Potential Security Event Handling Guide

Purpose

This document establishes guidelines, procedures, checklists, and training requirements for Corporation staff in regard to handling potential security events. The contents of this document should be used as a reference by Corporation staff during potential security event Discovery, Escalation, Response, and Lessons Learned. Within this document are the necessary procedures, technical processes, techniques, checklists, and forms to be utilized.

How to Use

Non Security Team Members

The only sections of this document that are relevant to your daily activities are Discovery and Escalation. Familiarize yourself with the principles established within that section to be able to properly discover and escalate a potential security event.

Security Team Members

This entire document should be thoroughly understood and followed during potential security event handling. The procedures in the Response section are most critical for your activities during potential security event handling.

Read Before Proceed – Important Notices

- Do NOT say the words "incident" or "breach".
    - Always refer to events as "potential security events".
- When escalating, a verbal confirmation is required from a security team member.
    - Do NOT add to SOC board and send a message, that is unacceptable for escalating.

Potential Security Event Handling Guide

Table of Contents

Potential Security Event Handling Guide

Discovery (For All Personnel)

Potential security event discovery is the first step, it identifies that a security policy has been potentially violated. This section will review guidelines for declaring that a potential security event has been discovered as well as scenarios to demonstrate.

When to consider escalating a security event

Throughout daily operations the staff of Corporation interacts with numerous systems and users. Each system and user have a set of accepted policies, whether documented or assumed. For example, just because there is no formal documented Acceptable Use policy for a client's computer, it is universally assumed that it is unacceptable for a user to install ransomware on their device. In the absence of formally established policies a basic level of security should always be assumed during evaluation in the potential security event discovery phase. Rely on your technical expertise and experience when evaluating indicators.

The following examples are not all inclusive but are attempting to provide a guideline of how to think when considering potential security event declaration:

Examples

- When interacting with systems and users a violation of policy might be a login attempt from an unknown source, meaning that you've identified a potential threat actor attempting to gain access to a system.
- A phishing email is received by a client and a response is sent back or a link is clicked. In other words, any action that is taken other than just deleting the email might be an potential security event.
- An alert is received from a system, vendor, or user that claims unauthorized access attempts or unauthorized data access.

Sources to Identify Potential Security Events

Alerts

- IDP products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDP products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDP software often produces false positives—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDP alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
- Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data.
- Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.

- File integrity checking software can detect changes made to important files during potential security events. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
- Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current potential security event activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other potential security event response teams.

Logs

- Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an potential security event occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate a potential security event.
- Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
- A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.

Publicly Available Information

- Keeping up with new vulnerabilities and exploits can prevent some potential security events from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Organizations such as US-CERT and CERT/CC periodically provide threat update information through briefings, web postings, and mailing lists.

People

- Users, system administrators, network administrators, security staff, and others from within the organization may report signs of potential security events. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during potential security event analysis, particularly when conflicting data is discovered.
- Reports of potential security events that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is

attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other potential security event response teams also may report potential security events. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Escalation (For All Personnel)

At this point, a potential security event has been discovered and you need to inform the proper team members through using appropriate procedure. Proper action and escalation are required to ensure all possible risk is mitigated throughout the entirety of the potential security event handling procedure. The following procedures are not all inclusive so the final procedure acts as a catch-all to ensure the Security Team receives the handoff and is activated.

- If above identified security event/s is/are login failure/s discovered by no successful logins from unauthorized threat actors.
    - Follow Catch-All notification procedure.
- If above identified security event/s is/are login/s to user account/s from unauthorized threat actor
    - Lock the associated account.
    - Follow Catch-All notification procedure.
- If above identified security event/s is/are computer system/s, server/s, IoT device/s, or any physical compute device/s is affected.
    - Isolate the device using SentinelOne
    - Disconnect network cable.
    - Disable WiFi.
        - At this point there should be no method for this device to communicate outside of itself.
    - Follow Catch-All notification procedure.
- Catch-All Notification Procedure
    - Inform security team by phone at ***-***-****
        - An answer is required and verbal acceptance of the security event handoff.
    - If you cannot reach the security team by phone, call Person One at ***-***-****.
        - An answer is required and verbal acceptance of the security event handoff.

Response (For Security Team Personnel)

At this phase the Security Team is active and following along the contents of this document. Follow along the checklist to ensure proper handling per Corporation approved procedures. Only initiate this plan once you've validated that an incident is real and not a false positive.

Conditional Statement

If event is NOT related to a full security client;
then create a clear recommendation of how to proceed and notify CSM via Teams. A reply from the client's CSM within Teams constitutes a transfer of responsibility. Document time of transfer to CSM and

Potential Security Event Handling Guide

document time of returned guidance if client chose to proceed with an investigation and continue the steps below. Notify Person One that an escalation to a CSM for a realized event has occurred.

ELSE

If event is related to a full security client;
then proceed with the steps below.

1. Start a Master Station Log recording timeline of each event, such as:
    a. Indicators of Compromise.
    b. Actions Taken.
    c. Comments from Incident Handlers.
    d. Next steps to be taken.
        i. Be sure to put your initials at the end of each event recorded.
2. Synchronize system clocks.
    a. This is important for correlation of events.

Preparation

1. Identify the Incident Response Manager.
    a. A secondary in command, Incident Response Deputy, should be appointed if available.
        i. Approved Manager and Deputy List.
2. Identify the Customer Success customer communications coordinator.
    a. Inform them that an investigation has begun and to stand-by for updates.
3. Inform Corporation teams of an ongoing investigation and to stand down.
    a. Infrastructure
        i. Inform them that an investigation has begun and to stand-by for updates.
    b. Customer Support
        i. Inform them that an investigation has begun and to stand-by for updates.
4. Prepare appropriate communication plans.
    a. Clients
    b. Vendors
    c. Public
        i. Where applicable, authorized personnel should prepare to advise client in any public communication.
5. Remember Always
    a. DO NOT SAY “Breach”.
        i. Only authorized Corporation personnel may escalate the incident further.
            1. Person One
            2. Person Two

Detection & Analysis

1. Start screen recordings, screenshots, and chain of custody.
2. Collect all logs and relevant artifacts.
    a. Start Redline collector and let it run while investigating manually.
        i. Redline collector can be found in Resource at:
            1. https://Resource/

3. Identify all vulnerabilities that were exploited.
4. Correlate all events chronologically to create an accurate and complete storyline.
5. Identify any lack of logs that prohibits completion of a complete storyline.
6. Prioritize the incident based on relevant factors.
    a. Functional Impact
    b. Information Impact
    c. Recoverability Effort
7. Communicate updates to all personnel in the Preparation phase.
    a. This is an official moment where communications externally begin, be ready with a certainty level of your compiled storyline.

Containment – Eradication – Recovery

1. Acquire, preserve, secure, and document evidence.
2. Contain the incident.
3. Eradicate the incident.
    a. Remediate all vulnerabilities that were exploited.
    b. Remove malware, inappropriate material, reset accounts, and every other related component.
4. Recover from the incident.
    a. Return all affected systems to an operationally ready state.
    b. Confirm that the affected systems are functioning normally.
    c. If possible and available, implement additional monitoring to look for future related activity.

Post-Incident Activity

1. Create a follow-up report.
2. Hold a lessons learned meeting.
    a. Mandatory for major incidents
    b. Optional otherwise

Lessons Learned (For Security Team Personnel)

At this phase the Security Team has concluded all necessary Incident Response procedures and both the Security and Infrastructure teams have declared the systems and users fully and safely operational. A meeting should be held, when appropriate and where available, to analyze past events to better decide future actions. Involve all team members that would potentially have relevant information, possible improvements, relevant stakeholders, and those that would have future actions.