps and more. Falcon for Mobile provides the visibility you need, while protecting user privacy and eliminating the blind spots that lead to breaches.

### KEY BENEFITS

- Accelerates and simplifies mobile threat triage and response
- Provides real-time visibility into vulnerable mobile devices and risky configurations
- Maps detections with the MITRE ATT&CK® for Mobile framework
- Unifies EDR across mobile devices, endpoints and cloud workloads
- Protects user privacy and preserves device resources

**Mobile malware is real:** In a Ponemon survey, 67% of organizations say it was certain or likely they had a data breach as a result of employees using their mobile devices to access the company's confidential information.

CrowdStrike Store

ExtraHop

CROWDSTRIKE

Data Sheet

# EXTRAHOP REVEAL(X) 360: FULL-COVERAGE NDR AND EDR FOR WHEN SECONDS MATTER

Combining complete network intelligence with endpoint protection to secure your hybrid and multi-cloud environment

## CHALLENGES

Cyberattackers are growing more sophisticated at evading security measures, and businesses that are growing rapidly and dynamically need security that can keep up without introducing friction. But security staffing is more challenging than ever, and siloed legacy technology and bolted-on security solutions can't keep pace.

## SOLUTION

Tightly integrated network detection and response (NDR) and endpoint detection and response (EDR) form the foundation for evolving security operations against both common and advanced threats. The purpose-built integration of ExtraHop Reveal(x) 360 with the CrowdStrike Falcon® platform combines complete network intelligence with world-class endpoint security into a single, seamless solution that delivers both NDR and EDR functionality as well as next-generation intrusion detection (NG-IDS) and network forensics with real-time decryption. This solution provides complete detection and response capabilities across every attack surface in your hybrid, multi-cloud enterprise.

## KEY BENEFITS

- **Unified threat intelligence:** Share IOCs across EDR and NDR solutions for unified threat detection
- **Real-time response:** Automatically contain both network- and endpoint-based attacks
- **Security for every device:** Discover and monitor unmanaged devices, mobile devices, IoT, BYOD, remote workforce and more
- **Complete MITRE ATT&CK® coverage:** Cover the entire attack chain with endpoint and network TTPs
- **EDR and NDR forensics combined for full coverage:** Endpoint details and network decryption and analysis are correlated in one place for rapid investigation and incident response

CrowdStrike Store

EXTRAHOP REVEAL(X) 360

## KEY CAPABILITIES

Reveal(x) 360 integrates with several CrowdStrike Falcon products to correlate network intelligence and insights from Reveal(x) 360 with endpoint behavior details and indicators of compromise from Falcon.

- **Reveal(x) 360 + CrowdStrike Falcon Intelligence**
  The Reveal(x) 360 integration with Falcon Intelligence correlates IPs and domains listed as IOCs in Falcon Intelligence with network behavior data about those IPs and domains, providing rapid investigation of potential attacks in progress.

- **Reveal(x) 360 + CrowdStrike Falcon Real Time Response**
  Reveal(x) 360 detects network-based threats that may soon impact specific endpoints but have not yet conducted malicious behavior on the endpoint itself. Reveal(x) 360 can notify the Falcon agent about affected endpoints to contain the endpoint, preventing further spread of the threat.

- **Reveal(x) 360 + CrowdStrike Threat Graph**
  Reveal(x) 360 gathers network transaction metrics, transaction records and full packets and decrypts them in real time, providing complete network intelligence at cloud speed and scale.

- **Reveal(x) 360 for Unmanaged IoT, BYOD and Remote Connections**
  Reveal(x) 360 can discover and identify any device that communicates on the network and identify whether the Falcon agent is installed on the device by observing network traffic, helping customers ensure complete coverage, and security detection and response capabilities — even for unmanaged or unmanageable devices.

## ABOUT EXTRAHOP

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop breaches 84% faster — get started at **www.extrahop.com/freetrial**

**Start Free Trial**
**of Next-Gen AV**

Learn more **www.crowdstrike.com**



## ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

**CrowdStrike: We stop breaches.**

Learn more:
**https://www.crowdstrike.com/**

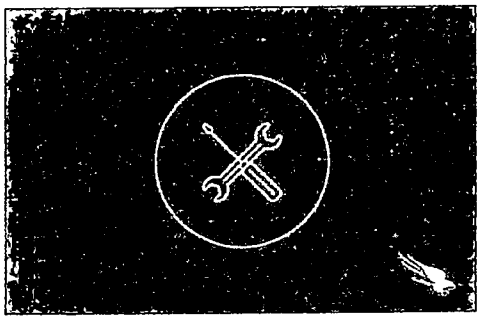
Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
**https://www.crowdstrike.com/free-trial-guide/**

CROWDSTRIKE BLOG

BACK TO TECH CENTER

# How the Falcon Platform Simplifies Deployment and Enhances Security



## Introduction

Traditional requirements for security are overly complicated and brittle. The large number of pieces that are required not only complicate the deployment but make getting the promised value of the solution challenging at best. CrowdStrike has developed a powerful platform that takes the hassle out of deployment. This means that not

[redacted]

CROWDSTRIKE BLOG

## Deployment

The CrowdStrike solution is cloud native with a single user interface that delivers all of the functionality including management, configuration and policy.

The single, lightweight agent can be downloaded and installed for Windows, Mac and Linux to deliver complete protection without impacting resources or productivity. The install is fast and easy. For larger deployments, most companies prefer to use their existing software distribution process. The CrowdStrike agent can be deployed with all common deployment tools including SCCM, intune and JAMF. You can also build the agent into gold images or templates for cloud systems to ensure new hosts are protected from the beginning.

The CrowdStrike solution does not require any complex tuning, managed services or even signature updates to be effective. Instead, it delivers immediate value as systems are protected as soon as the agent is installed.

[redacted]

Featured

Recent

Videos

Categories

Start Free Trial

CrowdStrike Store

ExtraHop

CROWDSTRIKE

Data Sheet

# EXTRAHOP REVEAL(X) 360: FULL-COVERAGE NDR AND EDR FOR WHEN SECONDS MATTER

Combining complete network intelligence with endpoint protection to secure your hybrid and multi-cloud environment

## CHALLENGES

Cyberattackers are growing more sophisticated at evading security measures, and businesses that are growing rapidly and dynamically need security that can keep up without introducing friction. But security staffing is more challenging than ever, and siloed legacy technology and bolted-on security solutions can't keep pace.

## SOLUTION

Tightly integrated network detection and response (NDR) and endpoint detection and response (EDR) form the foundation for evolving security operations against both common and advanced threats. The purpose-built integration of ExtraHop Reveal(x) 360 with the CrowdStrike Falcon® platform combines complete network intelligence with world-class endpoint security into a single, seamless solution that delivers both NDR and EDR functionality as well as next-generation intrusion detection (NG-IDS) and network forensics with real-time decryption. This solution provides complete detection and response capabilities across every attack surface in your hybrid, multi-cloud enterprise.

## KEY BENEFITS

**Unified threat intelligence:** Share IOCs across EDR and NDR solutions for unified threat detection

**Real-time response:** Automatically contain both network- and endpoint-based attacks

**Security for every device:** Discover and monitor unmanaged devices, mobile devices, IoT, BYOD, remote workforce and more

**Complete MITRE ATT&CK® coverage:** Cover the entire attack chain with endpoint and network TTPs

**EDR and NDR forensics combined for full coverage:** Endpoint details and network decryption and analysis are correlated in one place for rapid investigation and incident response

CrowdStrike Store

EXTRAHOP REVEAL(X) 360

# KEY CAPABILITIES

Reveal(x) 360 integrates with several CrowdStrike Falcon products to correlate network intelligence and insights from Reveal(x) 360 with endpoint behavior details and indicators of compromise from Falcon.

- **Reveal(x) 360 + CrowdStrike Falcon Intelligence**
  The Reveal(x) 360 integration with Falcon Intelligence correlates IPs and domains listed as IOCs in Falcon Intelligence with network behavior data about those IPs and domains, providing rapid investigation of potential attacks in progress.

- **Reveal(x) 360 + CrowdStrike Falcon Real Time Response**
  Reveal(x) 360 detects network-based threats that may soon impact specific endpoints but have not yet conducted malicious behavior on the endpoint itself. Reveal(x) 360 can notify the Falcon agent about affected endpoints to contain the endpoint, preventing further spread of the threat.

- **Reveal(x) 360 + CrowdStrike Threat Graph**
  Reveal(x) 360 gathers network transaction metrics, transaction records and full packets and decrypts them in real time, providing complete network intelligence at cloud speed and scale.

- **Reveal(x) 360 for Unmanaged IoT, BYOD and Remote Connections**
  Reveal(x) 360 can discover and identify any device that communicates on the network and identify whether the Falcon agent is installed on the device by observing network traffic, helping customers ensure complete coverage, and security detection and response capabilities — even for unmanaged or unmanageable devices.

# ABOUT EXTRAHOP

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop breaches 84% faster — get started at **www.extrahop.com/freetrial**

**Start Free Trial**
**of Next-Gen AV**

Learn more **www.crowdstrike.com**



## ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk—endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

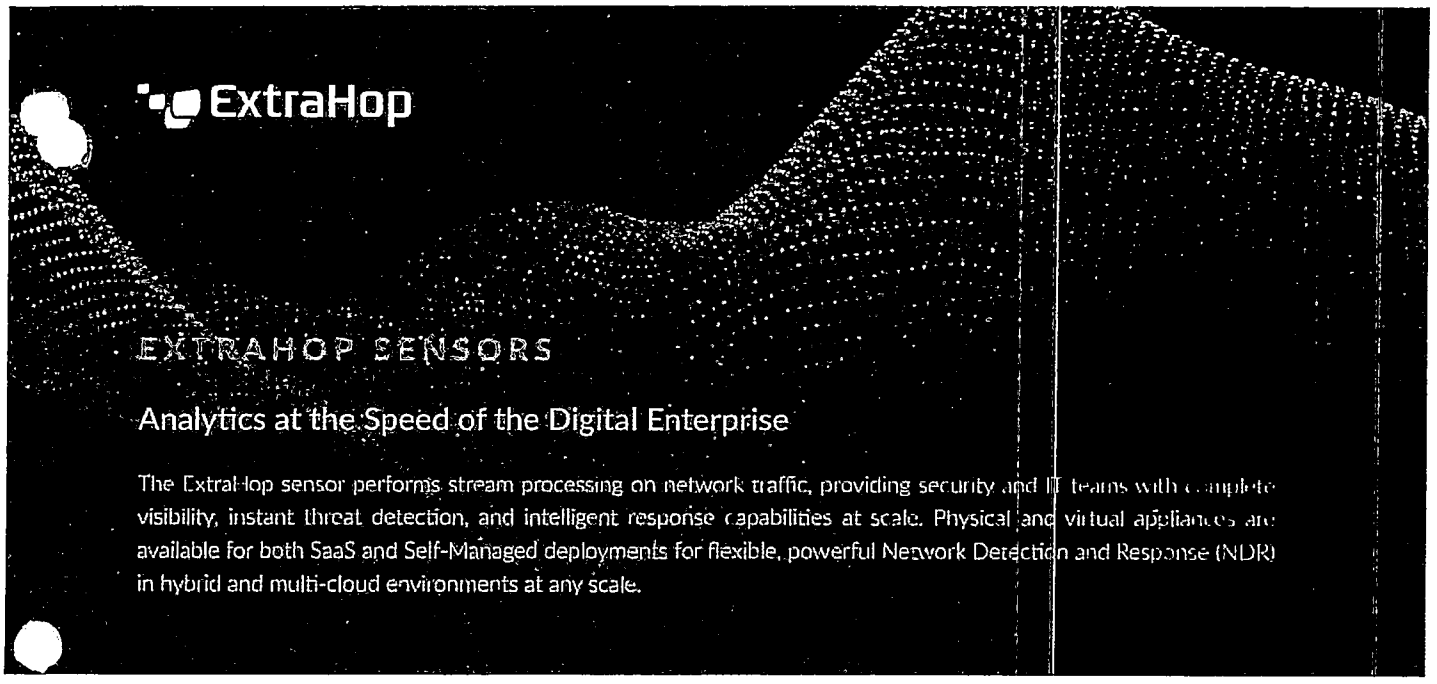
Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
**https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
**https://www.crowdstrike.com/free-trial-guide/**




**UNMATCHED SCALABILITY**

A single ExtraHop sensor can analyze behavior for up to 100,000 endpoints up to a sustained 100 Gbps, equivalent to more than 1 PB of analysis each day, while still guaranteeing at least 90 days of lookback.

**VALUABLE DETAILS**

The ExtraHop real-time stream processor extracts over 5,000 L2-L7 metrics from network traffic, providing rich data for our cloud-scale ML security detections, enabling 95% faster threat detection and 84% faster incident response.

**THE ONLY NDR WITH TLS 1.3/ PFS DECRYPTION**

ExtraHop is the only NDR product that can decrypt TLS 1.3 with perfect forward secrecy in real time for analysis, enabling covert detection of the stealthiest threats.

**IMMEDIATE VALUE FOR ALL TEAMS**

ExtraHop sensors are available as physical or virtual appliances for both SaaS and Self-Managed deployments, including hybrid environments and in the cloud in AWS, Azure, and Google Cloud. Reveal(x) 360 is available as a pure SaaS service in AWS.

## SaaS SENSORS

| Reveal(x) 360 SaaS for AWS | 1Gbps |
|---|---|
| Premium (Sensor only) | Yes |
| Ultra (Sensor + Continuous PCAP) | Yes |
| Record Lookback | 90 days |

## PHYSICAL SENSORS

| SPECIFICATIONS | EDA 6200 | EDA 4200 | EDA 1200 |
|---|---|---|---|
| **TRAFFIC ANALYTICS** | | | |
| Throughput | 10 Gbps | 5 Gbps | 1 Gbps |
| **NETWORK** | ExtraHop appliances can receive data via RPCAP, ERSPAN, VXLAN, or physical ports. | | |
| Management ports | 4 x 1 GbE copper | 4 x 1 GbE copper | 1000BASE-T |
| High Speed Monitoring Connectivity Options | 2 x 10GbE LC fiber<br>2 x customer-supplied SFP+ DAC | 2 x 10GbE LC fiber<br>2 x customer-supplied SFP+ DAC | 1x1 GbE |
| **CHASSIS** | | | |
| Datastore | 1.2 TB (RAID 10 optional) | Included 240gb SSD | 88 GB |
| Packet capture (optional) | 480 GB | 480 GB | 140 GB |
| Power supply | 2 x 750W | 2 x 495W | 1x100W |
| Rack Unit | 1U | 1U | See physical dimensions below |
| Height | 4.28 cm (1.68 in.) | 4.28 cm (1.68 in.) | 5.9 cm (2.3 in.) |
| Width | 43.4 cm (17.08 in.) | 43.4 cm (17.08 in.) | 19.3 cm (7.5 in.) |
| Depth | 73.4 cm (29.61 in.) | 73.4 cm (29.61 in.) | 20.0 cm (7.9 in.) |
| Weight | 21.9 kg (48.28 lbs) | 21.9 kg (48.28 lbs) | 1.9 kg (4.2 lbs) |
| **ENVIRONMENT DETAILS** | | | |
| Heat dissipation | 2891 BTU/hr maximum | | |
| Operating temperature | 10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment | | 0 °C to 40 °C |
| Storage temperature | -40 °C to 65 °C (-40 °F to 149 °F) | | -20 °C to +70 °C (4 °F to 158 °F) |
| Operating relative humidity | 10% to 80% RH with 29°C (84.2°F) max. dew point | | |
| Operating vibration | 0.26 G rms at 5 Hz to 350 Hz (all operation orientations) | | |
| Operating altitude | 3,048 m (10,000 ft) | | |
| Operating shock | Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms | | |
| Operating system | The operating system is a security-hardened embedded Linux with a networking microkernel developed specifically for high-speed packet processing via the ExtraHop real-time stream processor | | |
| Remote management | iDRAC8 remote management controller | | N/A |

# What is CrowdStrike? Falcon platform FAQ

Want to see the CrowdStrike Falcon® platform in action? Start with a free trial of next-gen antivirus

## CAPABILITIES

+ What does CrowdStrike Falcon® do?

+ What solutions are offered within the CrowdStrike Falcon® platform?

+ What is Falcon Fusion?

+ What modules do I need to use Falcon Fusion?

+ What is Falcon Prevent?

+ What is Falcon Insight?

+ What is Falcon OverWatch?

+ What is Falcon Discover?

+ Can I use CrowdStrike Falcon® to replace my current AV solution?

+ Is CrowdStrike Falcon® certified for AV replacement?

+ Which products can CrowdStrike Falcon® help me replace?

+ Can CrowdStrike Falcon® be used for compliance requirements?

+ How does CrowdStrike Falcon® compare to other "next-generation" endpoint protection solutions? What makes Falcon unique?

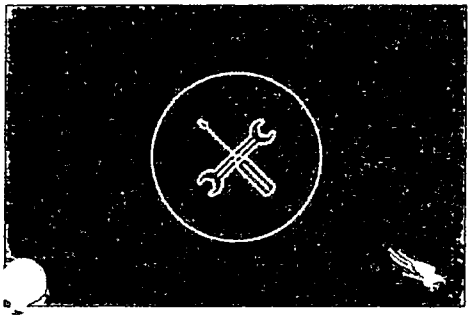
+ Can I use CrowdStrike Falcon® for incident response?

− Can Falcon Prevent block attacks?

Yes, Falcon Prevent offers powerful and comprehensive prevention capabilities. Falcon Prevent can stop execution of malicious code, block zero-day exploits, kill processes and contain command and control callbacks.

# How to Install Falcon in the Data Center

June 6, 2017 Peter Ingebretsen 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

ExtraHop

CROWDSTRIKE

Data Sheet

# EXTRAHOP REVEAL(X) 360: FULL-COVERAGE NDR AND EDR FOR WHEN SECONDS MATTER

Combining complete network intelligence with endpoint protection to secure your hybrid and multi-cloud environment

## CHALLENGES

Cyberattackers are growing more sophisticated at evading security measures, and businesses that are growing rapidly and dynamically need security that can keep up without introducing friction. But security staffing is more challenging than ever, and siloed legacy technology and bolted-on security solutions can't keep pace.

## SOLUTION

Tightly integrated network detection and response (NDR) and endpoint detection and response (EDR) form the foundation for evolving security operations against both common and advanced threats. The purpose-built integration of ExtraHop Reveal(x) 360 with the CrowdStrike Falcon® platform combines complete network intelligence with world-class endpoint security into a single, seamless solution that delivers both NDR and EDR functionality as well as next-generation intrusion detection (NG-IDS) and network forensics with real-time decryption. This solution provides complete detection and response capabilities across every attack surface in your hybrid, multi-cloud enterprise.

## KEY BENEFITS

**Unified threat intelligence:** Share IOCs across EDR and NDR solutions for unified threat detection

**Real-time response:** Automatically contain both network- and endpoint-based attacks

**Security for every device:** Discover and monitor unmanaged devices, mobile devices, IoT, BYOD, remote workforce and more

**Complete MITRE ATT&CK® coverage:** Cover the entire attack chain with endpoint and network TTPs

**EDR and NDR forensics combined for full coverage:** Endpoint details and network decryption and analysis are correlated in one place for rapid investigation and incident response

CrowdStrike Store

EXTRAHOP REVEAL(X) 360

# KEY CAPABILITIES

Reveal(x) 360 integrates with several CrowdStrike Falcon products to correlate network intelligence and insights from Reveal(x) 360 with endpoint behavior details and indicators of compromise from Falcon.

☐ **Reveal(x) 360 + CrowdStrike Falcon Intelligence**
The Reveal(x) 360 integration with Falcon Intelligence correlates IPs and domains listed as IOCs in Falcon Intelligence with network behavior data about those IPs and domains, providing rapid investigation of potential attacks in progress.

☑ **Reveal(x) 360 + CrowdStrike Falcon Real Time Response**
Reveal(x) 360 detects network-based threats that may soon impact specific endpoints but have not yet conducted malicious behavior on the endpoint itself. Reveal(x) 360 can notify the Falcon agent about affected endpoints to contain the endpoint, preventing further spread of the threat.

☑ **Reveal(x) 360 + CrowdStrike Threat Graph**
Reveal(x) 360 gathers network transaction metrics, transaction records and full packets and decrypts them in real time, providing complete network intelligence at cloud speed and scale.

☐ **Reveal(x) 360 for Unmanaged IoT, BYOD and Remote Connections**
Reveal(x) 360 can discover and identify any device that communicates on the network and identify whether the Falcon agent is installed on the device by observing network traffic, helping customers ensure complete coverage, and security detection and response capabilities — even for unmanaged or unmanageable devices.

# ABOUT EXTRAHOP

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop breaches 84% faster — get started at **www.extrahop.com/freetrial**

**Start Free Trial**
**of Next-Gen AV**

Learn more **www.crowdstrike.com**



## ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
**https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
**https://www.crowdstrike.com/free-trial-guide/**

CrowdStrike Products

CROWDSTRIKE

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

Certified to replace legacy antivirus products — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

**Named a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)** — In addition to being positioned in the Leaders Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as innovation, marketing and product strategies, vertical industry and geographic strategies, as well as the validity of the business model as a whole.

## KEY BENEFITS

- Prevents all types of attacks
- Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery
- Deploys in minutes and immediately begins protecting your endpoints
- Replaces legacy antivirus quickly and confidently
- Operates seamlessly alongside AV as you migrate to simplify transition
- Provides full attack visibility

CrowdStrike Products

FALCON PREVENT NEXT-GENERATION ANTIVIRUS

# KEY CAPABILITIES

## STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

## INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

## FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

## SIMPLE, FAST AND LIGHTWEIGHT

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial of Next-Gen AV

Learn more at www.crowdstrike.com

CROWDSTRIKE

# FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Streaming the threat detection and response lifecycle with speed, automation and unrivaled visibility

## FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

## KEY PRODUCT CAPABILITIES

### SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

## KEY BENEFITS

- Detect and intelligently prioritize advanced threats automatically
- Speed investigations with deep, real-time forensics and sophisticated visualizations
- Respond and remediate with confidence
- See the big picture with CrowdScore, your enterprise threat score
- Reduce alert fatigue by 90% or more
- Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

CrowdStrike Products

CROWDSTRIKE

# FALCON COMPLETE

Managed detection and response (MDR) delivered by CrowdStrike's team of experts to protect endpoints, cloud workloads and identities

## CHALLENGES

Operating an effective security program is extremely challenging. Adversaries are increasingly fast and stealthy, don't respect time zones or holidays, and often execute damaging intrusions in hours. The necessary tools to defend against these threats can be difficult to use and can require a lot of resources to appropriately implement, operate and maintain.

The modern threat landscape continues to evolve with an increase in attacks leveraging compromised credentials. An attacker with compromised credentials all too frequently has free reign to move about an organization and carefully plan their attack before they strike.

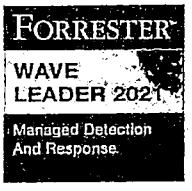
## SOLUTION

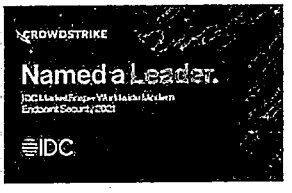
CrowdStrike Falcon Complete™ delivers 24/7 expert management, monitoring and response for the CrowdStrike Falcon® platform and is backed by CrowdStrike's industry-leading Breach Prevention Warranty.*

Falcon Complete is CrowdStrike's most comprehensive endpoint protection solution. It delivers unparalleled security by augmenting Falcon Prevent™ next-gen antivirus (NGAV), Falcon Insight™ endpoint detection and response (EDR), Falcon Identity Threat Protection and Falcon OverWatch™ managed threat hunting together with the expertise and 24/7 engagement of the Falcon Complete team. The team manages and actively monitors the Falcon platform for customers, remotely remediating incidents in minutes. The Falcon Complete team solves the challenge of implementing and running an effective and mature security program without the difficulty, burden and costs associated with building one internally.

A leader in...

- Forrester MDR[1]
- IDC MDR[2]




1. IDC MarketScape US Managed Detection and Response
2. Services Vendor Assessment IDC #US48129921 August 2021

## KEY BENEFITS

**Immediate value with a seamless extension of your team:**

- Delivers focused expertise 24/7 to stop breaches
- Provides the equivalent of 5 expert SOC analysts and 5 elite human threat hunters
- Supplies continuous management, optimization and monitoring
- Completes onboarding and provides full protection in an average of 10 days

**Rapid response and surgical remediation in minutes:**

- Provides rapid response at the endpoint, cloud workload and identity layers
- Conducts hunting at unprecedented speed and cloud-scale
- Reduces business disruption to processes or users
- Instills confidence that threats are handled completely and correctly

**Reduced cybersecurity risk and enormous cost savings:**

- Shrinks the attack surface across endpoints, cloud workloads and identities
- Saves over 2,500 hours per year from a reduction in security incidents
- Delivers an ROI of more than 400%**
- Is backed by the industry's strongest Breach Prevention Warranty*

* Breach Prevention Warranty not available in all areas. See FAQ for details.

** Total Economic Impact of Falcon Complete, February 2021 Forrester Wave for Managed Detection and Response, Q12021

# FALCON COMPLETE: A SYMBIOSIS OF PEOPLE, PROCESS AND TECHNOLOGY

**Falcon Complete Expertise**

Provides expert security analysts to manage, monitor, respond to and remediate threats

**Falcon Discover: IT Hygiene**

Provides visibility into assets, systems and applications for a comprehensive topography of your IT environment

**People, Process, Technology**

Falcon Complete's unique combination of technology, people and process delivers concrete improvements for our customers, transforming day-to-day operations

**Falcon Prevent: Next-gen AV**

Provides the ideal AV replacement solution by combining the most effective prevention technologies with full stack visibility and simplicity

**Falcon Insight: Endpoint Detection and Response**

Delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches are stopped

**Falcon OverWatch: Managed Threat Hunting**

Adds a human threat detection engine that operates as an extension of your team, hunting relentlessly to see and stop the most sophisticated hidden threats

**Falcon Identity Threat Protection**

Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

**Cybersecurity 101 › Indicators of Compromise (IOC)**

# INDICATORS OF COMPROMISE (IOC) SECURITY

October 5, 2022

## Indicators of Compromise Explained

An **Indicator of Compromise (IOC)** is a piece of digital forensics that suggests that an endpoint or network may have been breached. Just as with physical evidence, these digital clues help information security professionals identify malicious activity or security threats, such as data breaches, insider threats or malware attacks.

Investigators can gather indicators of compromise manually after noticing suspicious activity or automatically as part of the organization's cybersecurity monitoring capabilities. This information can be used to help mitigate an in-progress attack or remediate an existing security incident, as well as create "smarter" tools that can detect and quarantine suspicious files in the future.

Unfortunately, IOC monitoring is reactive in nature, which means that if an organization finds an indicator, it is almost certain that they have already been compromised. That said, if the event is in-progress, the quick detection of an IOC could help contain attacks earlier in the attack lifecycle, thus limiting their impact to the business.

As cyber criminals become more sophisticated, indicators of compromise have become more difficult to detect. The most common IOCs—such as an md5 hash, C2 domain or hardcoded IP address, registry key and filename —are constantly changing, which makes detection more difficult.



## How to Identify Indicators of Compromise

When an organization is an attack target or victim, the cybercriminal will leave traces of their activity in the system and log files. The threat hunting team will gather this digital forensic data from these files and systems to determine if a security threat or data breach has occurred or is in-process.

Identifying IOCs is a job handled almost exclusively by trained infosec professionals. Often these individuals leverage advanced technology to scan and analyze tremendous amounts of network traffic, as well as isolate suspicious activity.

The most effective cybersecurity strategies blend human resources with advanced technological solutions, such as AI, ML and other forms of intelligent automation to better detect anomalous activity and increase response and remediation time.

## Why Your Organization Should Monitor for Indicators of Compromise

The ability to detect indicators of compromise is a crucial element of every comprehensive cybersecurity strategy. IOCs can help improve detection accuracy and speed, as well as remediation times. Generally speaking, the earlier an organization can detect an attack, the less impact it will have on the business and the easier it will be to resolve.

IOCs, especially those that are recurring, provide the organization with a window into the techniques and methodologies of their attackers. As such, organizations can incorporate these insights into their security tooling, incident response capabilities and cybersecurity policies to prevent future events.

## Examples of Indicators of Compromise

What are the warning signs that the security team is looking for when investigating cyber threats and attacks? Some indicators of compromise include:

- Unusual inbound and outbound network traffic
- Geographic irregularities, such as traffic from countries or locations where the organization does not have a presence
- Unknown applications within the system

- → Unusual activity from administrator or privileged accounts, including requests for additional permissions
- → An uptick in incorrect log-ins or access requests that may indicate brute force attacks
- → Anomalous activity, such as an increase in database read volume
- → Large numbers of requests for the same file
- → Suspicious registry or system file changes
- → Unusual Domain Name Servers (DNS) requests and registry configurations
- → Unauthorized settings changes, including mobile device profiles
- → Large amounts of compressed files or data bundles in incorrect or unexplained locations

## The Difference Between Indicator of Compromises (IoCs) and Indicators of Attack (IoAs)

An Indicator of Attack (IOA) is related to an IOC in that it is a digital artifact that helps the infosec team evaluate a breach or security event. However, unlike IOCs, IOAs are active in nature and focus on identifying a cyber attack that is in process. They also explore the identity and motivation of the threat actor, whereas an IOC only helps the organization understand the events that took place.

**Featured Articles**

CrowdStrike Products

CROWDSTRIKE

# FALCON PREVENT NEXT-GENERATION ANTIVIRUS

Ideal AV replacement combines the most effective prevention technologies with full attack visibility and simplicity

## INDUSTRY-RECOGNIZED LEGACY AV REPLACEMENT

For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, CrowdStrike® Falcon Prevent™ is here to help. Falcon Prevent delivers superior protection with a single lightweight agent that operates without the need for constant signature updates, on-premises management infrastructure or complex integrations. Even the largest organizations can be up and running in minutes with Falcon Prevent.

Certified to replace legacy antivirus products — Independent testing at AV-Comparatives and SE Labs has certified Falcon Prevent's antivirus capabilities. Falcon Prevent has also been validated for PCI, HIPAA, NIST and FFIEC regulatory requirements.

**Named a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)** — In addition to being positioned in the Leaders Quadrant, CrowdStrike is furthest for "completeness of vision," which includes Gartner criteria such as innovation, marketing and product strategies, vertical industry and geographic strategies, as well as the validity of the business model as a whole.

### KEY BENEFITS

- Prevents all types of attacks
- Simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery
- Deploys in minutes and immediately begins protecting your endpoints
- Replaces legacy antivirus quickly and confidently
- Operates seamlessly alongside AV as you migrate to simplify transition
- Provides full attack visibility

CrowdStrike Products

FALCON PREVENT NEXT-GENERATION ANTIVIRUS

# KEY CAPABILITIES

## STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

## INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

## FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

## SIMPLE, FAST AND LIGHTWEIGHT

The cloud-native CrowdStrike Falcon platform and lightweight Falcon agent eliminate complexity and simplify endpoint security operations.

- Falcon operates without constant signature updates, complex integrations or on-premises equipment
- The lightweight agent bears little impact on endpoints, from initial install to day-to-day use — no reboot is required after installation
- Minimal CPU overhead restores system performance and end-user productivity
- It works on Day One, deploys in minutes and is immediately operational
- It is automatically kept up to date with cloud-native architecture and SaaS delivery
- Falcon provides broad platform support including Windows, Windows Server, macOS and Linux
- Automated IOA remediation streamlines the removal of artifacts that may lead to reinfection

## FALCON PREVENT: THE EASIEST AV REPLACEMENT

Better protection

Fast and easy deployment

Optimal performance

Reduced complexity

## ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

**Start Free Trial of Next-Gen AV**

www.crowdstrike.com

**Closing**

Custom Indicators of Attack are available to enable companies to create organization specific rules in addition to the protections provided by CrowdStrike. These additional detections and preventions can be defined based on specific tools and expected behaviors to further enhance the value of the Falcon platform for your organization.

More resources

- CrowdStrike 15-Day Free Trial
- Request a demo
- Guide to AV Replacement
- CrowdStrike Products
- CrowdStrike Cloud Security





**Related Content**

How to Complete Your LogScale Observability Strategy with Grafana

Securing private applications with CrowdStrike Zero Trust Assessment and AWS Verified Access

# Going Beyond Malware: The Rise of "Living off the Land" Attacks

May 7 2019 Mark Goudie Endpoint & Cloud Security

*This article was originally published on CSO, April 30, 2019*

If you're living off the land, there are a few different methods you can use to survive, but you need to use what you find where you are. You do not have the option to bring in supplies to maintain yourself. If you are looking for someone living off the land, you must hunt — as they have blended into their new environment.

The same is true of cybersecurity because there is no silver bullet that can identify all types of threats at all times, especially when the adversary is using your tools they found in the environment. The ability to block advanced threats improves each year, but sophisticated adversaries are determined and creative, and their techniques evolve just as quickly.

While malware continues to be a tool often used in the initial intrusion, it is often only the precursor to an attack, not the ultimate objective. This initial intrusion is leading to more sophisticated and stealthy techniques, such as "living off the land" (LOTL), tradecraft that uses native tools already present on the system to accomplish the adversaries' main objective.

LOTL tactics, which do not involve malware, have picked up significantly in the world of cyber espionage in recent years. In fact, malware-free attacks in general have surged in recent years, accounting for 40 percent of the total number of cyberattacks globally last year: according to the 2019 CrowdStrike® Global Threat Report, attackers continue to shift to defense evasion methods, like living off the land techniques, to remain undetected. The longer an attacker can "dwell" or remain undetected in an environment, the more opportunity they have to find, exfiltrate and destroy data or operations.

The purpose of living off the land is two-fold. By using such features and tools, attackers are hoping to blend into the victim's network and hide their activity in a sea of legitimate processes. Secondly, even if malicious activity involving these tools is detected, it is much harder to attribute attacks. If everyone is using similar tools, it's more difficult to distinguish one group from another.

This raises a few questions: What do we do differently to avoid such attacks? When prevention fails, what do we have left to protect our organizations? How can we discover gaps as fast as possible?

Having techniques in play to detect and respond to ongoing attacks quickly is just as important as prevention. Here are a few options organizations can use:

## Compromise Assessment

A compromise assessment (CA) has the briefing of answering the key question "Am I compromised?" This is an exercise where current and historical events are examined to answer the key question. To effectively answer this question you must use tools that will identify signs of historical attacks, such as suspicious registry keys and suspicious output files, as well as identifying active threats. Many sophisticated adversaries spend months and years in their victims' networks without being detected and the CA historical analysis is critical to identifying if this has happened.

## Stopping "Silent Failure"

Regardless of how advanced your defenses are, there's a chance that attackers will do an "end run" on your security solution and slip through to gain access to your environment. Conventional defenses don't know and can't see when this happens, resulting in "silent failure." When silent failure occurs, it can allow attackers to dwell in your environment for days, weeks or even months without raising an alarm. Hence, more organizations are considering endpoint detection and response (EDR) solutions to address the incidents that aren't being handled adequately by their existing defenses. The solution lies in continuous and comprehensive visibility into what is happening on your endpoints in real time.

## Account Monitoring

Account monitoring and management controls can detect and prevent unauthorized activities by providing full visibility into work environments. It enables preventing loss of data due to such activities and violations of credentials, while allowing resource owners to control who has access to the data and indicating whether the access is inappropriately granted.

## Application Inventory

This proactively identifies outdated and unpatched applications and operating systems so you can securely manage all the applications in your environment. Streamlining your application inventory with an IT hygiene solution solves security and cost problems simultaneously. Visibility enabled via IT hygiene prevents exploits related to patches and system updates. It also optimizes your software configuration. Real-time and historical views of application usage identify unused software that can be removed, potentially saving your organization thousands of dollars in unnecessary licensing fees.

## Asset Inventory

Asset Inventory shows you what machines are running on your network and allows you to deploy your security architecture effectively to ensure that no rogue systems are operating behind your walls. It enables security and IT ops to differentiate between managed, unmanaged and unmanageable assets in your environment and take appropriate steps to improve overall security.

### Additional Resources

- *Download the CrowdStrike 2020 Global Threat Report*
- *Learn how the CrowdStrike Falcon®® endpoint protection platform stops malware-free threats with next-gen behavioral analysis tools.*
- *Download the white paper: "Endpoint Detection and Response: Automatic Protection Against Advanced Threats."*
- *Learn more about CrowdStrike Falcon® Discover™ IT Hygiene solution.*