TCWGlobal's Incident Management Process

Policy Area	Security Operations Team
Approved Date	6/10/2024
Approved By	Tom Kucharski, Erica Ostberg, Casey Prentice, Jesus Gomez
Effective Date	6/10/2024
Current Version	V1.5

Policy History			
Version	Date	Description	Approved by
V. 1.5	6/10/2024	Reviewed to be consistent with updates to IRP	Tom Kucharski, Erica Ostberg, Casey Prentice, Jesus Gomez
V 1.4	8/28/2023	Reviewed to be consistent with updates to IRP	Zack Abdou, Tom Kucharski, Erica Ostberg, Leslie Cruz, Jaime Nguyen
V 1.3	2/6/2023	Reviewed to be consistent with updates to IRP	Erica Ostberg, Zach Abdou, Tom Kucharski
V 1.2	2/4/2022	Reviewed to be consistent with updates to IRP	Erica Ostberg
V1.1	10/1/2021	Updated with new company logo and name	Robyn Ise
V1.0	2/14/2021	Version 1.0	Robyn Ise

Contents

Purpose: 2

Evaluation of Security Events 2

Events versus Incidents 2

Report 3

Assessment/Investigation 3

Incident Categorization 3

Incident Scope 5

Incident Impact 5

Escalation Criteria – when to enact Incident Response Plan 7

TCWGlobal's Incident Management Process

Purpose:

This Incident Management Process documentation is not a policy, rather, it is a set of protocols for reporting, evaluating, logging and managing events.

Evaluation of Security Events

When an employee or external party notices a suspicious anomaly in data, a system, or the network, or a system alert generates an event; IT Security Operations and/or SN AppSec/DevOps must perform an initial investigation and verification of the event.

Events versus Incidents

Events are observed changes in normal behavior of the system, environment, process, workflow or personnel.
Incidents are events that indicate a possible compromise of security or non- compliance with policy that negatively impacts (or may negatively impact) the organization.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security ***incidents***, which may include any or all of the following (also referenced in the Security Incident Response Plan):

- Email or phone notification from an intrusion detection tool
- Suspicious entries in system or network accounting, or logs
- Discrepancies between logs
- Repetitive unsuccessful logon attempts within a short time interval
- Unexplained new user accounts
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial/disruption of service or inability of one or more users to login to an account
- System crashes
- Poor system performance of dedicated servers
- Operation of a program or sniffer device used to capture network traffic. Unusual time of usage (e.g. users login during unusual times)
- Unusual system resource consumption. (High CPU usage)
- Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
- Unusual usage patterns (e.g. a user account associated with a user in finance is being used to login to an HR database).
- Unauthorized changes to user permission or access

Although there is no single symptom to conclusively prove that a security incident has taken place, observing one or more of these symptoms should prompt an observer to investigate more closely. Do not spend too much time with the initial identification of an incident as this will be further qualified in the containment phase.

TCWGlobal's Incident Management Process

NOTE: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later. ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.

Report

If it has been determined that an event is in fact a security incident, as per the Incident Response Plan, the incident must be reported ASAP to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT). The member of the SIRT receiving the report will advise the Incident Response Lead of the incident.

Assessment/Investigation

Once a potential incident has been identified, part or all of the SIRT may be activated by the Incident Response Lead (IRL) to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. The SIRT should work quickly to analyze and validate each incident, following the process outlined below, and documenting each step taken.

The Incident Response Lead will assign a team member to be "Recorder" to begin formal documentation of the incident. The below determined categorization, scope, and impact must be included with documentation of the incident.

Incident Categorization

The MITRE ATT&CK Framework is a globally-accessible knowledge base of adversary tactics and techniques and should be leveraged when categorizing security incidents. While many techniques may be used in a single incident, select the method that was primarily leveraged by the adversary. Some examples of this may be:

- Phishing
- Unsecured Credentials
- Network Sniffing
- Man-in-the-Middle
- Data Destruction
- OS Credential Dumping
- Event Triggered Execution
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Hijacking
- Defacement
- File and Directory Permission Modification

It should be noted that the MITRE ATT&CK Framework may not address some situations, specifically those without malicious intent, that trigger the Incident Response Management Plan. The following exceptions may require categories of their own as dictated by the organization's Risk Management entities or policies:

- Data loss
- Administrative errors
- Unsecured Credentials
- Data Destruction
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Misuse (non-malicious)

Incident Scope

Determining the scope will help the SIRT understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

- How many systems are affected by this incident?
- Is Confidential or Protected information involved?
- What is/was the entry point for the incident (e.g. Internet, network, physical)?
- What is the potential damage caused by the incident?
- What is the estimated time to recover from the incident?
- What resources are required to manage the situation?
- How could the assessment be performed most effectively?

Incident Impact

Once the categorization and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken in order to provide a resolution; however, in all instances an incident report must be completed and reviewed by the SIRT. **Functional** and **informational** impacts are defined with initial response activity below:

Functional Impact	Definition	SIRT Response
None	No effect to the organization's ability to provide all services to all users.	Create ticket (may be autocreated) and assign for remediation.
Limited	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.	Create ticket and assign for remediation, notify the CTO/CISO
Moderate	The organization has lost the ability to provide a critical service to a subset of system users.	Initiate full SIRT, involve the CTO/CISO and Team One
Critical	The organization is no longer able to provide some critical services to any user.	Initiate full SIRT, involve the CTO/CISO and Team One Consider activation of the Disaster Recovery

Informational Impact	Definition	SIRT Response
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	No action required
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate course of action.
Moderate	Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the CTO/CISO. CTO/CISO will work with management, legal, and data owners to determine appropriate course of action.
Critical	Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the CTO/CISO. CTO/CISO will work with legal to determine whether reportable, and the appropriate notification requirements.

Incidents classified as Sev. 1, 2, 3 must be logged in the Technology Services Security RCA Log.

The Response Level table below will help determine the severity of the incident and urgency of response activities.

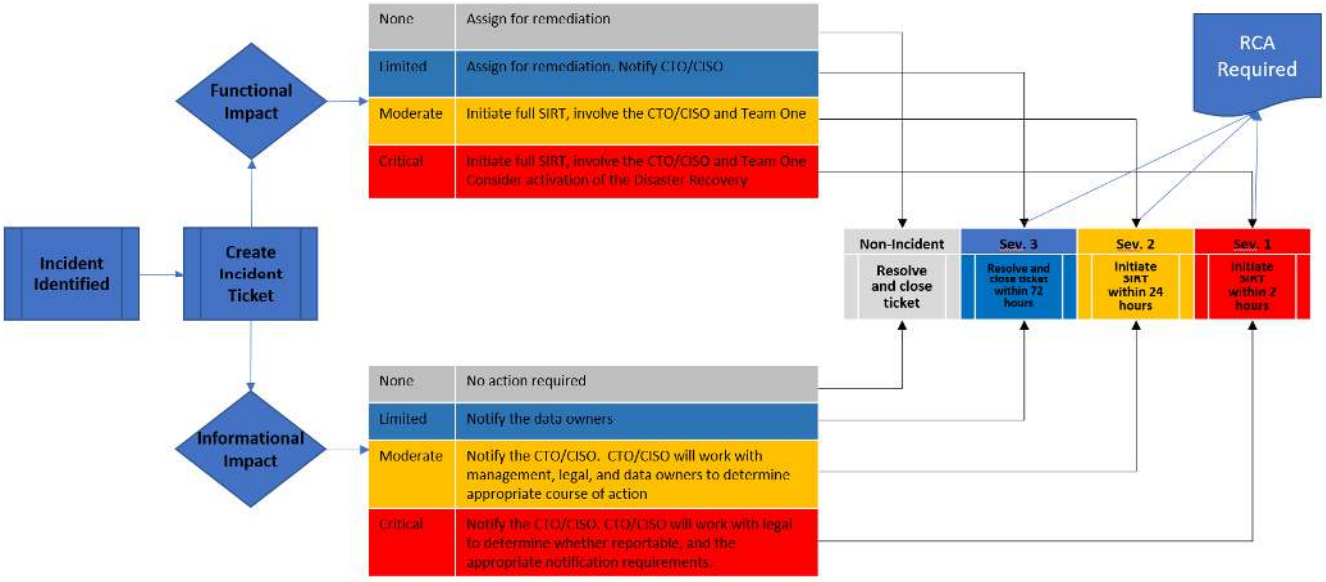
Response Level Classification		**Informational Impact**			
		None	**Limited**	**Moderate**	**Critical**
Functional Impact	**None**	N/A	Sev. 3	Sev. 2	Sev. 1
	Limited	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	Moderate	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	Critical	Sev. 1	Sev. 1	Sev. 1	Sev. 1

The severity level should be used to determine how rapidly initial response activities should occur.

Severity Level	SLA
Sev. 3	Within 72 hours
Sev. 2	Within 24 hours
Sev. 1	Within 2 hours

Escalation Criteria – when to enact Incident Response Plan

The following chart will help identify remediation and escalation steps for an incident:



If it is determined that SIRT must be activated, the individual or team should reference the Security Incident Response Plan for Roles and Responsibilities and plan steps.