

<p>4. The solution must be able to detect and prevent the following:</p> <ul style="list-style-type: none"> - exploitation behavior using IOAs and no signatures. - ransomware behavior using Behavior IOA patterns and no signatures. - file-less malware using Behavior IOA patterns. - malware-free tradecraft using Behavior IOA patterns. - BIOS level attacks - Privilege Escalation - Exfiltration - Connection to malicious command and control destinations 	<p>Y</p>	<p>Falcon Prevent simplifies operations with signatureless protection and software-as-a-service (SaaS) delivery. It also has Machine learning and artificial intelligence to prevent known and unknown malware, and behavior-based indicators of attack (IOAs) which prevent sophisticated attacks, including ransomware and fileless and malware-free attacks. Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities.</p> <p>Refer to Page 1-2, Signatureless based attack protection.pdf</p> <p>CrowdStrike becomes the first endpoint protection solution provider to integrate firmware attack detection capability, shining a bright light into one of the last remaining dark corners of the modern PC: the BIOS.</p> <p>Refer to Page 1, Bios Level Attack Prevention.pdf Source: https://www.crowdstrike.com/blog/crowdstrike-first-to-deliver-bios-visibility/</p> <p>Falcon Host or also known as Falcon Sensor offers prevention against malware. But it expands beyond just malware protection by also offering prevention against advanced targeted attacks and attacks that do not use malware, filling the wide gap left by solutions that primarily focus on malware. Falcon Host uses the right detection and prevention feature at the right time to prevent breaches across the entire attack continuum.</p> <p>Attack Unfold: Credential Theft / Privilege Escalation</p> <p>Refer to Page 1, Privilege Escalation Prevention.pdf</p> <p>Falcon Host offers prevention against malware. But it expands beyond just malware protection by also offering prevention against advanced targeted attacks and attacks that do not use malware, filling the wide gap left by solutions that primarily focus on malware. Falcon Host uses the right detection and prevention feature at the right time to prevent breaches across the entire attack continuum.</p> <p>Final Objective: E.G. Data Exfiltration</p> <p>Refer to Page 1, Data Exfiltration Prevention.pdf</p> <p>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.</p> <p>Refer to page 6, Comprehensive prevention.pdf Source: https://www.crowdstrike.com/products/faq/</p>
<p>5. The solution must be able to enrich a detected event with its own threat intelligence and not any third-party intelligence including mapping of the technique, tactic and procedure (TTP) against the MITRE ATT&ACK framework.</p>	<p>Y</p>	<p>For unparalleled alert context and visibility, Falcon Prevent:</p> <ul style="list-style-type: none"> - 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 <p>Refer to Page 1, MITRE ATT&ACK framework.pdf</p> <p>Falcon Insight XDR key capabilities</p> <p>Industry-leading threat intel</p> <p>Built-in world-class threat intelligence bolsters detection and supercharges your SOC. From automatic sandbox submissions to in-depth actor profiles, get complete understanding of the threat and adversary behind it.</p> <p>Refer to page 1, Falcon Insight XDR.pdf Source: https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/</p>

A.2.3 Threat Hunting and Response		
<p>1. The service provider must provide 24x7 Managed Threat Hunting Service, supported by experienced and certified analysts or incident responders for the remote response on endpoint incidents/events</p>	<p>Y</p>	<p>Falcon OverWatch is CrowdStrike's managed threat hunting service, built on the CrowdStrike Falcon platform. OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies.</p> <p>OverWatch is comprised of an elite team of cross-disciplinary specialists who harness the massive power of the CrowdStrike Threat Graph, enriched with CrowdStrike threat intelligence, to continuously hunt, investigate and advise on sophisticated threat activity in customer environments. Armed with cloud-scale telemetry and detailed tradecraft on more than 130 adversary groups, OverWatch provides unparalleled ability to see and stop the most advanced threats.</p> <p>Refer to Page 1, 24x7 Managed Threat Hunting Service.pdf</p>
<p>2. The service provider must have pre-built threat hunting applications and queries</p>	<p>Y</p>	<p>CrowdStrike Falcon provides multiple approaches to threat hunting.</p> <p>The Investigate App options allow administrators to search for indicators of compromise in their environment.</p> <p>The Event Search functionality is for power users who want to access all of their data in the CrowdStrike Threat Graph</p> <p>Refer to Page 1-3, How to Hunt for Threat Activity with Falcon Endpoint Protection.pdf Source: https://www.crowdstrike.com/blog/tech-center/hunt-threat-activity-falcon-endpoint-protection/</p>
<p>3. The service provider must be able to get context from indicators such as IP's, URL's, domains, or hashes using the tools within the platform, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others)</p>	<p>Y</p>	<p>Hunting and Investigation</p> <p>Falcon contains a suite of powerful search tools that allow you to analyze, explore, and hunt for suspicious or malicious activity in your environment. These tools include the pre-made search dashboards in the various Falcon apps as well as the ability to run custom queries on the page in the Investigate App.</p> <ul style="list-style-type: none"> -Host Search -Hash Search -User Search -Source IP Search -Bulk Hash Search -Event Search <p>Refer to pages 1,2,13,15-17, Hunting and Investigation.pdf Source: https://falcon.crowdstrike.com/documentation/page/f4c86392/hunting-and-investigation#m5r0aadd</p> <p>The Events Data Dictionary provides reference information about the events found in Investigate > Event Search. Event Search helps you get complete visibility into all hosts running the Falcon sensor.</p> <ul style="list-style-type: none"> -HostUri -ReferrerUri <p>Refer to page 1-2, Event search - URL.pdf Source: https://falcon.crowdstrike.com/documentation/page/e3ce0b24/events-data-dictionary#see9ec41</p> <p>The Falcon agent is constantly monitoring and recording endpoint activity and streaming it to the CrowdStrike Threat Graph in the cloud. The data gathered by Falcon is metadata, including things like process execution, network connections, file system activity, user information, service details, script activity and admin tool usage.</p> <p>Refer to page 1, How to Hunt for Threat Activity with Falcon Endpoint Protection.pdf Source: https://www.crowdstrike.com/blog/tech-center/hunt-threat-activity-falcon-endpoint-protection/</p> <ul style="list-style-type: none"> MITRE Heat Map Account Discovery Windows Management Instrumentation External Remote Services Scheduled Task/Job External Remote Services Account Discovery Disable or Modify System Firewall <p>Refer to page 19-20, CrowdStrike Report 2021 ThreatHunting.pdf</p>

<p>4. The solution shall be able to isolate "at-risk" endpoints, including the blocking the launching of suspicious or malicious applications.</p>	<p>Y</p>	<p>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.</p> <p>Refer to Page 1, Comprehensive prevention.pdf Source: https://www.crowdstrike.com/products/faq/</p> <p>Powerful response actions allow you to contain (isolate) and investigate compromised systems, and Falcon Real Time Response capabilities provide direct access to endpoints under investigation. This allows security responders to run actions on the system and eradicate threats with surgical precision.</p> <p>Refer to Page 1, Isolation.pdf</p> <p>CrowdStrike Falcon® capability is also referred to as "network quarantine" or "network isolation" and is typically used by administrators to remove an infected (or possibly infected) system from the network.</p> <p>Refer to Page 1 of How to Contain an Infected System With CrowdStrike Falcon.pdf Source: https://www.crowdstrike.com/resources/videos/how-to-contain-an-infected-system/</p>
<p>5. The solution shall allow blacklisting and whitelisting of hashes manually through the solution.</p>	<p>Y</p>	<p>Falcon allows you to upload hashes from your own black or white lists. To enable this navigate to the Configuration App, Prevention hashes window, and click on "Upload Hashes" in the upper right-hand corner.</p> <p>Please refer to Page 1, Prevent Malware with Custom Blocking in CrowdStrike Falcon.pdf Source: https://www.crowdstrike.com/blog/tech-center/how-to-prevent-malware-with-custom-blacklisting/</p>
<p>6. The solution shall provide remote response by administrators, analysts, or incident responders such as containment, deleting files, killing process among others without the need for additional tools or agents.</p>	<p>Y</p>	<p>Powerful response actions allow you to contain and investigate compromised systems, and Falcon Real Time Response capabilities provide direct access to endpoints under investigation.</p> <p>Please refer to Page 1, Falcon Real Time Response.pdf</p> <p>Real Time Response is a powerful tool that gives security administrators the ability to remotely access systems for administration tasks, remediation actions or forensics collection, etc. without requiring physical access to the system.</p> <p>Refer to Page 1, How to Remotely Remediate an Incident.pdf Source: https://www.crowdstrike.com/blog/tech-center/remotely-remediate-real-time-response/</p>
<p>7. The solution shall provide root cause analysis of all identified malicious activity.</p>	<p>Y</p>	<p>The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.</p> <p>Refer to Page 1, Root Cause Analysis - Insight.pdf</p> <p>CrowdStrike IR Tracker The benefit of using a tool like the CrowdStrike IR Tracker is that it provides a single place for synthesizing key incident information.</p> <p>The CrowdStrike IR Tracker also helps ensure that the root cause of the incident gets identified, so your organization can remediate the vulnerabilities that were exploited and led to the incident.</p> <p>Refer to pages 1 and 3, CrowdStrike Services Releases From Incident Response Tracker.pdf Source: https://www.crowdstrike.com/blog/crowdstrike-releases-digital-forensics-and-incident-response-tracker/</p>

<p>1. Security Information and Event Management (SIEM)</p> <p>1. The solution shall 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 time period. The agencies must be able to request customized dashboards and ad-hoc reports from the service provider.</p>	<p>Y</p>	<p>Trends will provide an 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 time period.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>Splunk Enterprise Security includes a number of built-in dashboards that provide real-time visibility into security events and help security analysts identify and respond to security threats. Here are some of the key built-in dashboards:</p> <p>Incident Review. View a summary of all security incidents and allows analysts to drill down into individual incidents to investigate and respond to security threats.</p> <p>Asset Investigator. See a comprehensive view of all assets in your IT infrastructure, including hosts, applications, and users, and investigate asset-related security incidents.</p> <p>Threat Activity. Get a real-time view of threat activity across your IT infrastructure, allowing you to identify potential threats and respond to them quickly.</p> <p>Splunk Enterprise Security provides a number of benefits in terms of visualizations and reports that can help organizations detect and respond to security threats more effectively. Some of the key benefits are:</p> <p>Real-time visibility. See security events in real-time through interactive dashboards and visualizations. This enables you to quickly detect anomalies, investigate incidents, and respond to threats as they happen.</p> <p>Actionable insights. The visualizations and reports in Splunk Enterprise Security provide actionable insights into security events, allowing security analysts to identify patterns and trends that may indicate a potential security breach.</p> <p>Customizable reports. Splunk Enterprise Security comes with a range of built-in reports that cover a variety of security use cases, but you can also customize these reports to meet your specific needs. This can help you get a more accurate and comprehensive view of your security posture.</p> <p>Refer to page 1, Splunk_Visualizations and reports.pdf Source: https://antem.splunk.com/Security/UCI/Prioritized_Actions/Visualizations_and_reports/Prescriptive_Adoption_Motion_-_Visualizations_and_reports</p> <p>Schedule the report so that it runs on a regular interval. Scheduled reports can perform actions each time they run, such as sending report results via email to a set of stakeholders.</p> <p>Refer to page 1, Reporting Manual - Create and edit reports.pdf Source: https://docs.splunk.com/Documentation/SplunkCloud/latest/Report/Createandeditreports</p> <p>After you create a search visualization or save a report, you can add it to a new or existing dashboard. There is also a Dashboard Editor that you can use to create and edit dashboards. The Dashboard Editor is useful when you have a set of saved reports that you want to quickly add to a dashboard.</p> <p>Refer to page 1, About dashboards - Splunk Documentation.pdf Source: https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/SearchTutorial/Aboutdashboards</p>
<p>2. The solution shall be capable to support collection of different types of metadata (e.g., logs, security events, network flows, among others) from data sources and shall include log compression and industry standard encryption at rest and in transit to ensure security of captured data from disclosure to disinterested parties.</p>	<p>Y</p>	<p>The Splunk platform can index any kind of data. In particular, the Splunk platform can index any and all IT streaming, machine, and historical data, such as Microsoft Windows event logs, web server logs, live application logs, network feeds, metrics, change monitoring, message queues, archive files, and so on.</p> <p>Refer to page 1, What data can I index - Splunk Documentation.pdf Source: https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/WhatSplunkcanmonitor</p> <p>Data Encryption in Transit Splunk Cloud uses industry standard SSL/TLS 1.2+ (Secure Sockets Layer/Transport Layer Security) encryption for data in transit. All forwarders and user sessions are secured in this manner. Electronic messaging is secured by opportunistic TLS encryption on email gateways.</p> <p>Data Encryption At Rest Splunk Cloud offers data encryption at rest using Advanced Encryption Standard (AES) 256-bit encryption. Encryption at rest is available as a premium service enhancement that customers can purchase.</p> <p>Refer to page 1-2, Encryption at Rest and in Transit.pdf Source: https://www.splunk.com/en_us/about-splunk/splunk-data-security-and-privacy/cloud-security-at-splunk.html</p>

<p>3. The data sources ingested by the solution shall include at least the events from perimeter security tools, active directory logs, endpoint protection, and endpoint detection and response tools, including events from sensors that may be deployed by the solutions provider, if needed.</p>	<p>Y</p>	<p>Splunk Cloud Platform provides tools to configure many kinds of data inputs, including those that are specific to particular application needs. Splunk Cloud Platform also provides the tools to configure any arbitrary data input types. In general, you can categorize Splunk Cloud Platform inputs as follows:</p> <ul style="list-style-type: none"> - Files and directories - Network events - Windows sources - HTTP Event Collector (HEC) - Metrics <p>Refer to page 1, Getting Data In.pdf Source: https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Data/WhatSplunkcanmonitor</p> <p>Splunk comes with tons of apps and add-ons that provide integrations and insights into different solutions. The following data sources' categories are some examples that are supported by the platform:</p> <ul style="list-style-type: none"> -Firewall -Directory Service -Endpoint -Others <p>Refer to page 1, Discover Apps - Splunk.pdf Source: https://splunkbase.splunk.com/apps</p>										
<p>4. The maximum aggregate daily data ingestion shall be as follows:</p> <table border="1" data-bbox="167 614 612 730"> <thead> <tr> <th>Agency</th> <th>Daily Event Log Aggregate Size in Gigabytes (GB)</th> </tr> </thead> <tbody> <tr> <td>BTr</td> <td>17 GB</td> </tr> <tr> <td>GSIS</td> <td>24 GB</td> </tr> <tr> <td>SSS</td> <td>48 GB</td> </tr> <tr> <td>PDIC</td> <td>15 GB</td> </tr> </tbody> </table>	Agency	Daily Event Log Aggregate Size in Gigabytes (GB)	BTr	17 GB	GSIS	24 GB	SSS	48 GB	PDIC	15 GB	<p>Y</p>	<p>The proposed SIEM has the daily data ingestion licenses based on the requirement;</p> <p>Refer to Bill of Materials</p>
Agency	Daily Event Log Aggregate Size in Gigabytes (GB)											
BTr	17 GB											
GSIS	24 GB											
SSS	48 GB											
PDIC	15 GB											
<p>5. The service shall have content packs that are prebuilt configurations for common security use cases that provide sets of rules, alarms, baselines, views, reports, variables, and watchlists.</p>	<p>Y</p>	<p>Overview of the Splunk App for Content Packs</p> <p>Splunk Content Packs provide prepackaged content that you can use to quickly set up your Splunk IT Service Intelligence (ITSI) or IT Essentials Work (ITE Work) environment. This content can include configured KPI base searches, service templates, saved glass tables, and other objects for use within ITSI or ITE Work.</p> <p>Refer to page 1, Splunk Content Packs.pdf Source: https://docs.splunk.com/Documentation/ContentPackApp/2.0.0/Overview/Overview</p> <p>Splunk Security Essentials provides out-of-the-box security use cases and actionable security content to begin addressing threats and assessing gaps quickly and efficiently. You can leverage the wide-ranging use case library to eliminate gaps in defensive posture, implement detections, measure and justify new sources of data based on coverage of threats and risks to the business.</p> <p>Security content library</p> <ul style="list-style-type: none"> -Browse, bookmark and deploy over 900 security detections with a few clicks. -Find the right security content by filtering via use case, threat, data source or cybersecurity framework. -Stay ahead of threats with content that pulls the latest detections from Splunk Threat Research Team. <p>Refer to page 1, Security Monitoring - Splunk.pdf Source: https://info.splunk.com/Security/UCF/Foundational_Visibility/Security_monitoring</p> <p>Splunk Enterprise Security includes more than 100 dashboards that provide integrated views and communicate key data that might be customized and shared with intended end users. Splunk Enterprise Security dashboards identify and investigate security incidents, reveal insights in your events, accelerate incident investigations, monitor the status of various security domains, and audit your incident investigations and your ES deployment.</p> <p>Refer to page 1, Use Splunk Enterprise Security - Introduction to the dashboards.pdf Source: https://docs.splunk.com/Documentation/ES/7.2.0/User/Domaindashboards</p>										

<p>5. The service shall provide advanced security capabilities, such as User and Entity Behavioral Analytics (UEBA), natively within its own platform.</p> <p>7. The solution must integrate with the global threat intelligence subscription service for data enrichment to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.</p> <p>8. The solution must be able to generate and send actionable items to the automation and orchestration tool as well as generate and send alerts to both service provider and agency analysts and incident responders.</p>	<p>Y</p>	<p>Splunk Enterprise Security (ES)</p> <p>Fast, ML-powered threat detection</p> <p>Defend against threats with advanced security analytics, machine learning and threat intelligence that focus detection and provide highly-fidelity alerts to shorten time to respond and raise true positive rates.</p> <p>Refer to page 1-9, Splunk Enterprise Security - Splunk.pdf</p> <p>Source https://www.splunk.com/en_us/products/es/enterprise-security.html</p> <p>With unparalleled search and reporting, advanced analytics, integrated intelligence, and prepackaged security content, Splunk ES accelerates threat detection and investigation, letting you determine the scope of high-priority threats to your environment so you can quickly take action.</p> <p>Refer to page 1 - 2, Splunk Enterprise Security Product Brief.pdf</p> <p>Splunk Enterprise Security has a comprehensive Threat Intelligence framework that can integrate with several open-source and premium solutions.</p> <p>The Threat Intelligence framework is a mechanism for consuming and managing threat feeds, detecting threats, and alerting. The framework consists of modular inputs that collect and emit threat intelligence data, lookup generation searches to reduce data to optimize performance, searches to correlate data and alert on the results, and data modeling to accelerate and store results. This framework also includes a number of audit dashboards that allow introspection into threat intelligence retrieval, normalization, persistence, and analysis.</p> <p>This framework is one of the frameworks in Splunk Enterprise Security with which you can integrate.</p> <p>Refer to page 1, Threat Intelligence framework in Splunk ES.pdf</p> <p>Source: https://dev.splunk.com/en/enterprise/docs/devtools/enterprise-security/threat-intelligence-framework/</p> <p>Cyber Threat Intel, a robust cybersecurity application developed on the Splunk platform, empowers users to monitor assigned alerts effectively. By utilizing the application, users can proactively avoid potential threats and acquire valuable insights that can be acted upon. It facilitates seamless collaboration, automates tasks, and ensures compliance effortlessly. By embracing Cyber Threat Intel, organizations can strengthen their security operations and confidently protect their digital assets.</p> <p>Refer to page 1, Cyber Threat Intel - Splunkbase.pdf</p> <p>Source: https://apps.splunk.com/apps/650/</p> <p>The Cyber Vision platform has been successfully integrated with global technology solutions such as Palo Alto Cortex SOAR, Anomali Cyware TTP platform as well as SIEMs such as IBM QRadar, Splunk, and LogRhythm.</p> <p>Refer to page 16 of About Cyble.pdf</p>
<p>9. The service provider shall ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidences or 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.</p>	<p>Y</p>	<p>The Splunk app prepares cases with all of the relevant alerts and events from Splunk. There are two ways to ingest these cases into Chronicle SOAR: pull based, and push based methods.</p> <p>Chronicle SOAR: pull based, and push based methods.</p> <p>The first method is called pull based. Using this method, in order to ingest cases into Chronicle SOAR, you need to configure the Splunk Pull Connection, which pulls cases from the Splunk app. This method doesn't require any additional configuration in the Splunk app.</p> <p>The second method is called push based. Using this method, the Splunk app performs API calls to Chronicle SOAR to add a new case. In order to work with this method, you need to generate a Chronicle SOAR API key and add a Chronicle SOAR URI in the configuration of the app.</p> <p>Refer to page 1, Splunk - Chronicle - Integration.pdf</p> <p>Source: https://cloud.google.com/chronicle/docs/soar/markdown/prepare-cases-integrations/splunk</p>
<p>9. The service provider shall ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidences or 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.</p>	<p>Y</p>	<p>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 or 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.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_V1.docx</p> <p>Refer to Bill of Materials</p> <p>Logs beyond 12 months will be archived and shared to the agencies in an agreed file format. Agencies will provide a storage repository for the archived logs.</p>

<p>10. The service provider shall ensure that the data ingested from the insurance cluster is not shared or disclosed to or accessed by parties not mentioned in the contract unless explicitly granted permission by the cluster.</p>	<p>Y</p>	<p>Trends adheres to Splunk Cloud Security data Retention Protection and Cloud Security policies and standards</p> <p>Cloud Security at Splunk</p> <p>Cloud Infrastructure Splunk uses a range of technologies to prevent unauthorized access or compromise of Splunk's network, servers or applications, which include such things as logical and physical controls to segment data, systems and networks. Splunk monitors demarcation points used to restrict access such as firewalls and security group enforcement points. Remote users must authenticate with two-factor authentication prior to accessing Splunk networks containing customer content.</p> <p>Splunk Employee and User Authentication Authorized users supporting the delivery of Splunk services must identify and authenticate to the network, applications and platforms using their user ID and password.</p> <p>Refer to pages 1-3, Cloud Security at Splunk _ Splunk.pdf Source: https://www.splunk.com/en_us/about-splunk/splunk-data-security-and-privacy/cloud-security-at-splunk.html</p> <p>In certain locations, you may have rights under data protection law, such as to request access to or correction, deletion, or transfer of your Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our data request form, and we will respond as soon as reasonably practicable consistent with applicable law. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.</p> <p>Refer to page 2, Splunk Privacy Policy.pdf Source: https://www.splunk.com/en_us/legal/privacy-policy.html</p>
<p>A.4 Security Orchestration, Automation and Response (SOAR)</p>		
<p>1. The solution must be able to integrate with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass</p>	<p>Y</p>	<p>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 uses 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.</p> <p>Chronicle SOAR enables modern, fast and effective response to cyber threats by combining playbook automation, case management and integrated threat intelligence in one cloud-native, intuitive experience.</p> <p>Refer to page 1, datasheet-chronicle-soar.pdf</p> <p>The Splunk app prepares cases with all of the relevant alerts and events from Splunk. There are two ways to ingest these cases into Chronicle SOAR: pull based, and push based methods.</p> <p>The first method is called pull based. Using this method, in order to ingest cases into Chronicle SOAR, you need to configure the Splunk Pull Connector, which pulls cases from the Splunk app. This method doesn't require any additional configuration in the Splunk app.</p> <p>The second method is called push based. Using this method, the Splunk app performs API calls to Chronicle SOAR to add a new case. In order to work with this method, you need to generate a Chronicle SOAR API key and add a Chronicle SOAR URI in the configuration of the app.</p> <p>Refer to page 1, Splunk - Chronicle - Integration.pdf Source: https://cloud.google.com/chronicle/docs/soar/marketplace-integrations/splunk</p>
<p>2. The solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting</p>	<p>Y</p>	<p>Track real-time SOC metrics and KPIs:</p> <p>Choose from out-of-the-box interactive reports and dashboard templates to see how your team is performing on the metrics that matter to you - from response rates to cases closed to improvement over time.</p> <p>Refer to page 5, chronicle-security-operations.pdf Source: https://chronicle.security/suite/soar/</p> <p>Edit - users can duplicate reports to the shared and personal folders, share reports, edit reports, download reports, and delete shared reports.</p> <p>Refer to page 1, using-advanced-reports.pdf Source: https://cloud.google.com/chronicle/docs/soar/monitor-and-report/soar-reports/using-advanced-reports-looker</p>

<p>3. The solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner</p>	<p>Y</p>	<p>The platform provides an intuitive user interface that allows security analysts to investigate incidents, create workflows, and automate response actions without requiring extensive coding knowledge. Chronicle SOAR also uses machine learning to improve its accuracy and speed in identifying and responding to security incidents.</p> <p>Refer to page 1, chronicle-soar-overview.pdf Source: https://cloud.google.com/chronicle/docs/soar/overview-and-introduction/soar-overview</p>
<p>4. The solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization</p>	<p>Y</p>	<p>Automatically group related alerts into threat-centric cases: Patented technology automatically groups contextually related alerts into a single threat-centric case, enabling a single analyst to efficiently investigate and respond to a threat.</p> <p>Conduct context-rich investigations: Integrate threat intelligence at every step and visualize the most important contextual data for each threat – who did what, and when – and the relationships between all involved entities attached to an event, product, or source.</p> <p>Refer to page 4, chronicle-security-operations.pdf Source: https://chronicle.elevio.com/secure/soar/soar</p>
<p>5. The solution must be an open architecture that allows for easy connectivity and integrations to any existing system, bringing them all together into a single, contextual language. Integration with other solutions can either be out of the box or customized.</p>	<p>Y</p>	<p>The Chronicle Marketplace acts as the customer's toolbox, holding a wide range of utilities and options to choose from, including:</p> <p>Integrations: includes integrations to third party applications and custom integrations that you have built in the IDE.</p> <p>There are three types of integrations you can see in the Chronicle Marketplace:</p> <p>Commercial – integrations to third party applications which have been developed by Chronicle – including new and updated ones Community – integrations published by users (which have been validated by Chronicle and which will appear with user details next to them) Custom – integrations which you have created and which are only displayed on your Chronicle Marketplace</p> <p>Refer to page 1, Using the Chronicle Marketplace.pdf Source: https://cloud.google.com/chronicle/docs/soar/marketplace/using-the-marketplace</p> <p>Chronicle Marketplace allows you to get the most out of the incorporated solutions by using integrations, investigating threats, and automating your SOC team's work.</p> <p>Please see list of solutions that are supported out of the box by Chronicle marketplace for integrations.</p> <p>Refer to page 1, Chronicle Marketplace integrations.pdf Source: https://cloud.google.com/chronicle/docs/soar/marketplace-integrations</p>
<p>6. The solution must be able to accelerate security incident processes by automating or semi automating workflows</p>	<p>Y</p>	<p>Chronicle SOAR is a powerful security orchestration, automation, and response platform that helps organizations to enhance their security posture by automating security workflows, reducing response times, and improving the accuracy of security operations.</p> <p>Refer to page 1, chronicle-soar-overview.pdf Source: https://cloud.google.com/chronicle/docs/soar/overview-and-introduction/soar-overview</p>
<p>7. The solution must be include out of the box or customizable playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. Playbooks deployed shall include at least:</p> <ul style="list-style-type: none"> - Phishing enrichment and response - Malware endpoint response - Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc) - Unusual browsing activity - Web attack profiling and blacklisting 	<p>Y</p>	<p>Using predefined widgets in Playbook views They have been defined by Chronicle SOAR experts in order to return specific information for the action, thereby reducing the time required to customize and build the bespoke Playbook view.</p> <p>Refer to pages 1-2, Using predefined widgets in Playbook views.pdf Source: https://chronicle-soar.elevio.help/en/articles/798-using-predefined-widgets-in-playbook-views</p> <p>Working with Playbook Blocks Blocks are mini playbooks that users can create and reuse in other playbooks. The Blocks can implement workflows and logical decisions that might be useful in multiple playbooks</p> <p>Refer to pages 1-5, Working with Playbook Blocks - Chronicle SOAR Product Documentation.pdf Source: https://chronicle-soar.elevio.help/en/articles/439-working-with-playbook-blocks</p> <p>Simplify built-in playbooks See list of built-in / customize playbooks for reference.</p> <ul style="list-style-type: none"> -Brute Force Attempt -Virus Found -Admin Login Fail -Excessive Traffic Inbound (streaming, web, etc) -Login at off hours Night: Admin login in non-working hours 22:00-06:00 -Malware Infections -Malicious Website -Indicators of Compromise: Web Server -Spear Phishing Campaign <p>Refer to pages 1-3, 6, 10, 11, 18, 23, 24, 44, 64, 76, Simplify built-in playbooks.pdf</p>

<p>8. The solution should provide pre-set and customizable KPI metrics to monitor threat response efficacy and team performance.</p>	<p>Y</p>	<p>Track real-time SOC metrics and KPIs:</p> <p>Choose from out-of-the-box interactive reports and dashboard templates to see how your team is performing on the metrics that matter to you — from response rates to cases closed to improvement over time.</p> <p>Refer to page 5, chronicle-soar-overview.pdf Source: https://chronicle.security/suite/soar/</p> <p>Dashboards & Metrics</p> <ul style="list-style-type: none"> - Customizable Large Dashboards Screen - Custom KPI's & Metrics - Recommended KPI's & Metrics (e.g. Human Workload, Bottlenecks etc.) - SLA Tracking & Reporting - Thresholds & Alerting - Exporting to Report <p>Refer to page 1, Pre-set (and customizable) KPI metrics.pdf</p>
<p>B. Vulnerability Management and Penetration Testing</p>		
<p>B.1 Vulnerability Management</p>		
<p>1. The solution provided must be a cloud based service, integrated within the SIEM, that shall give immediate global visibility into where the Agency IT system might be vulnerable to the latest internet threats and how to protect them.</p>	<p>Y</p>	<p>Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.</p> <p>Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment.</p> <p>Refer to page 1, crowdstrike-falcon-spotlight-data-sheet.pdf</p> <p>The CrowdStrike Falcon Spotlight Vulnerability Data Technical Add-on for Splunk allows CrowdStrike customers to retrieve CrowdStrike Spotlight Vulnerability data from CrowdStrike Falcon Instance that have the Spotlight module enabled via API.</p> <p>Refer to page 3 - 5 of CrowdStrike Falcon Spotlight Vulnerability Data Add-on for Splunk.pdf</p>
<p>2. It should be able to continuously identify threats and monitor unexpected changes in the network before they turn into breaches. The solution can be agentless or agent-based if continuous monitoring is required on specific systems.</p>	<p>Y</p>	<p>Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.</p> <p>Refer to page 2, crowdstrike-falcon-spotlight-data-sheet.pdf</p>
<p>3. The solution should be able to scan systems anywhere in the Agency environment, from the same console; whether the asset is on the perimeter, the internal network, or cloud environments (such as Amazon Web Services, Oracle Cloud, Microsoft Azure or Google Cloud) with the ability to create custom reports showing each audience just the level of detail it needs to see.</p>	<p>Y</p>	<p>CrowdStrike-Falcon-Spotlight 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.</p> <p>Refer to page 1, How to Install Falcon in the Data Center.pdf Source: https://www.crowdstrike.com/blog/tech-center/install-falcon-datacenter/</p> <p>Customized Scheduled Reports - Reported based off dashboards or other data sources can be generated and sent automatically on a specified schedule.</p> <p>Refer to page 5, How to Use CrowdStrike Dashboards.pdf Source: https://www.crowdstrike.com/blog/tech-center/customizable-dashboards/</p>
<p>4. The solution should be able to identify and prioritize critical vulnerabilities and risks to enable the agencies to prioritize the remediation of the highest business risks using trend analysis, zero-day and patch impact predictions.</p>	<p>Y</p>	<p>Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.</p> <p>Refer to page 1, crowdstrike-falcon-spotlight-data-sheet.pdf</p>

<p>5. The solution should be able to track vulnerability data across hosts and time, to give a better understanding of the agencies security posture. The reports can be changed through existing pre-built templates, without the need to rescan. The reports can be generated on demand or scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV</p>	<p>Y</p>	<p>This document provides an overview of how to quickly filter and report the real-time vulnerability data in Falcon Spotlight. With custom filters, organizations can create custom views to focus on specific assets, products, and vulnerabilities. Those filters can then be saved for future reference and used to create shareable, custom dashboards.</p> <p>Refer to page 1, How to Use Custom Filters in Falcon Spotlight.pdf Source: https://www.crowdstrike.com/blog/tech-center/spotlight-custom-filters/</p> <p>Create scheduled reports to get automatic, recurring updates of the data that matters most to you. You can download and share your scheduled reports, and receive a notification each time a new report is available.</p> <p>When creating a new scheduled report, you customize settings in four main sections.</p> <ul style="list-style-type: none"> -Report Data: A new scheduled report begins with a Falcon data source that specifies the type of data you want to see in the report. Depending on the data source you select, additional filtering options may be available to narrow the scope of the data that displays. -Report Details -Report Schedule -Notifications <p>In the Report details section, provide basic information that defines your report.</p> <p>File format: Choose a file format for generating your reports.</p> <p>Vulnerability management and host reports: JSON (default) or CSV</p> <p>Dashboard reports: PDF</p> <p>Email: Send scheduled report notifications to a specified list of email addresses in your approved domains. You can designate up to 10 email notification recipients per scheduled report, including people who are not Falcon users.</p> <p>In addition to the scheduled generation of reports, use the Run report option to generate a current report on demand. Just like reports that run on a schedule, notifications are sent to recipients and the report is saved in the report history when processing is complete.</p> <p>Refer to pages 1, 2, 3, 6, and 12, Scheduled Report _Dashboards and Reports_Falcon.pdf Source: https://falcon.crowdstrike.com/documentation/page/d31f69e2/scheduled-reports</p>
<p>6. The solution should be able to automatically gather and analyze security and compliance data in a scalable backend, with provisioning additional capabilities as easy as checking a box.</p>	<p>Y</p>	<p>The resulting dashboard provides a visualization of the filter including a chart regarding remediation compliance. Using the "Settings" menu, each dashboard can be shared for the benefit of other team members, and the bookmark feature can be used for ease of use.</p> <p>Refer to page 1, How to Use Custom Filters in Falcon Spotlight.pdf Source: https://www.crowdstrike.com/blog/tech-center/spotlight-custom-filters/</p> <p>Falcon Spotlight allows you to search for installed patches on your network as part of compliance monitoring. This can be used to show evidence that a system is patched or configured correctly.</p> <p>Monitor patches on Windows-based hosts in your environment within the Falcon console.</p> <ul style="list-style-type: none"> -Identify hosts with active Windows Update patches. -Identify hosts with pending patches that require a reboot. -View patch details for individual hosts. -Export patching reports. <p>Refer to page 1, Vulnerability Management: Installed Patch Monitoring.pdf Source: https://falcon.crowdstrike.com/documentation/page/b8ddb0b4/vulnerability-management-installed-patch-monitoring</p>
<p>7. The solution should be able to proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify the agencies immediately, without the need to schedule scan windows or manage scanning credentials.</p>	<p>Y</p>	<p>This document provides an overview of how to quickly filter and report the real-time vulnerability data in Falcon Spotlight. With custom filters, organizations can create custom views to focus on specific assets, products, and vulnerabilities.</p> <p>Refer to page 1, How to Use Custom Filters in Falcon Spotlight.pdf Source: https://www.crowdstrike.com/blog/tech-center/spotlight-custom-filters/</p> <p>Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.</p> <p>Refer to page 2, crowdstrike-falcon-spotlight-data-sheet.pdf</p>

<p>8. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum:</p> <ul style="list-style-type: none"> - Identification of the specific vulnerabilities, at risk, and/or compromised assets - Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results 	Y	<p>With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.</p> <p>Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network.</p> <p>Falcon Spotlight is always on, seamlessly bridging the gap between vulnerability management and the rest of the Falcon platform, enriching threat detection and intelligence use cases. Simply select a vulnerability within the dashboard to see a wealth of data around threat actors, including threat intelligence reports and additional insights.</p> <p>Utilize the tight integration between the Falcon platform and other Falcon modules for additional in-depth research</p> <p>Refer to page 1-2, crowdstrike-falcon-spotlight-data-sheet.pdf</p> <p>Falcon Spotlight provides custom filters and dashboards and to help companies quickly understand vulnerability data, identify risk and prioritize remediation.</p> <p>Refer to page 1, How to Use Custom Filters in Falcon Spotlight.pdf Source: https://www.crowdstrike.com/blog/tech-center/spotlight-custom-filters/</p> <p>Refer to https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/</p>																				
<p>B.2 Vulnerability Assessment and Penetration Testing (VAPT)</p> <p>1. Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, if any and among others.</p>	Y	<p>This Vulnerability Assessment and Penetration Testing will be performed annually based on agreed schedules and scope with the agencies. The VAPT scope may include targets such as but not limited to network infrastructure, network devices, servers, workstations, applications, (e.g., public-facing web and mobile applications), and APIs, endpoints, hosts and database, including member service systems or kiosks, if any and among others.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0.docx, page 4 - Scope and Definition</p>																				
<p>2. The scope of VAPT shall be at least the following:</p> <table border="1" data-bbox="197 759 698 871"> <thead> <tr> <th>Agency</th> <th>Scope</th> </tr> </thead> <tbody> <tr> <td>BIT</td> <td>7 External resources, up to 80 IP addresses</td> </tr> <tr> <td>GSIS</td> <td>20 External resources, 2 mobile apps, up to 80 IP addresses</td> </tr> <tr> <td>SSS</td> <td>20 External resources, 1 mobile app up to 150 IP addresses</td> </tr> <tr> <td>PDIC</td> <td>8 External resources, up to 80 IP addresses</td> </tr> </tbody> </table>	Agency	Scope	BIT	7 External resources, up to 80 IP addresses	GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses	SSS	20 External resources, 1 mobile app up to 150 IP addresses	PDIC	8 External resources, up to 80 IP addresses	Y	<p>This Vulnerability Assessment and Penetration Testing will be performed annually based on agreed schedules and scope with the agencies. The VAPT scope may include targets such as but not limited to network infrastructure, network devices, servers, workstations, applications, (e.g., public-facing web and mobile applications), and APIs, endpoints, hosts and database, including member service systems or kiosks, if any and among others.</p> <p>The scope of VAPT will be at least the following:</p> <table border="1" data-bbox="1088 817 1700 906"> <thead> <tr> <th>Agency</th> <th>Scope</th> </tr> </thead> <tbody> <tr> <td>BIT</td> <td>7 External resources, up to 80 IP addresses</td> </tr> <tr> <td>GSIS</td> <td>20 External resources, 2 mobile apps, up to 80 IP addresses</td> </tr> <tr> <td>SSS</td> <td>25 External resources, 1 mobile app up to 150 IP addresses</td> </tr> <tr> <td>PDIC</td> <td>8 External resources, up to 80 IP addresses</td> </tr> </tbody> </table> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 16 - ANNEX 5. Scope of Vulnerability Assessment and Penetration Testing</p>	Agency	Scope	BIT	7 External resources, up to 80 IP addresses	GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses	SSS	25 External resources, 1 mobile app up to 150 IP addresses	PDIC	8 External resources, up to 80 IP addresses
Agency	Scope																					
BIT	7 External resources, up to 80 IP addresses																					
GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses																					
SSS	20 External resources, 1 mobile app up to 150 IP addresses																					
PDIC	8 External resources, up to 80 IP addresses																					
Agency	Scope																					
BIT	7 External resources, up to 80 IP addresses																					
GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses																					
SSS	25 External resources, 1 mobile app up to 150 IP addresses																					
PDIC	8 External resources, up to 80 IP addresses																					
<p>3. The service provider shall deliver and maintain a vulnerability database with relevant software version upgrades and security policy update recommendations, inclusive of changes to existing and new vulnerability and threat signatures.</p>	Y	<p>Trends VAPT team shall deliver and maintain a vulnerability database with relevant software version upgrade and security policy updates through various platforms and tools that shall be used to perform the vulnerability and penetration services.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 16 - ANNEX 5. Scope of Vulnerability Assessment and Penetration Testing</p>																				
<p>4. The service provider shall provide online reporting and metrics capability:</p> <ul style="list-style-type: none"> - VAPT results/data (including risk, remediation status, and data compromised, if any) and access to historical test result and trend analysis delivered via the service provider's portal shall be accessible to the agencies. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations. 	Y	<p>Trends will provide online reporting and metric capability. Trends will provide access to agencies to an online reporting portal that will include the VAPT results/ data (including risk, remediation status, and data compromised, if any) and access to historical test result and trends analysis delivered. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 7 - Section 4.4. Communicate</p>																				

<p>6. The service provider shall have predefined fields/templates for the generation of reports, such as, but not limited to:</p> <ul style="list-style-type: none"> - VAPT Report (i.e., Executive Summary, Conclusion for Management Area, and Specific Action Plans) - Security Profiling Results (including reports from automated scanning tools) - Detailed observations and recommendations 	Y	<p>This stage is focused on submitting the report and conducting a presentation.</p> <p>Trends has predefined fields/ templates for the generation of reports, such as but not limited to:</p> <ul style="list-style-type: none"> - VAPT report (i.e., Executive Summary, Conclusion for Management Area, and Specific Action Plans) - Security Profiling Results (including reports from automated scanning tools) - Detailed observations and recommendations. <p>After the results have been meticulously documented in a comprehensive report, this information will be presented to all designated Points of Contact through a formal presentation. Additionally, copies of the reports, available in file formats including but not limited to PDF and Excel, will be submitted via our portal. The portal includes all historical test reports and trend analysis.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 7 - Section 4.4. Communicate</p> <p>Trends provide two (2) types of VAPT report which are Executive Report and Technical Report that includes all the definitions, references, evidences and guide on how findings can be remediated.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 13 - ANNEX 2. Vulnerability Assessment and Penetration Testing Report.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 14 - ANNEX 3. Revalida Report.</p>
<p>6. Common Vulnerability Scoring System values:</p> <ul style="list-style-type: none"> - The service provider shall use CVSS v3.0 or later for risk ranking and prioritizing security vulnerabilities. - The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML. 	Y	<p>The severity rating for vulnerabilities is computed using the Common Vulnerability Scoring System 3.1 (CVSS v3.1) and the response time of findings will be based on the risk rating on each confirmed vulnerability. https://nvd.nist.gov/vuln-metrics/cvss</p> <p>Trends VAPT tools and platform can generate multi-format pre-built reports and can be exported using PDF, MS Excel, XML, CSV, and HTML.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 12 - ANNEX 1. Severity Rating.</p>
<p>7. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to:</p> <ul style="list-style-type: none"> - Windows (all versions) - Linux and other Unix flavors (all versions) - Network and security related equipment, whether software or hardware-based - User profile settings - Advanced password analysis 	Y	<p>During the discovery stage, VAPT engineer will commence the process of discovering, fingerprinting, and identifying vulnerabilities within the host, operating system (OS) and services.</p> <p>for the following, but not limited to:</p> <ul style="list-style-type: none"> - Windows (all versions) - Linux and other Unix flavors (all versions) - Network and security-related equipment, whether software or hardware-based - User profile settings - Advanced password analysis <p>This can be achieved through either manual or automated methods. Automated Vulnerability Assessment employs different scanning tools and in-house scripts. Subsequently, the findings are validated using a manual approach by the engineers to minimize false positives.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 6 - 4.2.1. Perform the Manual and Automated Vulnerability Assessment on the Target.</p>

<p>8. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:</p> <ul style="list-style-type: none"> - Application servers - Authentication servers - Backdoors and remote access services - Backup applications/tools - Database servers - Active Directory, Lightweight Directory Access Protocol (LDAP) - Domain Name Systems (DNS) - Mail servers and Simple Mail Transfer Protocols (SMTP) - Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS) - Network Time Protocols (NTP) - Remote Procedure Calls - Routing protocols - Simple Network Monitoring Protocol (SNMP) - Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) - Virtual Private Network (VPN) - Web and mobile applications - Web servers 	Y	<p>Furthermore, the engineer will perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:</p> <ul style="list-style-type: none"> - Application servers - Authentication servers - Backdoors and remote access services - Backup applications/tools - Database servers - Active Directory, Lightweight Directory Access Protocol (LDAP) - Domain Name Systems (DNS) - Mail servers and Simple Mail Transfer Protocols (SMTP) - Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS) - Network Time Protocols (NTP) - Remote Procedure Calls - Routing protocols - Simple Network Monitoring Protocol (SNMP) - Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) - Virtual Private Network (VPN) - Web and mobile applications - Web servers <p>This can be achieved through either manual or automated methods. Automated Vulnerability Assessment employs different scanning tools, and in-house scripts. Subsequently, the findings are validated using a manual approach by the engineers to minimize false positives.</p> <p>Please see document: TRENDS_VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROCESS_v1.0, page 6 - 4.2.1. Perform the Manual and Automated Vulnerability Assessment on the Target.</p>
C:Threat Intelligence		
<p>1. The solution shall deliver threat intelligence on the following:</p>	Y	
<ul style="list-style-type: none"> - Brand protection - company names/domain 	Y	<p>Cyble Vision works on keywords like Company Name, domains, executive id, logo etc. Vision continuously scans for any exposure of these keywords on Open Internet, Darkweb, Social media platforms, messaging channels like Telegram & Discord, if we identify any activity hampering the Brand of customer, tool immediately generate the alert with severity score.</p> <p>Domain name registration monitoring and search (newly registered domains) to detect suspicious domains or typo-squatted domains that are created to target your brand</p> <p>Refer to page 11, About Cyble.pdf</p>
<ul style="list-style-type: none"> - Social media pages 	Y	<p>Cyble monitors multiple social media platforms, to search for impersonated profiles & accounts of Customer executive, fake pages/groups & websites</p> <p>Refer to page 11, About Cyble.pdf</p>
<ul style="list-style-type: none"> - External Internet Protocol (IP) addresses 	Y	<p>Cyble Vision uses its own Internet scanner, through which on daily basis we're assessing more than 3 billion IP, services running on those assets & associated vulnerabilities. Cyble will regularly monitor all the external facing IP of customers, wherever there's a presence of client keywords at a meta data level like on SSL cert, HTML script, HTTP response string.</p> <p>With our ASM feature, you can</p> <ol style="list-style-type: none"> 1. Discover your domains and sub-domains, their hosting infrastructure along with the details of their discoverability and the IP reputation of these assets. 4. Visualize the dynamic risk score of every IP address to notify you whether there is any security risk or malicious activity reported for that asset to facilitate analysis and resolution of the issue. <p>Refer to page 8, About Cyble.pdf</p>

- Website and mobile application monitoring	Y	<p>Cyble vision monitors for all the fake websites that are misusing client's keywords & logos, Cyble vision also provides Web App scanning services via OWASP TOP 10 vulnerabilities</p> <p>Cyble's Vision monitors multiple app stores such as Google Playstore, Apple, Amazon, Tencent. We do close to real-time detection of the apps through our enterprise product Cyble Vision, and also perform security analysis on them by checking against our malware repositories for early signs of infections or nefarious activities.</p> <p>Website watermarking and monitoring to notify you whenever a fraudster mirrors your website or copies your code to setup a look alike phishing website</p> <p>Detection of fake mobile apps that are hosted on legitimate as well as third party app stores</p> <p>Refer to page 11, About Cyble.pdf</p>
- VIP e-mails	Y	<p>VIP Email monitoring is covered as a part of Executive monitoring Service.</p> <p>Cyble offers VIP/ Executive monitoring spanning social media as well as the Dark web by detecting and notifying you about suspicious activities.</p> <p>Refer to page 12, About Cyble.pdf</p>
- Sector monitoring Financial, Government, Insurance, and Healthcare	Y	<p>Cyble is currently catering to 100+ global BFSI customers, we do extensive research on DW & Open internet to identify issues in BFSI sector. Cyble provides sector & region specific Threat Intel in the form of Advisories, NewsFlashes & Ransomware updates</p> <p>Cyble threat library contains information on 41 sectors and industries.</p> <p>Refer to page 15, About Cyble.pdf</p> <p>Sector monitoring Financial, Government, Insurance, and Healthcare can be search it in Vision Portal</p> <p>Refer to Cyble Sector Monitoring Screenshots.pdf</p>
- Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes	Y	<p>SWIFT code will be considered as a keyword any exposure of that on Darkweb or on Open internet will be indexed on the dashboard itself.</p> <p>Refer to Cyble SWIFT Codes.pdf.pdf</p>
- Credit cards	Y	<p>Cyble is present on all the Darkweb marketplaces, TOR sites, Telegram channels which provides exposed credit card details, on a monthly basis we index around 2-3mn compromised cards on the platform itself, having card numbers, cvv, expiry & PII data of users</p> <p>Refer to page 4, About Cyble.pdf</p>
- GitHub	Y	<p>Platform monitor exposed sensitive codes on all of the platforms like: Github, BitBucket, Postman, Docker Hub</p> <p>Discover the exposure of your sensitive data (API keys, user accounts, access keys, passwords, sensitive IP addresses etc.) and software (application code and builds) via public insecure code repositories such as GitHub and Bitbucket etc.</p> <p>Refer to page 8, About Cyble.pdf</p>
- Custom queries	Y	<p>Client can perform custom queries using Boolean operands in spotlight search against 40+ services</p> <p>The Master Dashboard module in Cyble Vision provides an easy-to-use interface for clients to configure their search keywords, domains, assets and define the alerting rules for events of their interest.</p> <p>Refer to page 17, About Cyble.pdf</p>

- 25 Site take downs for each agency during the duration of the contract (i.e., phishing, social media sites, and others) however, should the agency need additional takedowns, this will be provided by the service provider at no additional cost.	Y	Trends and Cyble is providing takedown services for phishing, fake social media sites, malicious and suspicious domains etc. Refer to page 20, About Cyble.pdf Refer to Bill of Materials
- Scraping databases that contain large amounts of data found in the deep and dark web	Y	Through Cyble big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques. Refer to page 9, About Cyble.pdf
- Third party queries	Y	The agencies can monitor the attack surface exposure of their 3rd Parties with Cyble. Become aware of prominent data leaks, breaches, or ransomware-related breaches across the globe along with any organizational data or customer PII exposed in the breach/leak at a third party (business partner, vendor, consulting firm or service provider etc.) to assess its impact to your business; all these through our updated threat advisories and quick reports. Refer to page 10, About Cyble.pdf
- Investigation	Y	Trends and Cyble dark web monitoring and intelligence team continuously monitors the activities across various open as well as invite-only/private forums to gain early warning intelligence about a potential cyber-attack on a victim, any posts or chatter or messages on dark web forums that could indicate an access or data compromise involving the client organization, its employees, or its vendors. This allows Trends to initiate an appropriate response or conduct an internal investigation to identify the source of the incident. Refer to page 9, About Cyble.pdf
- Threat library	Y	Cyble is currently monitoring 3000+ Threat Actors, 150+ ransomware gangs, 1000+ malware operators & 80 Bn+ Threat indicators are indexed in the platform. Client can search for APT groups, Tools, Targeted Industry, Target Geography, IP details, Ransomware groups etc. Threat Library section, providing detailed intel on global Advanced Persistent Threat Groups, Ransomware groups, Threat Actors, Tools they use, their Aliases, IOCs, Country of Origin, Target Industry & Target Geography for effective monitoring and tracking. Refer to page 15, About Cyble.pdf
2. The threat intelligence solution must, at minimally, harvest data from the following open, technical and closed sources types:	Y	Cyble Vision provide a single dashboard to configure, manage, view and track users and incidents across Deep, Dark Web and Surface Web. It continuously monitors and generate the exposure results. Cyble monitors 6000+ cybercrime forums regularly which form 80% traffic of total Cyber crime markets. Vision on daily basis vision is scanning 4bn+ Digital assets, 40 bn+ OSINT pages, 1000+Malware operations, 3000+ Threat Actors & their TTP. Our Bots & team of researchers are present in various Threat Actor closed Telegram Chat groups, IRC chat rooms, I2P sites, TOR sites, Cybercrime Forums, Ransomware Forums etc, if we find any mention of our client's keywords like; credentials, documents, infra details sensitive codes etc. we immediately provide intelligence to our customers & provide the visibility of same on the dashboard itself. Cyble monitors multiple social media platforms, to search for impersonated profiles & accounts of Customer executive, fake pages/groups & websites Cyble has a group of human analyst performing research Refer to page 7, About Cyble.pdf

- Mainstream Media (including news, information security sites, vendor research, blogs, vulnerability disclosures)	Y	<p>Through Cyble big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.</p> <p>Harvest data from the mainstream media (including news, information security sites, vendor research, blogs, vulnerability disclosures) are being published in The Cyber Express.</p> <p>The Cyber Express by Cyble is a cybersecurity news publication that provides the latest news and analysis about the information security industry.</p> <p>We cover a wide range of topics, including cyber threats and vulnerabilities, data breaches, cybercrime, cyber defense and security, and the latest technologies and tools for protecting against cyber-attacks.</p> <p>Refer to page 1, The Cyber Express, No. 1 Trusted Cybersecurity News Site.pdf Source: https://thecyberexpress.com/firewall-daily/</p>
- Social Media	Y	<p>Detecting social media accounts/profiles (Instagram, Facebook, YouTube, LinkedIn, Reddit) that are created to impersonate the official accounts of the organization</p> <p>Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces</p> <p>Refer to page 9 and 11, About Cyble.pdf</p>
- Forums	Y	<p>Cyble gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces</p> <p>Refer to page 9, About Cyble.pdf</p>
- Paste Sites	Y	<p>Gather intelligence through scraping, API, manual collection, and other methods across a wide range of Deep and Dark Web sources including TOR, I2P, ZeroNet, and Paste Sites.</p> <p>Refer to Cyble Paste Sites - Dark Web & Deep Web Monitoring.pdf.pdf</p>
- Code Repositories	Y	<p>Discover the exposure of your sensitive data (API keys, user accounts, access keys, passwords, sensitive IP addresses etc.) and software (application code and builds) via public insecure code repositories</p> <p>Refer to page 8, About Cyble.pdf</p>
- Threat lists (including spam, malware, malicious infrastructure)	Y	<p>Detecting C2 or Phishing URLs by monitoring spam or phishing emails targeting client brands via spoofing</p> <p>The Platform must be able to create, monitor, automate alert and report for threat on Malware and Malicious Infrastructure related to Customer domain.</p> <p>Refer to page 10 and 12, About Cyble.pdf</p>
- Dark Web (including multiple users of underground communities and marketplaces)	Y	<p>Cyble gathers terabytes (TB) of data daily across dark web and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.</p> <p>Threat intelligence gathered from various sources, ranging from public sources, technical sources, dark web & deep web, Underground forums, special access sites, Code Repositories, Paste bin and human analyst</p> <p>Refer to page 9 and 14, About Cyble.pdf</p>

- Original research from in-house human intelligence analysts	Y	The Cyble Threat Research team also stays at the forefront of cutting-edge threat research by continuously discovering, analyzing, and reporting on emerging threat actors Our dark web monitoring and intelligence team continuously monitors the activities across various open Refer to page 9, About Cyble.pdf
3. The solutions provider must be able to:	Y	Trends and Cyble is providing takedown services for phishing, fake social media sites/accounts, malicious and suspicious domains, fake mobile apps from different app stores
- Detect and take down servers launching phishing attacks	Y	Trends and Cyble is providing takedown services for phishing, fake social media sites, malicious and suspicious domains etc. Refer to page 20, About Cyble.pdf
-Take down of fake applications that impersonate legitimate ones from app stores.	Y	Trends and Cyble is providing takedown services for phishing, fake social media sites, malicious and suspicious domains etc. Refer to page 20, About Cyble.pdf
-Take immediate action on the agencies behalf and provide all the context to execute rapid take-down of malicious servers, websites or social media accounts.	Y	Trends and Cyble is providing takedown services for phishing, fake social media sites, malicious and suspicious domains etc. Refer to page 20, About Cyble.pdf
4. The solution shall be capable to detect leaked Personally Identifiable Information (PIIs) and the agencies information from the deep and dark web, social media, and other forms of instant messaging platforms and provide recommended action plan.	Y	Cyble monitors various Threat Actor closed Telegram Chat groups, IRC chat rooms, I2P sites, TOR sites, Cybercrime Forums, Ransomware Forums etc, if we find any mention of our client's keywords like; PII data, credentials, documents, infra details sensitive codes etc. we immediately provide intelligence to our customer The Platform must be able to create, monitor, automate alert and report for threat on Dark Web. -Compromised PII such as Email ID, Phone number and Address. -Stolen / Compromised Login Credentials and Customer Account Information. Refer to page 10 and 12, About Cyble.pdf
5. The threat intelligence solution must be able to identify fraudulent social media accounts that are impersonating the agencies and its executives	Y	Covered as a Part of Social media monitoring & Executive monitoring services VIP/ Executive monitoring spanning social media as well as the Dark web by detecting and notifying you about following suspicious activity. -Creation of lookalike social media profiles (Twitter handles, Facebook pages, LinkedIn profiles, YouTube channels etc.) Refer to page 12, About Cyble.pdf
6. The solution shall monitor the domains and IP addresses that have bad reputation.	Y	Threat intelligence feed identify new global threats like Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc. Threat Intelligence of IOCs delivered with full context of related entities, such as related hashes, IPs, CVEs and Threat Actors, Threat Vectors, Malwares, Product impacted etc. The contextualized threat information should be delivered in a simple and easy to digest format. Refer to page 8, 14, About Cyble.pdf
7. The service provider shall consume internal and external threat intelligence into its threat analysis process.	Y	Cyble Vision provides "Out to In" visibility to customers, all exposures outside of clients firewall is monitored across 40+ services in Darkweb, Attack Surface, Brand Monitoring. Cyble's Threat Intelligence module is powered by a vast global big data repository of indicators of compromise gleaned from several different sources such as <ul style="list-style-type: none"> • our own and managed global honeypot sensor intelligence network • the open internet, • open-source public threat intelligence sources • premium commercial threat intelligence provider feeds. Refer to page 13, About Cyble.pdf

<p>8. The service provider shall deliver weekly intelligence summary reports on the latest cyber threats, 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.</p>	<p>Y</p>	<p>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.</p> <p>During monthly service performance review, Trends will 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.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>Please see document: TRENDS_CYBER SECURITY INTELLIGENCE MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 9 - 6.1. Policy</p> <p>Furthermore, the Threat Intelligence tool is capable of providing curated daily feed of IOCs by integrating with client's cyber security monitoring platforms. It is also capable of publishing Global Sensor Intelligence Reports on a weekly basis, CTI Operations Reports monthly and Global Ransomware Intelligence Reports on a quarterly basis.</p> <p>Please see document: About Cyble.pdf, page 22 - 2.9. Service Delivery Approach</p>
<p>9. The service provider shall provide 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.</p>	<p>Y</p>	<p>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.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0</p> <p>Please see document: TRENDS_CYBER SECURITY INTELLIGENCE MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 9 - 6.1. Policy</p> <p>Please see document: TRENDS_CYBER SECURITY INTELLIGENCE MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 12 - 6.3.2. Internal Threat Discovery Procedure</p> <p>Furthermore, the Threat Intelligence tool is capable of providing curated daily feed of IOCs by integrating with client's cyber security monitoring platforms. It is also capable of publishing Global Sensor Intelligence Reports on a weekly basis, CTI Operations Reports monthly and Global Ransomware Intelligence Reports on a quarterly basis.</p> <p>Please see document: About Cyble.pdf, page 17-18 - 2.9. Service Delivery Approach</p>
<p>D. Incident Response</p>		
<p>1. The service provider shall review the 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:</p> <ul style="list-style-type: none"> - Escalation process - Incident containment process - Incident eradication process - Incident recovery process - Incident identification process - Process flow 	<p>Y</p>	<p>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.</p> <p>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.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 12 - Annex 8. Cybersecurity Maturity Assessment Sample</p>

<p>2. The service provider shall act as the Incident Response (IR) Manager and facilitate the six (6) phases of IR. The service provider must be on-call and will conduct the IR activities onsite, as necessary (i.e., in cases of breach). The IRs per agency shall cover 200 accumulated hours per year. Beyond the required 200 hours, the agencies shall shoulder the cost. In case the 200 hours allotted for IR is not fully or not consumed, it can be converted to other services, such as training among others, that the provider can render for information security.</p>	<p>Y</p>	<p>TRENDS shall assign an Incident Response (IR) Manager. The Incident Manager is responsible for maintaining the Incident Management Process and facilitating the six (6) phases of IR.</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 14 - 6.9. Incident Manager</p> <p>For the six (6) phases of IR, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 32-36 - Annex 6 – Guidelines in Handling of Specific Security Incidents</p> <p>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.</p> <p>Once the incident is resolved, Onsite Support Engineer or the Client notifies TRENDS Operations Center.</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 17 - Typical Incident Handling Procedure for Information Security Incident</p> <p>For 200 hours allocation, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 38 - Annex 8 Coverage of IR hours</p>
<p>3. The service provider shall conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness trainings to both technical and non-technical audiences of the agencies. The readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.</p>	<p>Y</p>	<p>TRENDS will conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness training to both technical and non-technical audiences of the agencies. The readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.</p> <p>Please see document: TRENDS_Training Plan for Govt Insurance Cluster_v1.0.docx</p> <p>For reference of Annual Incident Response Readiness Training, please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 23, ANNEX 18 – Snippet of Agenda Acceptance for Annual Incident Response Readiness Training (Details Redacted)</p>
<p>4. The service provider shall conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.</p>	<p>Y</p>	<p>During the Transition Phase, TRENDS will conduct process discovery and workshop, develop use cases, create playbooks and runbooks, and conduct tabletop exercises with the client.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>TRENDS will conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.</p> <p>Please see document: TRENDS_Training Plan for Govt Insurance Cluster_v1.0.docx</p> <p>For reference of Sample Tabletop Exercise, please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 10 - Annex 6 - Sample Tabletop Exercise</p> <p>For reference of Annual Incident Response Readiness Training, please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 23, ANNEX 18 – Snippet of Agenda Acceptance for Annual Incident Response Readiness Training (Details Redacted)</p>

<p>5. The Service Provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.</p>	<p>Y</p>	<p>During Transition Phase, 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.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>Part of Trends Service On-Boarding procedure is the due diligence process where in agencies will need to provide their asset inventory & criticality matrix. In this document, the assets shall be plotted against the Information Security Incident Use-cases and the prioritization and severity matrix shall be agreed upon by Trends and the agencies. This document will then be the reference document when customizing the service for each agency.</p> <p>Attack Vectors to which security use cases are aligned to can be found in: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 16 - Attack Vectors</p> <p>For reference of Incident Response Playbook, please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 24, ANNEX 19 – Snippet of Incident Response Playbook (Details Redacted)</p>
<p>6. The service provider shall deliver technical assistance to the agencies CSIRT's during emergency (successful) breach response.</p>	<p>Y</p>	<p>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.</p> <p>For invocation of CSIRT Process, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 18 - 6.1.4 Invocation of Computer Security Incident Response Team</p>
<p>7. The Service Provider shall have a facility to receive client's reported incident (via authorized point of contact from client) for incidents not captured on the monitoring tool.</p>	<p>Y</p>	<p>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:</p> <ul style="list-style-type: none"> •Hotline: 8811-8181 extn: 8703, 8708, 8710 8715, 8716 and 8727 •Trends-SOC Email: soc@trends.com.ph •ivanll ticket: https://mictsv2-ism.trends.com.ph/HEAT/ <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 2 - Annex 1 - Trends Contact Numbers (excerpt from Client Onboarding Presentation)</p>
<p>8. The service provider shall deliver network/firewall/web applications breach response.</p>	<p>Y</p>	<p>During Transition Phase, 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. Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p> <p>Any information security incident having a P1 priority level automatically invokes the CSIRT. The CSI Manager is responsible in mobilizing the CSIRT. The CSIRT is also responsible for providing technical assistance to the agencies' CSIRTs during emergencies or successful breach responses.</p> <p>TRENDS CSIRT is comprised of the following members:</p> <ul style="list-style-type: none"> - 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 (THI) Manager - Service Delivery Manager (SDM) <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN, page 18 - Invocation of Computer Security Incident Response Team (CSIRT)</p> <p>For Typical Incident Handling Procedure for Quality-of-Service Incident, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN, page 17- Typical Incident Handling Procedure for Quality-of-Service Incident</p> <p>For Fix Incident Procedure, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN, page 20 - Fix Incident Procedure</p> <p>For Digital Forensics Overarching Process, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN, page 21 - Section 6.14, Digital Forensics Overarching Process</p> <p>For Guidelines in Handling of Specific Security Incidents, please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN, page 32 - Annex 6 – Guidelines in Handling of Specific Security Incidents</p>

<p>9. The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.</p>	<p>Y</p>	<p>Trends follows Guidelines In Handling of Specific Security Incidents which covers the 6 incident response process in handling malware infections, including malicious code, spyware, and system file hacks:</p> <ul style="list-style-type: none"> - 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 <p>For the detailed process, please refer to: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN, page 32 - ANNEX 6. Guidelines in Handling of Specific Security Incidents</p>
<p>10. The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.</p>	<p>Y</p>	<p>Under the Digital Forensics Overarching Process, Trends shall provide report that includes the root cause analysis which identified the intrusion vector and the mitigating procedures conducted to address network and system vulnerabilities.</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 22 - D. During Engagement</p> <p>Attack Vectors to which security use cases are aligned to can be found in: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 16 - Attack Vectors</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 11 - Annex 7 - Sample Malware Incident Analysis & Recommendation</p> <p>For RCA and DF/CA Report, please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, pages 21-22, ANNEX 16 – Sample RCA Report (Details Redacted) & ANNEX 17 – Sample Digital Forensics/Compromise Assessment Report (Details Redacted)</p>
<p>11. The service provider shall identify indicators of compromise and scan the network to search for other related infected systems.</p>	<p>Y</p>	<p>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.</p> <p>Analyze the symptoms to identify the malware, its propagation, vectors, and countermeasures.</p> <p>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 alerts and logs.</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 32-36 - Annex 6 – Guidelines in Handling of Specific Security Incidents.</p>
<p>12. The service provider shall deliver insider threat investigation, as needed.</p>	<p>Y</p>	<p>Trends is using CrowdStrike Endpoint Detection & Response (EDR) which provides Investigate application that covers different tools such as Search, Hunt, Timelines, Custom Alerts, etc. All of these capabilities is designed to take the complexity out of threat hunting and meant for analysts to deep dive information about the target's movements and activities in their endpoint.</p> <p>The Threat Hunting team will review all the documents and/or any related case to the hypothesis from Threat Hunting Database and request for team's approval to conduct investigation. The following are the critical domains for investigation:</p> <ol style="list-style-type: none"> a) Endpoint Security Logs b) User-behavior Analytics c) Network Threat Analytics d) Application Threat Analytics. <p>Please see document: TRENDS_CYBER SECURITY INTELLIGENCE MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 11 - 6.3.2 Internal Threat Discovery Procedure</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, pages 32-36 - Annex 6 - Guidelines in Handling Specific Security Incidents</p>

<p>13. The service provider shall deliver employee misconduct investigations, as needed.</p>	<p>Y</p>	<p>By using Endpoint Detection & Response (EDR), Trends can provide log information based on activities performed by an endpoint or username. This is done by recording metadata including things like process execution, network connections, file system activity, user information, service details, script activity and admin tool usage.</p> <p>b) User-behavior Analytics. SOCs analyze user behavior anomalies for user and contextual data for insider threats and fraud. TH detect and look for any remaining signs of insider threat activity, such as new process execution, users accessing inappropriate endpoints, activity at unexpected hours or execution of unexpected applications.</p> <p>Please see document: TRENDS_CYBER SECURITY INTELLIGENCE MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 11 - 6.3.2 Internal Threat Discovery Procedure</p>
<p>14. The service provider shall deliver incident and investigation reports.</p>	<p>Y</p>	<p>Once an incident is resolved, an Incident Report should be written and made available to all the actors of the crisis management cell. The following themes should be described:</p> <ul style="list-style-type: none"> •Initial cause of the infection. •Actions and timelines of every important event. •What went right? •What went wrong? <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 32-36 - Annex 6 – Guidelines in Handling of Specific Security Incidents</p> <p>Furthermore, for incidents requiring Digital Forensic services, Evidence Documentation and Reporting SOP will be executed. The SOP outlines the systematic process for accurately documenting and reporting on the collection, analysis, and handling of evidence during investigations.</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 22 - B. During Engagement</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 11 - Annex 7 - Sample Malware Incident Analysis & Recommendation</p>
<p>15. The service provider shall have a certified and recently trained (at least in the past 12 months) in-house cyber security forensics specialist, to support advanced investigation.</p>	<p>Y</p>	<p>Refer to the documents in In-house Cyber Security Forensics Specialist Section</p>
<p>16. The service provider shall assist in the following:</p> <ul style="list-style-type: none"> - Incident handling preparation and execution - Crisis management - Breach communication - Forensic analysis including preservation of evidence for chain of custody requirements - Remediation 	<p>Y</p>	<p>Trends MICTS is certified with ISO/IEC 27001:2013 with the scope of Service Operations, Service Management and Compliance and Continual Improvement. Trends' with its competencies and disciplines shall assist agencies in their respective activities such as:</p> <ul style="list-style-type: none"> - Incident handling preparation and execution - Crisis Management - Breach Communication - Forensic analysis including preservation of evidences for chain of custody requirements - Remediation <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 4 - Annex 3 - TRENDS ISO/IEC 27001:2013 Certification</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 38, Annex 9 - Scope of Incident Response</p>
<p>17. The Service Provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).</p>	<p>Y</p>	<p>Part of Trends Service On-Boarding procedure is the due diligence process where in agencies will need to provide their asset inventory & criticality matrix. In this document, the assets shall be plotted against the Information Security Incident Use-cases and the prioritization and severity matrix shall be agreed upon by Trends and the agencies. This document will then be the reference document when customizing the service for each agency.</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 3 - Annex 2 - Asset Valuation & Categorization (excerpt from Operations Integration Document)</p> <p>Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 27 - Annex 2 - Trends Operations Center Incident Response & Update Time.</p>

Service Level Agreement (SLA) 1. Acknowledgement SLA - The Acknowledgement SLA Percentage shall be computed per month base on the total number of missed hours exceeding the Acknowledgement SLA guarantee of fifteen (15) minutes per incident			Y	Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 27 - Annex 2 - Trends Operations Center Incident Response & Update Time. Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 37 - Annex 7 - Sample measurement of Acknowledgement SLA.												
<table border="1"> <thead> <tr> <th>Service Level Target</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>98%</td> <td>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.</td> </tr> </tbody> </table>	Service Level Target	Description			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.										
Service Level Target	Description															
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. Incident Response SLA - Time to respond or provide request from when incident or request is reported based on severity level.			Y	Please see document: TRENDS_INCIDENT MANAGEMENT PSPG_v1.0_TLPGREEN.docx, page 27 - Annex 2 - Trends Operations Center Incident Response & Update Time.												
<table border="1"> <thead> <tr> <th>Priority Level</th> <th>Incident Response Time</th> <th>Reference:</th> </tr> </thead> <tbody> <tr> <td>P1 - Catastrophic</td> <td>Within 60 minutes</td> <td rowspan="4">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.</td> </tr> <tr> <td>P2 - Critical</td> <td>Within 90 minutes</td> </tr> <tr> <td>P3 - Marginal</td> <td>Within 120 minutes</td> </tr> <tr> <td>P4 - Negligible</td> <td>Within 160 minutes</td> </tr> </tbody> </table>	Priority Level	Incident Response Time			Reference:	P1 - Catastrophic	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.	P2 - Critical	Within 90 minutes	P3 - Marginal	Within 120 minutes	P4 - Negligible	Within 160 minutes		
Priority Level	Incident Response Time	Reference:														
P1 - Catastrophic	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.														
P2 - Critical	Within 90 minutes															
P3 - Marginal	Within 120 minutes															
P4 - Negligible	Within 160 minutes															
<table border="1"> <thead> <tr> <th colspan="3">Target Response Time % per Month</th> </tr> <tr> <th>Incident Priority</th> <th>1 and 2</th> <th>3 and 4</th> </tr> </thead> <tbody> <tr> <td></td> <td>>=90%</td> <td>>=80%</td> </tr> </tbody> </table>	Target Response Time % per Month			Incident Priority	1 and 2	3 and 4		>=90%	>=80%	Sum of the number of incidents meeting required Response Time for all days in the month						
Target Response Time % per Month																
Incident Priority	1 and 2	3 and 4														
	>=90%	>=80%														
II: Non-functional Requirements A: Access Management																
1. All credentials with the service provider shall be stored in a monitored central management system. These are leased to the agencies once strong authentication has been implemented and for the specific task for which it was authorized.			Y	All credentials shall be stored in a monitored central management system with a solution that can be accessed through a centralized portal, which enforces session timeouts, uses multi-factor authentication. Password will be stored and transmitted as encrypted hashes. Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 3-4 - 2.1 Protecting Password												
2. The service provider's solution shall be accessed through a centralized portal, which enforces session timeouts, mandates the use of multi-factor authentication (MFA), and provides anomaly detection for monitoring user behavior.			Y	All credentials shall be stored in a monitored central management system with a solution that can be accessed through a centralized portal, which enforces session timeouts, uses multi-factor authentication. Password will be stored and transmitted as encrypted hashes. Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 3-4 - 2.1 Protecting Password												
3. The service provider shall maintain logical access controls which are role-based, including principles of least privilege and segregation of duties.			Y	Access granted will be based on the roles and responsibilities of the requestor, aligning with the principles of least privilege. Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 2 - 1 Access Management Activities												

<p>4. All passwords must have a minimum of fifteen (15) characters. Passwords must be changed every ninety (90) days and cannot be the same as the prior three (3) passwords. The service provider's system must mask passwords when entered and store password files separately from the application system data. Only encrypted hashes of passwords may be stored and transmitted.</p>	<p>Y</p>	<p>Strong passwords must be selected, in the following way:</p> <ul style="list-style-type: none"> - using at least fifteen characters - using at least one numeric character - using at least one uppercase and at least one lowercase alphabetic character - using at least one special character - a password must not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards - passwords must not be based on personal data (e.g., date of birth, address, name of family member, etc.) - the last three passwords must not be re-used <p>Password must be changed every three months Password must be changed at first log-on to a system Password must not be stored in an automated log-on system (e.g., macro or browser)</p> <p>Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 4 - 2.2 Guidelines</p>
<p>6. All access from the service provider's managed endpoints to sensitive resources shall be done via VPN configured with MFA. Opportunistic Transport Layer Security (TLS) is configured by default for e-mail. Remote hardware is managed by comprehensive enterprise management software that allows for maintenance and access control management.</p>	<p>Y</p>	<p>Access to the operations network and sensitive resources via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Cisco Duo, MFA, etc.).</p> <p>Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 4 - 3 Remote Access Users</p>
<p>6. The service provider shall provide physical and environmental controls at the primary and secondary sites for this project.</p>	<p>Y</p>	<p>As ISO/IEC 27001:2013 certified, Trends MICTS has set of control protocols to implement, strengthen and comply with physical and environmental security controls. These control protocols provide physical security perimeters (i.e., physical entry controls), equipment security, protection against external and environmental threats, secured working areas, and implement access control.</p> <p>Trends Operations Center has several physical security controls such as biometrics, designated security guards, surveillance cameras or CCTV to prevent unauthorized access, damage, and compromised assets.</p> <p>Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 4 - 1.7 Physical Access Control</p>
<p>7. The agencies data shall be logically separated by using unique tagging to ensure segregation of data from the other agencies. The agencies should retain as the legal owner of the data processed and managed by the service provider.</p>	<p>Y</p>	<p>Each agency will be provided with individual set of solutions to ensure segregation of data. The agencies will be retained as the legal owner of the data processed and managed by Trends.</p> <p>Please see document: TRENDS_ACCESS MANAGEMENT_v1.0_TLPGREEN.docx, page 4 - 4. Scope of Access Management</p>
<p>B. Training and Other Requirements</p>		
<p>1. The service provider should facilitate at least once a year Continual Service Improvement (CSI) workshop with client for possible improvement of service through process, people and technology.</p>	<p>Y</p>	<p>Trends' Monthly Service Performance review, part of the agenda is to discuss improvement plans based on the learnings and improvement areas identified. This allows small incremental improvements to be incorporated in the day-to-day operations with the objective of realizing the benefits immediately.</p> <p>Trends conduct an annual CSI workshop every October or before the Business Planning schedule of agencies. This allows both parties to holistically discuss on major improvement plans that maybe included in the following year's business plan. Normally, this session is attended by Functional Heads and Top Management.</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 12 - Annex 3 - Cybersecurity Maturity Assessment Sample</p> <p>Please see document: TRENDS_Training Plan for Govt Insurance Cluster_v1.0.docx.</p>
<p>2. The service provider should provide security advisories with the client for the cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.</p>	<p>Y</p>	<p>Trends provide a Daily, Weekly and Monthly Digest for updates and trends in Cybersecurity space including emerging technologies and associated risks, viruses, malwares, targeted attacks and even the latest regulations for cyber-resilience.</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 13 - Annex 9 - Cybersecurity Daily Digest</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 14 - Annex 10 - Threat Hunting Advisory</p> <p>Please see document: TRENDS_Training Plan for Govt Insurance Cluster_v1.0.docx.</p>

<p>3. The service provider shall conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on each Government Agency based on the NIST or CIS Controls.</p>	Y	<p>Trends shall perform an annual Cyber Security Maturity Assessment using CIS Controls.</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.D_TLPGREEN.docx, page 12 - Annex B - Cybersecurity Maturity Assessment Sample</p> <p>Please see document: TRENDS_Training Plan for Govt Insurance Cluster_v1.0.docx.</p>
<p>Service Provider's Qualification and Requirements Note: Submission of required documents shall be during the submission of bids.</p>		
<p>1. The service provider must be a certified/authorized reseller of the brand(s) being offered and shall submit a valid certification from the manufacturer(s).</p>	Y	<p>Refer to Current Certifications from the manufacturer that the Service Provider is a certified/authorized reseller of the brands being offered section.</p>
<p>2. The service provider must submit the following certifications: a. For Cloud based Security Operations Center (SOC), that this is hosted in a provider categorized as a leader either in the latest Forrester Wave™: Public Cloud Development And Infrastructure Platforms report or Gartner Magic Quadrant for Cloud Infrastructure and Platform Services; b. For Endpoint Detection and Response (EDR), that solution is categorized as a leader either in the latest Forrester Wave™ report for Enterprise Detection and Response or Gartner Magic Quadrant for Endpoint Protection Platforms; c. For Security Information and Event Management (SIEM), the solution provided is categorized as a leader in the latest Forrester Wave™ report for Security Analytics Platforms or Gartner Magic Quadrant for Security Information and Event Management (SIEM).</p>	Y	<p>Refer to Gartner Magic Quadrant report for brands offered that has such requirement section</p> <p>a. Gartner Magic Quadrant for Cloud Infrastructure and Platform Services Refer to pages 1-2, Gartner Magic Quadrant for Cloud Infrastructure & Platform Services (CIPS).pdf</p> <p>b. Gartner Magic Quadrant for Endpoint Protection Platforms Refer to pages 1-2, Gartner Magic Quadrant for Endpoint Protection Platforms.pdf</p> <p>c. Gartner Magic Quadrant for Security Information and Event Management Refer to pages 1-2, Gartner Magic Quadrant for Security Information and Event Management.pdf</p>
<p>3. The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service), with a pool of at least 20 IT or Information Security related certified onsite support engineers within Metro Manila. A list of the support engineers shall be provided with their required qualifications, as stated in Item D. Personnel Qualifications / Requirements.</p>	Y	<p>Refer to the documents in Information Security-related certification of the onsite support engineers section</p>
<p>4. The service provider must have sales and technical offices located in the Philippines. The service provider should submit the list of their sales and technical offices in the Philippines, including the complete address and contact details. This is subject for actual site visit to the facility.</p>	Y	<p>Refer to the documents in List of Local sales and Technical office in the Philippines section</p>
<p>5. The SOC can be provided on the cloud or within the premises of the service provider. Should the Security Operations Center (SOC) with their SOC analysts be on premise, they should be housed in a Data Center with TIA-942 Rated 3 Facility Certification or any equivalent third party assessment indicating the capability of the SOC to provide the required security, scalability, stability and high performance. The proof of compliance shall be submitted.</p>	Y	<p>Refer to the documents in TIA-942 Rated 3 Facility Certification or ISO27001 Certification for Managed ICT Service sections.</p>
<p>6. However, if the service provider's SOC will be implemented through a cloud service provider (CSP), the SOC platform must be guaranteed with at least 99.9% uptime or availability. The proof of compliance shall likewise be submitted.</p>	Y	<p>Spunk SIEM</p> <p>Refer to page 1, Splunk uptime availability.pdf</p> <p>Chronicle SOAR is running on Google Cloud Platform.</p> <p>Refer to page 1-5, Google Compute Engine Service Level Agreement (SLA).pdf</p> <p>Splunk Cloud Platform Service Details</p> <p>Refer to Splunk Cloud Platform Service Details.pdf Source: https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/Service/SplunkCloudservice</p>
<p>7. The service provider's SOC Analysts must have at least one or more of the following certifications: Certified Ethical Hacker (CEH), CyberSec First Responder, Information Technology Infrastructure Library (ITIL), or any relevant product certification to the security products of the platform offered by the Service Provider.</p>	Y	<p>- For Tier 1 Analyst, please refer to Documents Regarding the Team Member/Tier 2 or Tier 1 Analyst</p> <p>- For Tier 2 Analyst, please refer to Documents Regarding the Team Member/Tier 2 or Tier 1 Analyst</p> <p>- For Tier 3 Analyst, please refer to Documents Regarding the Team Lead/Tier 3 Analyst</p> <p>- For SOC Manager or Tier 4 Analyst refer to Documents regarding the SOC Manager/Tier 4 Analyst.</p>

<p>8. The service provider must be at least five (5) years in Security and ICT Industry and must have more than three (3) years of experience in providing SOC services. The Service provider must have a SOC 2 Type II Attestation Report or ISO 27001 certification for Managed ICT Services or similar, done at least in 2021, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in place.</p>	<p>Y</p>	<p>Trends is a home-grown ICT company that has been providing Managed ICT services since 2017. It has been the Managed Security Service Provider of several institutions since 2018.</p> <p>Furthermore, Trends holds ISO 27001 certification, demonstrating a commitment to global standards and best practices in safeguarding data and ensuring regulatory compliance. Through regular recertification, Trends ensure ongoing compliance and continual improvement in Information security. Additionally, SOC 2 Type II compliance, aligned with ISAE 3402, provide valuable insights into the design, implementation, and maintenance of their security controls, offering clients strong security assurance.</p> <p>Please see Documents in Valid SOC 2 Type II Attestation Report or ISO27001 Certification of Managed ICT Services or similar service section</p>
<p>9. The prospective bidders shall be required during the post qual evaluation to demonstrate the salient features of this proposed Shared Cyber Defense solution at the Project Site or via online.</p>	<p>Y</p>	<p>Trends will demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online during the Post Qualification Evaluation.</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p>
<p>D. Personnel Qualifications/Requirements</p>		
<p>1. The service provider must have at least Two (2) local Certified Engineer on each of the following security tools below:</p> <ul style="list-style-type: none"> - SOAR - SIEM - Vulnerability Management <p>The certification must be the same with the brand that is being proposed.</p>	<p>Y</p>	<p>Refer to the documents in List of Local Certified Engineers for the (i) SOAR, (ii) SIEM and (iii) Vulnerability Management, including their respective Certifications on the brand/solution being proposed section</p>
<p>2. The service provider must assign a dedicated local SOC Manager that oversees the SOC and conducts regular monthly service performance review and reporting to client's management. A monthly service performance report shall be submitted and discussed by the SOC Manager. It shall contain the following:</p> <ul style="list-style-type: none"> - SLA Performance - Correlated Events Overview - Correlated Events Graph Distribution Over Time - Correlated Events and Rules Triggered Summary - Summary of Incident Ticket per Use Cases Incident Management <p>The service provider must also assign a dedicated Project Manager that will oversee the project implementation. A Monthly project Monitoring report shall be submitted and discussed by the Project Manager until the completion of the Phase I 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.</p>	<p>Y</p>	<p>Trends conduct a monthly service performance review with key stakeholder every 1st week of the month to discuss what has transpired in the previous month including the plans for the next month. This is regularly done for the entire duration of the engagement to ensure that there will be alignment of expectations and jointly address challenges and problems and agree on improvement plans. Normally the agenda of this meeting follows this format:</p> <ol style="list-style-type: none"> 1. IOCs detected - number, status, nature, impact, priority, source, etc. 2. SLA Compliance - report time, response time 3. Correlation Rules - current #, # of triggered Mitro ATT&CK tactics, newly created, decommissioned 4. Data Sources - added, inactive, removed 5. VAPT - # of vulnerabilities, status of previous vulnerabilities based on rescan conducted, newly discovered, type of vulnerabilities and impact, assets. 6. Threats - # of threats detected, type of threats and impact, updates and trends 7. CIS CAT score for its overall security posture - every quarter month. 8. Trainings or Enablement Programs - schedules, attendees, CSAT 9. Improvement Initiatives <p>Furthermore, part of the SOC Manager's role is to provide the following:</p> <ol style="list-style-type: none"> 1. SLA Performance 2. Correlated Events Overview 3. Correlated Events Graph Distribution Overtime 4. Correlated Events and Rules Triggered Summary 5. Summary of Incident Ticket per Use Cases Incident Management <p>For the assign dedicated Project Manager, please refer to Documents regarding the Project Manager section</p> <p>Please see document: TRENDS_REFERENCE MATERIALS_v1.0_TLPGREEN.docx, page 16 - Annex 12 - Sample Monthly Reports</p> <p>Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p>
<p>3. The service provider must submit the following for all the personnel to be assigned to the cluster, and failure to submit the any of the requirement below is subject for disqualification.</p> <ul style="list-style-type: none"> - Resume/CV of the Proposed Personnel - Company ID - Certificate of employment 	<p>Y</p>	<p>Please refer to Information Security Related Certifications of the onsite support engineers section</p>

<p>4. The service provider must have a dedicated 24x7x365 team assigned to the cluster, composed of at least:</p> <ul style="list-style-type: none"> - 2-Tier 1 analyst who will be responsible for the following tasks: <ol style="list-style-type: none"> 1. Monitoring via existing SIEM/Analytics Platform 2. Funneling of alerts (noise elimination) 3. Incident Validation 4. Case Management 5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up <ol style="list-style-type: none"> 6. General Communication 7. Weekly Summary Reports - 1-Tier 2 analyst who will be responsible to conduct further analysis and decides on a strategy for containment. <ol style="list-style-type: none"> 1. Proactive Searches/ Threat Hunting 2. Qualification of Incident Priority/Severity 3. Investigation via SIEM/Analytics Platform and other accessible sources 4. Rule Tuning 5. Ad hoc Vulnerability Advisory & Research 6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations - 1-Tier 3 senior analyst who will be responsible to manage critical incidents. Tier 3 analysts are also responsible for actively hunting for threats and assessing the vulnerability of the business. <ol style="list-style-type: none"> 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules - 1-Tier 4 analyst or the SOC manager, who will be in charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. The SOC manager will also be responsible for the management of the MSOC operations for the agency and cluster. 	Y	<p>Trends will have a dedicated 24x7x365 team assigned to the Government Insurance Cluster For the Roles and Responsibilities, please refer to: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0.docx</p>
<p>6. The service provider should ensure that there will be alternate personnel deployed to the cluster should the primary personnel be unavailable for whatever reason. The service provider shall be allowed to augment the dedicated personnel with foreign support staff from partners (hybrid) as long as the minimum staffing requirement are met.</p>	Y	<p>Trends will ensure that there will be alternate personnel deployed to the Insurance Cluster should the primary personnel be unavailable for whatever reason. Please see document: TRENDS_Project Management Program Plan for Govt Insurance Cluster_v1.0. docx</p>
<p>6. Qualifications</p> <ul style="list-style-type: none"> - Project Manager: <ul style="list-style-type: none"> - Must be with the service provider's organization at least one (1) year before the bid opening - Has handled project management for at least two (2) financial corporations or should have at least two (2) successful project implementations of at least Php 20M in amount in the last two (2) years. - Must provide a list of projects handled in the last 6 years, indicating the Project Name, Project Duration (Start date and end-date) and Contact Person with details for verification. - Must have a valid project management certification 	Y	<p>Refer to Documents regarding the Project Manager</p>

<p>- SOC Manager/Tier 4 Analyst:</p> <ul style="list-style-type: none"> - Must be with the service provider's organization one (1) year before the bid opening - Has performed and managed three (3) engagements within the last five (5) years comparable to the proposed engagement - Must have at least five (5) years active IT security experience - Must have at least three (3) years SIEM or system and network administration experience. - Has any two (2) of the following unexpired professional certifications: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), GIAC Security Essentials (GSEC), GIAC Continuous Monitoring (GMON), GIAC Certified Detection Analyst (GCDA), GIAC Web Application Penetration Tester (GWAPT), GIAC Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFE), GIAC Certified Intrusion Analyst (GCI), Cisco Certified Network Associate (CCNA), Information Technology Infrastructure Library (ITIL), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Network Defense Architect (CNDA), CyberSec First Responder (CFR), CompTIA Security+, Certified Vulnerability Assessor (CVA), Offensive Security Certified Professional (OSCP), Certified Information System Security Professional (CISSP), Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), GIAC Exploit Researcher & Advanced Penetration Tester (GXPN), EC-Council Licensed Penetration Tester (LPT) Master, Certified Penetration Tester (CPT), Certified Expert Penetration Tester (CEPT), Certified Mobile and Web Application Penetration Tester (CMWAPT), CompTIA PenTest+, Certified Payment Card Industry Security implementer (CPISI), or other security-related certifications. 	Y	Refer to Documents regarding the SOC Manager/Tier 4 Analyst
<p>- Team Lead/Tier 3 Analyst:</p> <ul style="list-style-type: none"> - Must be with the service provider's organization one (1) year before the bid opening - Has functioned as lead in the performance of three (3) engagements within the last five (5) years comparable to the proposed engagement - Must have at least five (5) years active IT security experience - Must have at least three (3) years SIEM or system and network administration experience - Has any two (2) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFE, GCI, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications. 	Y	Refer to Documents regarding the Team Lead/Tier 3 Analyst
<p>- Team Member/Tier 2 or Tier 1 Analyst:</p> <ul style="list-style-type: none"> - Must be with the service provider's organization one (1) year before the bid opening - Has performed three (3) engagements within the last five (5) years comparable to the proposed engagement - Must have at least three (3) years active IT security experience - Must have at least three (3) years SIEM or system and network administration experience - Has at least one (1) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFE, GCI, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications. 	Y	Refer to Documents regarding the Team Member/Tier 2 or Tier 1 Analyst

**Omnibus Sworn
Statement**

Form No. 6

Omnibus Sworn Statement

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF City of Makati) S.S.

AFFIDAVIT


I, **Wilfredo N. Aguilar**, of legal age, Married, Filipino, and residing at B4 L12 Madelaine Place, Camella SPV, Molino 3, Bacoor Cavite, after having been duly sworn in accordance with law, do hereby depose and state that:

1. I am the duly authorized and designated representative of **Trends & Technologies, Inc.** with office address at 6th Floor Trafalgar Plaza, 105 H.V. Dela Costa Street, Salcedo Village, Makati City, Philippines;
2. I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for **Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster with Project Identification Number LBP-HOBAC-ITB-GS-20230725-01** of the Land Bank of the Philippines, as shown in the attached duly notarized Secretary's Certificate;
3. **Trends & Technologies, Inc.** is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, **by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;**
4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;
5. **Trends & Technologies, Inc.** is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;
6. None of the officers, directors, and controlling stockholders of **Trends & Technologies Inc.** is not related to the following LANDBANK Officers, employees and consultants: 1) members of the Board of Directors; 2) President and CEO; 3) members of the Head Office Bids and Awards Committee (HOBAC); 4) members of the HOBAC Secretariat; 5) members of the Technical Working Group, if applicable; 6) personnel of Procurement Department; 7) personnel of the implementing unit or the end-user unit; and 8) project consultants, if applicable, by consanguinity or affinity up to the third level degree;
7. **Trends & Technologies, Inc.** has no unsatisfactory performance with its ongoing projects;
8. **Trends & Technologies, Inc.** complies with existing labor laws and standards; and
9. **Trends & Technologies, Inc.** is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
 - a. Carefully examining all of the Bidding Documents;



- b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
 - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
 - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the **Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster with Project Identification Number LBP-HOBAC-ITB-GS-20230725-01.**
10. **Trends & Technologies, Inc.** did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.
11. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

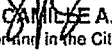
IN WITNESS WHEREOF, I have hereunto set my hand this 09 OCT 2023 day of 2023 at Makati City, Philippines.


Wilfredo N. Aguilar
 Account Director
 Trends & Technologies, Inc.
 Authorized Representative
 Affiant

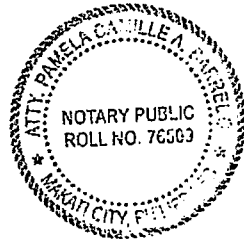
SUBSCRIBED AND SWORN to before me this 09 OCT 2023 day of _____, in Makati City, Philippines. Affiant is personally known to me and was identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant exhibited to me his Passport, with his photograph and signature appearing thereon, with no. P3957268B and his Community Tax Certificate No. 25816214 issued on January 31, 2023 at Bacoor City, Cavite.

Witness my hand and seal this 09 OCT 2023 day of _____.

Notary Public


ATTY. PAMELA CAMILLE A. BARREDO
 Notary Public for and in the City of Makati
 Appointment No. M-041 (2023-2024)
 Until 31 December 2024
 Roll of Attorneys No. 78508; 5 May 2022
 PTR No. 9582131/12 January 2023/Makati City
 IBP No. 278895/9 January 2023/Pasig City
 23/F Trafalgar Plaza Building
 105 H.V. Dela Costa St., Salcedo Village
 Makati City, Philippines 1227

Doc. No. 473 ;
 Page No. 96 ;
 Book No. II ;
 S. of 2023



The names of specific LANDBANK officers, employees and consultants being referred to are shown in Annexes E-1 to E-2.

**Current Certifications
from the manufacturer
that Service Provider is a
certified/authorized
reseller of the brands
being offered**

Google Cloud
Partner Advantage

Partner Certificate

Date of Issuance: October 3, 2023.

REYNALDO C. CAPA
Senior Vice President Chairperson,
Bids and Awards Committee
Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
1004 Malate, Manila

Project Name: Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster - LBP-HOBAC-ITB-GS-20230725-01

This is to certify that TRENDS & TECHNOLOGIES, INC. is a certified/authorized Google, Cloud Partner with the current status as described below and in the Partner Directory for Google Cloud Partner Advantage:

Partner Level: Partner		
Product	Engagement Model	Partner Advantage Region
Google Cloud Platform	Sell	• Other Asia Pacific

Partner Level: Partner	
Specialization/ Expertise/ Initiative	Specialization/ Expertise/ Initiatives Name
Initiative	• SecOps Reseller Initiative

This certificate is valid until¹ December 31, 2023.

Very truly yours,



Kim Lasseter
Global Director, Partner Advantage Program

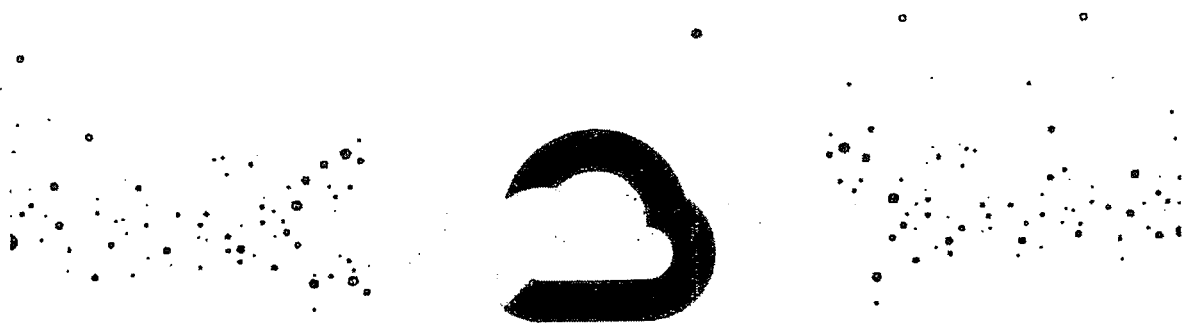
¹Provided that partner is current with all the mandatory requirements of the program



Security & Identity

Raising the bar in Security Operations: Google Acquires Siemplify

January 4, 2022



Sunil Potti

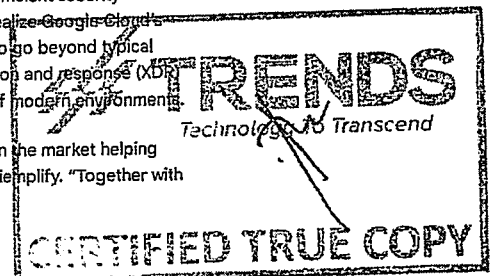
VP/GM, Google Cloud Security

At Google Cloud, we are committed to advancing invisible security and democratizing security operations for every organization. Today, we're proud to share the next step in this journey with the acquisition of Siemplify, a leading security orchestration, automation and response (SOAR) provider. Siemplify shares our vision in this space, and will join Google Cloud's security team to help companies better manage their threat response.

In a time when cyberattacks are rapidly growing in both frequency and sophistication, there's never been a better time to bring these two companies together. We both share the belief that security analysts need to be able to solve more incidents with greater complexity while requiring less effort and less specialized knowledge. With Siemplify, we will change the rules on how organizations hunt, detect, and respond to threats.

Providing a proven SOAR capability unified with Chronicle's innovative approach to security analytics is an important step forward in our vision. Building an intuitive, efficient security operations workflow around planet-scale security telemetry will further realize Google Cloud's vision of a modern threat management stack that empowers customers to go beyond typical security event and information management (SIEM) and extended detection and response (XDR) tooling, enabling better detection and response at the speed and scale of modern environments.

"We're excited to join Google Cloud and build on the success we've had in the market helping companies address growing security threats," said Amos Stern, CEO at Siemplify. "Together with



Chronicle's rich security analytics and threat intelligence, we can truly help security professionals transform the security operations center to defend against today's threats."

The Siemplify platform is an intuitive workbench that enables security teams to both manage risk better and reduce the cost of addressing threats. Siemplify allows Security Operation Center analysts to manage their operations from end-to-end, respond to cyber threats with speed and precision, and get smarter with every analyst interaction. The technology also helps improve SOC performance by reducing caseloads, raising analyst productivity, and creating better visibility across workflows.

We plan to invest in SOAR capabilities with Siemplify's cloud services as our foundation and the team's talent leading the way. Our intention is to integrate Siemplify's capabilities into Chronicle in ways that help enterprises modernize and automate their security operations.

We're looking forward to welcoming the Siemplify team to Google Cloud and working with them to help security operations teams accomplish so much more in defense of their organizations. You can read [Siemplify CEO Amos Stern's blog](#) for more on this exciting news.

Posted in [Security & Identity—Google Cloud](#)

Related articles



Security & Identity
How Sensitive Data Protection can help secure generative AI workloads
By Scott Ellis • 5-minute read



Security & Identity
Introducing Google Cloud Firewall Plus with intrusion prevention
By Megan Yahya • 3-minute read



Security & Identity
Cloud CISO Perspectives: Late September 2023
By Phil Venables • 7-minute read



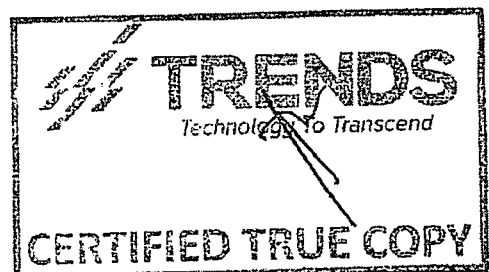
Security & Identity
Introducing Advanced Vulnerability Insights for GKE
By Greg Mucci • 3-minute read

Follow us



[Google Cloud](#) [Google Cloud Products](#) [Privacy](#) [Terms](#)

[Help](#) [English](#)





250 North Bridge Road #39-04
Raffles City Tower, Singapore
179101

Manufacturer's Authorization Letter

To: REYNALDO C. CAPA
Senior Vice President Chairperson,
Bids and Awards Committee
Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
1004 Malate, Manila

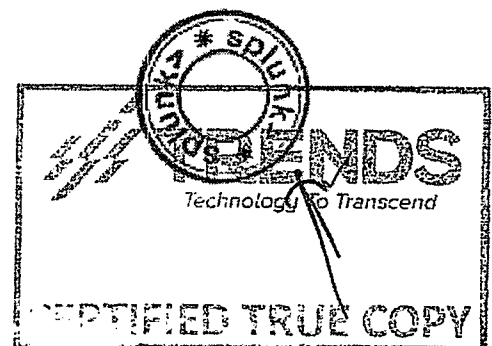
We, Splunk Services Singapore Pte Ltd, are a computer software manufacturer founded under U.S. Laws, with its principal place of business at 250 North Bridge Road #39-04 Raffles City Tower Singapore 179101. We hereby confirm Trends & Technologies, Inc. (the "Authorized Reseller"), a company incorporated under the laws of the Philippines is the authorized reseller of Splunk Services Singapore Pte Ltd who may perform the following activities under the capacity of independent contractor:

The Authorized Reseller is authorized by Splunk Services Singapore Pte Ltd to resell Splunk products in the Philippines to you for the invitation of project Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster - LBP-HOBAC-ITB-GS-20230725-01.

- 1) The Authorized Reseller shall independently bear all responsibilities with respect to the provision of the Splunk products to you in accordance with the agreed terms between you and the Authorized Reseller.
- 2) As the manufacturer, Splunk Services Singapore Pte Ltd will provide the Splunk products and/or services to the Authorized Reseller in accordance with the terms and conditions of the Splunk Reseller Agreement entered into between Splunk Services Singapore Pte Ltd and the Authorized Reseller.
- 3) Splunk Services Singapore Pte Ltd will provide the Splunk products and/or services to you, the End User, via its Authorized Reseller, in accordance with the terms and conditions of Splunk Software License Agreement located at: https://www.splunk.com/en_us/legal/splunk-software-license-agreement-bah.html.

IN WITNESS WHEREOF, this Authorization Letter is hereby executed as of 19th September 2023.

Manufacturer Name: Splunk Inc.
Authorized Name: Raen Lim
Title: Group Vice President, Asia





18 September 2023

Mr. REYNALDO C. CAPA
Senior Vice President Chairperson,
Bids and Awards Committee
Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
1004 Malate, Manila

Dear Sir,

LAND BANK OF THE PHILIPPINES
Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster - LBP-
HOBAC-ITB-GS-20230725-0

CrowdStrike, Inc., hereby confirms that Trends & Technologies, Inc of 23rd Floor
Trafalgar Plaza, 105 H.V. Dela Costa St., Salcedo Village, Makati City 1227,
Philippines, is a CrowdStrike authorized Reseller and Managed Service Provider.

Trend & Technologies will be supplying Support to Land Bank of the Philippines for
the said Project listed above; and we are happy to confirm that we will also be
providing Land Bank of the Philippines with our support in accordance with our
Terms & Conditions.

This certification is issued in compliance with the post-qualification requirements of
Land Bank of the Philippines.

Yours faithfully,

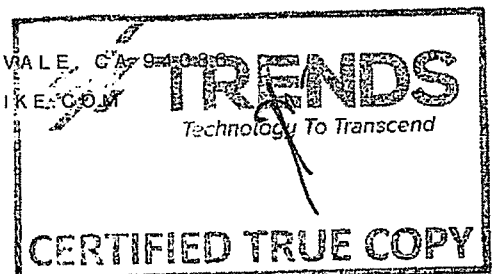
DocuSigned by:
Michael Rogers
9107287BCAD64E6...

CROWDSTRIKE INC.
Name: Michael Rogers
Title: Vice President
Date: 9/19/2023

DS
km

150 MATHILDA PLACE, SUITE 300, SUNNYVALE, CA 94085

T: @CROWDSTRIKE W: CROWDSTRIKE.COM





Tenable Network Security Ireland Limited
81b Campshires
Sir John Rogerson's Quay
Dublin 2
Ireland

15 September 2023

Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
1004 Malate, Manila

Attention: REYNALDO C. CAPA, Senior Vice President Chairperson, Bids and Awards Committee

Project Name: Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster - LBP-HOBAC-ITB-GS-20230725-01

RE: MANUFACTURER'S AUTHORISATION FORM

Dear Sir

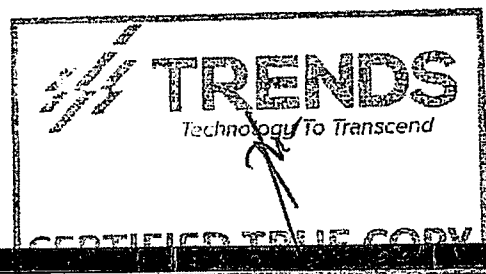
As of the date of this letter, Tenable Network Security Ireland Limited ("Tenable"), as the manufacturer/publisher of Tenable-branded products and solutions, verifies that **Trends & Technologies, Inc.** ("Reseller") of Trafalgar Plaza, 105 H.V. Dela Costa St., Salcedo Village, Makati 1227 Philippines, is authorized to resell Tenable's products to **Land Bank of the Philippines**. As such, Tenable will supply Reseller with sufficient quantities of its products, subject to the ongoing reseller/manufacture relationship between Reseller and Tenable.

Signed for and on behalf of Tenable

DocuSigned by:

374256260D0C491...

Thomas Parsons, GM





September 21st, 2023

To:
REYNALDO C. CAPA
Senior Vice President Chairperson,
Bids and Awards Committee
Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos St.
1004 Malate, Manila

Project Name: Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster - LBP-HOBAC-ITB-GS-20230725-01

To Whom It May Concern:

Cyble Singapore Private Limited, a cybersecurity company that is based at 45 North Canal Road #01-01 Lew Building Singapore 059301 confirms that as of today, Trends & Technologies Inc., ("Reseller"), a company incorporated under the laws of the Philippines located at 6F Trafalgar Plaza, H.V. Dela Costa Street, Salcedo Village, Makati City, Philippines is an authorized and non-exclusive MSSP Reseller/MSSP of all of Cyble products and services (collectively "Cyble Products") in Philippines.

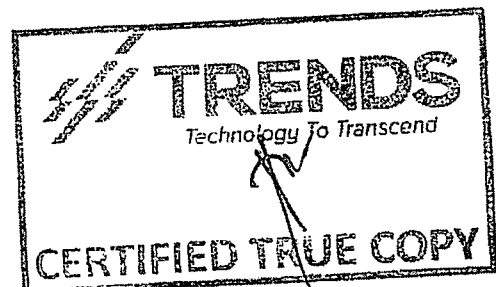
Best Regards,

DocuSigned by:

Manish Chachada

CDA26EAC0539436...

Cyble Singapore Private Limited
Mr. Manish Chachada
Authorized Signatory





September 15, 2023

Manufacturer's Authorization Letter

To: REYNALDO C. CAPA
Senior Vice President Chairperson
Bids and Awards Committee
Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
1004 Malate, Manila

Project Name: Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster – LBP-HOBAC-ITB-GS-20230725-01

ExtraHop Networks, Inc. ("ExtraHop"), a Delaware corporation with its principal place of business at 520 Pike Street, Suite 1600, Seattle, WA 98101, hereby confirms that as of the date of this letter and, absent termination for breach of its agreement with ExtraHop, for a period of six (6) months thereafter, Trends & Technologies Inc. ("Reseller"), a company incorporated under the laws of the Philippines is an authorized reseller of all of ExtraHop products and services (collectively "ExtraHop Products") in the Philippines.

All sales of ExtraHop Products are subject to the following end user license agreement: ExtraHop Master Customer Agreement, found at <https://www.extrahop.com/go/customeragreement/> ("MCA").

Should you have any questions regarding this matter, please do not hesitate to contact partners@extrahop.com.

Best Regards,

EXTRAHOP NETWORKS, INC.

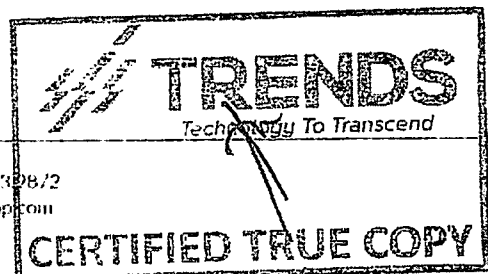
DocuSigned by:
BY: Lauren Zajac
164C98D4EAB8F03...

Name: Lauren Zajac
Title: Chief Legal Officer

EXTRAHOP NETWORKS, INC.
Cloud Native Network Detection & Response

520 Pike St., Suite 1600
Seattle, WA 98101

877.333.9872
extrahop.com



Date: 15 September 2023

REYNALDO C. CAPA
Senior Vice President Chairperson,
Bids and Awards Committee
Land Bank of the Philippines
1598 M.H. Del Pilar cor. Dr. J. Quintos Sts., Malate Manila

Dear Sir or Madam:

LETTER OF CONFIRMATION

Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster - LBP-HOBAC-ITB-GS-20230725-01 (the "Project")

We confirm as follows:-

1. Trends & Technologies, Inc. having an address at 8Th Floor Trafalgar Plaza 105 H.V. Dela Costa St., Salcedo Village Makati City (the "Bidder"), is authorized to quote and resell Dell products and/or services products in Philippines (the "Territory") as part of their bid for the abovementioned Project in their own capacity:-
 - o Dell EMC PowerEdge R750xs

The Bidder shall acquire such Dell products and/or services products from an Authorized Dell Distributor in the Territory listed at <https://www.dell.com/partner/en-sg/partner/find-a-partner.htm>.

2. The Bidder shall provide first level support to you in respect of all hardware-related issues pertaining to the Dell products and thereafter to escalate any unresolved issues to the Authorized Distributor. Dell will provide support and assistance for the Dell products and/or services to the Authorized Distributor in accordance with the terms of the prevailing channel partner agreement.
3. The Bidder is an independent contractor at all times and Bidder does not make any commitments/obligations on behalf of Dell.
4. The above confirmation for the supply of the above-mentioned products, or services and access to related technology, (the "Materials") is subject to the following conditions:-
 - The Materials are for your own use, not for resale, export, re-export or transfer.
 - The Materials is subject to compliance with export control and economic sanctions laws of the United States and the Territory.
 - The Materials and may not be used, sold, leased, exported, imported, re-exported, or transferred except with prior written authorization by Dell EMC and in compliance with such laws, including, without limitation, export licensing requirements, end-user, end-use, and end-destination restrictions, and prohibitions on dealings with sanctioned individuals and entities, including but not limited to persons on the Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List or the U.S. Department of Commerce Denied Persons List. Customer represents and warrants that it is not the subject or target of, and that Customer is not located in a country or territory (including without limitation, North Korea, Cuba, Iran, Syria, and Crimea) that is the subject or target of, economic sanctions of the United States or other applicable jurisdictions.

We respectfully look forward to receiving your cooperation in order for the above conditions to be implemented.

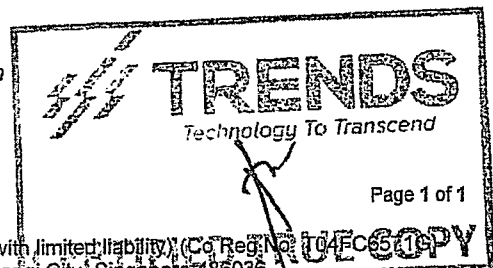
Thanking you in anticipation for your support to Dell.

Yours faithfully,
Dell Global B.V. (Singapore Branch)



Vincent Lee
General Manager
Channels – Singapore & South Asia

*To verify this document, please contact: Rache_Resurreccion@dell.com



**Data Sheets and
Documentations of the
brands and/or services
being offered**

I. Functional Requirements

A. Security Monitoring and Management

A.1
Security Operations
Center (SOC)



Managed ICT Services
Service Delivery with Flexibility

REFERENCE MATERIALS & ARTICLES

This document serves as compilation of reference materials and articles of Trends services.

DOCUMENT ID

DOCUMENT OWNER

MICTS Information Security Services Group

DOCUMENT CLASSIFICATION

TLP:GREEN INTERNAL

DOCUMENT STATUS

RELEASE

DOCUMENT VERSION

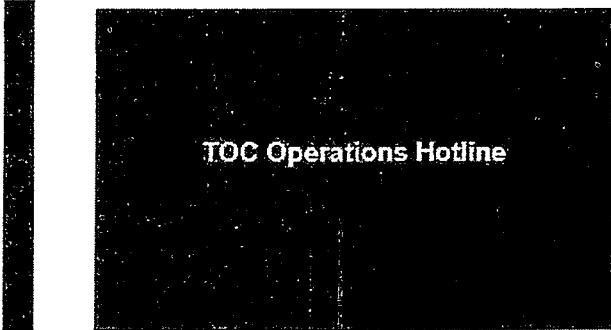
1.0

REVISION DATE

2023 SEPTEMBER 01



ANNEX 1 – Trends Contact Numbers (excerpt from Client Onboarding Presentation)



TOC Hotline:
0917 507 1812
0917 558 9675

Hotline – 8811 8181
Local: 8701 to 8703
Local: 8708 to 8710

Soc@trends.com.ph
TOC GSM Gateway:
0917 822 25 74
0917 845 60 85

© 2021 Trends & Technologies, Inc. All Rights Reserved

ANNEX 2 – Asset Valuation & Categorization (excerpt from Operations Integration Document)

4 IT Asset Valuation & Categorization

The IT asset valuation & classification guidelines provide guidance to achieve a consistent approach in assessing the physical IT assets of an organization that are online, attached to the network, and providing and/or receiving network and application services.

The method for IT asset valuation is anchored on the CIA model. The resulting measurement from the CIA model is then multiplied against the weight of an asset based on the asset's sensitivity within the client's organization.

Total Asset Value = Asset Value * Asset Weight

4.1 CIA Model for measuring Value of an Asset

Confidentiality	Integrity	Availability
The unauthorized disclosure of information/data could be expected to have a:	The unauthorized modification or destruction of information/data could be expected to have a:	The cessation of access to or use of information/data or an information system would be expected to have a:
Limited adverse effect on organizational operations, assets or individuals.	Limited adverse effect on organizational operations, assets or individuals.	Limited adverse effect on organizational operations, assets or individuals.
Serious adverse effect on organizational operations, assets or individuals.	Serious adverse effect on organizational operations, assets or individuals.	Serious adverse effect on organizational operations, assets or individuals.
Severe or critical adverse effect on organizational operations, assets or individuals.	Severe or critical adverse effect on organizational operations, assets or individuals.	Severe or critical adverse effect on organizational operations, assets or individuals.

CONFIDENTIALITY	LOW (1)			MEDIUM (2)			HIGH (3)			
	Integrity (1)	Integrity (2)	Integrity (3)	Integrity (1)	Integrity (2)	Integrity (3)	Integrity (1)	Integrity (2)	Integrity (3)	
AVAILABILITY	LOW (1)	1	4	5	4	1	6	5	6	7
MEDIUM (2)	4	5	6	5	6	7	6	7	8	9
HIGH (3)	5	6	7	6	7	8	7	8	9	10

4.2 Model for measuring Weight of an Asset

Category	Weight	Description
Low	1	The value of data in the container is low/non-existent based on business objectives, as compared to another similar container's data value.
Medium	2	The value of data in the container is medium based on business objectives, as compared to another similar container's data value.
High	3	The value of data in the container is high based on business objectives, as compared to another similar container's data value.

4.3 Asset Categorization

After having assets plotted against the CIA model and its weight identified, assets are now ready to be categorized. By multiplying the Asset Value with its weight, assets can then be categorized for its overall value. Category rating has a range of 1-3, 1 being the highest Asset Category for those assets having 21-27 in the Asset Value-Weight Matrix.

Asset Value	3	4	5	6	7	8	9	
Weight	1	3	4	5	6	7	8	9
2	6	8	10	12	14	16	18	
3	9	12	15	18	21	24	27	

Category	Asset Value-Weight Matrix
3	21-27
2	12-20
1	3-10

4.4 Asset Valuation & Categorization Listing

Category	IP	Vendor	Type	Confidentiality	Integrity	Availability	Weight	Asset Value	Overall Value	Category
AD Server 1		Microsoft	Windows Server 2012 R2	3	3	3	3	27	18	3
AD Server 2		Microsoft	Windows Server 2012 R2	3	3	3	3	27	18	3
AD Server 3		Microsoft	Windows Server 2012 R2	3	3	3	3	27	18	3
AD Server 4		Microsoft	Windows Server 2012 R2	3	3	3	3	27	18	3
AD Server 5		Microsoft	Windows Server 2012 R2	3	3	3	3	27	18	3

6.4 Mapping of Typical Incidents to Assets

CRITICAL
Network Defense <ul style="list-style-type: none"> Denial of Service Attacks Successful inbound traffic from a known malicious or suspicious site Application Defense <ul style="list-style-type: none"> Successful login of privileged account on any IT Asset Category Unauthorized escalation of privileges of normal account on any IT Asset Category Endpoint Defense <ul style="list-style-type: none"> Malware entering the network on IT Asset Category 1 Uncleaned, unquarantined malware on IT Asset Category 1 Database Defense <ul style="list-style-type: none"> Unauthorized extraction of confidential and/or sensitive information on any IT Asset Category
P2 – HIGH
Network Defense <ul style="list-style-type: none"> Persistent reconnaissance scan Application Defense <ul style="list-style-type: none"> Multiple failed login of privileged account on any IT Asset Category Endpoint Defense <ul style="list-style-type: none"> Malware alerts on IT Asset Category 1 (i.e. client databases) that have been cleaned and/or quarantined Uncleaned, unquarantined malware on IT Asset Category 2
P3 – MEDIUM
Application Defense <ul style="list-style-type: none"> Failed login of privileged account on any IT Asset Category Multiple failed login of normal accounts on IT Asset Category 3 Network Defense <ul style="list-style-type: none"> Successful Outbound traffic to a known GTI site Endpoint Defense <ul style="list-style-type: none"> Uncleaned, unquarantined malware on IT Asset Category 3
P4 – LOW
Application Defense <ul style="list-style-type: none"> Failed login of authorized normal account on IT Asset Category 3 Endpoint Defense <ul style="list-style-type: none"> Malware alerts on IT Asset Category 2 (i.e. internal databases & systems) that have been cleaned and/or quarantined
INFORMATIONAL
Endpoint Defense <ul style="list-style-type: none"> Malware alerts on IT Asset Category 3 (i.e. workstations) that have been cleaned and/or quarantined

ANNEX 3 – TRENDS ISO/IEC 27001:2013 Certification



SOCOTEC

CERTIFICATE

No. SCU001708D

certifies that :

Trends & Technologies, Inc.

20th Trafalgar Plaza, 105 HV Dela Costa, Saicedo Village Makati, Philippines

operates a management system that has been assessed as conforming to :

ISO/IEC 27001:2013

for the scope of activities :

Trends Managed ICT Services- Service Operations Group which consists of
Trends Operations Center, Systems & Platforms, Service Management and
Compliance & Continual Improvement

Statement of Applicability: MICTS-SO-Statement of Applicability Version 6 effective July 20, 2020

Issue date : 14 April 2021
Valid until : 28 October 2023 (Subject to adherence to the agreed ongoing programme, successful endorsement of certification following each audit and compliance with the terms and conditions of certification.)
Original date of certification : 29 October 2017

Mo Ghaua Operations Director SOCOTEC Certification UK





SOCOTEC Certification UK Ltd, 6 Gordano Court
Serbert Close, Portishead, Bristol BS20 7FS
UNITED KINGDOM
<http://socotec-certification-international.co.uk>

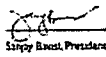
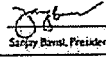


ANNEX 4 – Personnel Certifications


ANNEX 4.1 – EC-Council Certified Ethical Hacker

<p>EC-Council Certificate Number: ECC9254601873</p> <p>CEH Certified Ethical Hacker</p> <p>This is to acknowledge that DELFIN JR BARQUILLA has successfully completed all requirements and criteria for Certified Ethical Hacker certification through examination administered by EC-Council</p> <p>Issue Date: 16 March, 2023 Expiry Date: 15 March, 2026</p> <p>ANSI Certified</p> <p>Sergio Garay, President</p>	<p>EC-Council Certificate Number: ECC3985402716</p> <p>CEH Certified Ethical Hacker</p> <p>This is to acknowledge that Jestoni Morales has successfully completed all requirements and criteria for Certified Ethical Hacker certification through examination administered by EC-Council</p> <p>Issue Date: 02 June, 2023 Expiry Date: 01 June, 2026</p> <p>ANSI Certified</p> <p>Sergio Garay, President</p>
<p>EC-Council Certificate Number: ECC9347825601</p> <p>CEH Certified Ethical Hacker</p> <p>This is to acknowledge that Mardy Anne Vizcarra has successfully completed all requirements and criteria for Certified Ethical Hacker certification through examination administered by EC-Council</p> <p>Issue Date: 20 October, 2021 Expiry Date: 19 October, 2024</p> <p>ANSI Certified</p> <p>Sergio Garay, President</p>	<p>EC-Council Certificate Number: ECC3140697852</p> <p>CEH Certified Ethical Hacker</p> <p>This is to acknowledge that ERLYN BARREDO has successfully completed all requirements and criteria for Certified Ethical Hacker certification through examination administered by EC-Council</p> <p>Issue Date: 11 October, 2022 Expiry Date: 10 October, 2025</p> <p>ANSI Certified</p> <p>Sergio Garay, President</p>

ANNEX 4.2 – EC-Council Certified Incident Handler (ECIH)

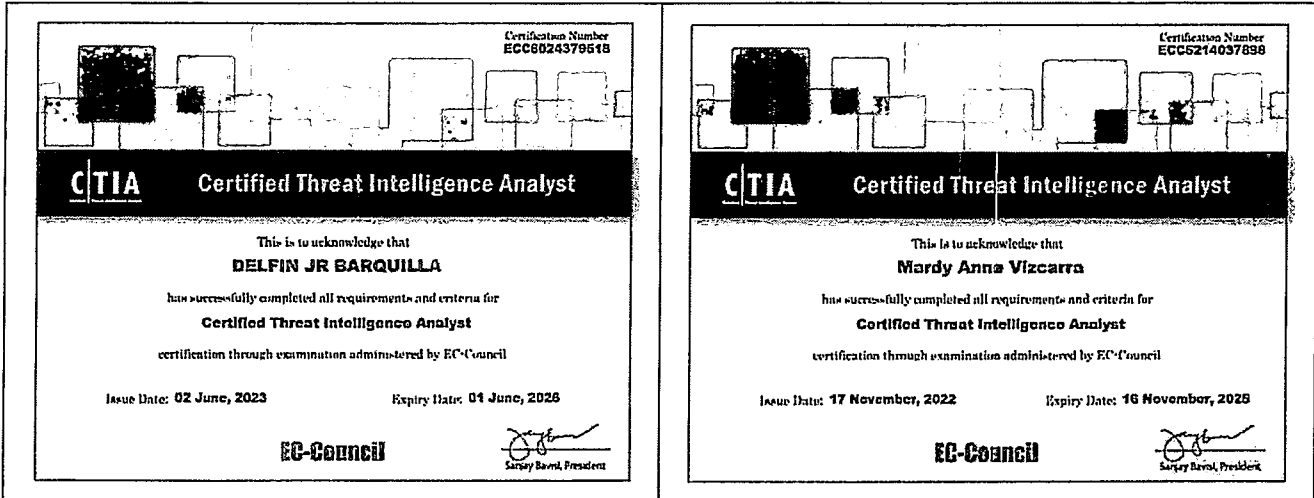
<p style="text-align: right;">Certification Number ECC0247138895</p> <p>E CIH EC-Council Certified Incident Handler</p> <p>This is to acknowledge that Jestoni Morales has successfully completed all requirements and criteria for EC-Council Certified Incident Handler certification through examination administered by EC-Council</p> <p>Issue Date: 28 December, 2022 Expiry Date: 27 December, 2025</p> <p>EC-Council </p>	<p style="text-align: right;">Certification Number ECC0975281436</p> <p>E CIH EC-Council Certified Incident Handler</p> <p>This is to acknowledge that Gemalyn Cabanos has successfully completed all requirements and criteria for EC-Council Certified Incident Handler certification through examination administered by EC-Council</p> <p>Issue Date: 20 July, 2022 Expiry Date: 19 July, 2023</p> <p>EC-Council </p>
---	---

ANNEX 4.3 – EC-Council Certified Security Specialist

<p style="text-align: right;">Certification Number ECC0012B59347</p> <p>E CSS EC-Council Certified Security Specialist</p> <p>This is to acknowledge that Mardy Anna Vizcarra has successfully completed all requirements and criteria for EC-Council Certified Security Specialist v9 certification through examination administered by EC-Council</p> <p>Issue Date: 03 December, 2021</p> <p>EC-Council </p>	Empty space for the second certificate
--	--



ANNEX 4.4 – EC-Council Certified Threat Intelligence Analyst



ANNEX 4.6 – ITIL FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT

<div style="display: flex; justify-content: space-between; align-items: center;"> </div> <p style="text-align: center; margin-top: 20px;">The certificate is issued to Mardy Anne M. Vizcarra</p> <p style="text-align: center; margin-top: 10px;">Has been certified by ITIL® Foundation Certificate in IT Service Management</p> <p style="font-size: small; margin-top: 10px;">Effective from: 03 Aug 2020 Location: NA</p> <p style="font-size: x-small; margin-top: 5px;">Certificate ID: GR571142578V Certificate Number: 954059172545133</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> </div> <p style="font-size: x-small; margin-top: 5px;">Mardy Anne M. Vizcarra PeopleCert, 10000000000000000000</p> <p style="font-size: x-small; margin-top: 10px;">ITIL 4 Edition Released 14th Nov 2019 This certificate is only valid if accompanied by the corresponding certificate. Only those certificates issued by PeopleCert are valid. ITIL® Foundation Certificate in IT Service Management</p>	<div style="display: flex; justify-content: space-between; align-items: center;"> </div> <p style="text-align: center; margin-top: 20px;">The certificate is issued to Gemalyn Cabanos</p> <p style="text-align: center; margin-top: 10px;">Has been certified by ITIL® Foundation Certificate in IT Service Management</p> <p style="font-size: small; margin-top: 10px;">Effective from: 18 May 2019 Location: NA</p> <p style="font-size: x-small; margin-top: 5px;">Certificate ID: GR571014201CC Certificate Number: 9580025002331561</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> </div> <p style="font-size: x-small; margin-top: 5px;">Gemalyn Cabanos PeopleCert, 10000000000000000000</p> <p style="font-size: x-small; margin-top: 10px;">ITIL 4 Edition Released 14th Nov 2019 This certificate is only valid if accompanied by the corresponding certificate. Only those certificates issued by PeopleCert are valid. ITIL® Foundation Certificate in IT Service Management</p>
--	--

Certification > >

Showing 1 - 6 of 6

First Name	Last Name	Country	ITIL Certificate	Issue	Module	Expiry date
Delfin Jr	Barquilla	100***16	ITIL	Foundation		2012-11-09

ANNEX 5 – Sample Email Notification

Hi [Redacted]

This incident is under investigation. Complete details to follow.

ADVISORY NUMBER 66418	
Client Name:	[Redacted]
Date and Time Incident is Detected:	02/21/2022 12:59:27
Affected Site:	[Redacted]
Ticket Number:	66418
Event Name:	Inbound Traffic from GTI Known Malicious Source - Not Blocked
Priority:	P3

Regards,
Jan Patrick San Miguel
SOC Analyst
Service Operations Group
Trends Managed ICT Services (MCTS)

M +63 9178786617
T +63 2 811 8181

Mon-Fri 0830-1800
Immediate Superior: Alyssa Santiago
Next OoO: 20220226-20220227

Trends & Technologies, Inc.
20th Floor Trafalgar Plaza
105 H.V. Dela Costa St., Salcedo Village,
Makati City 1227 Philippines

www.trends.com.ph

ANNEX 6 – Sample Tabletop Exercise on Incident Handling

1 Procedure

1. Attendees: POCs, leads, and one-level below (if POCs and leads deem them necessary).
2. The game masters will lay out the scenarios and their constraints. Prescribed references:
 - a. Trends: call tree
 - b. Trends and [redacted] playbook
 - c. [redacted]: internal procedures as appropriateAllowed references
 - a. [redacted]: call an internal resource (answer must be relayed into the game)
3. Participants will provide answers to the questions raised. Answers must be straightforward, concise, and complete. Participants may be asked follow-up questions on how tasks will be specifically performed, particularly on internal required processes and procedures.
4. Game masters may interrupt at any time to insert relevant information.
 - a. Trends game master: Pierre
 - b. [redacted] game master: [redacted]
5. Observers will record the answers as well as other observations.
 - a. Trends observer: JQWY
6. After the participants have provided their answers, new information and constraints will be provided by successive injections and the above procedures will be repeated until end.
7. In the event a scenario "hangs" as judged by the observers, the game masters will provide the correct answers so that the scenario may proceed.
8. After each simulation, observers will provide feedback.

2 Duration of exercise (simulation and immediate feedback)

- Scenario 1 – 45 mins
- Scenario 2 – 45 mins
- Scenario 3 – 60 mins

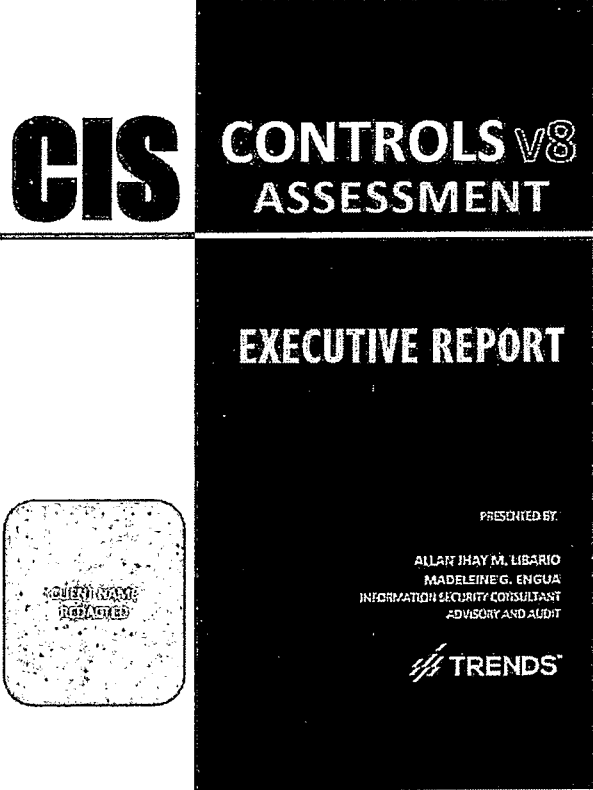
3 Scenarios

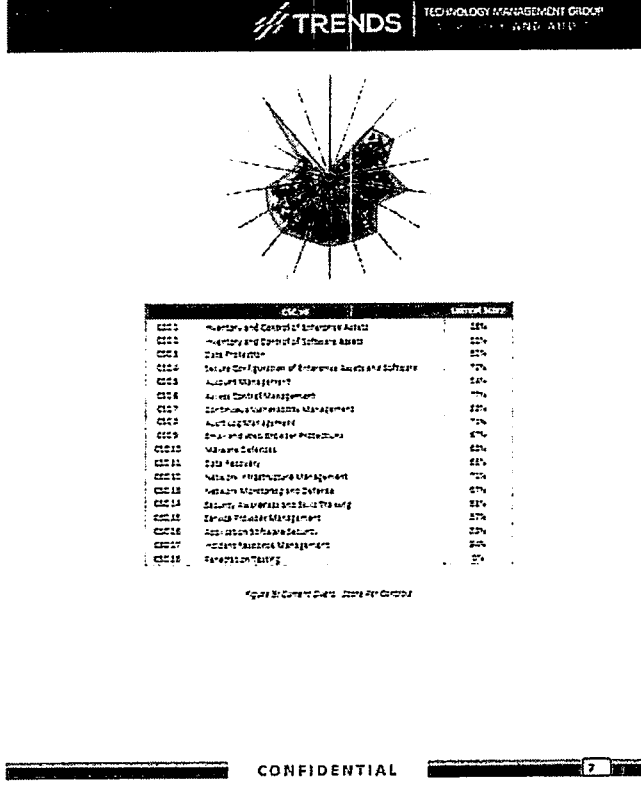
- I. Simple (Brute force attack)
- II. Intermediate (Malware and phishing attack detected on both sides, internal only)
- III. Advanced (Advanced Persistent Threat)

ANNEX 7 – Sample Malware Incident Analysis & Recommendation

ADVISORY NUMBER 66519 Client Name: [Redacted] Date and Time Incident is Detected: 02/23/2022 15:34:34 Ticket Number: 66519 Event Name: Malware Detected – Checkpoint – Not Blocked Priority: P3 Affected Site: [Redacted]	PACKET DETAILS
INCIDENT DETAILS Description: Generic:REP.gelmi - Malware in this family enables cybercriminals to control infected computers remotely. These programs are used to create large groups of zombie computers, known as botnets, which are then exploited for malicious purposes without user knowledge. Criminals can use the infected computers to send spam, crack passwords on remote systems, and perform DDoS attacks and other malicious actions. Source IP: [Redacted] Source Port: 49531 Destination IP: 52.89.4.199 Destination Port: 25 Policy Name: [Redacted] Threat Name: [Redacted] Direction: Outbound Event Subtype: alert Remarks: Device Action: monitor Malware action: Access to site known to contain malware Email detected: groundlines@perbound.net Links: <ul style="list-style-type: none">• http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd• http://www.w3.org/1999/xhtml• http://gar-building.azurewebsites.net/redconerkt.php?utm_source=936utm_content=8• https://content.linkedin.com/content/dam/me/about/LinkedIn_Icon.jpg.original.jpg• https://static.linkedin.com/sc/p/com.linkedin.email-assets-frontend%3Aemail-assets-frontend-static-content%2B_latest_jf%2Femail-asset-f Related Email: N/A	
RECOMMENDATION <ul style="list-style-type: none">• Perform Full Scan on the affected endpoint.• Refrain from accessing/downloading any files/applications from unknown sources.• Kindly block the detected external IP address• For continuous SOC monitoring.	

ANNEX 8 – Cybersecurity Maturity Assessment Sample






Control ID	Control Name	Control Score
CS01	Inventory and Control of Software Assets	55%
CS02	Inventory and Control of Software Assets	55%
CS03	Data Protection	55%
CS04	Secure Configuration of Enterprise Assets and Software	70%
CS05	Account Management	55%
CS06	Access Control Management	60%
CS07	Continuous Vulnerability Management	55%
CS08	Audit Log Management	75%
CS09	Email and Web Browser Protection	60%
CS10	Malware Defenses	65%
CS11	Data Recovery	55%
CS12	Network Architecture Management	70%
CS13	Network Monitoring and Defense	60%
CS14	Security Incident Response Planning	55%
CS15	Security Incident Response Planning	55%
CS16	Application Software Security	55%
CS17	Incident Response Management	55%
CS18	Recovery Planning	55%



ANNEX 9 – Cybersecurity Daily Digest



Managed ICT Services
Service Delivery with Flexibility

THREAT HUNTING DAILY DIGEST

JAN 27 2022

TOP 5 SUSPICIOUS IP Address

1 23.94.159.201	Hits 39
Risk Score: 25 Related to: Phishing	
2 92.255.85.135	Hits 38
Risk Score: 64 Related to: Brute Force Blocking	
3 46.161.27.133	Hits 37
Risk Score: 46 Related to: Brute Force Blocking	
4 212.70.149.72	Hits 19
Risk Score: 69 Related to: Brute Force Blocking	
5 92.255.85.237	Hits 16
Risk Score: 60 Related to: Brute Force Blocking	

You can block IP addresses with the risk score of 40 and higher in your network. Otherwise, add to watchlist.

TOP 5 GLOBAL Vulnerabilities

1 CVE-2021-33742	Hits 1093
NIST Severity: High Related to: CVE 2021-27306	
2 CVE-2021-44228	Hits 576
NIST Severity: Critical Related to: Log4j, Ransomware	
3 CVE-2021-4034	Hits 557
NIST Severity: Medium Related to: HTTPS	
4 CVE-2021-27308	Hits 309
NIST Severity: Medium Related to: HTTPS	
5 CVE-2016-10045	Hits 5
NIST Severity: High Related to: HTTPS	

Remember to check if these exploited vulnerabilities are already patch in your system.

TOP MALWARE IN GLOBAL CYBER ATTACKS

Pegasus

Classification: Spyware
Attack Vector: Spam Campaigns
Target: Vulnerable Organizations
Hits: 132

Description:
Pegasus is a spyware developed by the Israeli cyberarms firm NSO Group that can be covertly installed on mobile phones (and other devices) running most versions of iOS and Android. The spyware is named after Pegasus, the winged horse of Greek mythology. It is a Trojan horse computer virus that can be sent "flying through the air" to infect cell phones.

LATEST INFORMATIONAL NOTES

A bug lurking for 12 years gives attackers root on most major Linux distros

The link for this article is included in this email. Stay tuned for more Cybernews update daily.

Prepared by: TRENDS Operation Center

ANNEX 10 – Threat Hunting Advisory

THREAT HUNTING ADVISORY
OCT 20 2021

ADVISORY FROM SECURITY PROFESSIONALS

Conti/Lockbit MalSpam Campaign

Ransomware • MalSpam
▲ Spike in Cyber Reference

THE THREAT

Through sensitive source reporting, our threat intelligence partner, Insikt Group, recently identified an ongoing TrickBot malspam campaign targeting a large number of personal and corporate email addresses. In this campaign, TrickBot is used as the first stage for initial access to victim networks, with the subsequent deployment of the Conti ransomware variant.



In total, Insikt Group are aware of several million email addresses listed as targets in this campaign. The presence of an email address in this dataset does not imply active TrickBot or Conti infection, but indicates that these recipients are being actively targeted by email spearphishing attempts to initiate an attack.

WHAT'S IN IT FOR YOU?

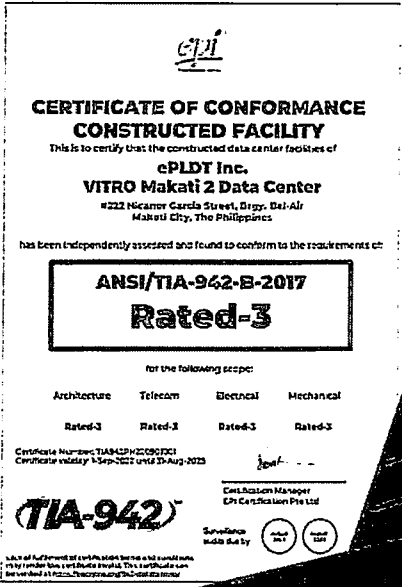

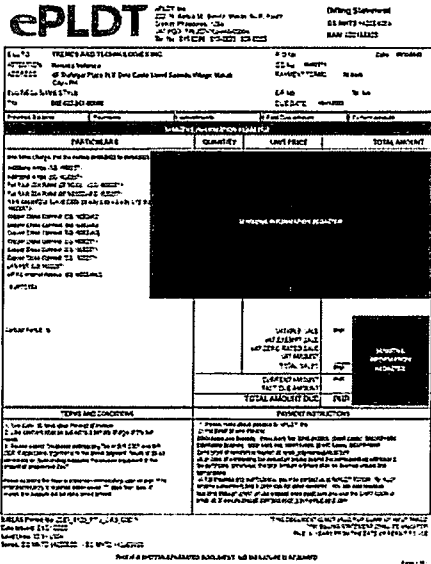
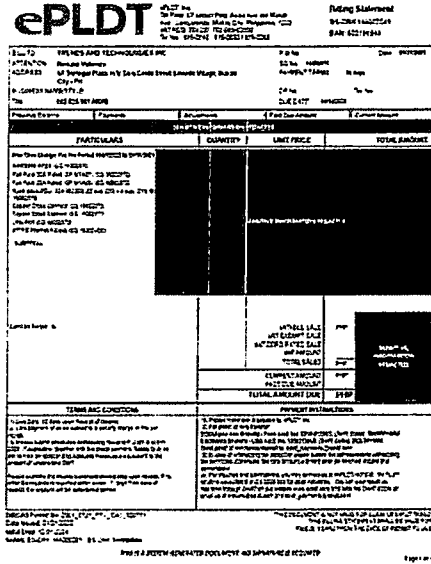
Per checking, after a broader search for any emails with ".com.ph" or ".ph" in the list, none of such domains were found. Do note that this does not mean that the Philippines is free from Trickbot infection, but rather indicates that there is no known active targeting or spearphishing attempts to initiate an attack.

RECOMMENDATIONS

- The Threat Hunting Team recommends the following next actions:
- Use YARA rules to hunt for Conti/Lockbit Ransomware (if applicable).
 - Keep the antimalware, firewalls, and machines updated.
 - Fortify email security with strong spam filters.
 - Keep email security policy in check (DKIM, DMARC, SPF, etc.)



ANNEX 11 – Datacenter Certification

PRIMARY DATACENTER (Makati)	BACKUP DATACENTER (DR SITE) (Clark)																								
 <p>CERTIFICATE OF CONFORMANCE CONSTRUCTED FACILITY This is to certify that the constructed data center facilities of ePLDT Inc. VITRO Makati 2 Data Center #222 Nicamor Garcia Street, Digny, Dal-Air Makati City, The Philippines has been independently assessed and found to conform to the requirements of ANSI/TIA-942-B-2017 Rated-3 for the following scope: Architecture Telecom Electrical Mechanical Rated-3 Rated-3 Rated-3 Rated-3 Certificate Number: TIA942P142090001 Certificate Validity: 1-Sep-2022 until 31-Aug-2025 Certification Manager EPI Certification Pte Ltd Surveillance made on by: [Signature]</p>	 <p>CERTIFICATE OF CONFORMANCE CONSTRUCTED FACILITY This is to certify that the constructed data center facilities of ePLDT Inc. VITRO Clark Data Center VITRO Clark, Lot 3, Hnroy Aquino Avenue Clark Freeport Zone, Pampanga The Philippines has been independently assessed and found to conform to the requirements of ANSI/TIA-942-B-2017 Rated-3 for the following scope: Architecture Telecom Electrical Mechanical Rated-3 Rated-3 Rated-3 Rated-3 Certificate Number: TIA942P142090001 Certificate Validity: 22-Aug-2022 until 21-Aug-2025 Certification Manager EPI Certification Pte Ltd Surveillance made on by: [Signature]</p>																								
 <p>ePLDT Billing Statement To: TRENDS AND TECHNOLOGIES INC Attn: Mr. [Name] Address: [Address] City: [City] Tel: [Phone] Fax: [Fax]</p> <table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th>PARTICULARS</th> <th>QUANTITY</th> <th>UNIT PRICE</th> <th>TOTAL AMOUNT</th> </tr> </thead> <tbody> <tr> <td>... (Detailed list of services and charges) ...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>TOTAL AMOUNT DUE</td> <td></td> <td></td> <td>[Amount]</td> </tr> </tbody> </table> <p>TERMS AND CONDITIONS 1. This bill is valid for 30 days from the date of issue. 2. Payment must be made within 15 days from the date of issue. 3. Late payment will result in a 5% penalty per month. 4. This bill is subject to the terms and conditions of the Service Order Agreement. 5. The client agrees to pay the amount shown on this bill. 6. The client agrees to pay the amount shown on this bill. 7. The client agrees to pay the amount shown on this bill. 8. The client agrees to pay the amount shown on this bill. 9. The client agrees to pay the amount shown on this bill. 10. The client agrees to pay the amount shown on this bill.</p>	PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT	... (Detailed list of services and charges) ...				TOTAL AMOUNT DUE			[Amount]	 <p>ePLDT Billing Statement To: TRENDS AND TECHNOLOGIES INC Attn: Mr. [Name] Address: [Address] City: [City] Tel: [Phone] Fax: [Fax]</p> <table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th>PARTICULARS</th> <th>QUANTITY</th> <th>UNIT PRICE</th> <th>TOTAL AMOUNT</th> </tr> </thead> <tbody> <tr> <td>... (Detailed list of services and charges) ...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>TOTAL AMOUNT DUE</td> <td></td> <td></td> <td>[Amount]</td> </tr> </tbody> </table> <p>TERMS AND CONDITIONS 1. This bill is valid for 30 days from the date of issue. 2. Payment must be made within 15 days from the date of issue. 3. Late payment will result in a 5% penalty per month. 4. This bill is subject to the terms and conditions of the Service Order Agreement. 5. The client agrees to pay the amount shown on this bill. 6. The client agrees to pay the amount shown on this bill. 7. The client agrees to pay the amount shown on this bill. 8. The client agrees to pay the amount shown on this bill. 9. The client agrees to pay the amount shown on this bill. 10. The client agrees to pay the amount shown on this bill.</p>	PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT	... (Detailed list of services and charges) ...				TOTAL AMOUNT DUE			[Amount]
PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT																						
... (Detailed list of services and charges) ...																									
TOTAL AMOUNT DUE			[Amount]																						
PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT																						
... (Detailed list of services and charges) ...																									
TOTAL AMOUNT DUE			[Amount]																						

[Handwritten signature]

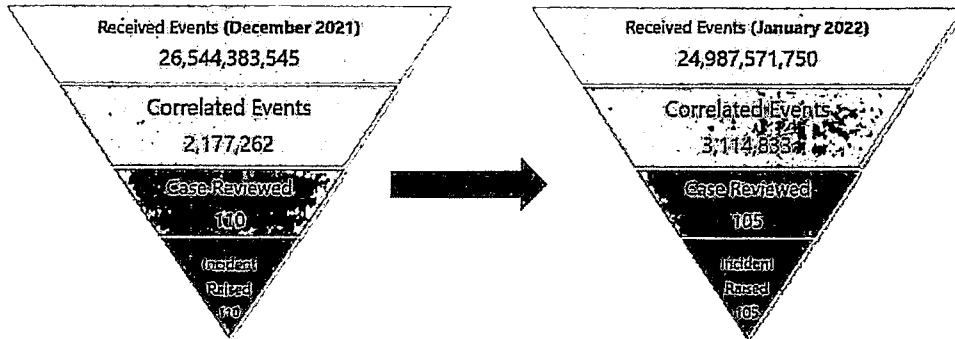
ANNEX 12 – Sample Monthly Reports

Excerpt of Monthly Report for Client A

SIEM: Executive Overview



- Data sources are from 232 devices
- These are events gathered from January 01, 2022 to January 31, 2022
- Correlated events are decreased due to SIEM Correlation Rules fine-tuning activities of Trends TMG-Sec team.

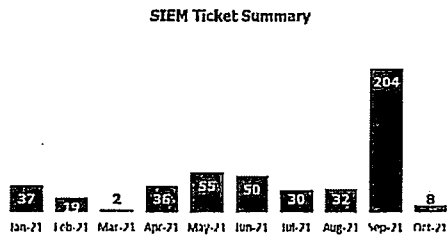


© 2019 Trends & Technologies, Inc. All Rights Reserved.

3

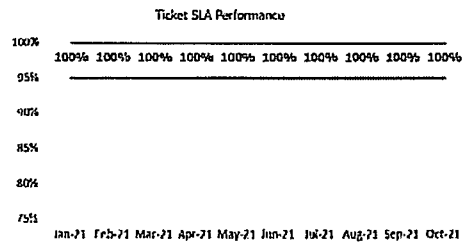
Excerpt of Monthly Report for Client B

SIEM Ticket Summary



SENSITIVE INFORMATION REDACTED

© 2019 Trends & Technologies, Inc. All Rights Reserved.



100% Month-on-Month Running Average SLA Hit Rate

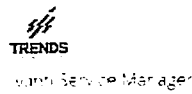
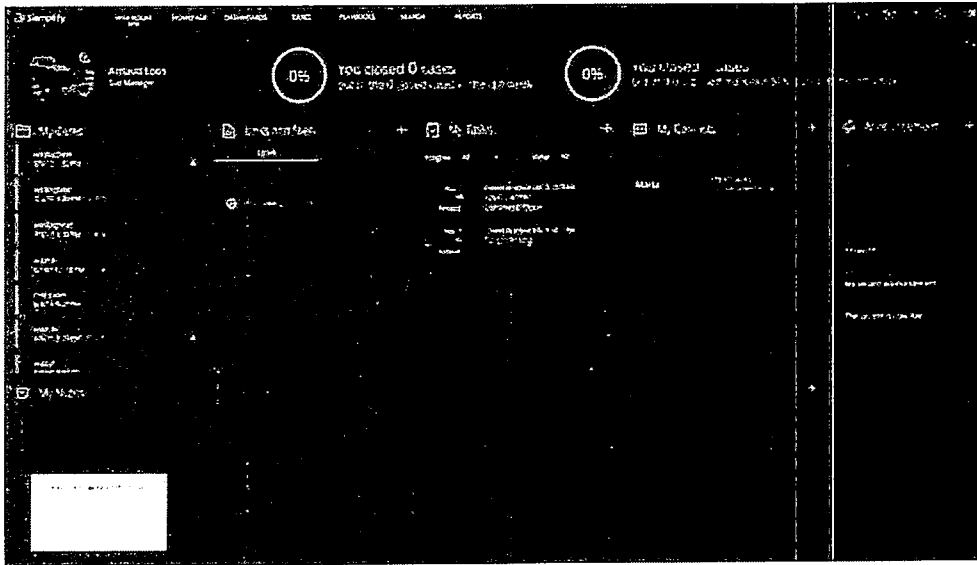
0 P1 and P2 Events Handled (P1-0, P2-0) **204** P3 and P4 Events Handled (P3-8, P4-0)

5



ANNEX 13 – Ticketing Tool

Trends shall use the provided case management to capture and track incidents and facilitate routing to appropriate resolving groups. Below are the sample screenshots of the Ticketing tool.



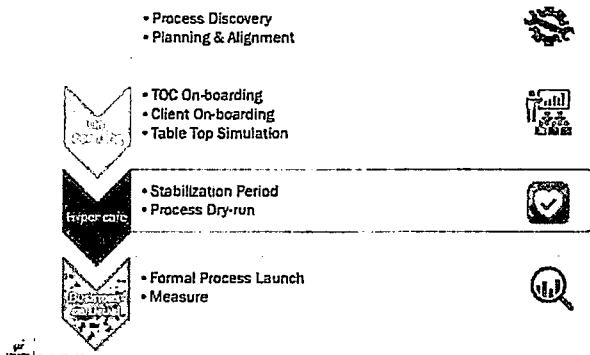
ANNEX 14 – Sample Onboarding Presentation



Overview

- Objective
- Transition Strategy
- On-boarding
- Service Delivery Architecture
- Incident Reporting Process
- Incident Response Playbook
- On-boarding
- Appendices

Transition Strategy



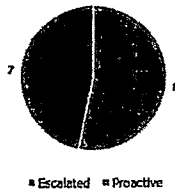
[Handwritten signature]

ANNEX 15 – Sample Security Briefing Presentation

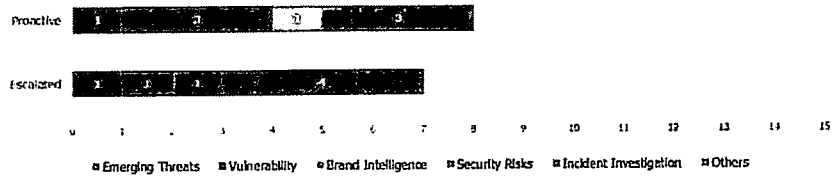
Responding & Adapting to a Changing Cyber Landscape



TH Advisories in January



Analyzed and Reported Advisories by Category



15 Total analyzed and reported advisories for the month of January.

Key Notes:

- All recommended actions from proactive advisories and assessments were followed by MICTS Security Team such as IOC blocking, risk assessment, SIEM/AV rules update, etc.
- From the Weekly Digests, we have proactively blocked 8 trending suspicious IPs in the wild related to different intrusion methods.
- All advisories are resolved.

Advisory Highlights

1. New Multi-Platform "SysJoker" Malware
2. CVE-2022-0166 McAfee Agent Bug
3. Threat Assessment on PwnKit
4. Lazarus Group Latest Campaign
5. Weekly Digest
6. Potential Typosquatted Domain - SENSITIVE INFORMATION REDACTED

THREAT HUNTING

See More Technical Details

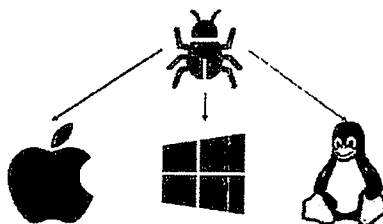
Responding & Adapting to a Changing Cyber Landscape



Advisory of the Month: New Multi-Platform "Sysjoker" Malware

Summary:

- Sysjoker is a remote access trojan and a backdoor that targets Windows, macOS, and Linux operating systems.
- It has advanced backdoor capabilities and can remain undetected for every antivirus scan for several months.
- It masquerades as a system update and generates its four separate Command-and-Control servers by decoding a string retrieved from a text file hosted on Google Drive.



<p>Actions Taken:</p> <ul style="list-style-type: none"> ✓ Successfully blocked the Sysjoker IOCs in McAfee, Symantec, and all perimeter firewalls. ✓ Confirmed that anti-malware solutions (McAfee and Symantec) have their signatures updated. ✓ Created a new correlation rule and alarm to monitor Sysjoker movements. ✓ Confirmed no hits to correlation rule. 	<p>Cyber Posture Assessment:</p> <ul style="list-style-type: none"> ✓ Each Sysjoker techniques has a corresponding correlation rules and security control deployed. ✓ Scanning results showed no detected Sysjoker signatures on endpoints and server. 	<p>THREAT HUNTING</p> <p>See More Technical Details</p>
--	---	--

ANNEX 16 – Sample RCA Report (Details Redacted)



INCIDENT REPORT

Case No. _____

INCIDENT DETAILS			
	Name	Organization	Date
IR Requestor (Person who submitted the IR)			Date Requested: _____
Incident Report Owner			Date Submitted: _____
Resource Person/s and/or Team/s			Date Approved: _____
IR Approved by:			

PROBLEM DETAILS	
Problem Record Number:	
Problem Record Date and Time:	RCA Completed Date: _____
Repeat Problem (Y/N):	

ANNEX 17 – Sample Digital Forensics/Compromise Assessment Report (Details Redacted)

TRENDS Managed ICT Services		TLP:AMBER
TABLE OF CONTENTS		
1 EXECUTIVE SUMMARY		3
2 EVIDENCE INFORMATION OVERVIEW		3
2.1		3
2.2		3
3 DATA ACQUISITION PROCEDURE		4
3.1 TOOLS USED		4
3.2 WORKFLOW		4
3.2.1 PHASE 1		4
3.2.2 PHASE 2		4
3.2.3 PHASE 3		5
4 ARTIFACTS FINDINGS		6
4.1		6
4.1.1 SUMMARY		6
4.1.2 USERS		6
4.1.3 MALWARE		7
4.1.4 OS CONFIGURATION		8
4.1.5 NETWORK & PROCESS MONITORING		8
4.2		9
4.2.1 SUMMARY		9
4.2.2 USERS		9
4.2.3 MALWARE		10
4.2.4 OS CONFIGURATION		11
4.2.5 NETWORK & PROCESS MONITORING		11
APPENDIX		13

Digital Forensics Report's Table of Contents

TRENDS Managed ICT Services		TLP:AMBER
TABLE OF CONTENTS		
1 OVERVIEW		3
1.1		3
1.2		3
2 SERVER (RAC) AND MEMORY DUMP FINDINGS		4
3 ITEM FINDINGS		7
3.1		7
3.2		9
4 CONCLUSION		12
5 RECOMMENDATIONS		12
DOCUMENT ACCEPTANCE		12

Compromise Assessment Report's Table of Contents

**ANNEX 18 – Snippet of Agenda Acceptance for Annual Incident Response Readiness Training
(Details Redacted)**

**Agenda Acceptance for
Annual Incident Response Readiness Training**

Good day, ~~_____~~

Trends and Technologies Inc. (Trends) is pleased to present the proposed agenda for the Annual ~~_____~~

About:

Trends' Annual Incident Response Readiness Training is an event that aims to effectively address the stipulated objectives of fortifying incident response capabilities and fostering a culture of heightened IT security awareness across various stakeholders. By extending training to both technical experts and non-technical personnel within the agencies, it aims to foster a unified understanding of the incident response processes.

Proposed Agenda:

Objectives:

~~_____~~

~~_____~~

~~_____~~

Target Audience: ~~_____~~

Proposed Date and Time: ~~_____~~

Proposed Venue: Trends & Technologies Inc., 16th floor, Trafalgar Plaza, 105 H.V. Dela Costa, Makati, 1227

ANNEX 19 – Snippet of Incident Response Playbook (Details Redacted)

3 Incident Playbook

3.1 Data Theft

A. About

- 1. This play covers the detection, analysis, containment, eradication, and recovery of data theft incidents.
- 2. The play is designed to be executed by the Incident Response Team (IRT) in collaboration with the relevant business units.
- 3. The play is a living document and will be updated as needed.

B. Tools:

- 1. Network traffic analysis tools (e.g., Wireshark, NetworkMiner)
- 2. Endpoint protection tools (e.g., Symantec, McAfee)
- 3. Data loss prevention (DLP) tools (e.g., Symantec, McAfee)
- 4. Forensic tools (e.g., FTK, Encase)
- 5. Incident response management (IRM) tools (e.g., Splunk, ServiceNow)

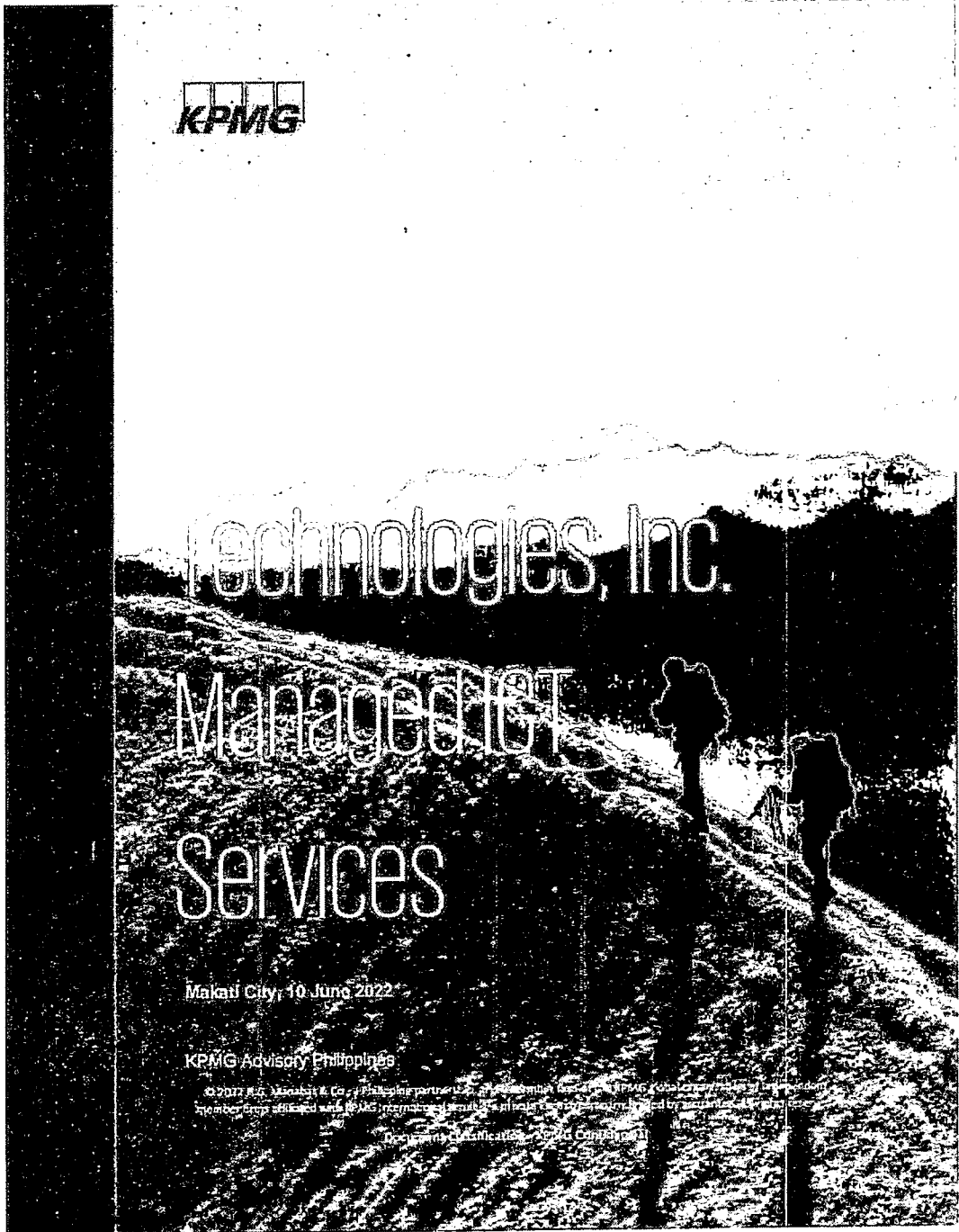
C. Detection and Analysis

- 1. Monitor network traffic for suspicious activity (e.g., large data transfers, unusual destinations).
- 2. Monitor endpoint activity for suspicious behavior (e.g., unauthorized file access, data exfiltration).
- 3. Monitor DLP alerts for data loss events.
- 4. Investigate the source of the data theft and identify the affected systems and data.
- 5. Determine the scope of the data theft and the potential impact on the organization.

D. Containment and Eradication

- 1. Isolate the affected systems and networks to prevent further data loss.
- 2. Disable the accounts of the suspected attacker.
- 3. Remove the attacker's access to the organization's systems and data.
- 4. Investigate the root cause of the data theft and identify the vulnerabilities that were exploited.
- 5. Implement measures to prevent a recurrence of the data theft (e.g., patching vulnerabilities, strengthening access controls).
- 6. Notify the relevant business units and stakeholders of the data theft and the actions being taken.
- 7. Conduct a post-incident review to identify lessons learned and improve the organization's incident response capabilities.

ANNEX 20 – TRENDS SOC 2 Type II Attestation Report



ANNEX 21 – SAMPLE SOC DASHBOARDS

splunk enterprise App: ES Motherhip App for Splunk Administrator Messages Settings Activity Help Find
Environments Multi ES Dashboards Search ES Motherhip App for Splunk

Environments 4 environments being monitored New Environment

ID	Name	Management Server	Web Server	Errors	Status	Actions
>	ES Nighth 1	man-srv-1-instance-0009 LE	web-srv-1-instance-0000 LE		✓ Ok	Edit ↓
>	ES Nighth 2	man-srv-2-instance-0009 LE	web-srv-2-instance-0000 LE		✓ Ok	Edit ↓
>	ES Nighth 3	man-srv-3-instance-0009 LE	web-srv-3-instance-0000 LE		✓ Ok	Edit ↓
>	ES Nighth 4	man-srv-4-instance-0009 LE	web-srv-4-instance-0000 LE		✓ Ok	Edit ↓

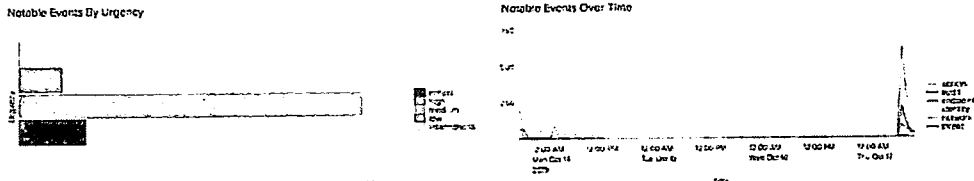
splunk enterprise App: ES Motherhip App for Splunk Administrator Messages Settings Activity Help Find
Environments Multi ES Dashboards Search ES Motherhip App for Splunk

Multi ES Security Posture Select an environment All environments Get Report

Select an environment: All

Security Posture: All environments

Access Notables	Endpoint Notables	Network Notables	Identity Notables	Audit Notables	Threat Notables
Total Count	Total Count	Total Count	Total Count	Total Count	Total Count
528	710	2319	14	18	17



splunk enterprise App: ES Motherhip App for Splunk Administrator Messages Settings Activity Help Find
Environments Multi ES Dashboards Search ES Motherhip App for Splunk

Multi ES Incident Review Select an environment All Get Report

Select an environment: All

Environment	Urgency	Status	Owner	Security Domain	Resolution
ES Nighth 1	High	Assigned	IT-001	Network	Investigating
ES Nighth 2	Medium	Assigned	IT-002	Endpoint	Investigating
ES Nighth 3	Low	Assigned	IT-003	Access	Investigating
ES Nighth 4	Info	Assigned	IT-004	System	Investigating
ES Nighth 1	High	Assigned	IT-001	Network	Investigating
ES Nighth 2	Medium	Assigned	IT-002	Endpoint	Investigating
ES Nighth 3	Low	Assigned	IT-003	Access	Investigating
ES Nighth 4	Info	Assigned	IT-004	System	Investigating
ES Nighth 1	High	Assigned	IT-001	Network	Investigating
ES Nighth 2	Medium	Assigned	IT-002	Endpoint	Investigating
ES Nighth 3	Low	Assigned	IT-003	Access	Investigating
ES Nighth 4	Info	Assigned	IT-004	System	Investigating
ES Nighth 1	High	Assigned	IT-001	Network	Investigating
ES Nighth 2	Medium	Assigned	IT-002	Endpoint	Investigating
ES Nighth 3	Low	Assigned	IT-003	Access	Investigating
ES Nighth 4	Info	Assigned	IT-004	System	Investigating

