Contents

CYBERSECURITY INCIDENT RESPONSE PLAN

SYNOPSIS

A cybersecurity incident response plan (IRP) to help responders with the *tactical aspects* of incident response.

SCOPE

This document applies to all individuals (Personnel) responsible or involved with cybersecurity incident response activities. Personnel shall be informed of this document by the organization's Information Security Office or Officer(s) (ISO).

This document is designated as Traffic Light Protocol (TLP): AMBER. Recipients may share TLP: AMBER information with members of their organization who need to know, and only widely as necessary to act on that information.

This document contains confidential and privileged material. Any interception, review, retransmission, dissemination or other use of or taking any action upon this information by persons or entities other than the intended recipient(s) is prohibited by law and may subject them to criminal or civil liability. This document contains material that may have been commissioned by counsel in anticipation of litigation. It should be treated as confidential to avoid waiver of the attorney/client privilege, the work-product privilege, or another applicable privilege. It was prepared for the sole use of the named recipient, and must not be relied upon by any third party.

This document is a deliverable that meets or exceeds a standard of reasonable cybersecurity practices.

This document meets or exceeds the following standards, compliance and/or regulatory requirements:

Standards:

1. NIST Special Publication 800-61
2. NIST Cybersecurity Framework (CSF)

Compliance:

1. ISO 27001 – A.16
2. PCI DSS 3 – 10, 12.9

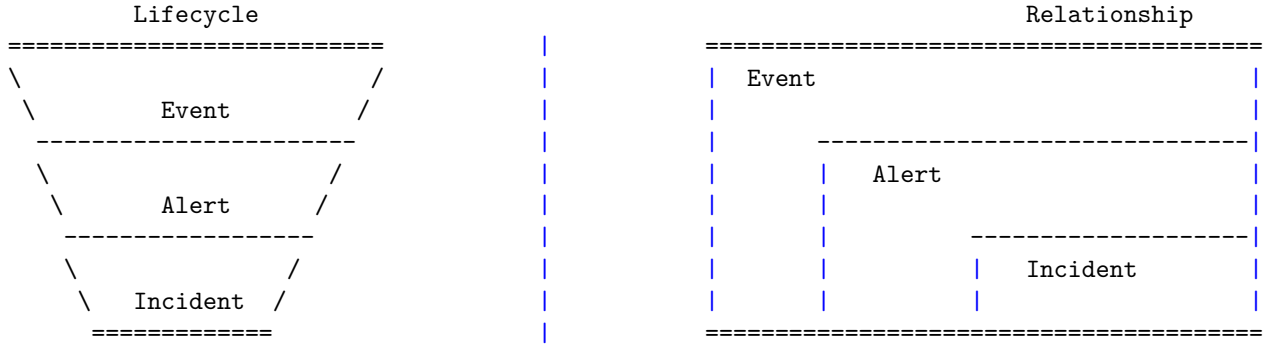
Regulation:

1. EU GDPR – Article 33, 34
2. CA CCPA - Standard of Reasonable Cybersecurity - Incident Response Plan

DESCRIPTION

Prologue

Taxonomy



Cybersecurity

The words cybersecurity and security are synonymous and used interchangeably herein.

Cybersecurity is the state of being protected against the violation of computer security policies, acceptable use policies, or standard security practices, or the measures taken to achieve this.

Asset

The words asset, information asset, information technology resource, and other processing activities are synonymous and used interchangeably herein.

Event

An event is an observable occurrence in a digital ecosystem or computer network. Event examples include a login, a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Alert

The words alert and alarm are synonymous and used interchangeably herein.

An alert is an event having a security context usually generated from threat detection assets or treat hunting routines. Alerts may be the result of a negative consequence and generally require subsequent inspection. Examples of alerts include system crashes, unauthorized use of system privileges, unauthorized access to sensitive data, execution of malware, and destruction of data.

Incident

The word incident and the term event of critical interest are synonymous and used interchangeably herein.

An event of critical interest is an event or alert that signifies a violation, or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that requires critical triage and a more in-depth investigation known as ***incident response***.

During disciplined cybersecurity operations, including investigating and analyzing alerts, it is common for information security professionals to label the resulting analysis in terms of risk of compromise. An event of critical interest is an analysis that results in a declaration of real or imminent danger and significant risk of asset compromise or confirmation thereof. Take two classes of typical cybersecurity events: "Potentially Unwanted Program" and "Ransomware." The latter, Ransomware, represents an event of critical interest because its progression through the environment represents real and imminent danger and could result in a significant risk of compromise to critical assets.

Instruction

Implementers of this IRP use a **PICERL** model as guidance for organizing courses of action (COA):

1. Preparation
2. Idenification
3. Containment
4. Eradication
5. Recovery
6. Lessons / Opportunities For Improvement

Implementers or this IRP uses an **OODA** loop as guidance for conducting COA:

1. Observe
2. Orient
3. Decide

4. Act

CONTAINMENT IS THE MOST IMPORTANT COA DURING INCIDENT RESPONSE

SEE https://github.com/guardsight/gsvsoc_mission-model

Preparation

Roles

1. ISO
    1. The Information Security Office or Officer(s) or designated representative(s) shall be responsible for ensuring the *strategic* effectiveness of this IRP.
2. CSIRT
    1. The Computer Security Incident Response Team or designated representative(s) shall be responsible for ensuring the *tactical* effectiveness of this IRP.

Risk Management

The ISO shall be responsible for establishing risk management strategies that meet or exceed a standard of reasonable cybersecurity practices. These activities protect information assets, controls, and processes against a violation of the organization's computer security policies or acceptable use policies. The ISO is responsible for establishing controls and processes aligned with the five (5) core functions of Cybersecurity Risk Management as defined by the NIST Cybersecurity Framework (CSF).

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Cybersecurity Technology Controls

The CSIRT shall routinely conduct inspections of the cybersecurity technology controls (cyber weapon assets) used to detect and or prevent incidents to ensure cyberweapon readiness. The CSIRT shall own the responsibility of remediating defects, disruptions, or degradation of cyber weaponry assets and security controls. The ISO shall routinely request from the CSIRT a report of the state of cyber weaponry assets and security controls readiness. The CSIRT shall promptly comply with an ISO request for a report of the state of cyber weaponry assets, and security controls readiness and maintain the provided report for no less than one (1) year.

Severity Ratings

This IRP uses the priority levels defined in the US National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System (CISS) as the model for rating the severity of an Information Security Incident. SEE NCCIC CISS Severity Rating Model

Severity rating levels shall be used to determine the necessary force and resource prioritization required to handle and respond to an incident. The CISRT is responsible for declaring the initial severity rating. The ISO is responsible confirming and adjusting security ratings that meet or exceed a High rating.

Tactics, Techniques & Procedures

The CSIRT and ISO shall use qualified Information Security Personnel, and cyber weapons, and security controls capable of defending and preventing adversaries from using specific tactics, techniques, and procedures as described by the MITRE ATT&CK Framework.

Log Retention

The ISO shall be responsible for ensuring that log data transmitted by assets is properly preserved, protected, and maintained for a period of one (1) year.

Alert Response & Threat Hunting

The CSIRT shall respond to alerts generated by cyber weapons and security controls. The CSIRT shall routinely patrol (threat hunt) and audit log data and assets for indicators of compromise.

Evidence Collection & Preservation

The CSIRT shall establish an electronic/virtual evidence locker to store and protect evidence collected during incident response. The CSIRT should maintain an electronic journal (manifest) of collection activities and their related evidence artifacts. The CSIRT shall maintain an electronic chain of custody ledger that includes the date, the evidence artifact, the transferrer, and the transferee for all activities involving the transfer of collected artifacts from the evidence locker to authorized recipients or electronic media. The ISO shall approve all transfers of evidence artifacts to authorized recipients or electronic media.

The ISO shall maintain and protect evidence locker artifacts collected during an Information Security Incident for one (1) year from the date of the initial detection. The ISO shall maintain and protect the Information Security Incident after-action incident report and any related communications for one (1) year from the date of the initial detection.

Restoring Operations

The ISO shall certify that assets impacted by a successful compromise are eligible for being restored to their normal operational state only after remediation activities have prevented the assets from further risk of intrusion.

After Action Report

The CSIRT shall produce an after-action report that provides the details of the incident. The CSIRT should produce content for the report iteratively during the response. The ISO shall approve all dissemination of the report.

SEE Mission Model Report

Coordination, Sharing & Notifications

Internal

The ISO shall be responsible for coordinating and sharing details of and incident to internal authorized Personnel, without undue delay on a need to know basis, when the ISO deems that sharing is beneficial to response activities and per the organization's data classification policies.

Individuals, Customers & Data Subject Notifications (EU GDPR 34)

The ISO shall be responsible for coordinating and delivering notifications, without undue delay, to individuals, customers, and data subjects for the purposes of complying with statutes, regulation, or ordinances if the ISO determines the incident is likely to result in an infringement of, or high risk to, the rights and freedoms of those individuals, customers, and data subjects that have been impacted by the compromised assets.

Controller & Supervisory Authority Notifications (EU GDPR 33)

The ISO shall be responsible for coordinating and delivering notifications, within seventy two (72) hours of identifying an incident, to the supervisory authority (when organization is acting as a controller) or the controller (when organization is acting as a processor) for the purposes of compliance with the EU GDPR regulation if the ISO determines the incident is likely to result in an infringement of, or high risk to, the rights and freedoms of those individuals, customers, and data subjects that have been impacted by the compromised assets and/or information technology resources.

US State Authority Notifications

The ISO shall be responsible for coordinating and delivering notifications, without undue delay, to various state authorities (SEE here and here) for the purposes of complying with statutes, regulation, or ordinances if the ISO determines the Information Security Incident is likely to result in an infringement of, or high risk to, the rights and freedoms of those individuals, customers, and data subjects that have been impacted by the compromised assets and/or information technology resources.

Law Enforcement

The ISO shall be responsible for notifying law enforcement to comply with statutes, regulation, or ordinances or threat actor prosecution if the ISO determines the incident meets the standard of a condition identified through discussions with law enforcement representatives provided such discussions have previously taken place. The ISO shall refrain from contacting multiple agencies when reporting an incident to avoid jurisdictional conflicts. The following is a list of law enforcement agencies:

1. Federal Bureau of Investigation
2. U.S. Secret Service
3. District Attorney
4. State Attorney General

Media

The ISO shall be responsible for coordinating and sharing the relevant details of an incident, without undue delay on a need to know basis, with the media when the ISO deems that sharing is beneficial to response activities and per the organization's data classification policies.

External Service Providers

The ISO shall be responsible for coordinating and sharing the relevant details of an incident, without undue delay on a need to know basis, with the organization's trusted 3rd party service providers when the ISO deems that sharing is beneficial to response activities and per the organization's data classification policies.

1. Cybersecurity-as-a-Service Providers
2. Incident Response Partners
3. Legal Counsel
4. Crisis Management Partners
5. Cybersecurity Insurance Broker

Response Practice

1. Use real world IOC-Negative scenarios as if they were IOC-Positive to train response personnel and gauge response effectiveness
2. Become Familiar With Breach Notification Laws
3. Security Breach Notification Laws

Identification

Assess & Rate

1. Breathe
2. Think "smooth is fast"
3. Inspect change logs to determine if activity is possibly the result of an authorized change
4. Review system baselines to determine if activity is possibly the result of expected behavior
5. Ask asset owners what they know in terms of Indicators Of Compromise (IOC) and record the results
    1. SEE Top Indicators of Compromise (TOP-IOC) below for hints
    2. SEE MITRE ATT&CK Framework for hints
6. Ask asset owners ***"Was there a loss of data?"*** and record the results
7. Ask asset owners ***"Was restricted data at risk?"*** and record the results
8. Assign a severity rating

1. SEE NCCIC CISS Severity Rating Model

Memorialize & Share

IMPORTANT - When possible encrypt communication - threat actors may be listening to the channel

1. Make notes of actions you took during the assessment phase
2. What you do, see, and hear will be used by investigators, after action reporting, and maintained for posterity purposes
3. Record times
4. Communicate using 24HR/military time (e.g. 0900, 1330, 1845)
5. Record atomic attributes
6. Record behavioral attributes
7. Make factual assertions backed by evidence
8. Peer review observations and assertions with experienced personnel
9. Mark email communication with "CONFIDENTIAL//ATTORNEY-CLIENT PRIVILEGE//TLP:AMBER" labels
10. Use encryption or an alternative band of communication if the material is extremely sensitive

Collect

IMPORTANT - Keep a system POWERED ON prior to the collection of volatile media (isolate the host from the network)

IMPORTANT - Keep a system POWERED ON reserve valuable evidence (isolate the host from the network)

1. Journal collection activities
2. Conduct log analysis
3. Conduct system forensics
    1. Use a DFIR checklist
    2. Acquire volatile media
    3. Acquire non-volatile media

Store

SEE NIST Special Publication 800-66

1. Follow a consistent evidence process that achieves the objective of provenance
2. Journal evidence activities
3. Establish an evidence locker
4. Preserve evidence

Contain

SEE Mission Model Containment

Think Inventory + 6 D's

1. Inventory
2. Detect
3. Deny
4. Disrupt
5. Degrade
6. Deceive
7. Destroy

Eradicate / Remediate

1. Inspect the asset to ensure the threat has been fully eradicated
2. Remediate all known vulnerabilities
3. Apply controls to prevent further intrusion

Recover / Restore

IMPORTANT - Restore only after remediation activities have prevented the assets from further risk of intrusion

1. Restore to a normal state
    1. Recovery point objective (RPO)
    2. Recovery time objective (RTO)

Lessons / Opportunities For Improvement (OFI)

1. Develop OFI as gaps are discovered during the response
2. Record the OFI in the after-action report

Produce After-Action Report

SEE Mission Model Report

1. Develop content for the report in an iterative manner as response activities are being conducted
2. Supply detailed and factual statements and artifacts
    1. Summary
    2. Timelines (attack & response sequences)
    3. Indicators of Compromise (IOC) (the nouns of the attack)
    4. Intrusion Kill Chain (IKC) (threat actors activity - bad guy verbs)
    5. Courses of Action (COA) (reponders activity - good guy verbs)
    6. Opportunities for Improvement (OFI) (lessons learned)
3. Disseminate the report

Notify External Entities

1. Individuals, Customers, & Data Subjects
2. Data Controllers
3. Supervisory Authorities
4. US State Authorities
5. Law Enforcement
6. Credit Reporting Agencies
7. The Media

Engage 3rd Party Service Providers

1. Cybersecurity-as-a-Service Providers
2. Incident Response Partners
3. Legal Counsel
4. Crisis Management Partners
5. Insurance Brokerage

EXAMPLES

TOP-IOC Annotation Statements

```
# IOC NEGATIVE
## TOP-IOC: Attack surface DOES NOT exist
## TOP-IOC: Attack surface vulnerability DOES NOT exist
## TOP-IOC: Mitigating controls DO EXIST and ARE currently protecting the asset
## TOP-IOC: Subsequent attack activity DOES NOT exist
## TOP-IOC: Corroboration from other assets DOES NOT exist
## TOP-IOC: NOT CONSISTENT with unusual egress network traffic
## TOP-IOC: NOT CONSISTENT with unusual lateral movement
## TOP-IOC: NOT CONSISTENT with login anomalies
## TOP-IOC: NOT CONSISTENT with suspicious domain controller activity
## TOP-IOC: NOT CONSISTENT with suspicious byte counts
```

```
# IOC POSITIVE
## TOP-IOC: Attack surface DOES exist
## TOP-IOC: Attack surface vulnerability DOES exist
## TOP-IOC: Mitigating controls DO NOT EXIST or ARE NOT currently protecting the asset
## TOP-IOC: Subsequent attack activity DOES exist
## TOP-IOC: Corroboration from other assets DOES NOT exist
## TOP-IOC: CONSISTENT with unusual egress network traffic
## TOP-IOC: CONSISTENT with unusual lateral movement
## TOP-IOC: CONSISTENT with login anomalies
## TOP-IOC: CONSISTENT with suspicious domain controller activity
## TOP-IOC: CONSISTENT with suspicious byte counts
```

NOTES

Threat Analysis Model

1. Analysts shall use a TAM similar to the TOP-IOC
2. Analysts shall annotate cases using one or more TOP-IOC annotation statements
3. All ticket annotation shall start with IOC-NEGATIVE -or- IOC-POSITIVE
4. Evidence that intelligence assets were searched and analyzed is required
5. Annotations should indicate the COA related to the specific activities conducted

TOP Indicators Of Compromise (TOP-IOC)

1. Attack Surface Vulnerability Exists
2. Corroboration From Multiple Intelligence Assets
3. Unusual Egress Network Traffic
4. Unusual Ingress Network Traffic
5. Anomalies In Privileged User Account Activity
6. Geographical Irregularities
7. Log-In Anomalies
8. Volume Increase For Database Reads
9. HTML Response Size Anomalies
10. Large Numbers Of Requests For The Same File
11. Mismatched Port-Application Traffic
12. Suspicious Registry Or System File Changes
13. DNS Request Anomalies

14. Unexpected Patching Of Systems
15. Mobile Device Profile Changes
16. Data In The Wrong Places
17. Unusual Lateral Movement
18. Velocity Increase For Share / Mount Activity
19. Time Based Anomalies
20. Suspicious Byte Counts
21. Suspicious Domain Controller Activity
22. Subsequent Activity By Attacker Address / GEO
23. HTML Response Code Success

Top Insider Threat Indicators of Compromise

1. Logons To New Or Unusual Systems
2. New Or Unusual Logon Session Types
3. Unusual Time Of Day Activity
4. Unusual GEO
5. Unlikely Velocity
6. Shared Account Usage
7. Privileged Account Usage
8. Unusual Program Execution
9. New Program Execution
10. High Volume File Access
11. Unusual File Access Patterns
12. Cloud-based File Sharing Uploads
13. New IP Address Association
14. Bad Reputation Address Association
15. Unusual DNS Queries
16. Bandwidth Usage
17. Unusual Or Suspicious Application Usage
18. Dark Outbound Network Connections
19. Known Command And Control Connections
20. Building Entry And Exits
21. High Volume Printing Activity
22. Unusual Time Period Printing
23. Endpoint Indicators Of Compromise
24. Sensitive Table Access
25. Sensitive Data Movement Combined With Other Risk Indicators

Protecting Against Ransomware

1. Prioritize software updates for internet facing systems and systems having access to the internet
2. Practice least privilege principles including role based access controls and access limitations
3. Implement end point detection / host based intrusion technologies
4. Maintain backups of mission critical data
5. Educate the user community
6. Create a response / MISSION plan and assign a strike force to execute that plan when it becomes necessary

Protecting Against Phishing

1. Conduct security awareness training
2. Conduct phishing simulation tests
3. Deploy Application Whitelisting (AWL)
4. Deploy Endpoint Detection and Response (EDR) technology
5. Inspect outbound URLs

6. Ensure user accounts do not execute with elevated (admin) privileges
7. Use inbound email sandboxing
8. Deploy packet capture inspection technology with decryption capability
9. Deploy HTTPS inspection technology that validates certificate chains

Top Observations For Network and Packet Analysis

1. Known Signatures
2. Reputation
3. IP Addresses
4. Domains
5. DNS Queries
6. DLP Indicators
7. Anomalous Traffic Patterns
8. Protocols
9. Inconsistent Protocols
10. Malformed Protocols
11. Masquerading Protocols
12. Prohibited Protocols

Top Indicators Of A Suspicious Domain

1. Domain registered date is recent
2. Domain registrant is anonymous or non-reputable
3. Domain shares similar characteristics with prior known bad
4. Domain has a suspicious email infrastructure
5. Domain has a suspicious website infrastructure
6. Domain has a disreputable history
7. Domain has suspicious IP addresses / DNS data

Top Azure & Office 365 IOCs

1. Privileged account logon from foreign address
2. Creation of accounts in Azure AD
3. Traffic restriction loosened on Virtual Network
4. Storage account accessed via stolen key from foreign address
5. Subscription Administrator added
6. Windows level intrusion of VM
7. High priority target's mailbox is accessed

SEE ALSO

1. https://github.com/guardsight/gsvsoc_mission-model
2. https://www.nist.gov/cyberframework
3. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
4. https://nvd.nist.gov/800-53/Rev4/control/IR-8
5. https://nvd.nist.gov/800-53/Rev4/family/INCIDENT%20RESPONSE
6. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
7. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System
8. https://www.eugdpr.org/
9. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
10. https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf
11. https://attack.mitre.org

12. https://zeltser.com/cheat-sheets
