

| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |



Cybersecurity Operations Center (CSOC)

OPERATIONS MANUAL

DRAFT

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

Contents

| | |
|---|-----------|
| 1. INTRODUCTION AND BACKGROUND | 4 |
| 1.1. Purpose and Delivery Scope | 4 |
| 1.2. Clients Interaction Process | 5 |
| 1.3. CSOC Organization | 6 |
| 2. TECHNOLOGY PLATFORM AND ARCHITECTURE DESIGN | 7 |
| 3. SERVICE FUNCTIONS & ELEMENTS | 7 |
| 4. ROLES AND RESPONSIBILITIES | 8 |
| 4.1. Help Desk | 11 |
| 4.2. Tier 1 Operations | 12 |
| 4.3. Tier 2 Operations | 12 |
| 4.4. Tier 3 Operations | 12 |
| 5. CSOC OPERATION TOOLS | 12 |
| 5.1. Vulnerability and Asset Scanners | 14 |
| 5.2. Honeypot Sensors | 14 |
| 5.3. SIEM | 15 |
| 6. KNOWLEDGE BASE | 15 |
| 7. TICKETING SYSTEMS | 16 |
| 7.1. Open Incident Ticket (TT) | 16 |
| 7.2. Incident Ticket (TT) Status | 17 |
| 7.3. Incident Ticket State transition | 17 |
| 7.4. Reroute the Incident Ticket | 18 |
| 7.5. Update Incident Ticket | 18 |
| 7.6. Transfer of responsibility for Incident Ticket | 19 |
| 7.7. Close Incident Ticket | 19 |
| 7.8. Incident Ticket Lifecycle | 20 |
| 8. CSOC OPERATIONS SUPPORT PROCESS | 21 |
| 8.1. Incident Management | 21 |
| 8.2. Problem Management | 21 |
| 8.3. Change Management | 21 |
| 8.4. Release Management | 21 |
| 8.5. Device Management | 22 |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|---|-----------|
| 9. CYBER INTRUSION/ATTACK HANDLING PROCEDURE | 22 |
| 10. FAULT LEVELS/PRIORITY DEFINITIONS | 23 |
| 10.1. Incident Assignment | 23 |
| 10.2. Event Prioritisation | 25 |
| 10.2.1. Priority 1 Events | 25 |
| 10.2.2. Priority 2 Events | 25 |
| 10.2.3. Priority 3 Events | 25 |
| 10.2.4. Priority 4 Events | 25 |
| 10.3. Service Level Agreement | 25 |
| 10.3.1. Incident Response, Restoration and Resolution Times | 25 |
| 11. Key Performance Indicators (KPIs) Reporting | 26 |
| 12. COMMUNICATION FLOW | 27 |
| 12.1. Clients to CSOC | 27 |
| 12.2. CSOC to Clients | 27 |
| <u>13. CONTACT DETAILS</u> | 27 |
| <u>13.1. CSOC Escalation Matrix</u> | 27 |
| <u>13.2. CSOC Roster</u> | 28 |
| <u>13.3. Clients Contact Details</u> | 28 |




















| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |




1. INTRODUCTION AND BACKGROUND

Global Cybersecurity Resources (GCR) is a not-for-profit organization run by Carleton University's Lead to Win program. The organization is mandated with increasing the IT security of Ottawa region SMBs, increasing the availability of qualified security staff, and driving economic development for existing and new companies. A Cybersecurity operations centre (CSOC) is a centralized enterprise security monitoring team organized around the goal of improving the organization's risk posture through the use of technology and processes for incident detection, isolation, analysis and mitigation (SANS, 2015)

1.1. Purpose and Delivery Scope

One of the services of GCR is IT Intruder Alerting Service for Small Businesses delivered and supported through its Cybersecurity Operations Centre (CSOC). This document provides generic operational instructions in the delivery of IT Intruder Alerting Service for Small Business.

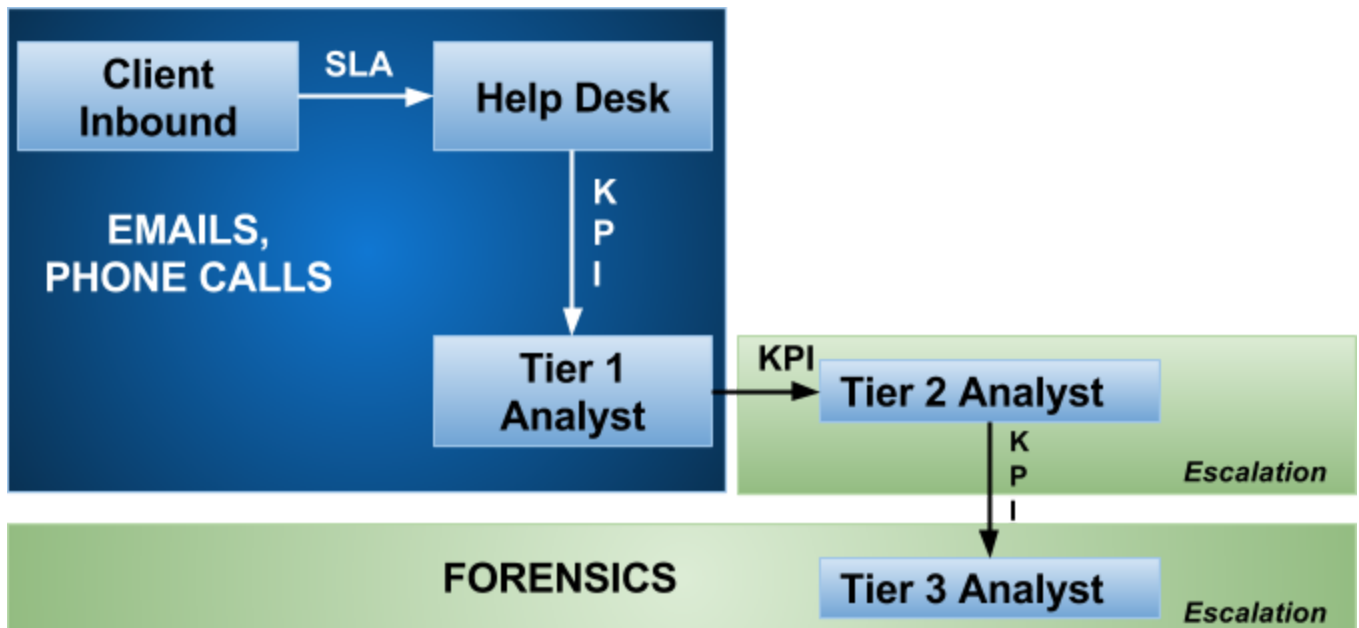
| S R E L V E I S C E | Inbound Request (Phone Call / Email) | Monitor Event & Alarms | IT Creation | Logs Incidents & Requests | Isolate & Validate Incidents | Create Shift Logs & Report | Plans & Implement Change | Forensic Investigation | Training & Resource Development | KPI Fulfilment | Management Communication & Overall CSOC Operations & Management |
|--|---|---|---|---|---|---|---|---|---|---|---|
| HELP DESK |  | | | | | | | | | | |
| TIER 1 ANALYST | |  |  |  |  |  | | | | | |
| TIER 2 ANALYST | |  |  |  |  |  |  | | | | |
| TIER 3 ANALYST | | | | |  |  |  |  | | | |
| CSOC MANAGEMENT | | | | | | | | |  |  |  |

 - Strictly by Helpdesk
 - Handled by more than one role
 - Strictly by Management

Reference: Creating & Maintaining A SOC-The Details Behind Successful Security Operations Center (Intel Security)

| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

1.2. Clients Interaction Process

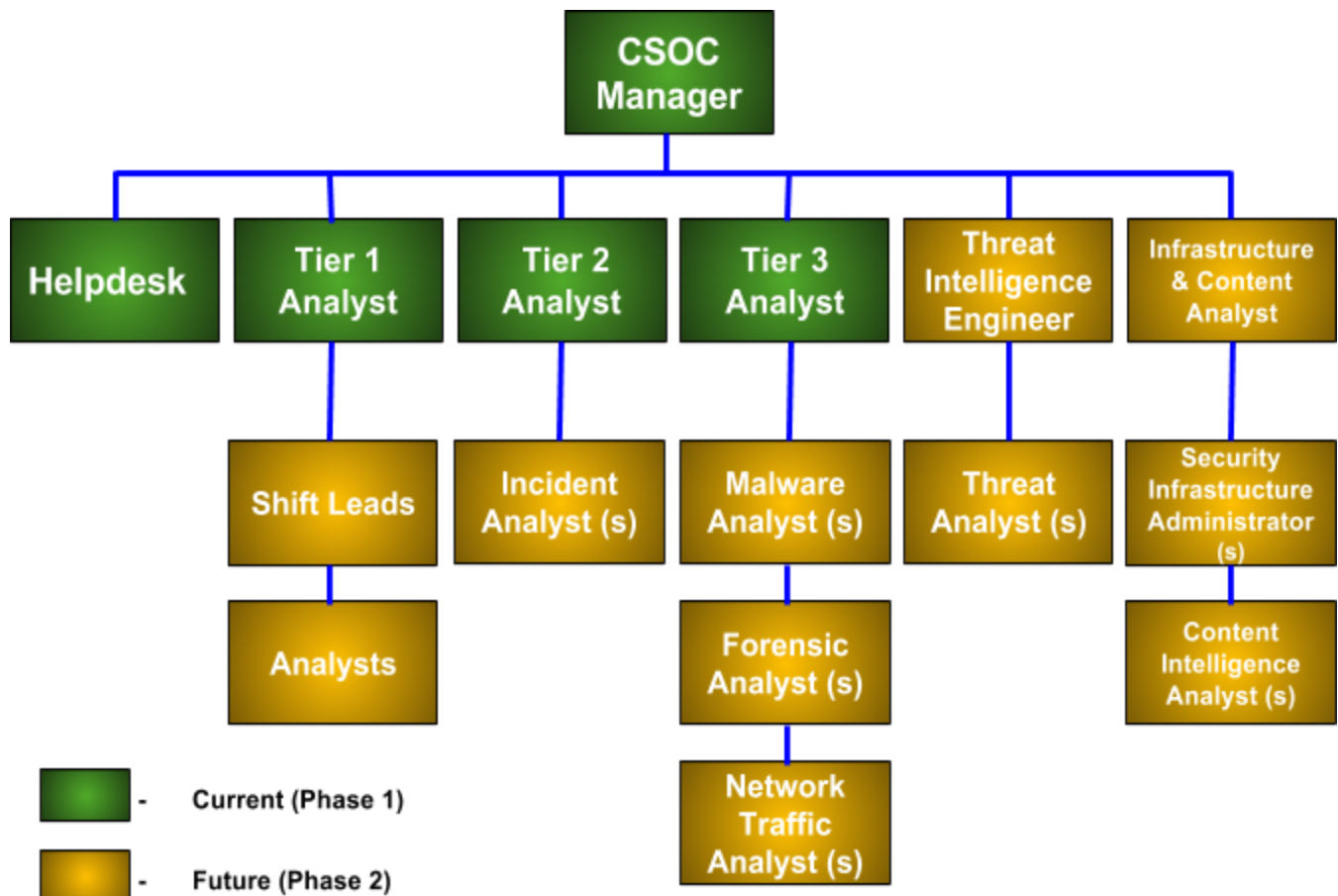


Reference: The Definitive Guide to Building A World Class SOC by Kenneth Ho

1.3. CSOC Organization

The CSOC team is grouped into 4 layers (presently), while we will grow into 6 layers of 4 teams running a 24/7 shift; whilst the rest of the team runs 8:00am-5:00pm regular hours.

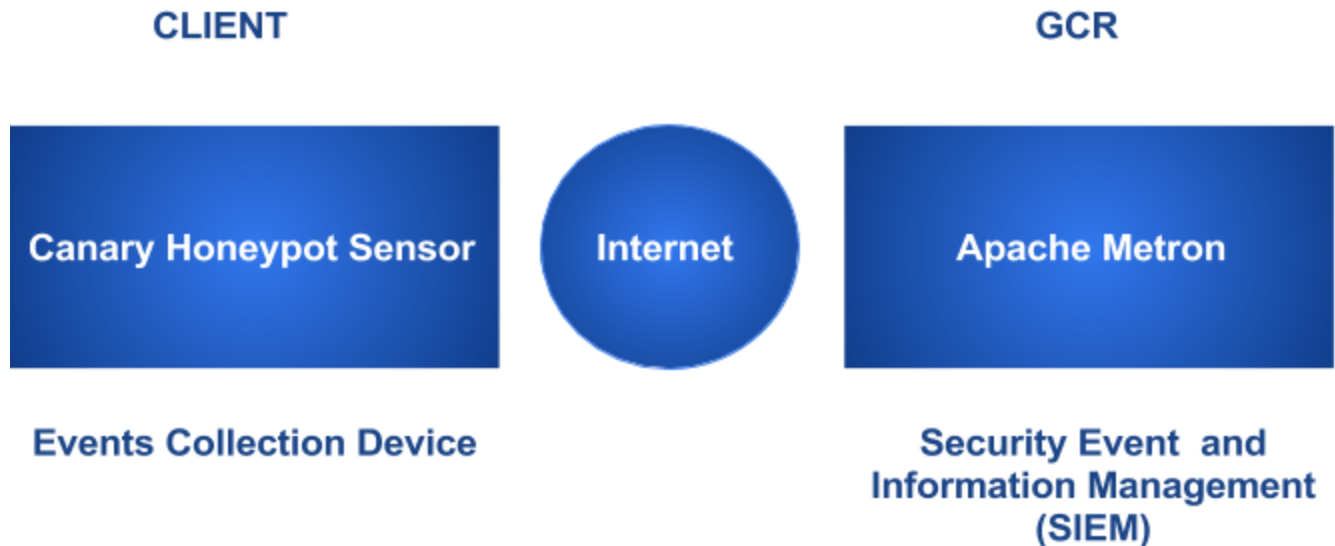
| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |



Reference: Keys to a successful SOC by Matthew Gardiner & Richard Nichols (RSA, 2015)

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |







2. TECHNOLOGY PLATFORM AND ARCHITECTURE DESIGN






3. Canary Honeypot Sensor automatically connects to the GCR hosted CSOC and sends notifications of suspicious interactions. Only information about intruder interactions with the Canary are sent to the CSOC. Apache Metron provides a scalable advanced security analytics framework built with the Hadoop Community evolving from the Cisco OpenSOC Project. A Cybersecurity application framework that provides organizations the ability to detect cyber anomalies and enable organizations to rapidly respond to identified anomalies (Apache Metron Website).

4. SERVICE FUNCTIONS & ELEMENTS

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| S R E O R L V E I S C E | Inbound Request (Phone Call / Email) | Monitor Event & Alarms | TT Creation | Logs Incidents & Requests | Isolate & Validate Incidents | Create Shift Logs & Report | Plans & Implement Change | Forensic Investigation | Training & Resource Development | KPI Fulfilment | Management Communication & Overall CSOC Operations & Management | Availability (Planned) | Availability (Future) |
|--|---|---|---|---|---|---|---|---|--|---|---|------------------------|-----------------------|
| HELP DESK |  | | | | | | | | | | | 8*5 EST | 24*7 EST |
| TIER 1 ANALYST | |  |  |  |  |  | | | | | | 8*5 EST | 24*7 EST |
| TIER 2 ANALYST | |  |  |  |  |  |  | | | | | 8*5 EST | 24*7 EST |
| TIER 3 ANALYST | | | | |  |  |  |  | | | | 8*5 EST | 8*5 EST |
| CSOC MANAGEMENT | | | | | | | | |  |  |  | 8*5 EST | 8*5 EST |

-  - Strictly by Helpdesk
-  - Handled by more than one role
-  - Strictly by Management

Reference: Creating & Maintaining A SOC-The Details Behind Successful Security Operations Center (Intel Security)

5. ROLES AND RESPONSIBILITIES

These functions include monitoring, detection, incident resolution, etc. As defined, they will guide the daily CSOC processes and procedures. Service functions are associated with various CSOC components.

Each tier within the CSOC is assigned responsibilities based on each analyst's level of expertise within the tier level.

Procedures will be revised continually as technologies advance and experience increases. The GCR CSOC Analysts are responsible for activities as listed below:

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| JOB TITLE | JOB DESCRIPTION |
|--|--|
| Tier 1 (Alert Analyst/Security Analyst) | <ul style="list-style-type: none"> • Triage Specialist (Separating the wheat from the chaff) • Continuously monitors the alert queue; triages security alerts; monitors health of security sensors and endpoints; collects data and context necessary to initiate Tier 2 work • Reviews the latest alerts to determine relevancy and urgency. Creates new incident tickets for alerts that signal an incident and require Tier 2 / Incident Response review. • Runs vulnerability scans and reviews vulnerability assessment reports. Manages and configures security monitoring tools (netflows, IDS, correlation rules, etc.) |
| Tier 2 (Incident Responder / Security Analyst) | <ul style="list-style-type: none"> • Incident Responder (IT's version of the first responder) • Performs deep-dive incident analysis by correlating data from various sources; determines if a critical system or data set has been impacted; advises on remediation; provides support for new analytic methods for detecting threats • Reviews incident tickets generated by Tier 1 Analyst(s) • Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack • Reviews and collects asset data (configurations, running processes, etc.) on these systems for further investigation • Determines and directs remediation and recovery efforts |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|--|--|
| Tier 3 (Subject Matter Expert / Expert Security Analyst) | <ul style="list-style-type: none"> • Threat Hunter (Hunts vs. defends) • Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications or underlying IT infrastructure; acts as an incident “hunter,” not waiting for escalated incidents; closely involved in developing, tuning and implementing threat detection analytics • Reviews asset discovery and vulnerability assessment data • Explores ways to identify stealthy threats that may have found their way inside your network, without your detection, using the latest threat intelligence • Conducts penetration tests on production systems to validate resiliency and identify areas of weakness to fix • Recommends how to optimize security monitoring tools based on threat hunting discoveries |
| Tier 4 (CSOC Manager) | <ul style="list-style-type: none"> • Operations & Management (Chief Operating Officer for the CSOC) • Supervises the activity of the CSOC team • Recruits, hires, train, and assess the staffs • Manages the escalation process and reviews incident reports • Develops and executes crisis communication plan to CISO and other stakeholders • Runs compliance reports and supports the audit process • Measures CSOC performance metrics and communicates the value of security operations to business leaders |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs; communicates with management; serves as organizational point person for business-critical incidents; provides overall direction for the CSOC and input to the overall security strategy • Reviews all incident records to ensure events and incidents are resolved within the parameters of the defined severity levels • The Manager must audit incidents records, particularly those which have exceeded standard resolution times |
|--|---|

5.1. Help Desk

The CSOC will facilitate calls and emails from the help desk. There will be only one main email address for use with customers. All customer interactions will be done using this eMail, and all email interactions will be logged against the customer account.

Helpdesk receives logs with Ticket System all inbound calls and emails from customers. There will be two ticketing systems used, one for customer accounts and one for internal engineering CSOC team usage.

The customer accounts ticketing will be managed by an AWS cloud hosted SuiteCRM.

5.2. Tier 1 Operations

| SERVICE ELEMENTS | |
|--|--------|
| Real-time monitoring, TT management and closure of false positives | YES |
| Aggregate logs/data, basic investigation and mitigation | YES |
| Coordination of response and remediation of: SIEM, IPS and DLP | Future |
| Initial diagnostics and incident isolation/triage | YES |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|--|---------|
| Reviews the latest alerts to determine relevancy and urgency | YES |
| Escalates an incident to Tier 2 for timely Incident Response | YES |
| Runs vulnerability scans and reviews vulnerability assessment reports | Planned |
| Manages and configures security monitoring tools (netflows, IDS, correlation rules, etc. | Future |
| Focuses on real-time feeds of events and other data visualizations | YES |

5.3. Tier 2 Operations

| SERVICE ELEMENTS | |
|---|---------|
| Reviews TT generated by Tier 1 Analyst | YES |
| Deep Investigations | YES |
| Problem Correction/Mitigation/recommends changes | YES |
| Reviews and collects asset data (configurations, running processes, etc.) on the systems for further investigation | YES |
| Advance Search/Subtle Event Detection/callout-notifications | Future |
| Security systems and software: update/test DAT definitions, Apply corrective IDS/IPS and Firewall rules, Apply other corrective software as instructed or required | Future |
| Computing equipment and endpoint devices: Remote Administration, Update Antivirus, Tune HIPS alerts, Configure Whitelisting | Future |
| Determines and directs remediation and recovery efforts. | Future |
| Work with third-party vendors | YES |
| Close incidents: Coordination with tier levels, Coordination with end users and system administrators | YES |
| Continue with threat investigation while leveraging emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack | Planned |

5.4. Tier 3 Operations

| SERVICE ELEMENTS | |
|--|--------|
| Advanced Investigations and functioning of specific applications or underlying IT infrastructure | Future |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|---|---------|
| Prevention and closely involved in developing, tuning and implementing threat detection analytics | Future |
| Threat Hunting and Forensics | Future |
| Counter-Intelligence | Future |
| Malware Reverser and Reverse Engineering | Future |
| Reviews asset discovery and vulnerability assessment data | Planned |
| Conducts penetration tests on production systems to validate resiliency and identify areas of weakness to fix | Future |
| Recommends how to optimize security monitoring tools based on threat hunting discoveries | YES |
| Reports | YES |

6. CSOC OPERATION TOOLS

GCR CSOC will not use commercial software, rather, will build and support OSS. The following tools will be used by CSOC for day to day operations.

| Software Tool | Functions |
|---------------|--|
| Apache Metron | SIEM |
| Suite CRM | CRM, Sales, Support Tickets |
| Cowrie | Honeypot SSH |
| Dionaea | Honeypot |
| OSSEC | IDS (for honeypot platform protection) |
| OpenVAS | Vulnerability and Asset Scanner |
| Mender | IoT Device Software Update Management |

6.1. Vulnerability and Asset Scanners

These are computer programs designed to assess computers, computer systems, networks or applications for weaknesses. In plain words, scanners are used to discover the weak points or

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

poorly constructed parts of a system. They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

A vulnerability scanner runs from the end point of the person inspecting the attack surface in question. The software compares details about the target attack surface to a database of information about known security holes in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts. The scanner software attempts to exploit each vulnerability that is discovered.

However, running a vulnerability scan can pose its own risks as it is inherently intrusive on the target machine's running code. As a result, the scan can cause issues such as errors and reboots, reducing productivity.

There are two notable approaches to vulnerability scanning, authenticated and unauthenticated scans. In the unauthenticated method, the tester performs the scan as an intruder would, without trusted access to the network. Such a scan reveals vulnerabilities that can be accessed without logging into the network. In an authenticated scan, the tester logs in as a network user, revealing the vulnerabilities that are accessible to a trusted user, or an intruder that has gained access as a trusted user.

Note that this is a future scope for the GCR CSOC (Canary VAS).

6.2. Honeypot Sensors

This is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked. Honeypot sensors can be classified based on their deployment (use/action) and based on their level of involvement. Based on deployment, honeypot sensors may be classified as

- production honeypots sensors
- research honeypots sensors

Production honeypot sensors are easy to use, capture only limited information, and are used primarily by corporations. Production honeypot sensors are placed inside the production network with other production servers by an organization to improve their overall state of security.

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

Normally, production honeypot sensors are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypot sensors.

Research honeypot sensors are run to gather information about the motives and tactics of the black hat community targeting different networks. These honeypot sensors do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats. Research honeypot sensors are complex to deploy and maintain, they can capture extensive information, and are used primarily by research, military, or government organizations.

GCR uses a low/medium interaction production honeypot device and sensors.

6.3. SIEM

The SIEM core technology acts as an information repository. SIEMs are an emerging technology solution for monitoring, investigating, and responding to malicious events. It goes beyond storage and alerts the analyst to manage a higher level of risk by providing:

- Real-time monitoring and correlation
- Events enrichment
- Historical analysis
- Automated response

For GRC the Apache Metron is used as the SIEM.

7. KNOWLEDGE BASE

The GCR CSOC has one main knowledge base system. This document is the master document and all content will by default be added to this document. As the size and content dictates, the content may be broken out into stand alone documents which this document will reference.

8. TICKETING SYSTEMS

There will be two ticketing systems used, one for customer accounts and one for internal engineering CSOC team usage. The customer accounts will be managed by SuiteCRM, while the internal engineering system will tentatively be Odoo (to be reviewed). TT in this document stands for Incident Ticket.

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

8.1. Open Incident Ticket (TT)

Helpdesk Resource/Tier 1 Analysts will open an Incident Ticket (TT) based on the source of information. All inbound calls/emails from Clients will be handled and TT raised by the Helpdesk, while all intrusions as may be detected or captured by Tier 1 Analyst will be logged by the Tier 1 Analyst.

It is required that a Customer Complaint or Event/Incident as may be detected from the system/network by the Tier 1 Analyst with proper classification of the Complaint/event is done before a TT is created. It can also be that Service/Systems Performance/Quality thresholds have been reached or breached, or that an Incident notification has been received from Customer through CSOC Helpdesk.

Therefore, if the Service/Systems Performance/Quality thresholds criteria are not fulfilled or there's a security breach, then an Incident Ticket can be generated. If new ticket is not needed, existing tickets need to be updated with current logs/data and information.

Furthermore, the below listed steps must be followed before new TT is created:

- Check if the event/incident has an opened TT. Refer to historical logs (Closed TT's) for this event/incident before creating a new Incident Ticket. For event/incident search on client's name and other keywords in the Incident Ticket Event Manager
- If a TT already exists, a new TT shall not be created, rather the old should be updated with the new information
- If no TT is found, create a new TT

8.2. Incident Ticket (TT) Status

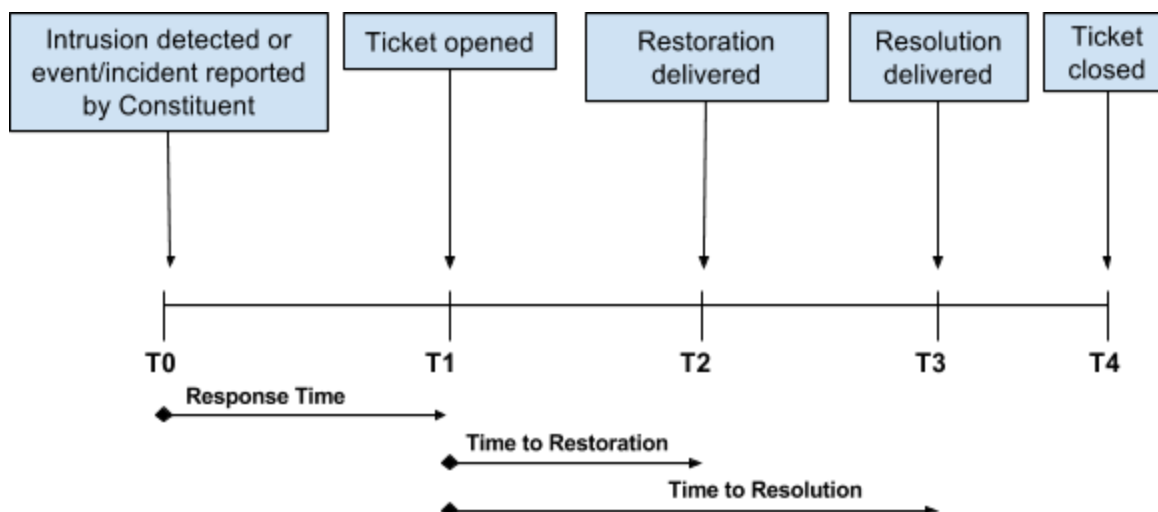
| Status | Description |
|--------|--|
| New | This State is the initial state, TT will be transited to queued state as soon as it is created |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|----------|---|
| Queued | A newly created Incident Ticket awaiting acceptance by an Analyst |
| Open | This State represent that work is in progress |
| Deferred | An incident ticket can be put in state ‘differed” meaning that the responsibility for the TT is transferred to an external organization, in this case countdown for resolution time is stopped, it is possible to set up an expected ready time and to initiate a notification when this time is about to exceed. |
| Cleared | This status shows the required work to resolve the event/incident has been completed or service/system has been restored .TT can only be put in clear state with “Solution”, Cleared time/date for a TT can be entered manually |
| Closed | This status shows that event/incident has been resolved and reason for fault has been known. The final remedy may be entered in solution field |

8.3. Incident Ticket State transition

Following are the possible transition of TT and all state changes are logged in the history log



| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

8.4. Reroute the Incident Ticket

Helpdesk Resource is required to assign/reroute the opened ticket as within five (5) minutes of Ticket opening to CSOC Tier 1 Analyst for immediate investigation.

CSOC Tier 1 Analyst is required to assign/reroute the tickets to CSOC Tier 2 Analyst (within 2 hours) if further analysis/investigation is required. CSOC Tier 1 Analyst must state clearly the extent of investigation/analysis already done, and if possible, attach logs/data that will help CSOC Tier 2 Analyst with further investigation.

CSOC Tier 2 Analyst is required to assign/reroute the same ticket to CSOC Tier 3 Analyst, (who also serves as the Subject Matter Expert), if he is not able to identify and resolve the problem. He should provide enough useful information, data/logs to CSOC Tier 3 Analyst that will aid timely resolution of the incident at hand.

CSOC Tier 3 Analyst reviews the ticket with data/logs attached, he analyses the logs and provides timely solution for the incident.

8.5. Update Incident Ticket

In the process of incident handling, all important updates of incident ticket are highlighted. All actions taken to restore the incident must be logged in the TT by everyone who works on the ticket from different Tiers/levels of analysis done.

8.6. Transfer of responsibility for Incident Ticket

An Analyst may and can transfer the responsibility for an incident ticket to another Analyst/Level for further analysis or resolution. When the responsibility for a ticket is transferred to another Analyst/Level that Analyst/Level must accept responsibility for the incident ticket. If the responsibility is not accepted within a certain time, the incident ticket will be escalated to the next level or to the CSOC Supervisor/Manager

However, in an event of delay in action on assigned TTs, the originator Analyst/Level must follow up with assigned Analyst/Level to take necessary actions.

| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

CSOC Tier 1 team must check TTs status not only at shift handover, but on or before TT breaches SLA . The Ticketing tool) would have an interface to reflect SLA breaches and about to breach SLA TTs, which should be monitored by CSOC Tier 1 Analyst.

The TT originator must ensure closure of TT upon confirming the seizure or resolution of Event/Incident, otherwise, whoever resolves the issue should ensure TT is closed accordingly with details of work done.

8.7. Close Incident Ticket

If the Event/Incident is ceased and the solution not known, the TT status should be set to Cleared.

- Accept the Incident Ticket. (Status must be Open before responsible Analyst can make changes)
- Describe the solution in the Solution Field and the action in the event Logbook
- Fill in solution time and actual Event/Incident duration in the Logbook
- **Note:** Actual Event/Incident duration is the service affecting disruption time in the network, not the solution time in total
- Change the Status to Cleared

If the Event/Incident is ceased and the solution is known, the status should be set to Closed.

- Describe the final solution in the Solution Field and the action in the event Logbook
- If Event/Incident problem occurs first time, transfer solution to Knowledge base document/archive
- Change the Status to Close

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

8.8. Incident Ticket Lifecycle

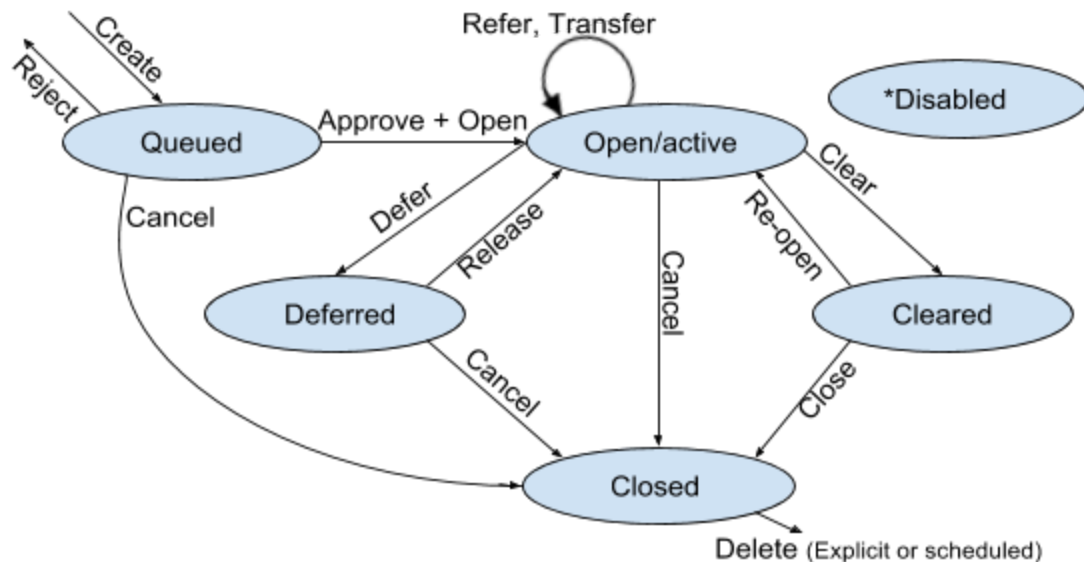


Figure – TT Lifecycle

The Clock-Stop period will commence according to the following:

- The clock stops running as CSOC passes the problem back to Clients or a Constituent's subcontracted third party, requiring this party's action, such as when more information is needed to be able to proceed
- The clock stops running when immediate action cannot be taken but scheduling is necessary, such as scheduling action outside "busy-hour" to reduce operational impact according to the planned work procedure

The clock-stop period will end (clock continues from where it was stopped) as an updated problem ticket returns to GCR CSOC Analyst re-commences problem clearing activities.

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

9. CSOC OPERATIONS SUPPORT PROCESS

9.1. Incident Management

An incident is an unplanned occurrence, interruption, disturbance and intrusion to an IT service. It is a reduction in the quality of an IT service, or a failure of a change which actually or potentially jeopardizes the Confidentiality, Integrity and Availability of an IT service. The purpose of incident management is to restore normal service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring timely resolution of all disturbances and intrusions that could affect levels of service quality. The incident management process is responsible for timely progression in all incidents from when they are first reported until they are closed. Effective incident management improves availability, ensuring that users are able to get back to work quickly following a disturbance

9.2. Problem Management

A problem is defined as an underlying cause of one or more existing or potential incidents. Problem management therefore is the process that investigates the cause of incidents and, wherever possible, implements a permanent solution to prevent recurrence. It aims to identify the root cause of incidents, to document known errors, and to take action to remedy them. It provides known error information, which enables incident management to restore service timely. It improves the overall quality and availability of services

9.3. Change Management

This controls the service lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services. It ensures adequate management of changes to service assets.

9.4. Release Management

This focuses on the release controls that are specified in the release policy. The role of release management is to ensure the successful introduction of changes into the live environment, minimizing the unpredicted impact to the business. It ensures delivered releases into the live environment are successful and well controlled

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

9.5. Device Management

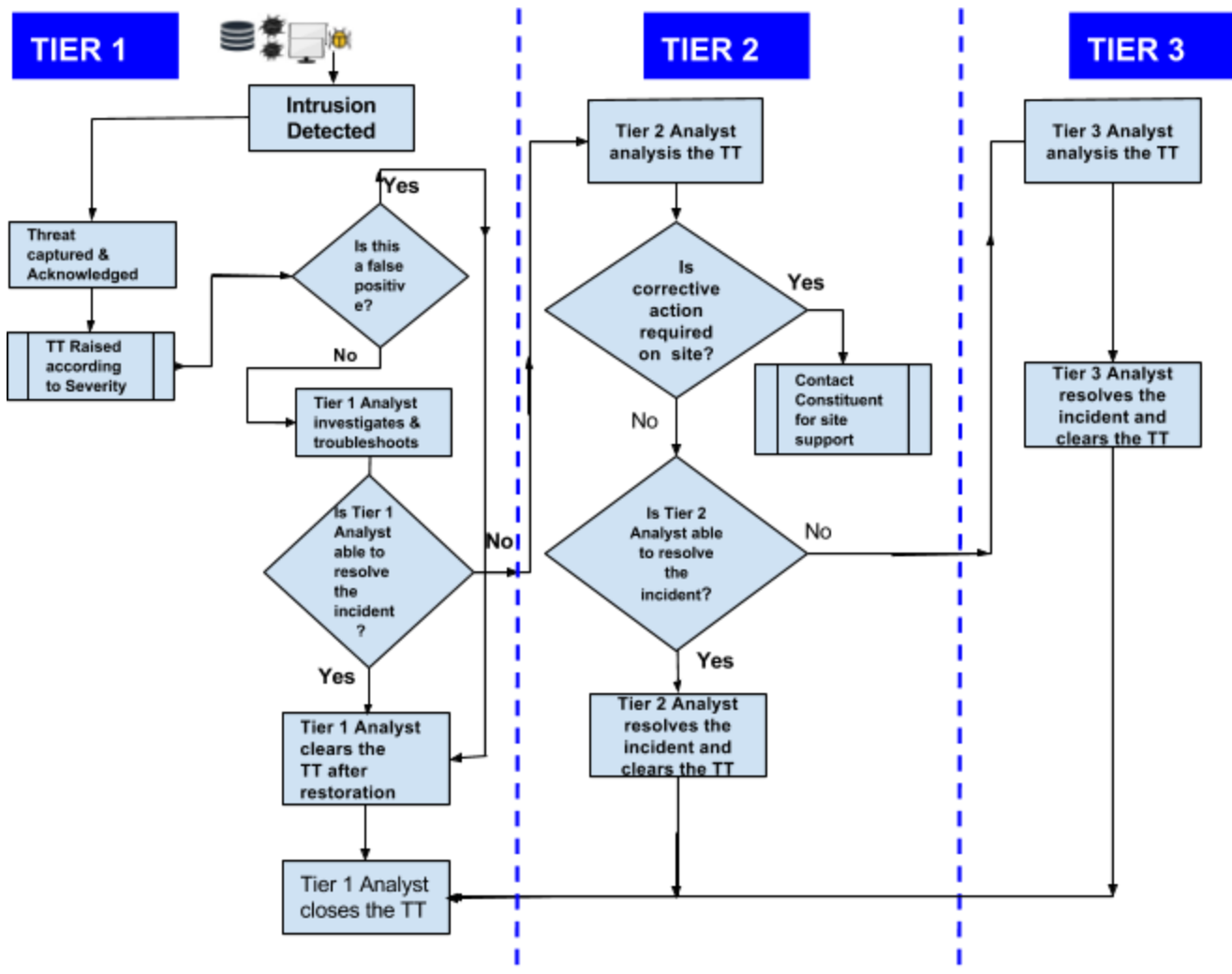
Device management provides a way to uniformly notify all applications and system features of changes that may affect their operation or access to resources. The system uses messages to notify applications of device changes and power changes. Applications and drivers can also define and use custom messages to enable notification of other types of events.

10. CYBER INTRUSION/ATTACK HANDLING PROCEDURE

The moment a detection is received or threat captured; CSOC Tier 1 Analyst raises incident ticket as per severity matrix and analyzes the Event/Incident for timely resolution. If unable to resolve the faults or the fault requires further intervention, then only should the ticket be forward to the next relevant Level/Stakeholders. It is expected that 80% ticket should be resolved at CSOC Tier 1 and only 20% or less should be forwarded to Tier 2 and Tier 3 (as the case may be).

For critical TT, CSOC Tier 1 will forward TT to CSOC Tier 2 with a voice call. CSOC Helpdesk / CSOC Tier 1 is responsible to send communications to the Clients affected or all stakeholders in case of critical TT raised.

| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |



11. FAULT LEVELS/PRIORITY DEFINITIONS

11.1. Incident Assignment

The primary intent is to ensure the system allows for the assignment of the ticket, handling of incident and handoff if the incident continues past the CSOC Analyst's normal work shift. Regardless of how the incident is assigned, the system must also provide a level of security. Incident tickets containing sensitive information may only be viewed and handled by those with prior approved access.

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

The incident priority level and prescribed timeline of the response must be followed as defined in the SLA. Priority assignment levels are not to be confused with incident and event severity. Priority assignments are task driven assignments to Analysts for review and action and interaction with the customer.

“Priority” is the level of response time identified when the incident ticket is created. It may be updated based on the discovered extent of the impact:

| PRIORITY | DESCRIPTION |
|----------|--|
| 1 | Multiple systems / devices are affected or compromised; a possible data breach has occurred: Respond within 10 minutes |
| 2 | Multiple devices / users are affected or compromised: Respond within 1 hour |
| 3 | A single device / user is affected or has been compromised: Respond within 8 hours |
| 4 | No impact; logging response: Respond within 12 hours |

Security Evaluation / Security Severity Clear and adequate descriptions and details regarding specific incident and event severity levels are required for all levels of the CSOC and its constituents. We will be using four severity levels in GCR CSOC:

| SEVERITY | DESCRIPTION |
|-----------------------|---|
| 1 SEVERE | Critical Impact or Compromise – Widespread outages causing a critical service disruption or publicly-displayed attack among honey pots |
| 2 HIGH | Major Impact or Compromise – High level performance disruption among honey pots with major effects which is potential for Severe damage to multiple customers |
| 3 ELEVATED | Minor intermittent incidents or alerts identified with a moderate to low level of disruption |
| 4 | Informational (no security impact) |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|----------------|--|
| GUARDED | |
|----------------|--|

11.2. Event Prioritisation

The events within the scope will be categorized into 4 priority levels based on defined criteria by the GCR CSOC Management. KPI values for high priority events are higher. The GCR CSOS Management shall put a system in place for effective prioritization as defined by the Constituent. The Employer will revise the priority level of cells and make necessary adjustments quarterly.

11.2.1. Priority 1 Events

Priority 1 (P1) events are Critical problems that severely affect the Employer's revenue, service levels, network capacity, traffic levels, performance systems, and maintenance capabilities. Multiple systems / devices are affected or compromised; a possible data breach has occurred. All P1 events require immediate corrective action, regardless of time of day or day of the week.

11.2.2. Priority 2 Events

Priority 2 (P2) events are incidents that have a serious impact on the system operation, maintenance, or administration. Multiple devices / users are affected or compromised. All P2 events require immediate attention. The urgency is less than that of a P1 event because of an impending effect on systems performance, end-users, operation, and revenue.

11.2.3. Priority 3 Events

Priority 3 (P3) events are system faults not viewed as P1 or P2 faults. P3 events neither significantly impair the normal functioning of the system nor significantly affect the service to end-users. Most cases, a single device / user is affected or has been compromised.

11.2.4. Priority 4 Events

Priority 4 (P4) events are those not included in P1, P2 or P3 events. No impact; logging response

11.3. Service Level Agreement

11.3.1. Incident Response, Restoration and Resolution Times

| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | Severe P1 | High P2 | Elevated P3 | Guarded P4 |
|---------------------------|-----------|-----------|-------------|------------|
| Response / Detection Time | <=10 Mins | <=30 Mins | <=60 Mins | <=4 Hrs |
| Restoration Time | <=2 Hrs | <=4 Hrs | <=8 Hrs | <=12 Hrs |
| Resolution Time | <=3 Hrs | <=6 Hrs | <=10 Hrs | <=12 Hrs |
| Update frequency | 30 Mins | 1 Hr | 2 Hrs | 4 Hrs |
| TARGET | >99% | >90% | >85% | >80% |

Table: Incident Management Metric Parameters

- **Response / Detection Time:** Time interval between incident occurrence and notification to the Clients/Stakeholders and the moment a TT is opened
- **Restoration Time:** Time interval between incident occurrence and notification to the Clients/Stakeholders and until a service is restored either via a workaround or permanent solution
- **Update frequency during restoration:** Time interval when update is expected to be provided to the Clients and Management
- **Resolution Time:** Time interval between incident occurrence and notification to the Clients/Stakeholders and until the underlying cause of the incident is determined and solved (or a solution proposed to MSIP Operations Assurance via a RCA document)

| | | | | |
|---|---------|--------------------|-----------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

12. KEY PERFORMANCE INDICATORS (KPIS) REPORTING

13. COMMUNICATION FLOW

13.1. Clients to CSOC

All communication to CSOC shall be through the CSOC official email address :(xxxxx@....com). In the cases of outages where very urgent support is required, this shall be done via phones.

13.2. CSOC to Clients

All communication from CSOC shall be through the CSOC official email address :(xxxxx@....com). In the cases of outages where very urgent support/information is required from Clients or 3rd Party, this shall be done via phones with the consent of the CSOC manager.

14. CONTACT DETAILS

14.1. CSOC Escalation Matrix

CSOC Escalation
Matrix.xls

14.2. CSOC Roster

CSOC Shift
Roster.xlsx

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

14.3. Clients Contact Details

Constituents Contact

12. DEFINITION AND ACRONYMS

| | |
|-------------------------|---|
| TTP | Tactics, Techniques, and Procedures |
| APT | Advanced Persistent Threat |
| CSOC | Cybersecurity Operations Center <i>(Alternative names include: Security Defense Center (SDC), Security Intelligence Center, Cybersecurity Center, Threat Defense Center, Security Intelligence and Operations Center (SIOC), Infrastructure Protection Center (IPC))</i> |
| CND | Computer Network Defense |
| CSIRT | Computer Security Incident Response Team |
| CIRT | Computer Incident Response Team |
| CSIRC | Computer Security Incident Response Capability |
| CERT | Computer Emergency Response Team |
| Constituency | Customers being provided services to by the CSOC |
| Event | Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. |
| Tier 1 Security Analyst | Tier 1 CSOC Analyst supports a 24x7x365 Security Operations Center and monitors security tools, assesses threats, and risks involving client infrastructure, |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|--------------------------------|---|
| | and provides first tier response to security incidents for managed services customers. |
| Tier 2 Security Analyst | Reviews trouble tickets generated by Tier 1 Analyst(s). Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack. Reviews and collects asset data (configurations, running processes, etc.) on these systems for further investigation. Determines and directs remediation and recovery efforts. |
| Incident | An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies. |
| MIN | Major Incident Notification (Time interval between event/incident occurrence and notification to the Constituents and major stakeholders) |
| NOC | Network Operations Center |
| SIEM | Security Information and Event Management |
| OODA Loop | Observe, Orient, Decide, and Act Loop |
| TT | Incident Ticket |
| OSS | Open Source Software |
| RAT | Remote Access Trojan |
| EDR | Endpoint Detection and Response |
| CCIRC | Canadian Cyber Incident Response Centre (CCIRC), which acts as Canada's national cyber emergency operations centre and supplies a variety of threat reports |
| CSE | Communications Security Establishment (CSE), which is the government's lead technical cyber agency. They monitor and actively defend federal government systems and identify, prepare for, and respond to sophisticated cyber threats. |
| Canadian Cyber Threat Exchange | The (CCTX) is a private sector initiative that is a cross-sector, not-for-profit, membership-funded organization that was launched in December 2015 and became operational in February 2017. The Board of Directors is comprised of senior private sector members and supported by government and academic |

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

| | |
|-------|--|
| | advisors. Membership in the CCTX is available to all privately-owned Canadian businesses and multinational organizations legally registered to conduct business in Canada. The CCTX, through the CCTX Data Exchange, provides a current, focused view of cyber events directly impacting Canadian business along with mitigation options and tools to combat or nullify identified threats. By aggregating threat, vulnerability, and risk inputs and applying analysis to convert this raw data into pertinent, timely and actionable information, the CCTX adds value which it shares with its participants. |
| CREST | Centre for Research and Evidence on Security Threats |
| CAIDA | Center for Applied Internet Data Analysis |
| PII | Personally Identifiable Information |

14. REFERENCES

- Carder, J.: How to build a SOC with limited resources-Your Guide to Detecting and Responding to Threats Fast—Even if You Don't Have a 24x7 SOC

[http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/\\$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf](http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf)

- EY, 2014: Security Operations Centers: helping you get ahead of Cybercrime

[http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/\\$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf](http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf)

- How to build a Security Operations Center on Budget, www.alienvault.com

http://learn.alienvault.com/c/security-operations-?utm_internal=soc-irlookbook&x=5v9G6V&xs=917

- Kadivar, M. 2014: Cyber-Attack Attributes. Technology Innovation Management Review, 4(11): 22-27. <http://timreview.ca/article/846>
- SANS 2017: Trainings <https://www.sans.org/find-training/index/12392295/search/#results>

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

- Ajzen, I.: From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl and J. Beckmann, editors, Action Control: From Cognition to Behavior, pages 11–39. Springer Berlin Heidelberg, Berlin, Heidelberg, Sept. 1985

<http://www.duluth.umn.edu/~kgilbert/educ5165-731/Readings/Theory%20of%20Planned%20Behavior-%20Ajzen.pdf>
- Sundaramurthy, S.C et al. 2015: A Human Capital Model for Mitigating Security Analyst Burnout

<https://www.usenix.org/system/files/conference/soups2015/soups15-paper-sundaramurthy.pdf>
- Martins, G. 2015: Here's What The US Has To Do To Prevent Massive Cyberattacks

<http://www.businessinsider.com/what-we-have-to-do-to-stop-cyberattacks-2015-1>
- Lohrmann, D. 2016: Idea to retire: Cybersecurity kills innovation

<https://www.brookings.edu/blog/techtank/2016/03/30/idea-to-retire-cybersecurity-kills-innovation/>
- Solarwinds, 2012: How to choose the right SIEM

<https://www.slideshare.net/SolarWinds/choosing-the-right-siem-solution>
- National Institute of Standards and Technology. 2012. Security and Privacy Controls for Federal Information Systems and Organizations. April.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- Building a SOC
<https://www.splunk.com/pdfs/technical-briefs/building-a-soc-with-splunk-tech-brief.pdf>
- Jahankhani, H. et al. 2014: Cyber Crime Classification And Characteristics

https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics_Ch12.pdf
- Gordon, S. & Ford, R. 2016: On the definition and classification of cybercrime

<https://link.springer.com/content/pdf/10.1007/s11416-006-0015-z.pdf>
- Sommer, P. & Brown, I. 2011: Reducing Systemic Cybersecurity Risk

| | | | | |
|--|---------|---------------------------|------------------|-----------|
| Prepared (also subject responsible if other) Adefemi Debo-Omidokun | | No | | |
| Approved Brian Hurley | Checked | Date 2017-11-08 | Rev V1 | Reference |

<https://www.oecd.org/gov/risk/46889922.pdf>