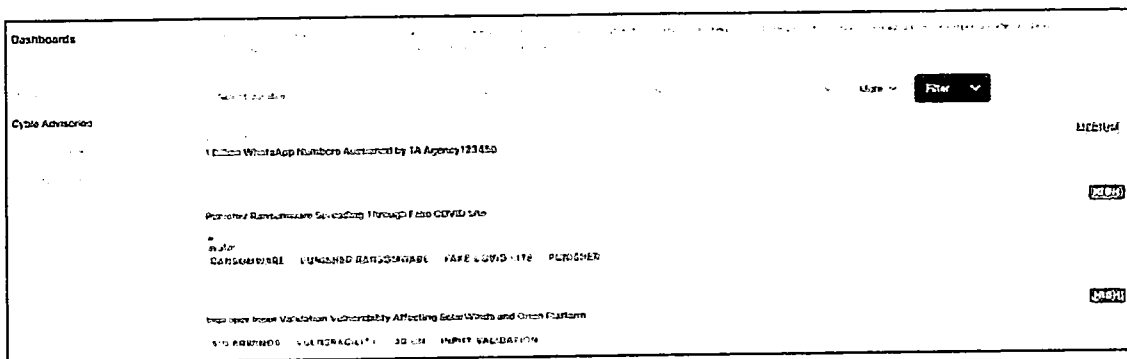


Cyber Threat Intelligence

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

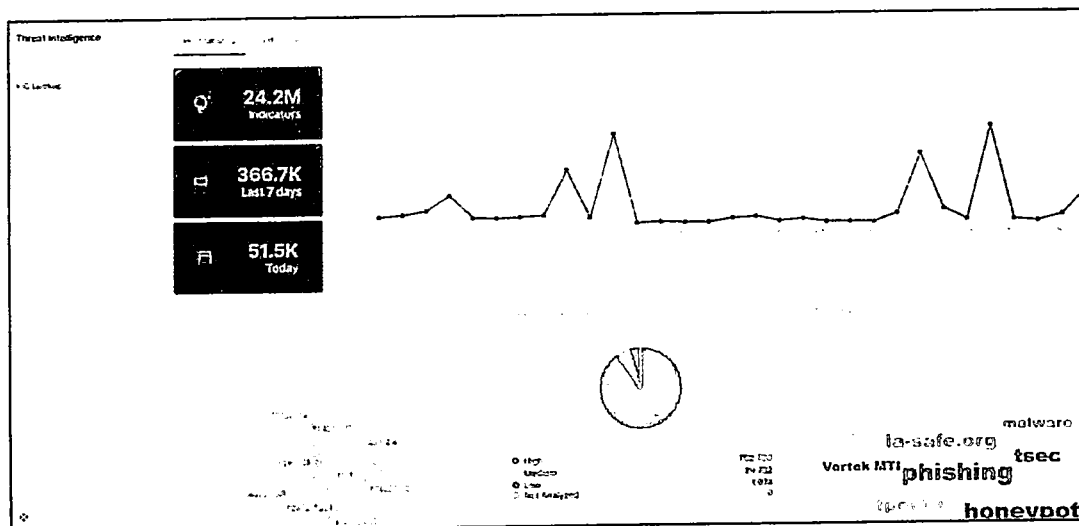
- our own and managed global honeypot sensor intelligence network
- the open internet,
- open-source public threat intelligence sources
- premium commercial threat intelligence provider feeds.

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



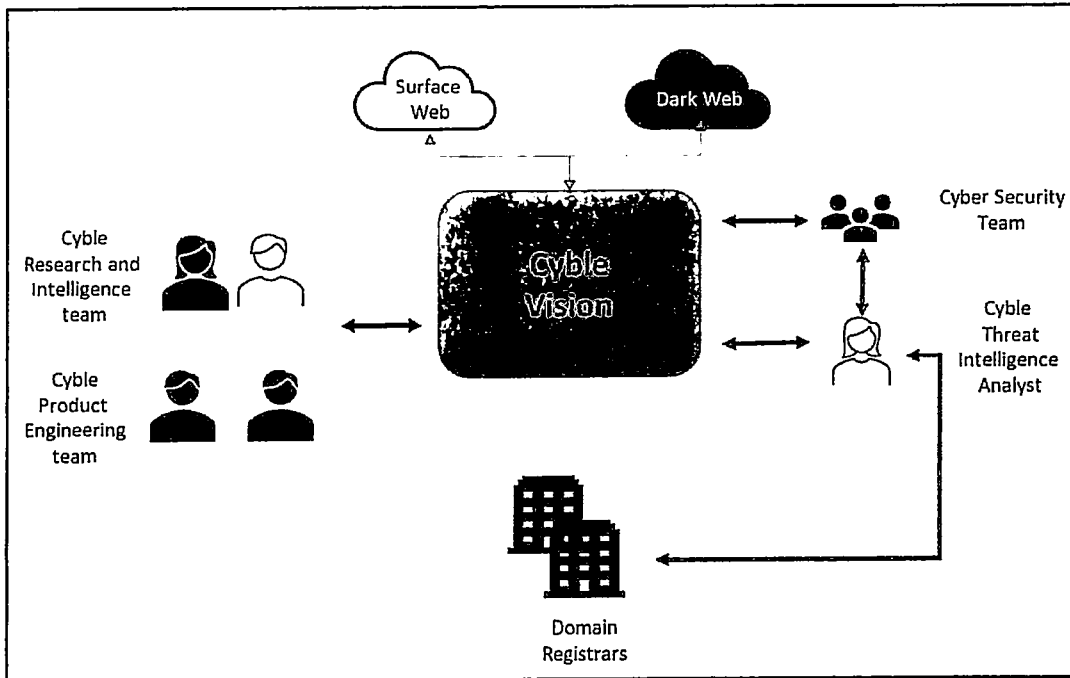
Cyble Advisories

2.5.1 Global IOC Repository



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

Service Delivery Approach



Annual Subscription to the Cyble Vision platform also includes the services of a dedicated delivery manager to assist clients in operationalizing the Cyble Vision service and managing their queries and support requests on an ongoing basis, throughout the tenure of the contract. Our delivery manager carries out the following activities as part of our service –

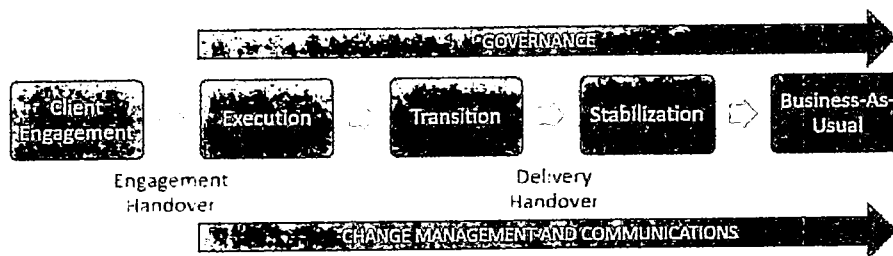
1. Conducting training sessions for the client team members to familiarize them with the Cyble Vision Platform and onboarding team members onto the Cyble Vision platform by provisioning access, configuring search queries and helping clients in analyzing search query results
2. Handling queries and requests for assistance related to configuration, product feature navigation, report generation etc
3. Reviewing the alerts from Cyble Vision and notifying the concerned team members about events of interest monthly basis.
4. Working with the Cyble Research and Intel team at the backend for servicing specific / ad-hoc emergency intelligence requests from the client team
5. Sharing relevant cyber threat intelligence advisories and reports with the client team
6. Coordinating with concerned third parties for take-down requests authorized by the client
7. Coordinating with the Cyble product engineering team to enable Cyble Vision platform integration with client systems for threat feed / alert integration
8. Publishing Global Sensor Intelligence Reports on a weekly basis, CTI Operations Reports monthly and Global Ransomware Intelligence Reports on a quarterly basis
9. Organizing and attending monthly engagement review meetings with Cyble Delivery Leadership and client teams for service governance and continuous improvement



PROJECT MANAGEMENT PROGRAM PLAN FOR GOVERNMENT INSURANCE CLUSTER

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

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



1. Client Engagement.

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

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

2. Execution.

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

Trends & Technologies, Inc.

6th Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines

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

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

3. Transition.

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

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

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

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

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

4. Stabilization.

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

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

5. Business-As-Usual.

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

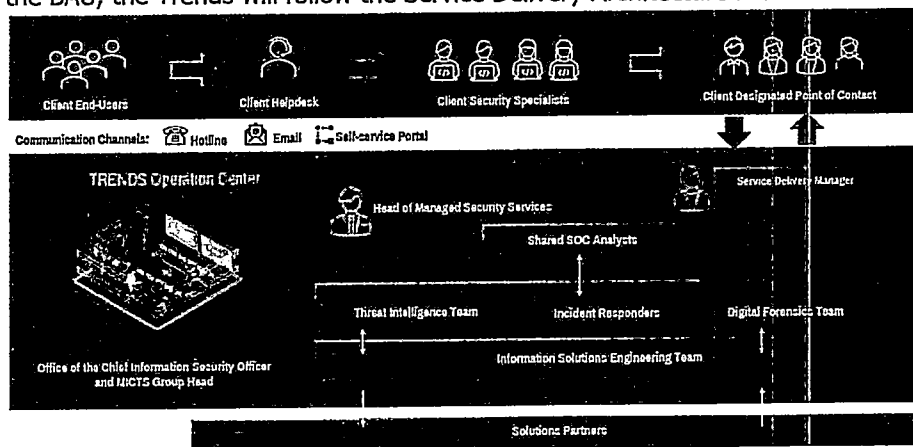


Trends will provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a period of time.

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

Service Delivery Architecture

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



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

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

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

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

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

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

Manpower Resources

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

Personnel	Roles and Responsibilities
SOC Manager or Tier 4 Analyst (1)	In charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. Responsible for the management of the MSOC operations for the agency and cluster.
Tier 3 Analyst (1)	Responsible for managing critical incidents. Responsible for actively hunting for threats and assessing the vulnerability of the business. 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
Tier 2 Analyst (1)	Responsible for conducting further analysis and deciding on a strategy for containment. 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
Tier 1 Analysts (2)	Responsible for the following tasks: 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 6. General Communication 7. Weekly Summary Reports

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

Reports and Meetings

- **Monthly Service Performance Report.**

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

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

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

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

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

- **Monthly Service Performance Review Meeting.**

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

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



CYBER SECURITY INTELLIGENCE MANAGEMENT POLICIES, STANDARDS, PROCEDURES & GUIDELINES

This document serves as a policy framework that sets out procedures and goals and objectives that may be used as guidance for decision-making, guide in making a more detailed set of policies or to guide ongoing maintenance of an organization's policies.

DOCUMENT ID

DOCUMENT OWNER **TRENDS MICTS**

DOCUMENT CLASSIFICATION **TLP:GREEN INTERNAL**

DOCUMENT STATUS **RELEASE**

DOCUMENT VERSION **1.0**

REVISION DATE **2023 SEPTEMBER 01**



TABLE OF CONTENTS

1 INTRODUCTION	3
1.1 OVERVIEW	3
1.2 PURPOSE OF THE DOCUMENT	3
1.3 TARGET READERSHIP	3
1.4 DOCUMENT DEFINITIONS	3
1.5 REFERENCE DOCUMENTS & BIBLIOGRAPHY	3
2 PURPOSE AND OBJECTIVE	5
2.1 PURPOSE	5
2.2 OBJECTIVE	5
3 SCOPE AND DEFINITION	6
4 COMPLIANCE	7
5 AWARENESS	8
6 CYBER SECURITY INTELLIGENCE MANAGEMENT	9
6.1 POLICY	9
6.2 PROCESS	9
6.2.1 COLLECTION	9
6.2.2 PROCESSING	9
6.2.3 ANALYSIS	9
6.2.4 DISSEMINATION	9
6.3 PROCEDURES	10
6.3.1 THREAT DISCOVERY PROCEDURE	10
6.3.2 INTERNAL THREAT DISCOVERY PROCEDURE	11
6.3.3 MALWARE DISCOVERY PROCEDURE	12
6.3.4 VULNERABILITY DISCOVERY PROCEDURE	13
6.3.5 THREAT HUNTING SYSTEM ENHANCEMENT	14
6.4 GUIDELINES	15
6.4.1 SECURITY FRAMEWORKS	15
6.4.2 VULNERABILITY MANAGEMENT	15
7 CYBER SECURITY INTELLIGENCE METRICS	16
7.1 SUCCESS CRITERIA	16
7.2 EFFICIENCY & EFFICACY CRITERIA	16
8 KEY PERFORMANCE INDICATORS	16
ANNEX	17
ANNEX 1 – THREAT HUNTING TOOLS FOR DISCOVERY PROCESS	18
ANNEX 2 – THREAT HUNTING DATABASE SCHEMA (TH-DB)	20

1 Introduction

1.1 Overview

Cyber threats are ever evolving. The threat actors are becoming more creative and more active than ever. Threat actors and attacks are now coming from different sectors with varying motives and objectives. This poses greater risks in today's interconnected environment. To be able to have a fighting chance against these threats, an organization can no longer stay reactive and rely on response to cyber threats and attacks. In this day and age, actionable information is the game changer. Vulnerabilities and threats must now be hunted, analyzed and establish preemptive, protective and preventive controls to deter, prevent and avoid being compromised by these threats. In addition to protective controls, detection mechanisms must be in place as well as a well thought of incident mitigation and response plan.

1.2 Purpose of the Document

This document serves as a policy framework that sets out procedures and goals and objectives that may be used as guidance for decision-making, guide in making a more detailed set of policies or to guide ongoing maintenance of an organization's policies.

1.3 Target Readership

This document is prepared for the following:

- Trends Cyber Security Intelligence
- Trends Managed ICT Services
- Any authorized person or entity requiring information and education about the subject matter at hand.

1.4 Document Definitions

Term	Definition
Cyber security	Refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures. ¹
Security Posture	The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. ²

1.5 Reference Documents & Bibliography

<https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
https://en.wikipedia.org/wiki/Policy_framework
https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

¹ CyBOK v1, <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>

² <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

https://en.wikipedia.org/wiki/Security_Policy_Framework
https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53
https://en.wikipedia.org/wiki/Kill_chain

2 Purpose and Objective

2.1 Purpose

Cyber space is full of cyber threats that may well affect any organization at any time. Cyber threat detection should be an important part in every organization incident response plan and overall IT security strategy. Furthermore, by investing and focusing on threat detection, organizations and companies can avoid many cyber threats. The importance of cyber threats early detection can be summarized in the below points:

- The earlier detection gives the security teams the chance to contend the threats before the attacks.
- Earlier detection allows quicker protection against emerging threats in cyber space.
- The detection of undiscovered security breaches and malware infections will be easier and more accurate.
- Sufficient threat information allows the automation of incident response using smart response.
- Proactive protection will save the organizations in terms of cost and reputation in case of successful cyber-attacks.
- Early detection then prevention can protect the organizations from future cyber-attacks.

It is with this premise that Cyber Security Intelligence Management is established.

2.2 Objective

The objectives of having documented Cyber Security Intelligence Management Policies, Standards, Procedures and Guidelines are the following:

- To have a unified document that contains all pertinent information that are related to Cyber Security Intelligence Management.
- Maintain client satisfaction.
- To establish KPIs for measuring the effectivity and efficiency of the standards and procedures

3 Scope and Definition

It is the intention of the Cyber Security Intelligence Management to encompass information security improvement on all fronts. This means that Cyber Security Intelligence Management shall establish the policies, standards, procedures, and guidelines that would protect an organization from the adverse effects of vulnerabilities and plethora of cyber-space threats.

4 Compliance

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

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

5 Awareness

It is the responsibility of the Compliance and Continual Improvement department to establish informational training regarding the Cyber Security Intelligence Policy.

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

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

6 Cyber Security Intelligence Management

6.1 Policy

The Cyber Security Intelligence Management establishes and provides for the following:

1. To establish working units that would be responsible for establishing information security frameworks that would be used to measure and improve the security posture of TRENDS and its clients.
2. To establish working units that would be responsible for hunting vulnerabilities and threats on the various facades of the internet (surface, deep, dark web).
3. To establish working units that would look for, assess, select and implement information security solutions that would enable an organization to effectively promote information security awareness, protection and early detection of threats.
4. To establish working units that would be responsible for performing digital forensics on sensitive and critical compromised assets.
5. To provide intelligence reports or notice on the latest cyber threats or information or detection of targeted attacks against TRENDS and its clients.

6.2 Process

6.2.1 Collection

- Information gathering
 - Private or public threat feeds
 - Forums
 - Social media
 - and Open-source Intelligence (OSINT) to identify potential threats.
- No records kept. Viewing only

6.2.2 Processing

- Collected information will be subjected to:
 - Review/Filtering/tool fine tuning
 - Removing of irrelevant/inaccurate data
 - Data Enrichment

6.2.3 Analysis

- Processed information is then analyzed to:
 - Identify pattern.
 - Trends
 - and Anomalies that may indicate potential threats.
- Includes both:
 - Quantitative and Qualitative assessment.

6.2.4 Dissemination

- If the analysis is completed, the findings are disseminated to the relevant stakeholders based on purpose:
 - Security team
 - Management

6.3 Procedures

6.3.1 Threat Discovery Procedure

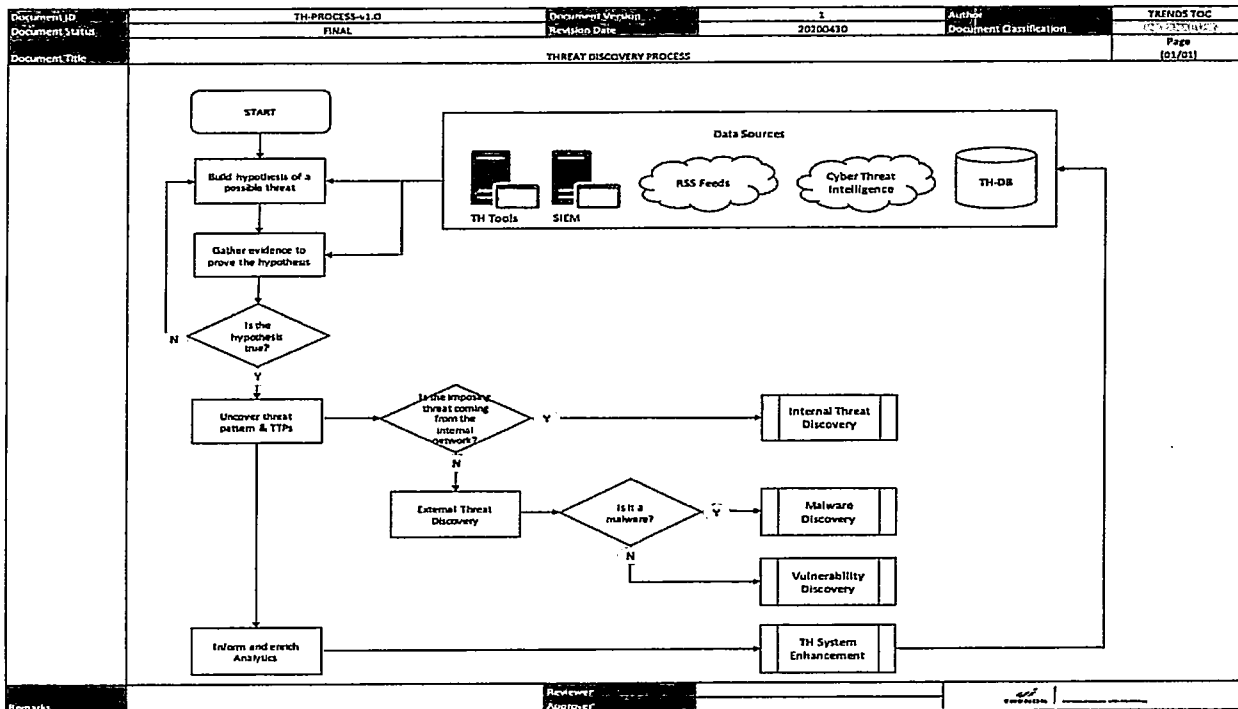


Figure 1 – Threat Discovery Process

1. The Threat Hunter builds a hypothesis for a potential threat driven by either of the following methodologies: Analytics, Intelligence, and Awareness.
2. Next, the TH hunts all relevant data sources for the existence of any related indicators of threats. This includes Threat Hunting tools, SIEM, RSS feed, Cyber Threat Intelligence (CTI), and/or Threat Hunting Database (TH-DB).
 - The hypotheses are marked by true or false. If the hypothesis is true, the team will warrant a deeper investigation and develop the scope for the kill chain.
3. Then, the TH concentrates on collecting and analyzing the data to find any new trends or tactics that may have been executed or will be executed to carry out the attack. The findings are identified, immediate action is performed for detected intrusions or malicious activities and an incident is declared.
 - a) If the imposing threat is detected under the radar of organization’s network, it will proceed to internal threat discovery process;
 - b) Otherwise, it will be on the external threat discovery process wherein the threats from the wild are being investigated to see how it can impact the organization and mitigate the damage that it can cause.
 - There are two classifications on the external threat hunting process namely: malware discovery and vulnerability discovery.
4. The final step consists of utilizing the knowledge and discoveries made to improve the security detection and refine the alerting procedures during the investigation.

- TH System Enhancement focuses on improvement of the technology used to detect the threat. It includes but not limited to the following: fine-tuning of SIEM, applying and fine-tuning machine learning on SIEM, updating TH-Database, developing the centralized RSS feeds, and remodeling the process if necessary.

6.3.2 Internal Threat Discovery Procedure

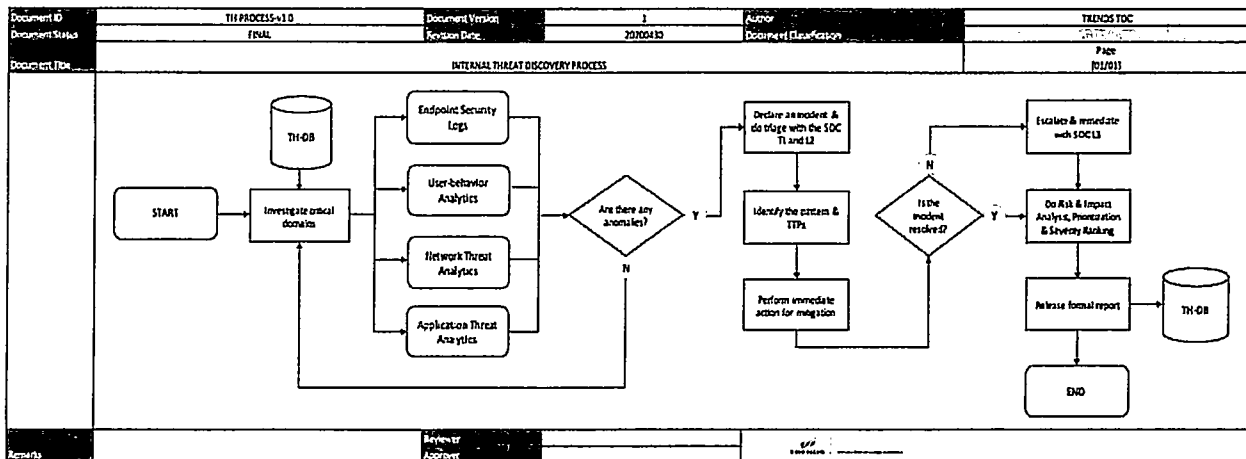


Figure 2 – Internal Threat Discovery Process

This section highlights the high-level perspective of malware-incident handling. Refer to the **TRENDS_Incident Management PSPG-v1.0_TLPGREEN : ANNEX 6** for thorough process.

- The TH will review all the documents and/or any related case to the hypothesis from TH-DB and request for team's approval to conduct investigation. The following are the critical domains for investigation:
 - Endpoint Security Logs. Endpoints are monitored by the SOC for any compromise or suspicious activities. The first-level team investigates the spread to block the attacks. TH then verify and remove the false positives and analyze logs to detect attacks that may have bypassed other endpoint and security controls.
 - 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.
 - Network Threat Analytics. TH analyze multiple cyber intelligence sources from vendors and threat advisories as well as SIEM logs and data feeds to sniff out suspicious activities on the network and application systems. Hidden fileless malware or unknown threats are correlated with anomalies across a number of data pools. This helps to provide full visibility for identifying complex, multi-channel attacks.
 - Application Threat Analytics. Vulnerability intelligence from vendors and data flow analysis help TH identify high-risk applications for vulnerable entry points and track low footprint applications that are often attractive targets for attack with zero-day exploits.
- Next, the TH will declare an incident and request a triage with SOC TL & SOC L2 if there are any confirmed anomalies found on the critical domains. Otherwise, further investigation on critical domains must be done.



3. Based on the gathered data and with the help of MITRE's Att&ck Framework, the team will identify the threat pattern and its TTP to see what it had already done and its next step.
4. After the investigation, the team will perform all the immediate action for mitigation and other countermeasures to prevent it.
5. The team will evaluate the risk and the extent of its impact once the attack becomes successful. Then, determine the severity of the finding. In case the incident is not yet resolved, the team will escalate the case and remediate with SOC L3.
6. The team will then release a formal report or advisory that indicates (but not limited to) the following: executive summary, overall assessment and rating, severity and prioritization of findings, scope and targets, details of threat, impact and risk analysis, mitigation recommendations and actions taken. For all critical findings, advisory must be released as soon as possible.
7. The results of the investigations and collected information will be stored into TH Database (TH-DB) for future reference.

6.3.3 Malware Discovery Procedure

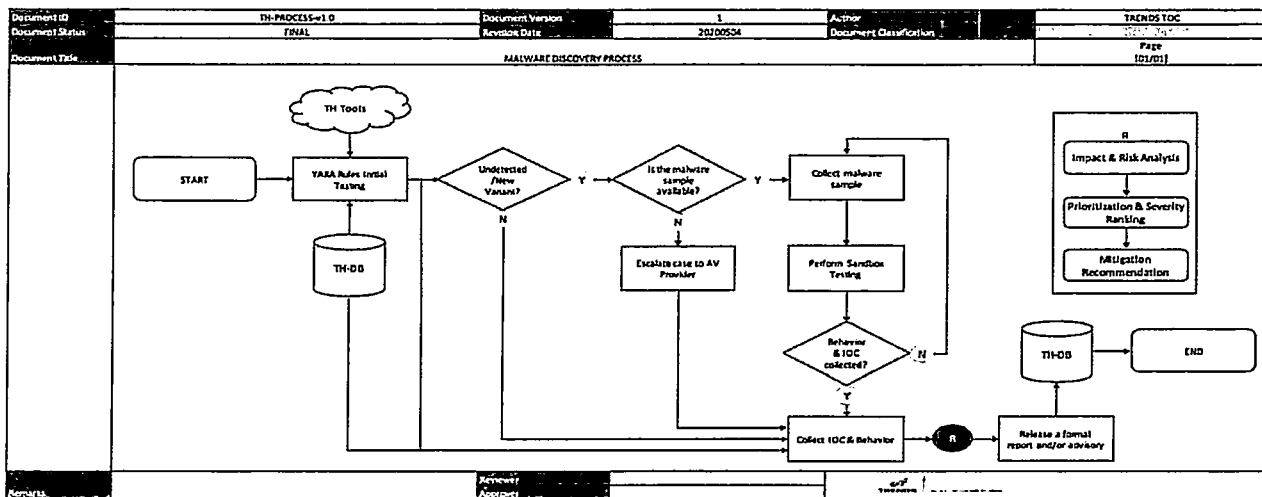


Figure 3 – Malware Discovery Process

This section highlights the high-level perspective of malware-incident handling. Refer to the **TRENDS_Incident Management PSPG-v1.0_TLPGREEN: ANNEX 6** for thorough process.

1. Check if there's a detection based on the TH-tools or predefined YARA rules. These rules are modified based the information fed on the TH-DB.
2. Check the availability of the information regarding the malware from the mentioned sources.
 - a) If the malware is not a new variant or undetected, gather all the latest information about the malware (IOCs & behavior).
 - b) If the malware is a new variant or undetected, check the availability of the sample for deep-divide analysis.
 - (1) If there's no available sample, escalate the case to the AV provider and gather all the information about the malware.
 - (2) If the sample is available, gather it and conduct sandbox testing to collect all IOCs and its behavior.
3. Analyze and understand the findings:

- a) Determine the risk and extent of impact it can cause to the organization.
 - b) Determine the overall severity of the finding based on the impact and risk analysis.
 - c) Determine the appropriate mitigation procedures.
4. Release a formal report or advisory that indicates (but not limited to) the following: executive summary, overall assessment and rating, severity and prioritization of findings, scope and targets, details of malware, impact and risk analysis, mitigation recommendations. For all critical findings, advisory must be released as soon as possible.
 5. The results of the investigations and collected information will be stored into TH Database (TH-DB) for future reference.

6.3.4 Vulnerability Discovery Procedure

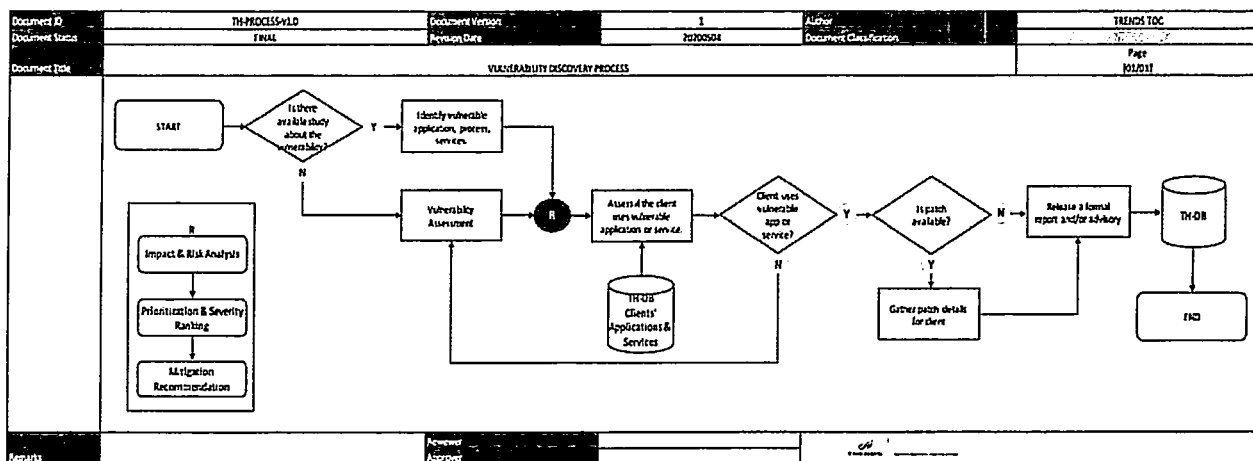


Figure 4 – Vulnerability Discovery Process

The TH have generated a hypothesis about vulnerability then, the team will:

1. Conduct further research about the vulnerability from the data sources.
 - a) If there's enough available studies, the TH will identify and collect information about the vulnerable resources (its behavior, patterns, and targets).
 - b) If there's no available studies, the TH will conduct its own vulnerability assessment for identifying its behavior, patterns, and targets.
2. Analyze and understand the findings:
 - a) Determine the risk and extent of impact it can cause to the organization.
 - b) Determine the overall severity of the finding based on the impact and risk analysis.
 - c) Determine the appropriate mitigation procedures.
3. Conduct an assessment if the client's application and services stored in the TH-DB are vulnerable to the threat.
 - a) If the client resources are not vulnerable to the threat, TH will conduct another Vulnerability Assessment test.
 - b) If the client resources are vulnerable to the threat, TH will conduct a research on how to eradicate the vulnerability.
 - (1) If the patch is available, TH will collect all the data like URL link of downloadable patch for the resources.
 - (2) If the patch is not yet available, TH will generate a report about the possible outcome of the vulnerability if not eradicated.

[Handwritten signature]

4. Release a formal report or advisory that indicates (but not limited to) the following: executive summary, overall assessment and rating, severity and prioritization of findings, scope and targets, details of vulnerabilities, impact and risk analysis, proof of exploit and mitigation recommendations. For all critical findings, advisory must be released as soon as possible.
5. The results of the investigations and collected information will be stored into TH Database (TH-DB) for future reference.

6.3.5 Threat Hunting System Enhancement

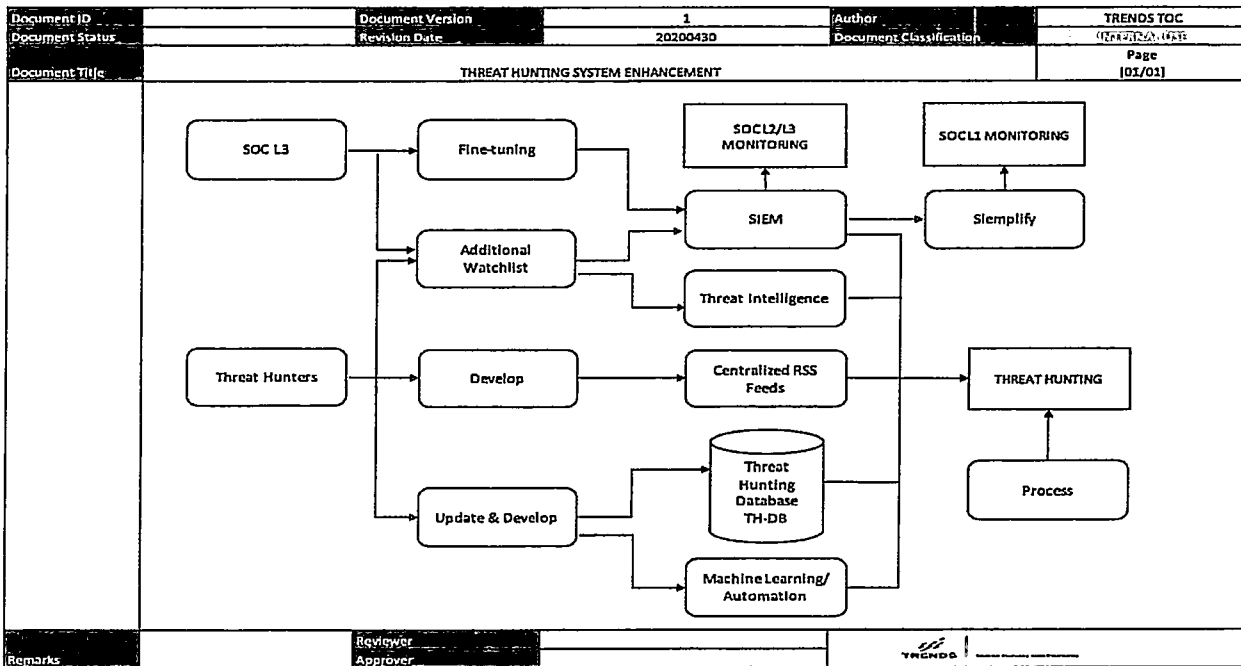


Figure 5 – Threat Hunting Service Enhancement

TH System Enhancement focuses on improvement of the technologies used to detect the threat. The following are the responsibilities of Threat Hunters on the specified technologies:

1. SIEM – Add watchlist for monitoring.
2. Threat Intelligence – Add watchlist for research and monitoring.
3. Centralized RSS Feeds – Develop the feeds for the use of organization.
4. Threat Hunting – Database (TH-DB) – Frequently update with the investigated threats. Develop for ease of accessibility.
5. Machine Learning / Automation – Integrate machine learning in threat hunting. Develop methods to automate tasks.

Process – If necessary, change/modify the process for more efficient threat hunting.

6.4 Guidelines

6.4.1 Security Frameworks

6.4.1.1 Framework for Improving Cybersecurity

The framework to be used as a guide in improving the cybersecurity posture is the NIST Cyber Security Framework (NIST CSF 1.1).

6.4.1.2 Security Controls Framework

NIST 800-53r5, CIS Controls V8 are the 2 suggested security controls framework that will determine the security posture of an organization.

6.4.1.3 Kill Chain Framework

MITRE ATT&CK is the suggested underlying framework for the development of threat modeling, protection and detection.

6.4.2 Vulnerability Management

An Information Security Continuous Monitoring capability that identifies vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.³

³[https://csrc.nist.gov/glossary/term/vulnerability_management#:~:text=Definition\(s\)%3A,extend%20compromise%20to%20the%20network.](https://csrc.nist.gov/glossary/term/vulnerability_management#:~:text=Definition(s)%3A,extend%20compromise%20to%20the%20network.)

7 Cyber Security Intelligence Metrics

7.1 Success Criteria

The success of the Cyber Security Intelligence shall be measured through:

- Annual review on a serviced organization's security posture where the security posture rating has improved against the previous year.
- Annual review of security incidents (if any).

7.2 Efficiency & Efficacy Criteria

The efficiency and efficacy criteria for the Cyber Security Intelligence Management are as follows:

- Ability to discover emerging threats and vulnerabilities within a prescribed amount of time from the time the emerging threat or vulnerability was published from a trusted vulnerability managing entity such as NIST NVD and/or MITRE CVE.
- Ability to publish technical news, articles, advisories or digests within a prescribed amount of time from the time the emerging threat or vulnerability was published from a trusted vulnerability managing entity such as NIST NVD and/or MITRE CVE.

8 Key Performance Indicators

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

Below are the baseline KPIs that need to be measured:

- The prescribed amount of time to discover emerging threats and/or vulnerabilities is 24hrs.
- The prescribed amount of time to publish news, articles, advisories, or digests is 48hrs.

ANNEX

- ANNEX 1 – Threat Hunting Tools for Discovery Process
- ANNEX 2 – Threat Hunting Database Schema (TH-DB)



Annex 1 – Threat Hunting Tools for Discovery Process

1. Overview

The Threat Hunting tools for discovery process, that will be mentioned later, are the essentials for the first stage of Incident Management. It allows the team to proactively seek threats and vulnerabilities ahead of what's incoming.

2. Threat Intelligence

The TH is currently pursuing to have a tool that can collect data such as Ips, hashes, domains, news, and other relevant information that can help the team to form a hypothesis of upcoming threat or do analysis over an existing new threat.

TI will deliver notable cyber events related to the financial, government, insurance, and healthcare industries from social media, news articles, and cyber intelligence solutions.

3. YARA Rules for Malware Detection

The TH is currently pursuing a tool that can make patterns (signatures) for malware detection and at the same time harvest it for analysis.

4. Sandbox Testing Tools

The TH can also perform Sandbox Testing that will let them identify the characteristics of malware such as auto-start mechanism, APIs gathering, conditions for infections, and file & system changes. The following are the major tools for this activity:

Tool	Description
VMware Workstation	VMware Workstation enables users to set up virtual machines on a single physical machine and use them simultaneously along with the actual machine.
OillyDbg	OillyDbg is an x86 debugger that emphasizes binary code analysis, which is useful when source code is not available.
IdaPro	IdaPro is primarily a multi-platform, multi-processor disassembler that translates machine executable code into assembly language source code for purpose of debugging and reverse engineering.
SysTracer	SysTracer is a system utility tool that can scan and analyze your computer to find changed (added, modified or deleted) data into registry and files.
HIEW (Hacker's View)	HIEW is a popular console hex editor for Windows written that can view files in text, hex and disassembly mode. It is particularly useful for editing executable files such as COFF, PE or ELF executable files.
Wireshark	Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
RetDec	RetDec is an open-source machine-code decompiler based on LLVM. The decompiler is not limited to any particular target architecture, operating system, or executable file format.

5. Vulnerability Assessment Tools

Listed below are the tools needed by the Threat Hunters to conduct Vulnerability Assessment:

Tool	Description
Penetration Testing Platform	Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
Web Application Test Suite	Burp Suite is a graphical tool for testing Web application security.
Vulnerability Scanner	Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. OpenVAS is a software framework of several services and tools offering vulnerability scanning and vulnerability management.

6. Monitoring Tools

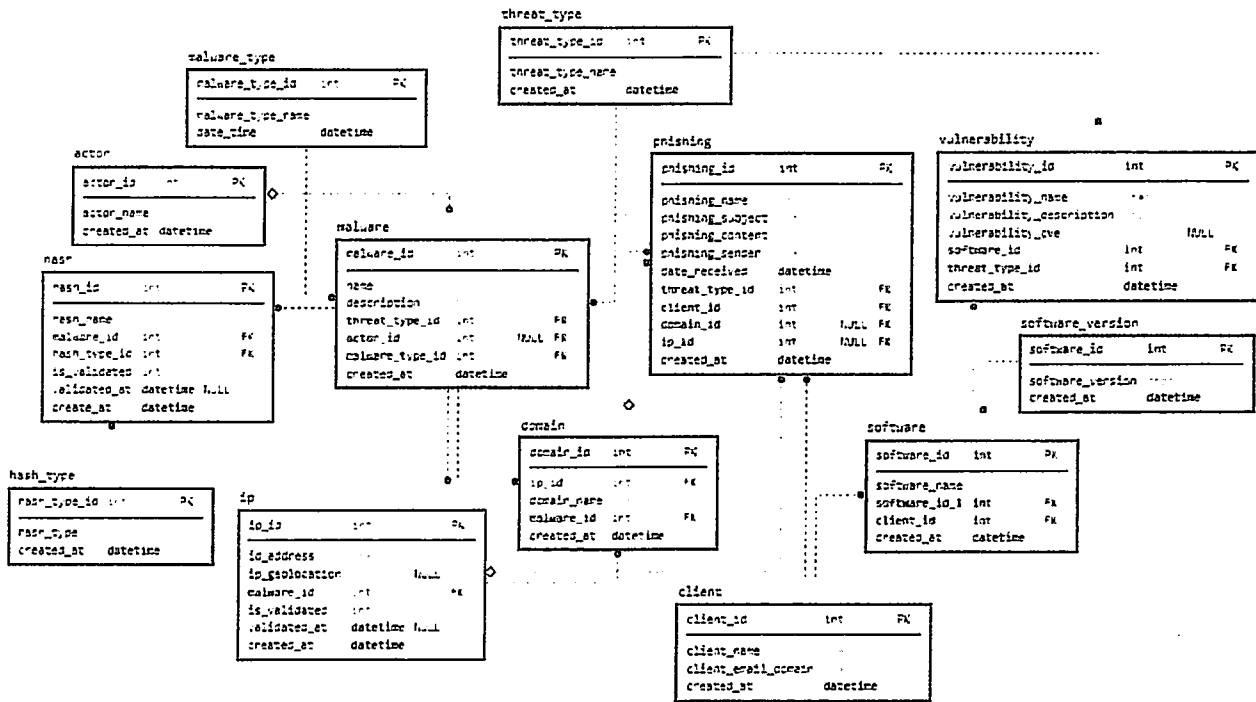
The TH can use SIEM as reference for threat hunting and sometimes will receive request for insights.

The SOC Team is currently using the SIEM to monitor the events happening in the network and system of the clients. Its continuous fine-tuning process helps the entire Service Operations manage and detect early signs of breach. The following are the platforms used by Service Operations:

Tool	Description
SIEM	The Splunk SIEM solution is comprised of several appliance-based platforms working in conjunction to deliver unmatched value and performance to enterprise security professionals within an enterprise.
SOAR	Siemplify is a security orchestration, automation, and response (SOAR) provider. It is integrated with McAfee SIEM for easier navigation and monitoring of events.



Annex 2 – Threat Hunting Database Schema (TH-DB)



[Handwritten signature]

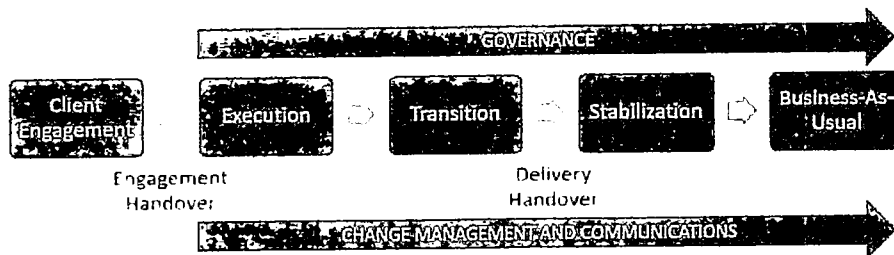
D. Incident Response



PROJECT MANAGEMENT PROGRAM PLAN FOR GOVERNMENT INSURANCE CLUSTER

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

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



1. Client Engagement.

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

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

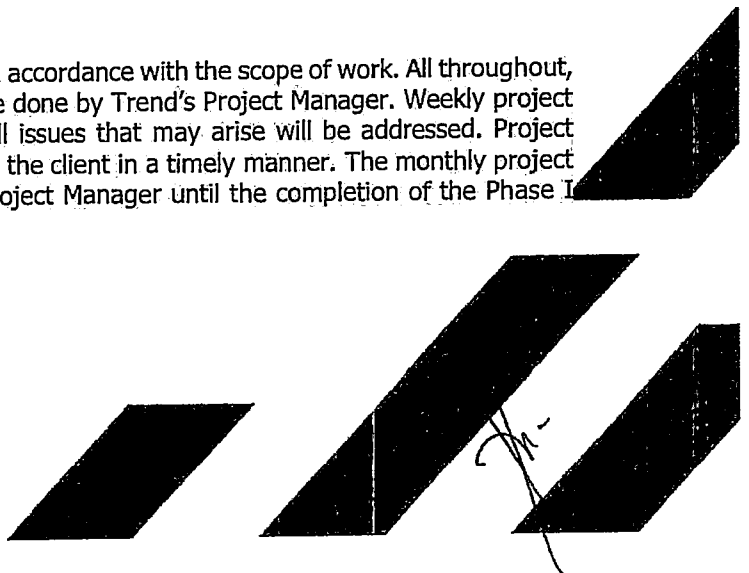
2. Execution.

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

Trends & Technologies, Inc.

6th Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines

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



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

3. Transition.

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

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

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

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

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

4. Stabilization.

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

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

5. Business-As-Usual.

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

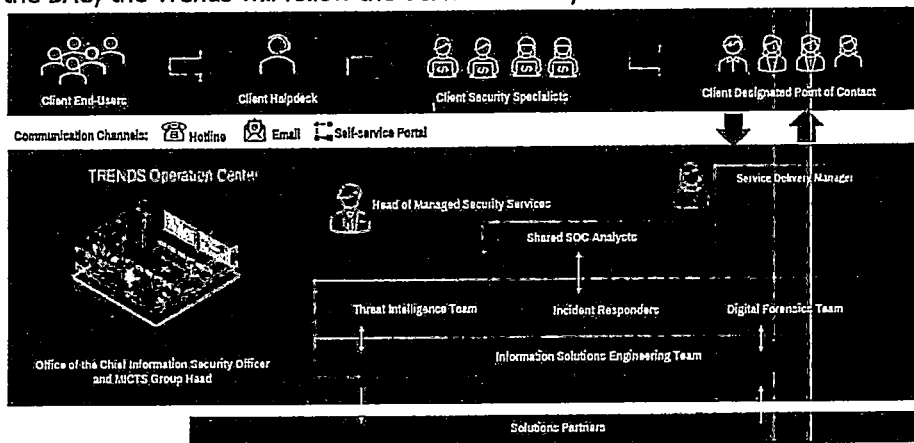


Trends will provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a period of time.

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

Service Delivery Architecture

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



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

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

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

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

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

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

Manpower Resources

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

Personnel	Roles and Responsibilities
SOC Manager or Tier 4 Analyst (1)	In charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. Responsible for the management of the MSOC operations for the agency and cluster.
Tier 3 Analyst (1)	Responsible for managing critical incidents. Responsible for actively hunting for threats and assessing the vulnerability of the business. 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
Tier 2 Analyst (1)	Responsible for conducting further analysis and deciding on a strategy for containment. 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
Tier 1 Analysts (2)	Responsible for the following tasks: 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 6. General Communication 7. Weekly Summary Reports

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

Reports and Meetings



- **Monthly Service Performance Report.**

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

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

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

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

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

- **Monthly Service Performance Review Meeting.**

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

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





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

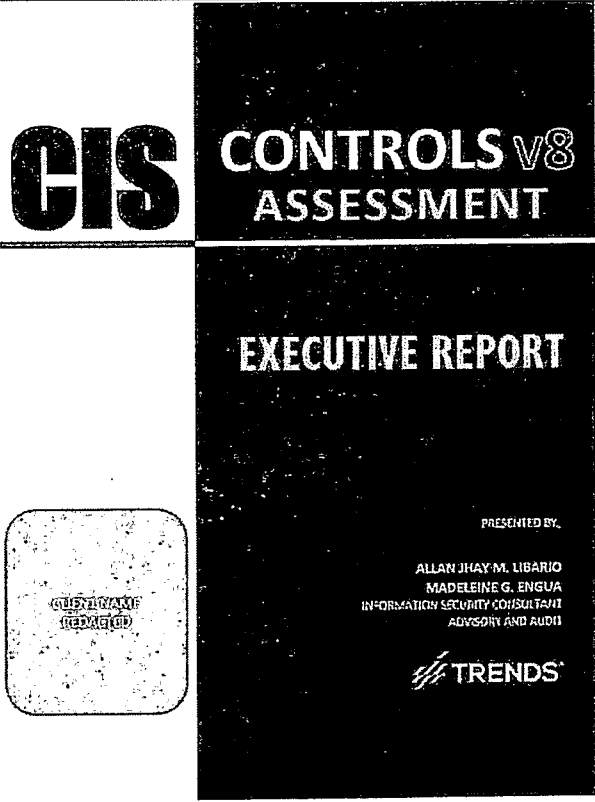
DOCUMENT VERSION

1.0

REVISION DATE

2023 SEPTEMBER 01

ANNEX 8 – Cybersecurity Maturity Assessment Sample




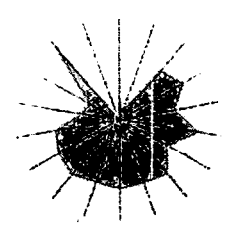
CIS CONTROLS v8 ASSESSMENT

EXECUTIVE REPORT

PRESENTED BY:

ALLAN JHAY M. LIBARIO
MADELEINE G. ENGUA
INFORMATION SECURITY CONSULTANT
ADVISORY AND AUDIT

TRENDS

CCID	Category	Current Score
CC01	Inventory and Control of Information Assets	100%
CC02	Retention and Control of Information Assets	100%
CC03	Data Protection	87%
CC04	Secure Configuration of Information Assets and Software	75%
CC05	Access Management	84%
CC06	Account Control Management	79%
CC07	Continuous Vulnerability Management	81%
CC08	Asset Log Management	71%
CC09	Incident Detection and Response	87%
CC10	Malware Defense	85%
CC11	Data Recovery	82%
CC12	Network Infrastructure Management	85%
CC13	Network Monitoring and Defense	67%
CC14	Security Awareness and Security Training	81%
CC15	Security Program Management	87%
CC16	Assessment Software Security	81%
CC17	Assessment Hardware Security	84%
CC18	Assessment Software Security	71%

CONFIDENTIAL

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

3 Incident Playbook

3.1 Data Theft

A. About

- 1. This incident response playbook is designed to provide a structured approach to handling data theft incidents.
- 2. The primary goal is to minimize damage and prevent further data loss.
- 3. This playbook is applicable to all employees and contractors.

B. Tools:

- 1. Incident Response Team (IRT)
- 2. Network Security Monitoring (NSM)
- 3. Data Loss Prevention (DLP)
- 4. Forensic Analysis Tools (e.g., Encase, FTK)
- 5. Communication Tools (e.g., Email, Phone)

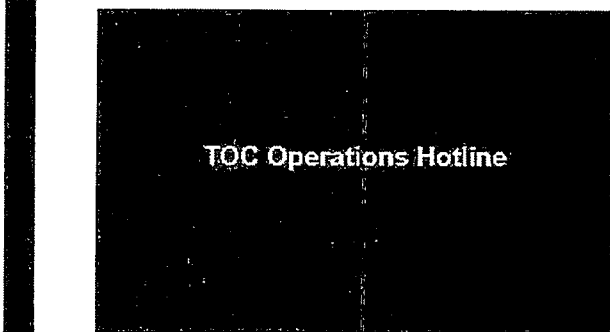
C. Detection and Analysis

- 1. Monitor network traffic for unusual activity.
- 2. Review logs for unauthorized access or data exfiltration.
- 3. Investigate the source of the data theft.
- 4. Determine the scope and impact of the incident.
- 5. Identify the affected systems and data.

D. Containment and Eradication

- 1. Isolate affected systems to prevent further data loss.
- 2. Disable compromised accounts and credentials.
- 3. Remove malware and rootkits.
- 4. Patch vulnerabilities that were exploited.
- 5. Restore data from secure backups.
- 6. Conduct a forensic investigation to determine the cause and extent of the incident.
- 7. Eradicate the root cause of the incident.
- 8. Verify that the incident has been resolved and systems are secure.

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 7 – Sample Malware Incident Analysis & Recommendation

<p>ADVISORY NUMBER 66519</p> <p>Client Name: [Redacted]</p> <p>Date and Time Incident is Detected: 02/23/2022 15:34:34</p> <p>Affected Site: [Redacted]</p> <p>Ticket Number: 66519</p> <p>Event Name: Malware Detected – Checkpoint – Not Blocked</p> <p>Priority: P3</p>	<p>PACKET DETAILS</p> <p>[Extremely faint and illegible packet analysis data]</p>
<p>INCIDENT DETAILS</p> <p>Description: Generic BEZ agent - 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.</p> <p>Source IP: [Redacted]</p> <p>Source Port: 49551</p> <p>Destination IP: 52.89.4.199</p> <p>Destination Port: 25</p> <p>Policy Name: [Redacted]</p> <p>Threat Name: [Redacted]</p> <p>Direction: Outbound</p> <p>Event Subtype: alert</p> <p>Remarks: Device Action: monitor Malware action: "Access to site known to contain malware" Email detected: groundliness@portbound.net</p> <p>Links:</p> <ul style="list-style-type: none"> • http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd • http://www.w3.org/1999/xhtml • http://gai-building.azurewebsites.net/redconerkt.php?utm_source=93&utm_content=e • https://content.linkedin.com/content/dam/me/about/LinkedIn_Icon.jpg.original.jpg • https://static.linkedin.com/sc/p/com.linkedin.email-assets-frontend%3Femail-assets-frontend-static-content%26_latest_/f%3Femail-assets-f <p>Related Email: N/A</p>	
<p>RECOMMENDATION</p> <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 16 – Sample RCA Report (Details Redacted)



INCIDENT REPORT

Case No. [REDACTED]

IR DOCUMENT DETAILS			
Name	Organization	Date	
IR Requestor: <i>(Person who requested the IR)</i>		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:	

[Handwritten signature]

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 HARDWARE		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		10
4.2.3 HARDWARE		11
4.2.4 OS CONFIGURATION		11
4.2.5 NETWORK & PROCESS MONITORING		11
APPENDIX		12

Digital Forensics Report's Table of Contents

TABLE OF CONTENTS	
1 OVERVIEW	3
1.1 Key Summary	3
1.2 ATTACK PHASE AND EVIDENCE CHAIN	3
2 AT-RISK IMAGE AND HISTORY DUMP FINDINGS	4
3 STEIN FINDINGS	7
3.1	7
3.2	9
4 CONCLUSION	11
5 RECOMMENDATIONS	12
DOCUMENT ACCEPTANCE	12

Compromise Assessment Report's Table of Contents

ANNEX 3 – TRENDS ISO/IEC 27001:2013 Certification



SOCOTEC

CERTIFICATE

No. SCU001708D

certifies that :

Trends & Technologies, Inc.

20th Trafalgar Plaza, 105 HV Dela Costa, Salcedo 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 Ghau Operations Director-SOCOTEC Certification UK





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

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

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

4.2 Model for measuring Weight of an Asset

Weight	1	2	3
Low	1	2	3
Medium	2	3	4
High	3	4	5

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 1-27, 1 being the highest Asset Category for those assets having 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	9	12	15	18	21	24

Asset Value	3	4	5	6	7	8	9
Weight	1	3	4	5	6	7	8
	9	9	12	15	18	21	24

4.4 Asset Valuation & Categorization Listing

Assets Name	IP	VENDOR	Type	Confidentiality	Integrity	Availability	Total	Asset Weight Value	Category
AD-Server-1		Microsoft	Windows Server 2012 R2	3	3	3	9	3	27
AD-Server-2		Microsoft	Windows Server 2012 R2	3	3	3	9	3	27
AD-Server-3		Microsoft	Windows Server 2012 R2	3	3	3	9	3	27
AD-Server-4		Microsoft	Windows Server 2012 R2	3	3	3	9	3	27
AD-Server-5		Microsoft	Windows Server 2012 R2	3	3	3	9	3	27

6.4 Mapping of Typical Incidents to Assets

Incident Severity	Typical Incidents
P1 - 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
P5 - 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

INCIDENT MANAGEMENT POLICIES, STANDARDS, PROCEDURES & GUIDELINES

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

DOCUMENT ID

DOCUMENT OWNER

TRENDS Cyber Security Intelligence

DOCUMENT CLASSIFICATION

TLP:GREEN INTERNAL

DOCUMENT STATUS

RELEASE

DOCUMENT VERSION

1.0

REVISION DATE

2023 SEPTEMBER 01



TABLE OF CONTENTS

1	INTRODUCTION	4
1.1	OVERVIEW	4
1.2	PURPOSE OF THE DOCUMENT	4
1.3	TARGET READERSHIP	4
1.4	DOCUMENT DEFINITIONS	4
1.5	REFERENCE DOCUMENTS & BIBLIOGRAPHY	6
2	PURPOSE AND OBJECTIVE	7
2.1	PURPOSE	7
2.2	OBJECTIVE	7
3	SCOPE AND DEFINITION	8
4	COMPLIANCE	9
5	AWARENESS	10
6	INCIDENT MANAGEMENT	11
6.1	POLICY	11
6.2	CLASSIFICATION OF INCIDENT	11
6.3	INCIDENT RESPONSE LIFE CYCLE	11
6.3.1	INFORMATION SECURITY INCIDENT RESPONSE LIFE CYCLE	11
6.3.2	QUALITY-OF-SERVICE INCIDENT RESPONSE LIFE CYCLE	12
6.4	IDENTIFICATION OF INCIDENT	12
6.5	INCIDENT PRIORITIZATION	12
6.6	LOGGING OF INCIDENTS	12
6.7	INCIDENT RESPONSE UPDATING, RESTORATION, RESOLUTION AND ROOT CAUSE ANALYSIS TIME	13
6.8	INCIDENT MONITORING	14
6.9	INCIDENT MANAGER	14
6.10	COMMON PROCEDURES	15
6.10.1	INCIDENT REPORTING	15
6.10.2	CHRONOLOGICAL ESCALATION	15
6.10.3	PRIORITY ESCALATION & DE-ESCALATION	16
6.11	INFORMATION SECURITY INCIDENT MANAGEMENT	16
6.11.1	ATTACK VECTORS	16
6.11.2	TYPICAL INCIDENT HANDLING PROCEDURE FOR INFORMATION SECURITY INCIDENT	17
6.11.3	GUIDELINES ON HANDLING OF CERTAIN SPECIFIC INFORMATION SECURITY INCIDENTS	18
6.11.4	INVOCATION OF COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)	18
6.12	QUALITY-OF-SERVICE INCIDENT MANAGEMENT	18
6.12.1	TYPICAL INCIDENT HANDLING PROCEDURE FOR QUALITY-OF-SERVICE INCIDENT	18
6.12.2	FIX INCIDENT PROCEDURE	19
6.13	CALL TREE	20
6.14	DIGITAL FORENSICS OVERARCHING PROCESS	21
7	KEY PERFORMANCE INDICATORS	24
	ANNEX	25
	ANNEX 1 – TRENDS OPERATIONS CENTER IMPACT CRITERIA, URGENCY CRITERIA AND PRIORITY MATRIX	26



ANNEX 2 – TRENDS OPERATIONS CENTER INCIDENT RESPONSE & UPDATE TIME	27
ANNEX 3 – TRENDS OPERATIONS CENTER QUALITY-OF-SERVICE RESTORATION TIME	29
ANNEX 4 – TRENDS OPERATIONS CENTER INFORMATION SECURITY RESOLUTION TIME	30
ANNEX 5 – TRENDS OPERATIONS CENTER ROOT CAUSE ANALYSIS RESPONSE TIME	31
ANNEX 6 – GUIDELINES IN HANDLING OF SPECIFIC SECURITY INCIDENTS	32
ANNEX 7 – SAMPLE MEASUREMENT OF ACKNOWLEDGEMENT SLA	37
ANNEX 8 – COVERAGE OF IR HOURS	38
ANNEX 9 – SCOPE OF INCIDENT RESPONSE	38

1 Introduction

1.1 Overview

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

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

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

1.2 Purpose of the Document

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

1.3 Target Readership

This document is prepared for the following:

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

1.4 Document Definitions

Term	Definition
Information Security	The preservation of confidentiality, integrity, and availability of information.
Information Security Management System	Part of overall management process that takes care of planning, implementing, maintaining, reviewing, and improving the information security. ¹
ISGAB	Information Security Governance and Advisory Board
CI	Configuration Item
Incident	An unplanned interruption to an IT service, reduction in the quality of a service. ²
Configuration Item	Any component that needs to be managed in order to deliver an IT service. Components that make up a service in which a configuration item is an item that will assist in facilitating outcomes. CIs may be any of the following: <ul style="list-style-type: none"> • Software (e.g.: Applications, Internet Services) • Hardware (e.g.: Laptops) • Environment (e.g.: Location, Power) • People (e.g.: Person or Role)

¹ ISO Consultants Toolkit

² ITIL Foundation – ITIL 4 Edition, Axelos, 2019



	<ul style="list-style-type: none">• Infrastructure (e.g.: Network)• Documentation (e.g.: Licenses, Contracts, Training)
Event	Any change of state that has significance for the management of a configuration item (CI) or IT service.
Availability	The ability of an IT service or other configuration item to perform its agreed function when required.
Service	A means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks.

1.5 Reference Documents & Bibliography

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

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

2 Purpose and Objective

2.1 Purpose

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

2.2 Objective

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

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

³ ITIL Intermediate Certification Companion, Sybex, 2017

3 Scope and Definition

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

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

4 Compliance

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

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

5 Awareness

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

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

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

6 Incident Management

6.1 Policy

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

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

6.2 Classification of Incident

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

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

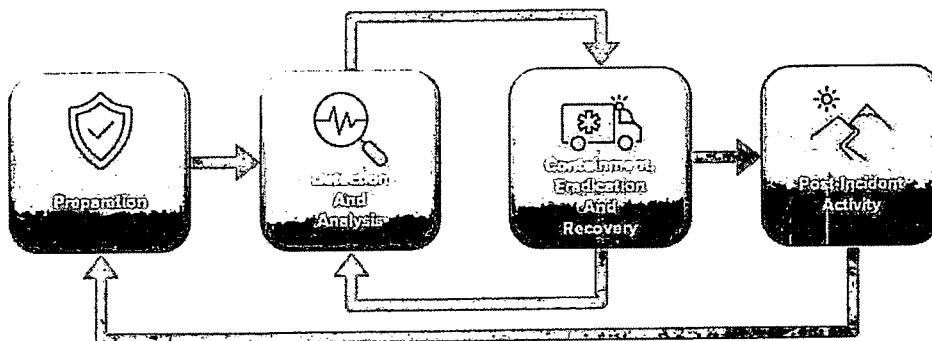
On the other hand, Quality-of-Service Incident relates to degradation, unavailability, or inability of an IT service to deliver the intended outcome a client wants to achieve.

6.3 Incident Response Life Cycle

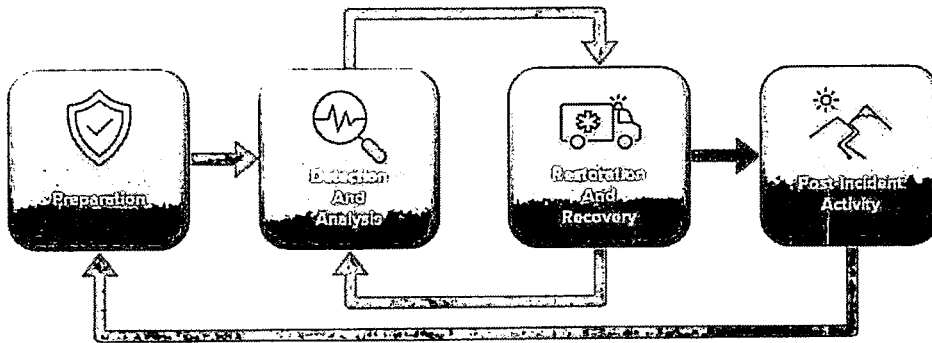
The Incident Response Life Cycle that the MICTS Service Operations follows is based on the NIST SP 800-61 revision 2 (Computer Security Incident Handling Guide) which is a 4-step process as follows:

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

Information Security Incident Response Life Cycle



Quality-of -Service Incident Response Life Cycle



6.4 Identification of Incident

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

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

6.5 Incident Prioritization

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

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

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

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

6.6 Logging of Incidents

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

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

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

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

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

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

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

6.8 Incident Monitoring

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

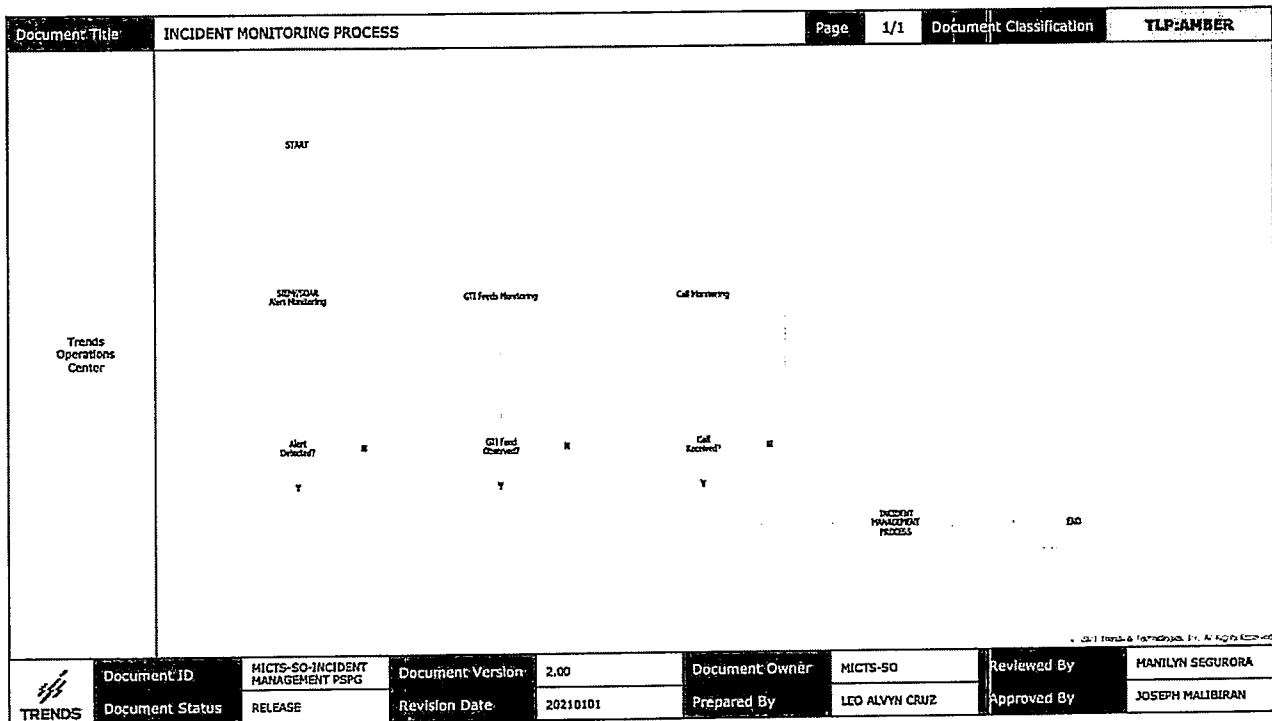


Figure 1 – Incident Monitoring Process

6.9 Incident Manager

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

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

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

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

6.10 Common Procedures

Incident Reporting

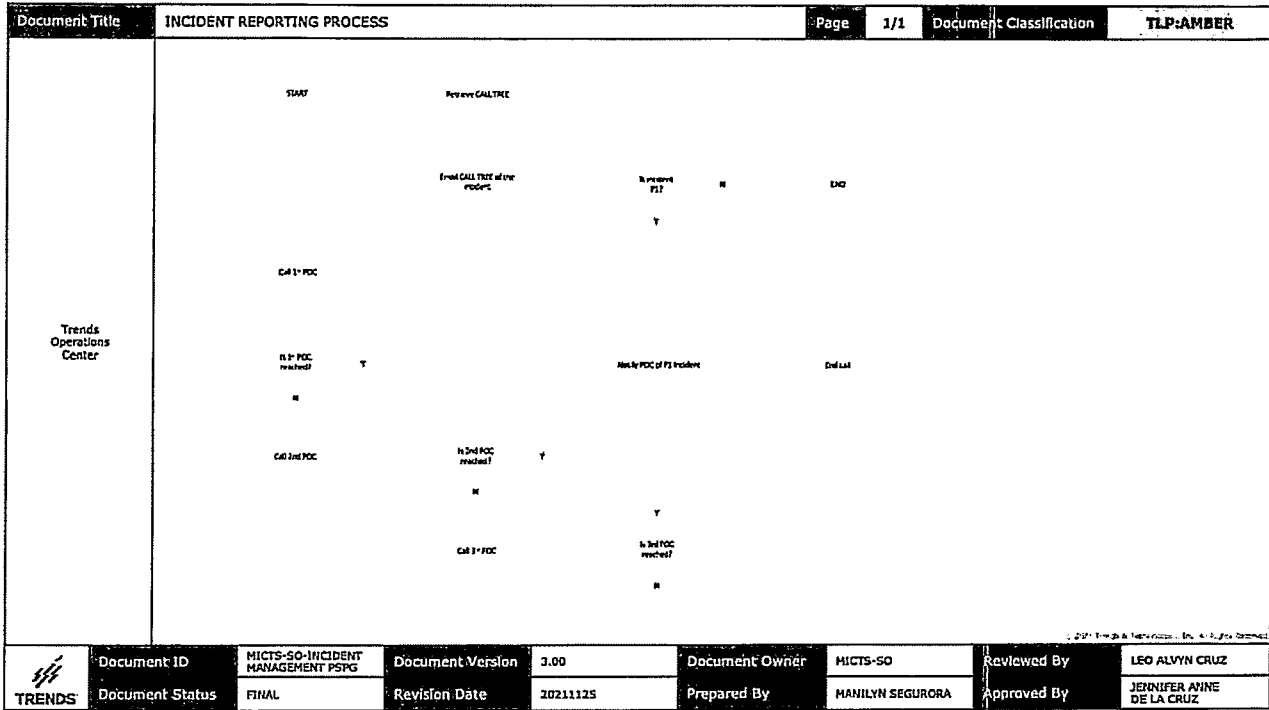


Figure 2 – Incident Reporting Process

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

Chronological Escalation

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

Priority Escalation & De-escalation

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

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

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

6.11 Information Security Incident Management

Attack Vectors

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

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

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

Typical Incident Handling Procedure for Information Security Incident

Document Title	INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS						Page	1/1	Document Classification	TLP:AMBER
SOC L1 ANALYST	Identify the incident	Investigate the incident	Identify the root cause	Containment	Eradication	Recovery				
SOC L2 SPECIALIST	Identify the incident	Investigate the incident	Identify the root cause	Containment	Eradication	Recovery				
SOC L3 PROFESSIONAL	Identify the incident	Investigate the incident	Identify the root cause	Containment	Eradication	Recovery				
TMG	Identify the incident	Investigate the incident	Identify the root cause	Containment	Eradication	Recovery				
Client/ Onsite Support Engineer	Identify the incident	Investigate the incident	Identify the root cause	Containment	Eradication	Recovery				
TRENDS	Document ID	MICTS-SO-INCIDENT MANAGEMENT PSPG	Document Version	7.00	Document Owner	MICTS-SO	Reviewed By	MANILYN SEGUORA		
TRENDS	Document Status	RELEASE	Revision Date	20210620	Prepared By	LEO ALVYN CRUZ	Approved By	JOSEPH MALIBIRAN		

Figure 3 – Information Security Incident Management Process

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

Guidelines on Handling of certain specific Information Security Incidents

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

Invocation of Computer Security Incident Response Team (CSIRT)

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

TRENDS CSIRT is comprised of the following members:

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

6.12 Quality-of-Service Incident Management

Typical Incident Handling Procedure for Quality-of-Service Incident

Document Title	QUALITY OF SERVICE INCIDENT MANAGEMENT				Page	1/1	Document Classification	TLP:AMBER
SOC L1 ANALYST	Start	Check for alert	Open IR Ticket	Escalate to L2	Escalate to L2	Escalate to L2	Escalate to L2	Escalate to L2
SOC L2 SPECIALIST	Investigate and resolve	Escalate to L3	Escalate to L3	Escalate to L3	Escalate to L3	Escalate to L3	Escalate to L3	Escalate to L3
SOC L3 PROFESSIONAL	Escalate to TMG	Escalate to TMG	Escalate to TMG	Escalate to TMG	Escalate to TMG	Escalate to TMG	Escalate to TMG	Escalate to TMG
TMG	Escalate to Third Party	Escalate to Third Party	Escalate to Third Party	Escalate to Third Party	Escalate to Third Party	Escalate to Third Party	Escalate to Third Party	Escalate to Third Party
Third Party	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer	Escalate to Client/Onsite Support Engineer
Client/Onsite Support Engineer	Document ID	MICTS-SO-INCIDENT MANAGEMENT PSPG	Document Version	2.00	Document Owner	MICTS-SO	Reviewed By	MANILYN SEGURORA
	Document Status	FINAL	Revision Date	20210101	Prepared By	LEO ALMYN CRUZ	Approved By	JOSEPH MALIBIRAN

Figure 4 – Quality of Service Incident Management Process

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

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

Fix Incident Procedure

Document Title	FIX INCIDENT PROCESS		Page	1/1	Document Classification	TLP:AMBER
TRENDS OPERATIONS CENTER/ TMG/ THIRD PARTY	TIME	Employee	Identify restoration activity	Is change required?	Perform restoration activity	END
				Y		
			INCIDENT MANAGEMENT PROCESS			
TRENDS	Document ID	MICTS-SO-INCIDENT MANAGEMENT PROC	Document Version	2.00	Document Owner	MICTS-SO
	Document Status	RELEASE	Revision Date	20211123	Prepared By	HANILYN SEGURDIA
					Reviewed By	LEO ALVIN CRUZ
					Approved By	JOSEPH MALIBIRAN

Figure 5 – Fix Incident Process

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

6.13 Call Tree

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

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

Fix Incident Procedure

Document Title	FIX INCIDENT PROCESS		Page	1/1	Document Classification	TLP:AMBER		
TRENDS OPERATIONS CENTER/ TMG/ THIRD PARTY	ETIM2	Employee	Identify/restore activity	Is change required?	Perform restoration activity	END		
						INCIDENT MANAGEMENT PROCESS		
TRENDS	Document ID	MICTS-SO-INCIDENT MANAGEMENT PSPG	Document Version	2.00	Document Owner	MICTS-SO	Reviewed By	LEO ALVIN CRUZ
	Document Status	RELEASE	Revision Date	20211123	Prepared By	HANILYN SEGURDA	Approved By	JOSEPH MALIBIRAN

Figure 5 – Fix Incident Process

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

6.13 Call Tree

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

6.14 Digital Forensics Overarching Process

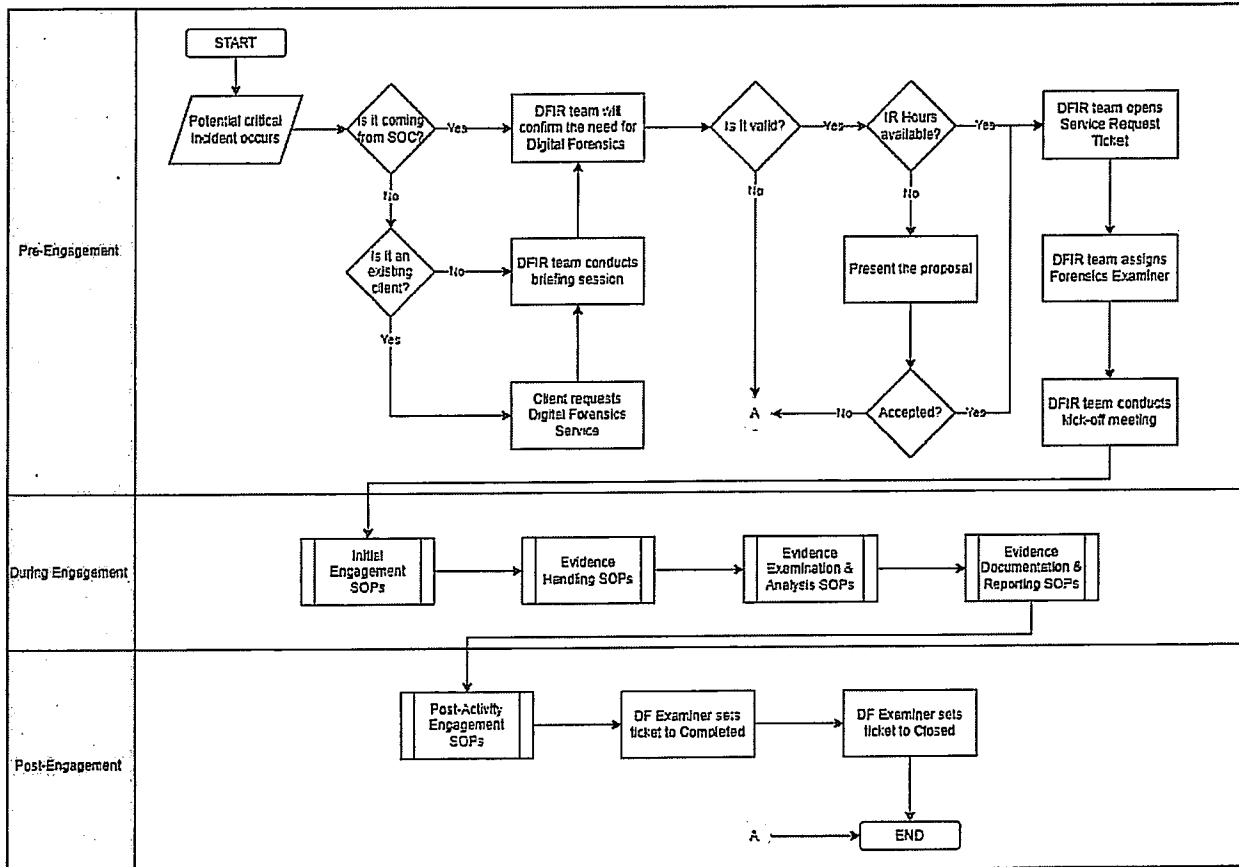


Figure 6 - Trends Digital Forensics Overarching Process

A. Pre-Engagement

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

- ii. Otherwise, the DFIR Team will start discussion with the Business Unit Group about the cost implications. If the client accepts the proposal, please refer to the previous bullet. Otherwise, the DFIR team will not proceed to the next steps.
3. The DFIR team sets a kick-off meeting with the client to provide a comprehensive overview of the activity and discuss the total incident response hour to spend.

B. During Engagement

1. The assigned Forensics Examiner will execute the various Standard Operating Procedures (SOPs) to ensure the successful completion of the activity.
2. Firstly, the Forensics Examiner shall do the Initial Engagement SOPs. The Initial Engagement phase serves as the starting point for conducting a thorough and effective investigation into digital evidence. This phase sets the foundation for the entire examination process, helping ensure that the investigation is well-planned, aligned with client's expectations, and conducted in a systematic and legally sound manner.
3. Next, Evidence Handling SOPs will be executed. Evidence handling is a critical component of digital forensic examination. It encompasses a set of procedures and protocols designed to ensure the integrity, security, and admissibility of digital evidence throughout the investigation process. There are two stages in this phase:
 - Evidence Intake SOPs – It outlines the systematic process for receiving and documenting physical evidence collected during investigations.
 - Evidence Acquisition SOPs – It ensures that evidence is properly preserved, documented, and protected throughout the investigation process.
4. Next, Evidence Examinations and Analysis SOP will be executed. This SOP outlines the systematic process for conducting thorough examinations, testing, and analysis of physical evidence collected during investigations. This procedure ensures that evidence is subjected to scientific analysis using standardized methods, maintaining its integrity and reliability.
5. Finally, Evidence Documentation and Reporting SOP will be executed. This SOP outlines the systematic process for accurately documenting and reporting on the collection, analysis, and handling of evidence during investigations. This procedure ensures that all pertinent information is recorded, maintained, and presented in a clear and organized manner, facilitating transparency, accountability, and legal admissibility. The report shall include the root cause analysis which identified the intrusion vector and mitigating procedures conducted to address network and system vulnerabilities.

C. Post-Engagement

1. Once everything is set, the DFIR team shall execute the SOPs related to the Post-Engagement Activity:
 - i. Post-Activity Engagement SOP outlines the systematic process for interacting with stakeholders and addressing key considerations after completing a digital forensic investigation. This procedure aims to gather insights, provide updates, and ensure effective collaboration, while also documenting findings for legal and reporting purposes.

- ii. Sanitization of Digital Media SOP outlines a systematic process to securely erase or destroy digital data from various types of media to prevent unauthorized access, maintain data privacy, and comply with data protection regulations. This procedure ensures that sensitive information is effectively removed, making the media suitable for reuse, disposal, or repurposing.
 - iii. Return of Evidence SOP outlines a systematic process for returning digital evidence to clients after the completion of forensic analysis. This procedure ensures that evidence is returned securely, maintaining the chain of custody, and preserving its integrity for potential legal proceedings.
2. Once the client accepts the final document, the Digital Forensics Examiner will set the SR ticket to Completed then eventually change it to Closed.

7 Key Performance Indicators

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

Below are the baseline KPIs that need to be measured:

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

ANNEX

- ANNEX 1 – TRENDS Operations Center Impact Criteria, Urgency Criteria and Priority Matrix**
- ANNEX 2 – TRENDS Operations Center Incident Response & Update Time**
- ANNEX 3 – TRENDS Operations Center Quality-of-Service Incident Restoration Time**
- ANNEX 4 – TRENDS Operations Center Information Security Incident Resolution Time**
- ANNEX 5 – TRENDS Operations Center Root Cause Analysis Response Time**
- ANNEX 6 – Guidelines in Handling of Specific Information Security Incidents – Malware**
- ANNEX 7 – Sample Measurement of Acknowledgement SLA**
- ANNEX 8 – Coverage of IR hours**
- ANNEX 9 – Scope of Incident Response**



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

Impact Criteria

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

Impact	Description
High	<ul style="list-style-type: none"> A large number of staff are affected and/or not able to do their job. A large number of customers are affected and/or acutely disadvantaged in some way. Involving IT Assets with Category 1. The damage to the reputation of the business is likely to be high.
Medium	<ul style="list-style-type: none"> A moderate number of staff are affected and/or not able to do their job properly. A moderate number of customers are affected and/or inconvenienced in some way. Involving IT Assets with Category 2. The damage to the reputation of the business is likely to be moderate.
Low	<ul style="list-style-type: none"> A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort. A minimal number of customers are affected and/or inconvenienced but not in a significant way. Involving IT Assets with Category 3. The damage to the reputation of the business is likely to be minimal.

Urgency Criteria

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

Urgency	Description
High	<ul style="list-style-type: none"> The damage caused by the Incident increases rapidly. Work that cannot be completed by staff is highly time sensitive A minor Incident can be prevented from becoming a major Incident by acting immediately. Several users with VIP status are affected.
Medium	<ul style="list-style-type: none"> The damage caused by the Incident increases considerably over time. A single user with VIP status is affected
Low	<ul style="list-style-type: none"> The damage caused by the Incident only marginally increases over time. Work that cannot be completed by staff is not time sensitive.

Priority Criteria

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

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

Annex 2 – TRENDS Operations Center Incident Response & Update Time

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

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

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

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

Measurement of Monthly SLA is computed as follows:

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

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

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

Annex 4 – TRENDS Operations Center Information Security Resolution Time

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



Annex 5 – TRENDS Operations Center Root Cause Analysis Response Time

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

Annex 6 – Guidelines in Handling of Specific Security Incidents

Malware Incident Response Guidelines

Definition

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

Purpose

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

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

Scope

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

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

Preparation

Build and maintain malware-related skills on Analysts.

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

Establish an organized designation of tasks and responsibilities

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

Acquire tools and resources for malware detection and investigation.

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

Has the capability to detect advance threat tactics and techniques.

Identification

Detect the infection

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

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

Identify the infection

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

Assess the perimeter of the infection

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

Containment

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

Containment Process

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

Containment through user participation

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

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

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

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

Containment through automated detection

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

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

Containment through disabling services

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

Containment through disabling connectivity

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

Remediation

Identify

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

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

Test

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

Deploy

Deploy the disinfection tools. Several options can be used:

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

Rebuilding

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

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

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

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

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

Recovery

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

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

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

Aftermath

Report

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

The following themes should be described:

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

Lessons Learned

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

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

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



Annex 7 – Sample measurement of Acknowledgement SLA

Type	Category	Subject	Created By	Created On
Notes	Status Update	Incident changed from Reported to Dismissed pending customer	rbayuban	17/02/2022 17:23
Email	Outgoing Email	Incident 66272 - Security / Inbound Traffic from GTI Known Malicious Source - No: Blocked ...	rbayuban	17/02/2022 17:23
Notes	Log	Incident was created	rbayuban	17/02/2022 17:23

Annex 8 – Coverage of IR hours

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

Annex 9 – Scope of Incident Response

Trends shall assist the Government Insurance Cluster in the following:

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



TRAINING PLAN FOR GOVERNMENT INSURANCE CLUSTER

TRENDS will facilitate at least once a year Continual Service Improvement (CSI) workshop with clients for possible improvement of service through process, people, and technology.

TRENDS will provide security advisories with the client for cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.

TRENDS will conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on each Government Agency based on the NIST or CIS controls.

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.

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.

Trends & Technologies, Inc.

6th Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo
Village Makati City 1227 Philippines

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





Managed ICT Services
Service Delivery with Flexibility

CYBER SECURITY INTELLIGENCE MANAGEMENT POLICIES, STANDARDS, PROCEDURES & GUIDELINES

This document serves as a policy framework that sets out procedures and goals and objectives that may be used as guidance for decision-making, guide in making a more detailed set of policies or to guide ongoing maintenance of an organization's policies.

DOCUMENT ID

DOCUMENT OWNER **TRENDS MICTS**

DOCUMENT
CLASSIFICATION

TLP:GREEN **INTERNAL**

DOCUMENT STATUS **RELEASE**

DOCUMENT
VERSION **1.0**

REVISION DATE **2023 SEPTEMBER 01**

- TH System Enhancement focuses on improvement of the technology used to detect the threat. It includes but not limited to the following: fine-tuning of SIEM, applying and fine-tuning machine learning on SIEM, updating TH-Database, developing the centralized RSS feeds, and remodeling the process if necessary.

6.3.2 Internal Threat Discovery Procedure

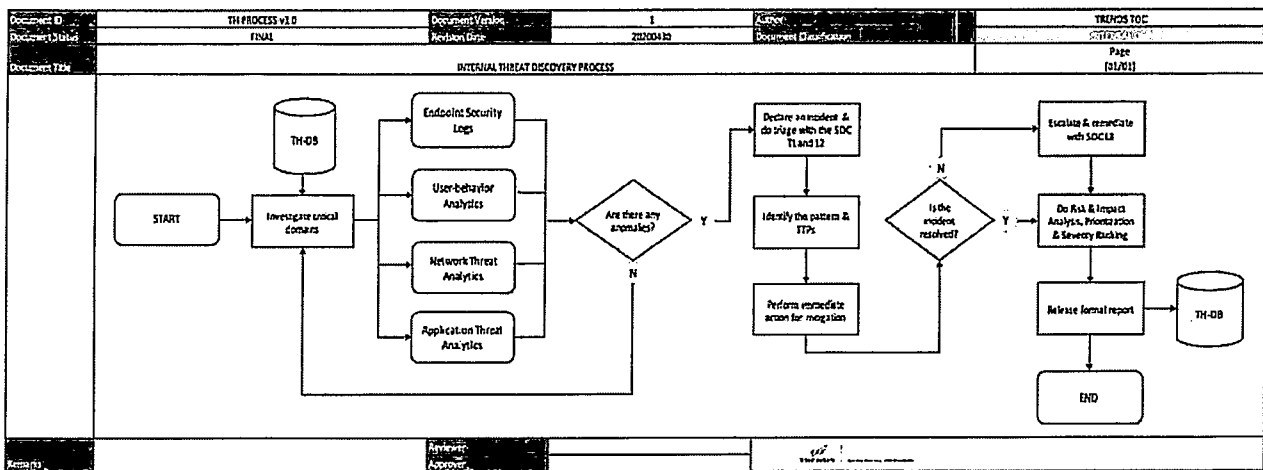


Figure 2 – Internal Threat Discovery Process

This section highlights the high-level perspective of malware-incident handling. Refer to the **TRENDS_Incident Management PSPG-v1.0_TLPGREEN : ANNEX 6** for thorough process.

- The TH will review all the documents and/or any related case to the hypothesis from TH-DB and request for team’s approval to conduct investigation. The following are the critical domains for investigation:
 - Endpoint Security Logs.** Endpoints are monitored by the SOC for any compromise or suspicious activities. The first-level team investigates the spread to block the attacks. TH then verify and remove the false positives and analyze logs to detect attacks that may have bypassed other endpoint and security controls.
 - 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.
 - Network Threat Analytics.** TH analyze multiple cyber intelligence sources from vendors and threat advisories as well as SIEM logs and data feeds to sniff out suspicious activities on the network and application systems. Hidden fileless malware or unknown threats are correlated with anomalies across a number of data pools. This helps to provide full visibility for identifying complex, multi-channel attacks.
 - Application Threat Analytics.** Vulnerability intelligence from vendors and data flow analysis help TH identify high-risk applications for vulnerable entry points and track low footprint applications that are often attractive targets for attack with zero-day exploits.
- Next, the TH will declare an incident and request a triage with SOC TL & SOC L2 if there are any confirmed anomalies found on the critical domains. Otherwise, further investigation on critical domains must be done.



3. Based on the gathered data and with the help of MITRE's Att&ck Framework, the team will identify the threat pattern and its TTP to see what it had already done and its next step.
4. After the investigation, the team will perform all the immediate action for mitigation and other countermeasures to prevent it.
5. The team will evaluate the risk and the extent of its impact once the attack becomes successful. Then, determine the severity of the finding. In case the incident is not yet resolved, the team will escalate the case and remediate with SOC L3.
6. The team will then release a formal report or advisory that indicates (but not limited to) the following: executive summary, overall assessment and rating, severity and prioritization of findings, scope and targets, details of threat, impact and risk analysis, mitigation recommendations and actions taken. For all critical findings, advisory must be released as soon as possible.
7. The results of the investigations and collected information will be stored into TH Database (TH-DB) for future reference.

6.3.3 Malware Discovery Procedure

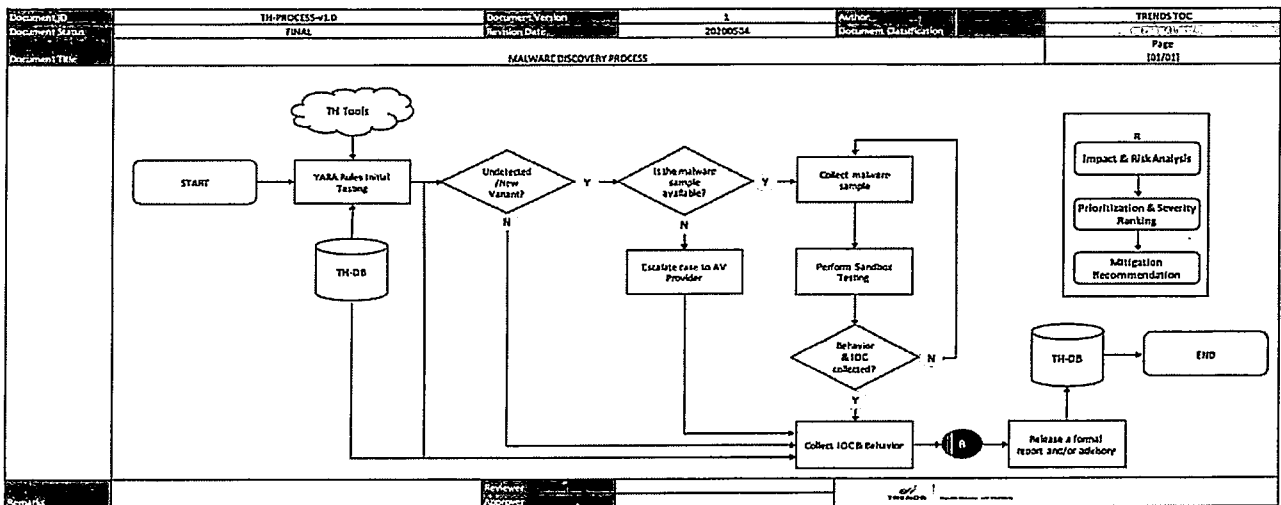


Figure 3 – Malware Discovery Process

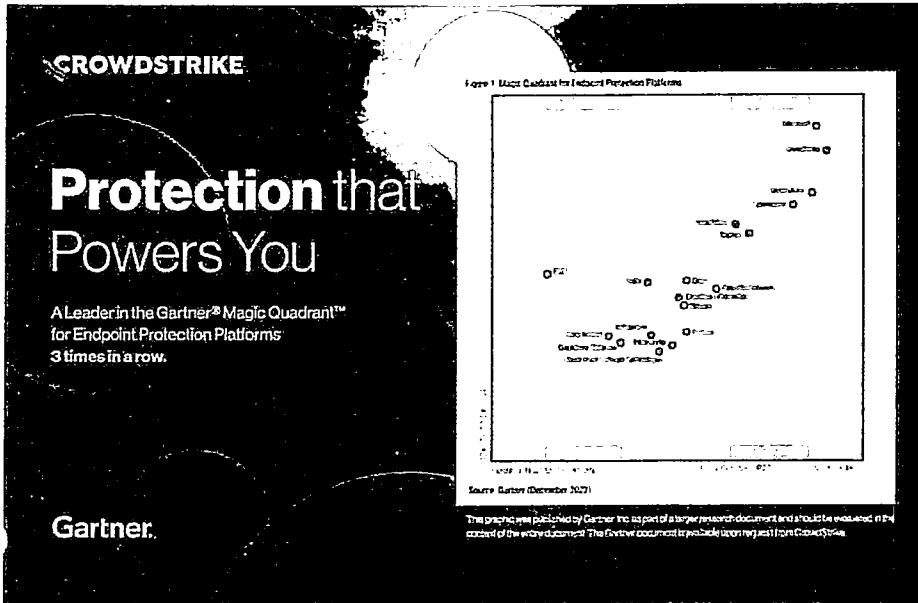
This section highlights the high-level perspective of malware-incident handling. Refer to the **TRENDS_Incident Management PSPG-v1.0_TLPGREEN: ANNEX 6** for thorough process.

1. Check if there's a detection based on the TH-tools or predefined YARA rules. These rules are modified based the information fed on the TH-DB.
2. Check the availability of the information regarding the malware from the mentioned sources.
 - a) If the malware is not a new variant or undetected, gather all the latest information about the malware (IOCs & behavior).
 - b) If the malware is a new variant or undetected, check the availability of the sample for deep-dive analysis.
 - (1) If there's no available sample, escalate the case to the AV provider and gather all the information about the malware.
 - (2) If the sample is available, gather it and conduct sandbox testing to collect all IOCs and its behavior.
3. Analyze and understand the findings:

CROWDSTRIKE BLOG

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

Three Times a Leader: CrowdStrike Named a Leader in Gartner® Magic Quadrant™ for Endpoint Protection Platforms



We believe our recognition in the 2022 Magic Quadrant for Endpoint Protection Platforms reinforces CrowdStrike's position as a cybersecurity leader, innovator and visionary placing farthest to the right for Completeness of Vision.

We are proud to share that CrowdStrike has once again been named a Leader in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP).

Download the report: [2022 Magic Quadrant for Endpoint Protection Platforms](#)

This marks the third consecutive time CrowdStrike has been named a Leader in the Gartner Magic Quadrant for Endpoint Protection Platforms, which we believe builds on the significant recognition CrowdStrike has received as a market, technology and innovation leader. CrowdStrike has recently been recognized as:

- The #1 market leader in worldwide modern endpoint security market share
- The highest detection coverage out of 16 vendors evaluated
- A leader in ransomware prevention with 100% prevention
- The best endpoint detection and response (EDR) and best product development
- A dominant leader in EDR
- The global technology innovation leader in endpoint security

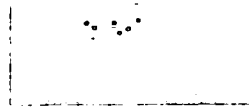
- Featured
- Recent
- Videos
- Categories
- Start Free Trial

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

[Handwritten signature]

CROWDSTRIKE **BLOG**

- [Featured](#) ▾
- [Recent](#) ▾
- [Videos](#) ▾
- [Categories](#) ▾
- [Start Free Trial](#)



(Click to enlarge)

CrowdStrike: Positioned Furthest to the Right for Completeness of Vision

CrowdStrike pioneered the EDR market, but we've never rested on our success. Our focus is to deliver the very best technology and groundbreaking innovations that drive the industry forward and deliver the outcomes that customers prioritize most: stopping breaches, consolidating point products to reduce complexity, and ensuring we have the easiest platform to deploy and manage.

Among 18 vendors evaluated, we are positioned furthest to the right on the Completeness of Vision axis in this Magic Quadrant, which evaluates vendors based on criteria including market understanding, market strategy, product strategy, innovation, business model and geographic strategy. We believe this placement demonstrates our diligence in helping customers across geographies and industries stay ahead of adversaries as enterprise work environments — and the threat landscape — continue to rapidly evolve.

We are extremely proud to be recognized as a three-time Leader in the Magic Quadrant for Endpoint Protection Platforms *and* placed furthest right in Completeness of Vision. We believe this recognition highlights the power of the CrowdStrike Falcon® platform in helping organizations thrive while defending against a broad range of threats. The Falcon platform protects customers without compromising on speed or performance, with a cloud-scale architecture that protects workloads and workforces anywhere, at any time.

Our priority from day one has been stopping breaches, and we believe in order to do this, you need the best technology, the best threat intelligence and the best people. We continue to develop our unified platform to achieve this vision. Only CrowdStrike delivers a generational platform approach that unifies world-class protection across endpoints, cloud workloads, identity and much more.

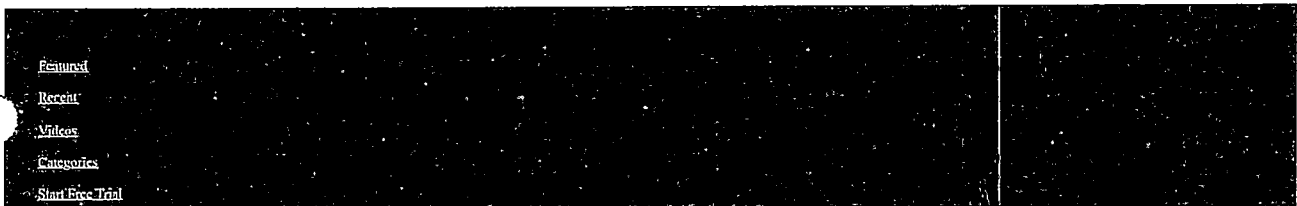
Industry-Leading EDR Is the Essential Foundation for XDR

CrowdStrike is relentlessly focused on building technologies to help organizations where they need it most: detecting and responding to security threats targeting a rapidly growing and changing attack surface. This is where XDR comes into play.

As we have long stated, XDR is the evolution of EDR — and it must be built on the strongest EDR foundation possible. The endpoint remains the most valuable source of security data, delivering unique visibility and telemetry that only a dynamic, lightweight agent can generate. We believe our recognition in the latest Gartner Magic Quadrant demonstrates that our 21,000+ customers have the best XDR foundation in the industry with our industry-leading EDR at the core.

Organizations can leverage the Falcon platform for a variety of XDR use cases that extend the aperture of detection and response beyond the endpoint to identify and remediate even the most sophisticated attacks.

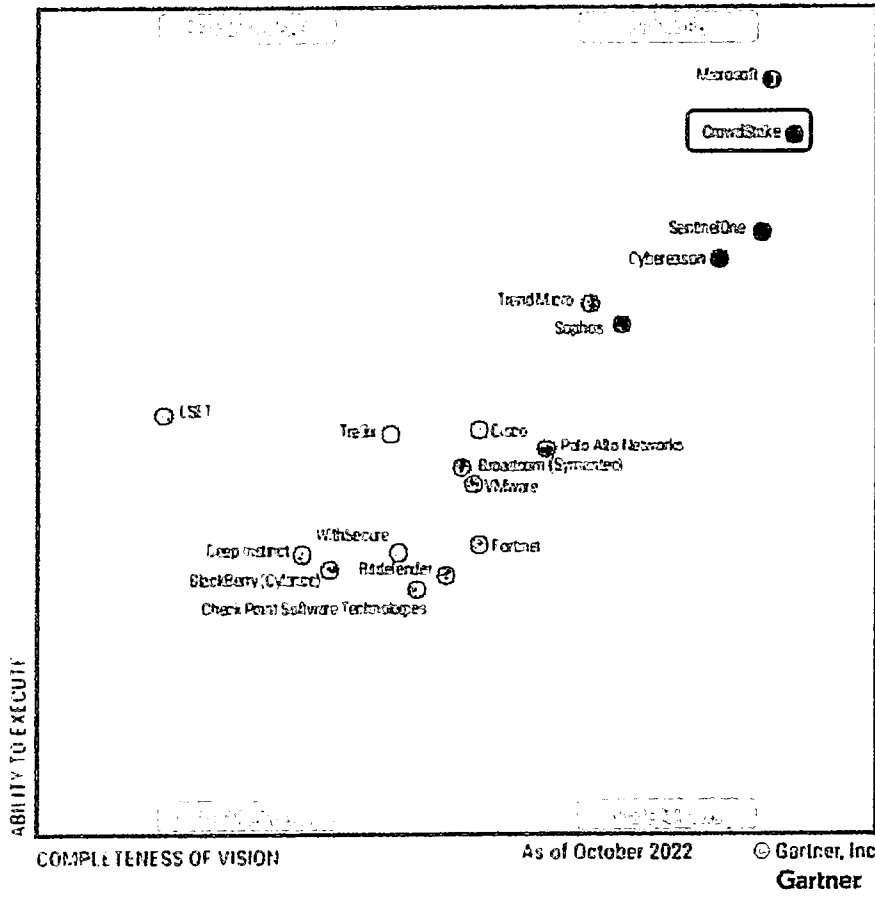
A Universally Recognized Vendor



A Leader for the third consecutive time

CrowdStrike named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms.

[View the report](#)



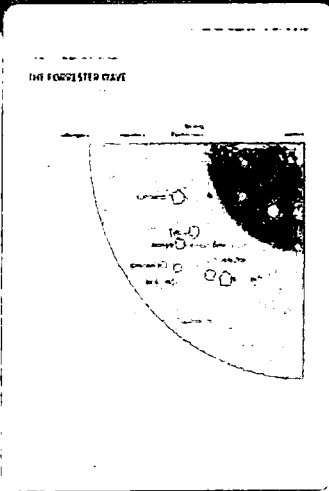
CROWDSTRIKE

Platform | Services | Why CrowdStrike? | Learn | Company

Start now

The Forrester Wave™: Managed Detection and Response, Q2 2023

First Name	Last Name
Business Email	Job Title
Phone Number	Company Name
Country	<input type="button" value="SUBMIT"/>



CrowdStrike Named a Leader in MDR

With the highest number of CrowdStrike in Leader in the 2023 Forrester Wave for Managed Detection and Response (MDR).

According to Forrester, CrowdStrike's exceptional list of complete MDR service blends products, platform, and services seamlessly for customers. Forrester evaluated 13 notable MDR providers and ranked them based on the strengths of their current offering, strategy, and market presence.

Read the Forrester Wave™ *Managed Detection and Response, Q2 2023* to learn:

- Why matters when selecting a managed MDR provider today
- Why CrowdStrike's innovative approach to MDR stands out
- Why the MDR market is heated and how CrowdStrike, in our opinion, is poised to take customer type and market trends.

DISCOVER MORE AT OUR RESOURCE CENTER

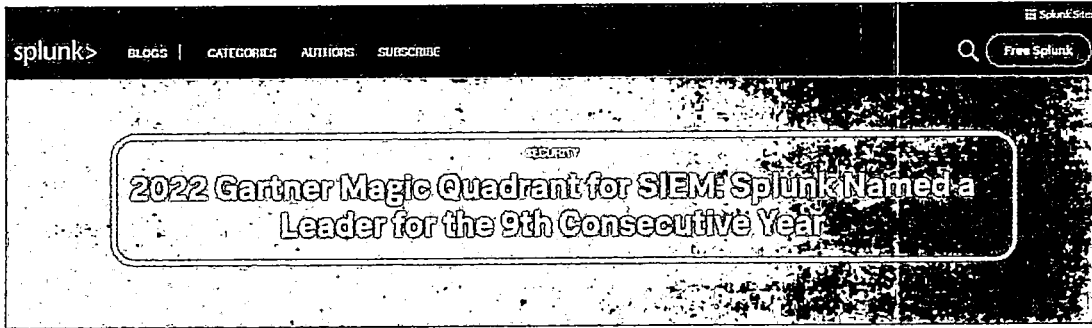
CASE STUDY	COMMAND TOOLS	CROWDCASTS	DATA SHEETS	DEMOS
GUIDES	INFOGRAPHICS	REPORTS	VIDEOS	WHITE PAPERS

TECHNICAL CENTER



For technical information on installation, policy configuration and more, please visit the CrowdStrike Tech Center.

[Visit the Tech Center](#)






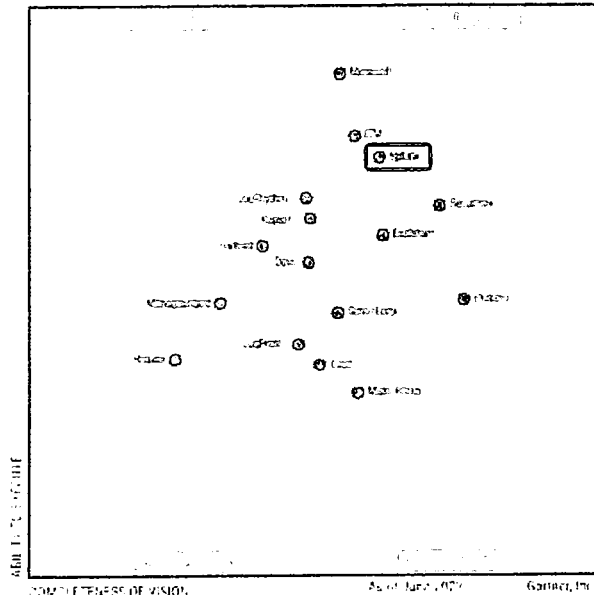



Splunk has been named a Leader in the 2022 Gartner® Magic Quadrant™ for Security Information and Event Management, marking the ninth consecutive year for Splunk in the Leaders Quadrant.

Figure 1: Magic Quadrant for Security Information and Event Management



Moreover, the recently released Gartner Market Share, All Software Markets, Worldwide 2021 report* places Splunk as #1 in SIEM market share with 30.25% market share.

We are honored to be recognized across these reports, and we are grateful to our customers and partners for making this recognition possible. We believe our position in the Leaders Quadrant for the last nine years is a testament to our commitment to delivering a data-centric security analytics solution that accelerates threat detection and investigation to build cybersecurity resilience for organizations.

Security Innovation and Integration

Over the last 12 months, we have continued to innovate our flagship security solution, Splunk Enterprise Security (SIEM), as well as the rest of our integrated security portfolio. These innovations are driven by a singular goal to help customers solve their most pressing security challenges by delivering faster and more effective detection, investigation, and response wherever data is stored, on-premises or multi-cloud. To that end, here's what we've delivered:

- Risk based alerting enhancements within Splunk Enterprise Security continue to effectively transform large volumes of noisy alerts into fewer high-fidelity incidents, prioritized by risk attribution. By correlating related events into a single incident, you can drive faster investigation and resolution, giving you time back in your day and more control over your security operations.
- Integration with Splunk Intelligence Management (formerly TruSTAR) delivers threat intelligence enrichment to help you quickly understand threat context, prioritize triage and accelerate investigations and response.
- Enhanced orchestration and automation capabilities with Splunk SOAR Cloud to speed up investigations and response for your organization: now featuring over 100 out-of-the-box automation playbooks, enabling any security team to begin to automate their most routine security tasks.
- Threat research and detections developed by the Splunk Threat Research Team fuel Splunk Security products, helping you stay one step ahead of emerging threats. Real-time content updates together with pre-packaged detection, machine learning models, and responses will help you realize faster time to value, increase threat visibility and remediate threats faster.
- Our Splunk Platform is the core foundational element of our data-driven security analytics approach. New Splunk 9.0 and Splunk Cloud Platform innovations will supercharge security use cases for your organization.
 - Ingest actions that enable admins to deploy ingest-time transformations and routing, reducing ingest and storage costs for non-critical data sets. For example, you can use ingest actions to filter specific data from large streams of Enterprise Detection and Response (EDR) data, ensuring high-value data comes into Splunk.
 - Utilize Federated Search across distributed environments, on-premises or in the cloud, bringing valuable distributed data to security use cases or performing threat hunting on remote data sets at scale using data models and stats.
 - Data Manager for Splunk Cloud lets you onboard data from multiple services and accounts quickly, ingest and normalize data from AWS, Azure, and soon Google Cloud Platform easily and utilize multi-cloud security monitoring dashboards that build on this data.

Get Your Copy of the 2022 SIEM Magic Quadrant

To our customers and partners, thank you again for making this recognition possible. Download your complimentary copy of the 2022 Gartner Magic Quadrant for SIEM today to learn more about Splunk Security and Splunk Enterprise Security. To learn more about Splunk Enterprise Security, visit our website or take a tour.

©Gartner, Inc. 2022 Gartner Magic Quadrant for Security Information and Event Management. Pete Shoard, Andrew Davies, Mitchell Schneider, October 10, 2022

SPLUNK CLOUD SERVICE SERVICE LEVEL SCHEDULE *

Service Level Commitment

The Splunk Cloud Service will be available 100% of the time, as measured by Splunk over each calendar quarter of the Subscription Term, and subject to the exclusions set forth below (the "Service Level Commitment").

A Splunk Cloud Service is considered available if the Customer is able to login to its Splunk Cloud Service account and initiate a search using Splunk Software.

Service Level Credit:

If Splunk fails to achieve the above Service Level Commitment for a Splunk Cloud Service, Customer may claim a credit for such Splunk Cloud Service as provided below, up to a maximum credit per calendar quarter equal to one month's Splunk Cloud Service subscription fees.

PERCENTAGE AVAILABILITY PER CALENDAR QUARTER	CREDIT
100	NO CREDIT
99.99-99.999	2 HOURS
99.9-99.99	4 HOURS
99.0-99.9	8 HOURS
95.0-99.0	1 DAY
0-95.0	1 MONTH

Exclusions

A Customer will not be entitled to a service credit if it is in breach of its Agreement with Splunk, including payment obligations. The Service Level Commitment does not apply to any downtime, suspension or termination of the applicable Splunk Cloud Service (or any Splunk Content or Splunk Software operating in connection with the Splunk Cloud Service) that results from:

- A Customer's breach of, or termination due to customer's breach of, the Agreement.
- Regular scheduled maintenance (Splunk's Maintenance Policy is available at https://www.splunk.com/en_us/legal/splunk-cloud-platform-maintenance-policy.html).
- Disaster relief, emergency maintenance or an emergency caused by factors outside Splunk's reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Content, Third Party Content or Internet Service Provider failure(s) or delays.
- A Customer's equipment, software or other technology or third-party equipment, software or technology (other than those which are under Splunk's control).
- Issues resulting from software or technology for which Splunk is not responsible under the Agreement.
- Customer inability or inability to operate the Forwarder software is addressed by Splunk support services. For purposes of the Service Level Commitment, the Forwarder software is excluded from the calculation of the availability of the Splunk Cloud Services.

No Service Level Commitment is provided for free, proof-of-concept or unpaid trial services

Service Credit Claims.

To receive a service credit, a Customer must file a claim for service credit within the (15) days following the end of the calendar quarter in which the Service Level Commitment was not met for an applicable Splunk Cloud Service, by contacting Splunk at splunk_cloud_billing@splunk.com with a complete description of the downtime, how the Customer was adversely affected, and for how long. Splunk reserves the right to deny the service credit if the Customer does not qualify.

The service credit remedy set forth in this Service Level Schedule is the Customer's sole and exclusive remedy for the unavailability of any applicable Splunk Cloud Service.

**Inhouse Cyber security
Forencics specialist
section**



GUIDEM

CERTIFICATE OF COMPLETION

This Certificate is Presented to

Ria B. Perez

for successfully completing 40Hrs of training on

Digital Forensics & Memory Analysis

Given this 11th of June 2022

Mark Christian Secretario

Mark Christian Secretario
Instructor/Owner

M

Certification Number
ECC5183724609



CHFI
Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator

This is to acknowledge that

Rio Perez

has successfully completed all requirements and criteria for

Computer Hacking Forensic Investigator

certification through examination administered by EC-Council

Issue Date: **11 February, 2022**

Expiry Date: **10 February, 2025**

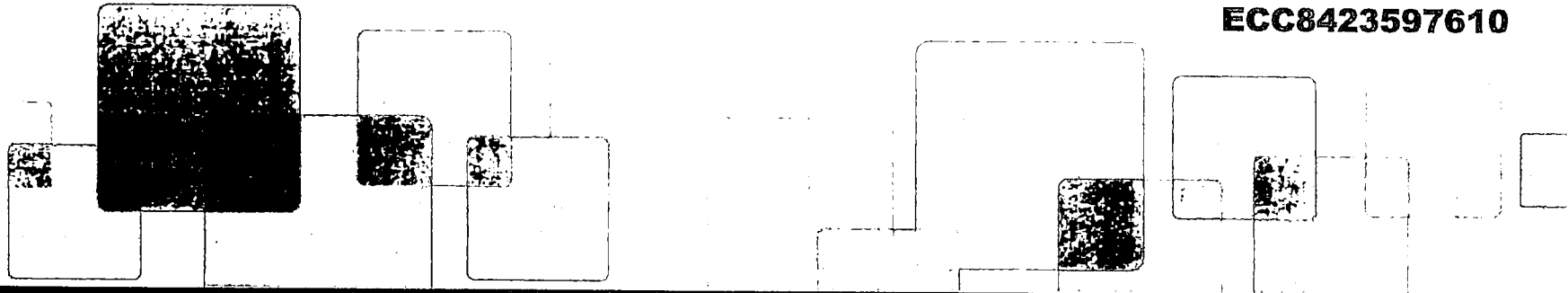


#0732
ISO/IEC 17024
Personnel Certification Program

EC-Council

Sanjay Bavisi, President

Certification Number
ECC8423597610



CHFI
Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator

This is to acknowledge that

Maria Carla Angela Belen

has successfully completed all requirements and criteria for

Computer Hacking Forensic Investigator

certification through examination administered by EC-Council

Issue Date: **11 February, 2022**

Expiry Date: **10 February, 2025**



ISO/IEC 17024
Personnel Certification Program

EC-Council

Sanjay Bavisi, President

II. Non-functional Requirements

A. Access Management



Managed ICT Services
Service Delivery with Flexibility

ACCESS MANAGEMENT

This document prescribes rules to ensure account and password management.

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

1 Access Management Activities

1.1 Requesting Access

All access-related requests shall be initiated through a Service Request (SR) Form. This applies to both internal and other external teams requiring access to internal services, systems and networks. The requestor shall fill-in the following details in the SR form.

- Request Date – the date of access request.
- Description of Request – describes the details of the request – system or network access/service and the duration of the needed access.
- Reason for Request – justification for the access request.

Access granted will be based on the roles and responsibilities of the requestor, aligning with the principles of least privilege.

1.2 Verification

This activity verifies the identity of the individual requiring the service and justification of the access or service requests.

1.3 Providing Rights

Once verification and appropriate approval is completed, the Access Management team will provide the required rights for the requested access, service or device.

1.4 Logging and Tracking Access

This ensures that the access being granted is used as intended. This will protect operations from any security gaps and risks.

1.5 Monitoring Activity Logs

This ensures user's activity logs are being monitored and reviewed by SOC. Security events such as unauthorized access, excessive incorrect login attempts are investigated and evaluated for security breaches weekly.

1.6 Removing or Restricting Rights

This activity involves removing or restricting access of a user. This is initiated by the HR Manager in case of employee's:

- Death
- Resignation
- Dismissal
- Change of role
- Disciplinary action

- Absence without leave.

Personnel with Prolonged Leaves

An employee who goes on a prolonged leave or extended leave of absence such as medical leave, Maternity Leave etc. shall be temporarily restricted from accessing the facilities and systems such as Active Directory account after 40 days of inactivity.

The employee shall request for reactivation of access upon his return and the IS shall review and approve the reactivation.

The Operations Head can likewise initiate the removal of access of an employee in special cases, i.e. during the occurrence of an incident where the user who requested the access is causing/caused the incident or in the case of an immediate resignation.

1.7 Physical Access Control

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.

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.

2. Use of Password Controls

According to the Data Protection Policy, as well as legal and contractual obligations, the organization must protect individual systems or information by means of the following password controls:

User / Administrator Generated Passwords	Password Manager	ITAAS Manager

The IT as a Service (ITAAS) Manager and Operations Head are responsible for safe keeping of all generated user and administrator passwords.

2.1 Protecting Passwords

The ITAAS Manager and Operations Head are responsible for prescribing the following rules regarding key management:

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least every three months or as frequently as is warranted based on risk.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.

- After the departure of an employee, any user-level accounts for that individual must be disabled or changed to a role suitable to their status, and all system-level passwords known to that individual should be changed as soon as possible, not to exceed three days.
- Passwords must not be inserted into email messages or other forms of electronic communication (unless encrypted in accordance with Acceptable Use Policy).
- 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.
- All user-level and system-level passwords must conform to the guidelines described below.

2.2 Guidelines

Users must apply good security practices when selecting and using passwords:

- Passwords must not be disclosed to other persons, including management and system administrators
- Passwords must not be written down unless a secure method has been approved by the Operations Head.
- User-generated passwords must not be distributed through any channel (by oral, written or electronic distribution, etc.); passwords must be changed if there are indications that passwords or the system might be compromised – in that case a security incident must be reported.
- Strong passwords must be selected, in the following way:
 - 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
- 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)

3. Remote Access Users

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.).

4. Scope of Access Management

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.



**Latest Forrester Leaders
and Gartner Magic
Quadrant report for
brands offered that has
such requirement**



Licensed for Distribution

Magic Quadrant for Cloud Infrastructure and Platform Services

Published 19 October 2022 - ID G00756608 - 29 min read

By Raj Bala, Dennis Smith, and 3 more

I&O leaders must weave through a perilous environment consisting of increasingly aggressive cloud providers further complicated by rising inflation, competition for cloud talent, regulatory mandates, and security and downtime incidents. Use this research to make strategic cloud provider selections.

Market Definition/Description

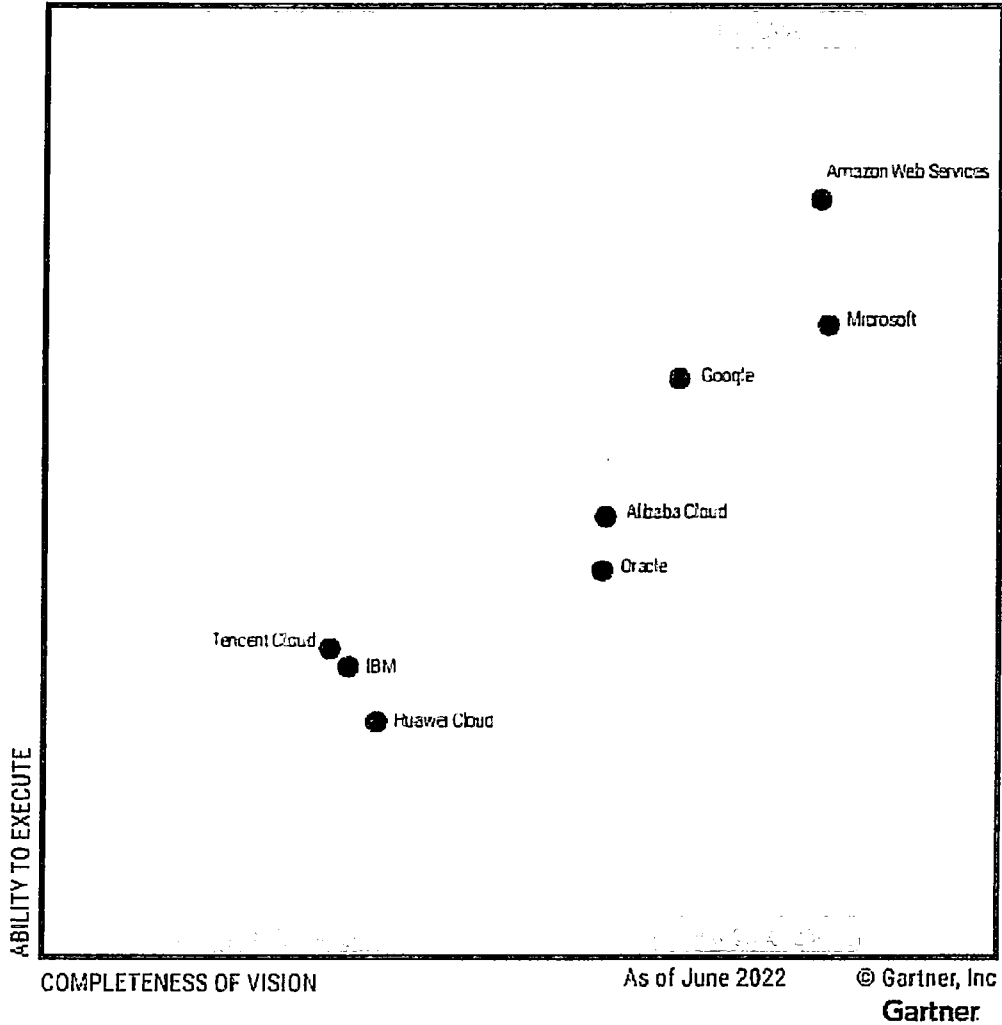
Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies. Gartner defines the cloud infrastructure and platform services (CIPS) market as standardized, highly automated offerings, in which infrastructure resources (e.g., compute, networking and storage) are complemented by integrated platform services. These include managed application, database and functions as-a-service offerings. The resources are scalable and elastic in near real time and are metered by use. Self-service interfaces, including a web-based user interface (UI) and an API, are exposed directly to the customer. The resources may be single-tenant or multitenant, and can be hosted by a service provider or on-premises in the customer's data center.

The scope of the Magic Quadrant for CIPS includes infrastructure as a service (IaaS) and integrated platform as a service (PaaS) offerings. These include application PaaS (aPaaS), functions as a service (FaaS), database PaaS (dbPaaS), application developer PaaS (adPaaS) and industrialized distributed cloud offerings that are often deployed in enterprise data centers.

Magic Quadrant

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services





Vendor Strengths and Cautions

Alibaba Cloud

Alibaba Cloud (also known as Aliyun in Chinese) is a Visionary in this Magic Quadrant. This Magic Quadrant evaluation is focused on Alibaba Cloud’s international business, which is headquartered in Singapore, and our technical assessment was performed using the international service.

Alibaba Cloud is a good fit for cloud-first digital business workloads for customers that are based in China or Southeast Asia. These customers either wish to leverage Alibaba Cloud’s technology to support their ecosystem or need to locate cloud infrastructure in China or Southeast Asia. Alibaba Cloud is focused on expanding its successes in Asia in addition to advancing use of ARM processors and database PaaS offerings.

Strengths

- **Regional and engineering leadership:** Alibaba Cloud continues to have a leadership position in China and the broader Sinosphere, and has a meaningful impact in surrounding countries in terms



Gartner.

Licensed for Distribution

Magic Quadrant for Endpoint Protection Platforms

Published 31 December 2022 - ID G00752236 - 55 min read

By Peter Firstbrook, Chris Silva

All vendors in this report have effective solutions for combating malicious attacks. Now that endpoint detection and response (EDR) is integrated into EPPs and evolving into extended detection and response (XDR), the main consideration for most buyers should be integration with security operations.

Strategic Planning Assumptions

By the end of 2025, 80% of Type C organizations will acquire endpoint detection and response (EDR) as a managed detection and response (MDR) service.

By the end of 2025, more than 50% of Type B organizations will consolidate EDR into a preferred vendor portfolio of security investments for more efficient security operations.

By the end of 2026, 80% of Type A organizations will be consuming EDR as part of a multitool extended detection and response (XDR) architecture.

Market Definition/Description

Note: Due to a pause in coverage of all Russian vendors by Gartner, there may be vendors that met the inclusion criteria described but were not evaluated. These vendors are not included in this research.

Endpoint protection platforms (EPPs) provide the facility to deploy agents or sensors to secure managed endpoints, including desktop PCs, laptop PCs, servers and mobile devices.

EPPs are designed to prevent a range of known and unknown malicious attacks. In addition, they provide the ability to investigate and remediate any incidents that evade protection controls.

The core capabilities of an EPP are:

- Prevention of, and protection against, security threats, including malware that uses file-based and fileless exploits.
- The ability to control (allow/block) scripts and processes.

- The ability to detect and prevent threats using behavioral analysis of device activity, application, identity and user data.
- Facilities to investigate incidents further and/or to obtain guidance for remediation when exploits evade protection controls.

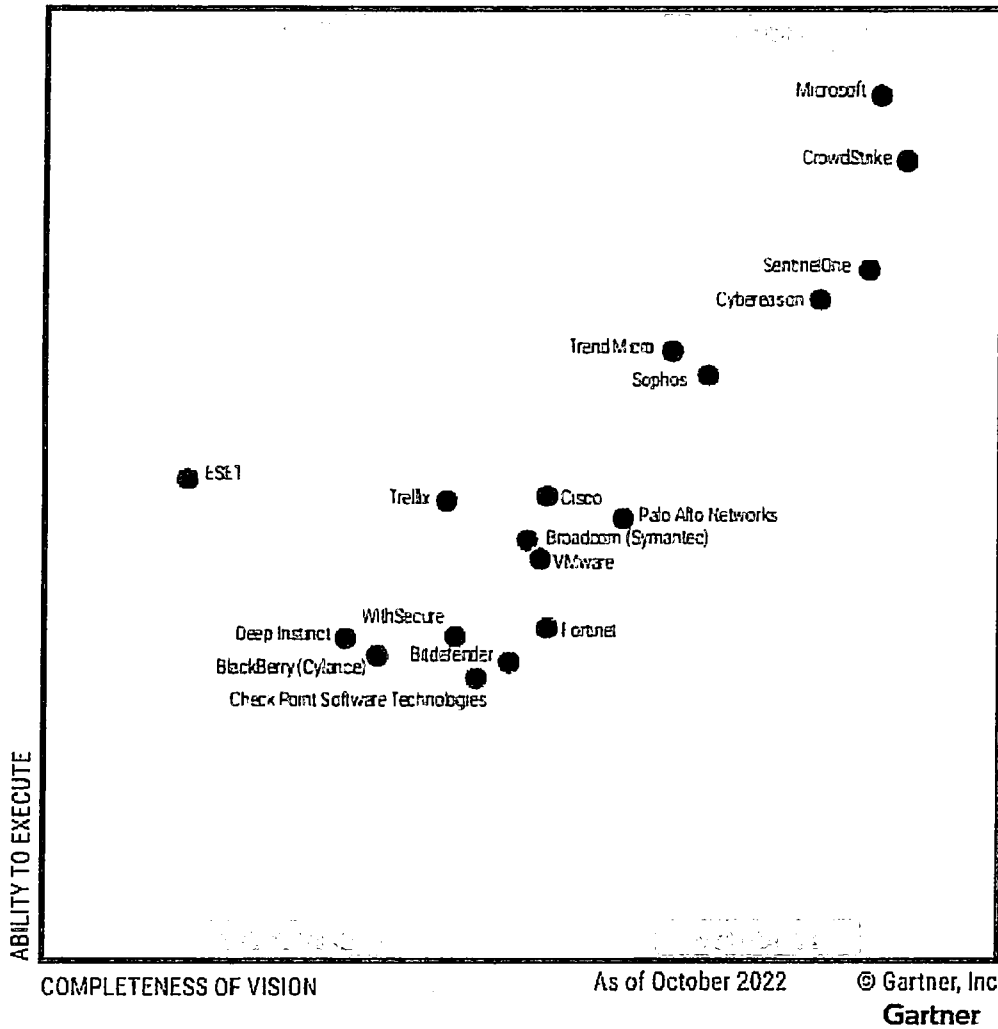
Optional capabilities often present in EPPs include:

- Risk reports based on inventory, configuration and policy management of endpoint devices.
- Management and reporting of operating system (OS) security control status, such as disk encryption and local firewall settings or substitute functionality.
- Facilities to scan systems for vulnerabilities and report on or manage the installation of security patches.
- Endpoint detection and response (EDR).
- Extended detection and response (XDR).
- Managed services.
- Extended OS compatibility with mobile, containers, virtual instances, and end-of-life and rare OSs.

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms





Source: Gartner (December 2022)

Vendor Strengths and Cautions

Bitdefender

Bitdefender is a Niche Player in this Magic Quadrant.

Its flagship product, the GravityZone platform, provides integrated EPP, EDR and now XDR capabilities, which are managed from the cloud. All other endpoint security products are provided as add-ons. Bitdefender also offers a rapidly expanding managed detection and response (MDR) service.

Bitdefender is best suited to Type B and C organizations in North America and EMEA that want easy-to-use and effective protection capabilities.

Strengths



Licensed for Distribution

Magic Quadrant for Security Information and Event Management

Published 10 October 2022 - ID G00755317 - 48 min read

By Pete Shoard, Andrew Davies, and 1 more

Security and risk management leaders continue to need a security system of record with comprehensive threat detection, investigation and response capabilities. SIEM is evolving into a security platform with multiple features and deployment models. This research will help you find the right solution.

Market Definition/Description

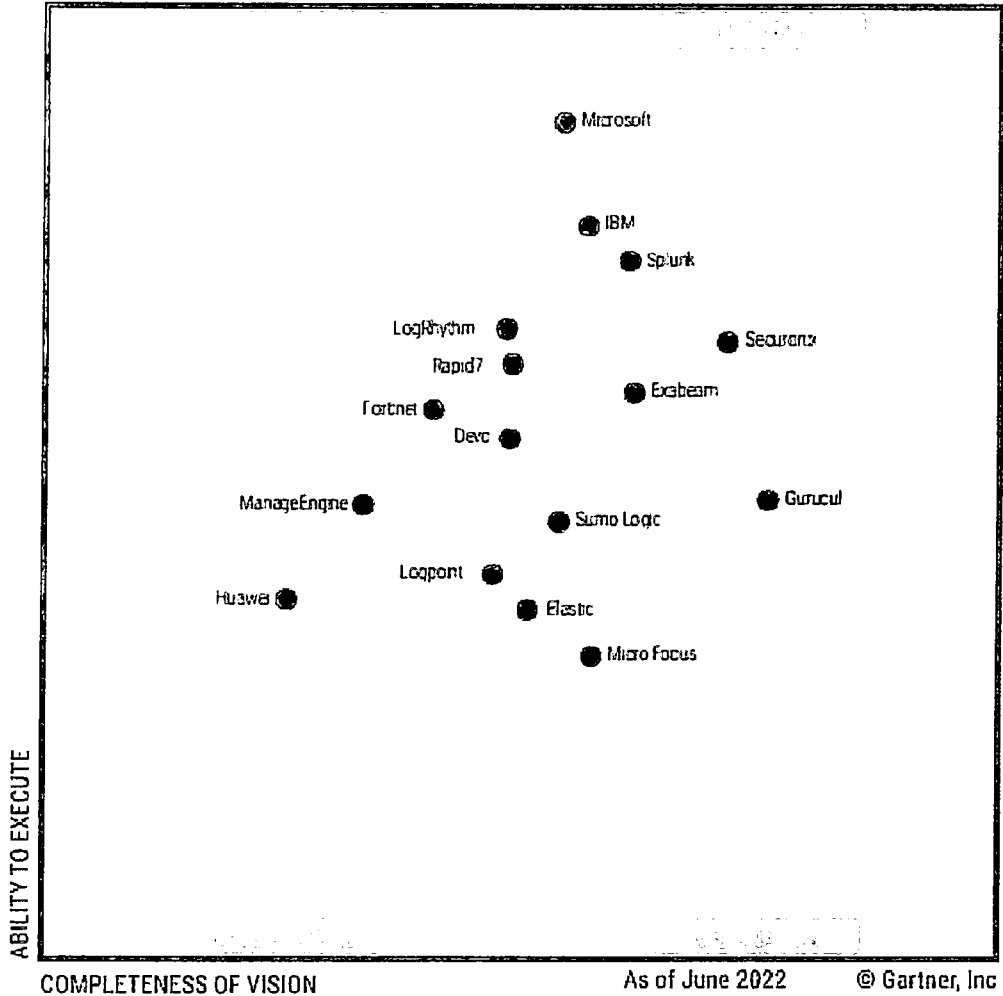
This document was revised on 12 October 2022. For more information, see the Corrections page on gartner.com.

SIEM aggregates the event data that is produced by monitoring, assessment, detection and response solutions deployed across application, network, endpoint and cloud environments. Capabilities include threat detection, through correlation and user and entity behavior analytics (UEBA), and response integrations commonly managed through security orchestration, automation and response (SOAR). Security reporting and continuously updated threat content through threat intelligence platform (TIP) functionality are also common integrations. Although SIEM is primarily deployed as a cloud-based service, it may support on-premises deployment.

Magic Quadrant

Figure 1: Magic Quadrant for Security Information and Event Management





COMPLETENESS OF VISION

As of June 2022

© Gartner, Inc

Gartner

Vendor Strengths and Cautions

Drag and drop this image to save

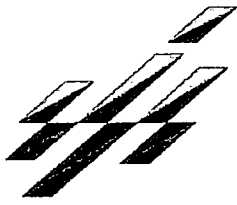
Devo

Devo is a Challenger in this Magic Quadrant. Its SIEM product, the Security Operations application, is delivered as a SaaS offering. Devo’s SIEM customer base is primarily in North America, followed by Europe and the Middle East, and is made up of small, midsize and enterprise organizations. Early in 2022, Devo achieved “In Process” status for the Federal Risk and Authorization Management Program (FedRAMP) standard, and expects to reach full authorization later in the year. Licensing, including its add-on capabilities (TIP via MISIP, hot storage, Entity Analytics and Devo Flow), is based on the volume of data ingested.

Strengths

- **IT observability coupled with security:** Devo delivers IT observability and security capabilities within the same UI and provides strong timelines, as well as adjacent views for joint functionality across security and I&O teams.

**List of local sales and
technical offices in the
Philippines**



TRENDS

Technology To Transcend

LIST OF LOCAL SALES AND TECHNICAL OFFICES IN THE PHILIPPINES

- Luzon
Metro Manila : Trends & Technologies, Inc.
6/F Trafalgar Plaza
105 H.V. Dela Costa St. Salcedo Village
Makati City
Tel. Nos. (02)811-8181
Fax No. (02) 814-0130
Contact Person: Rose S. Hernandez and
Wilfredo N. Aguilar
- Visayas : Trends & Technologies, Inc.- Cebu
The Penthouse
Trends Plaza Building
F. Ramos Street, Cebu City
Tel. Nos. (032) 520-8476
Fax No. (032) 262-7990
Contact Person: Jojit Lañas
- Mindanao : Trends & Technologies, Inc.- Davao
2nd Floor Building 1, ATU Plaza
Governor V. Duterte St., Davao City
Tel. No. (082) 222-6153
Fax No. (082) 222-6154
Contact Person: Jojit Lañas