IR Plan, Playbook and Policy

Week 6 day 4

Submitted by: NAVNEET KAUR

Executive summary: In this project I'm creating incident response plan (IR plan), playbook and policies for the Canadian tire cooperation where I elaborate seven steps of playbook and developing five policies that run the playbook which defines the relationship between policies and procedure(how thing are actually done in an organization).

Case study Canadian Tire Corporation and Stakeholders

Playbook for incident- UNAUTHORIZED ACCESS

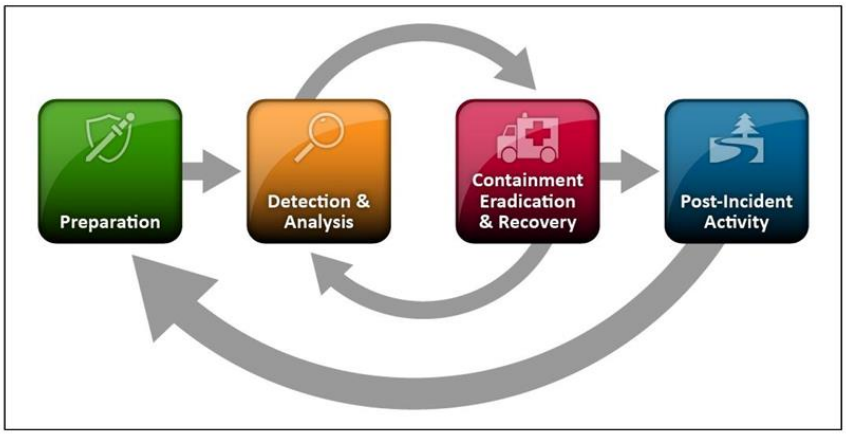
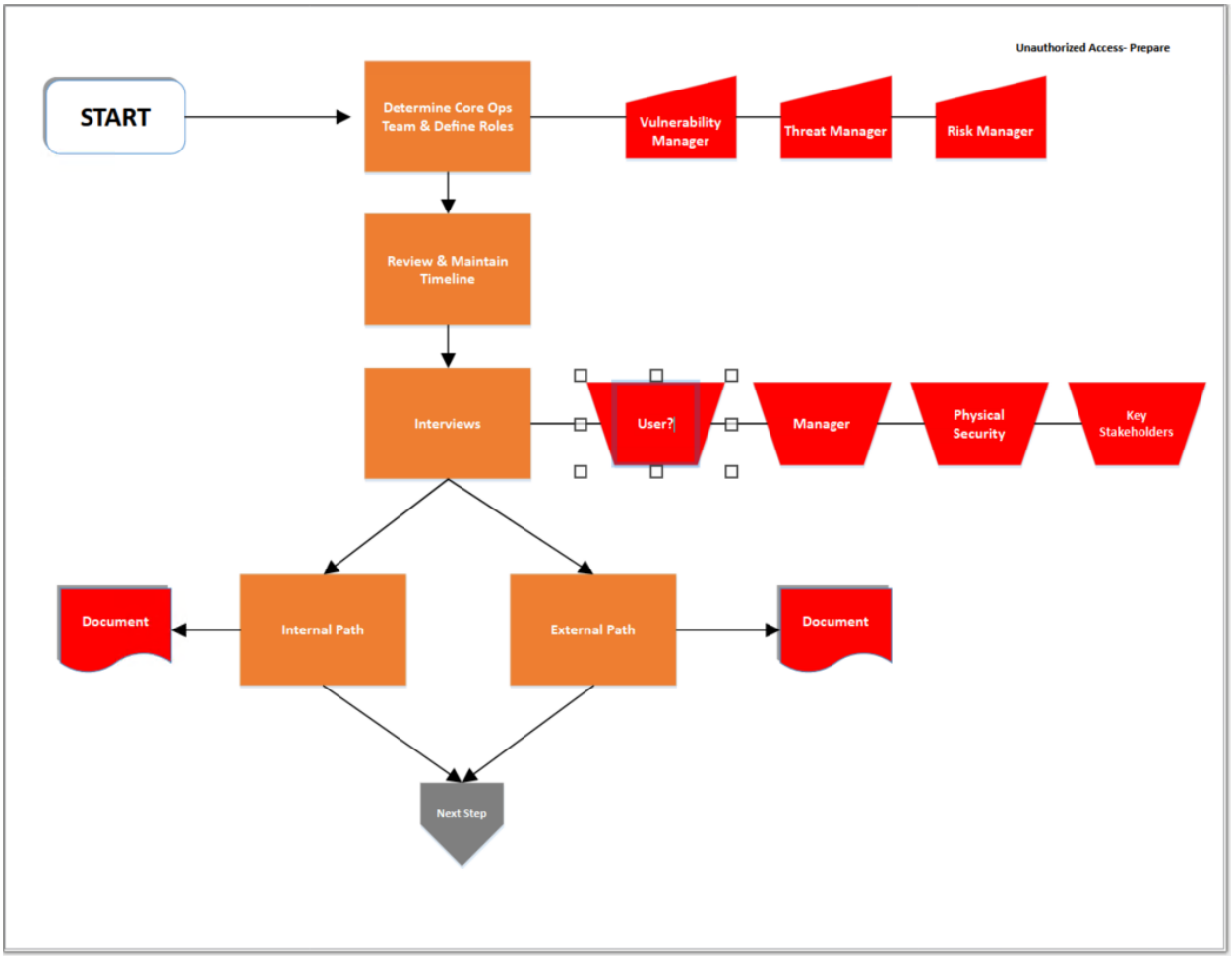
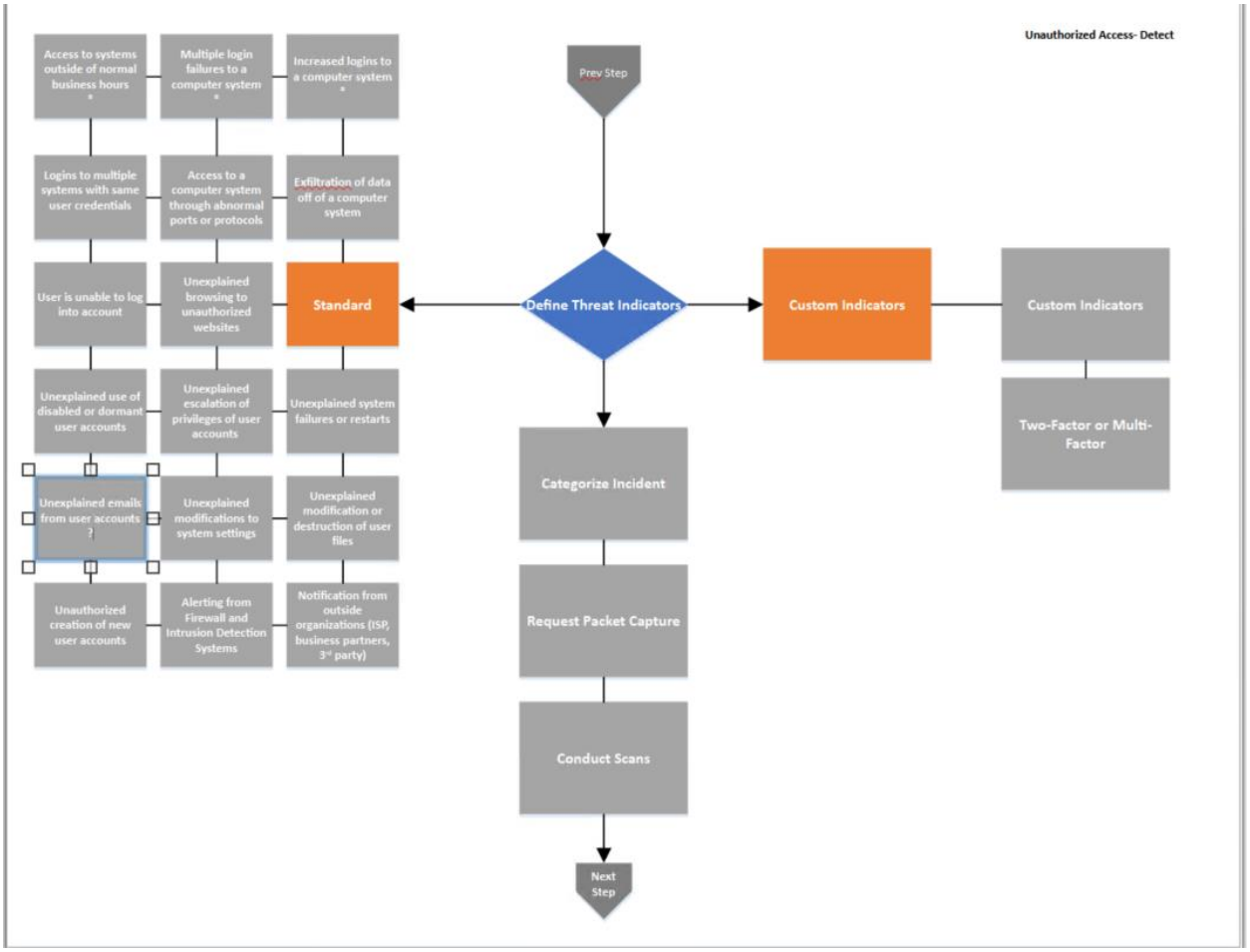


Figure 3-1. Incident Response Life Cycle

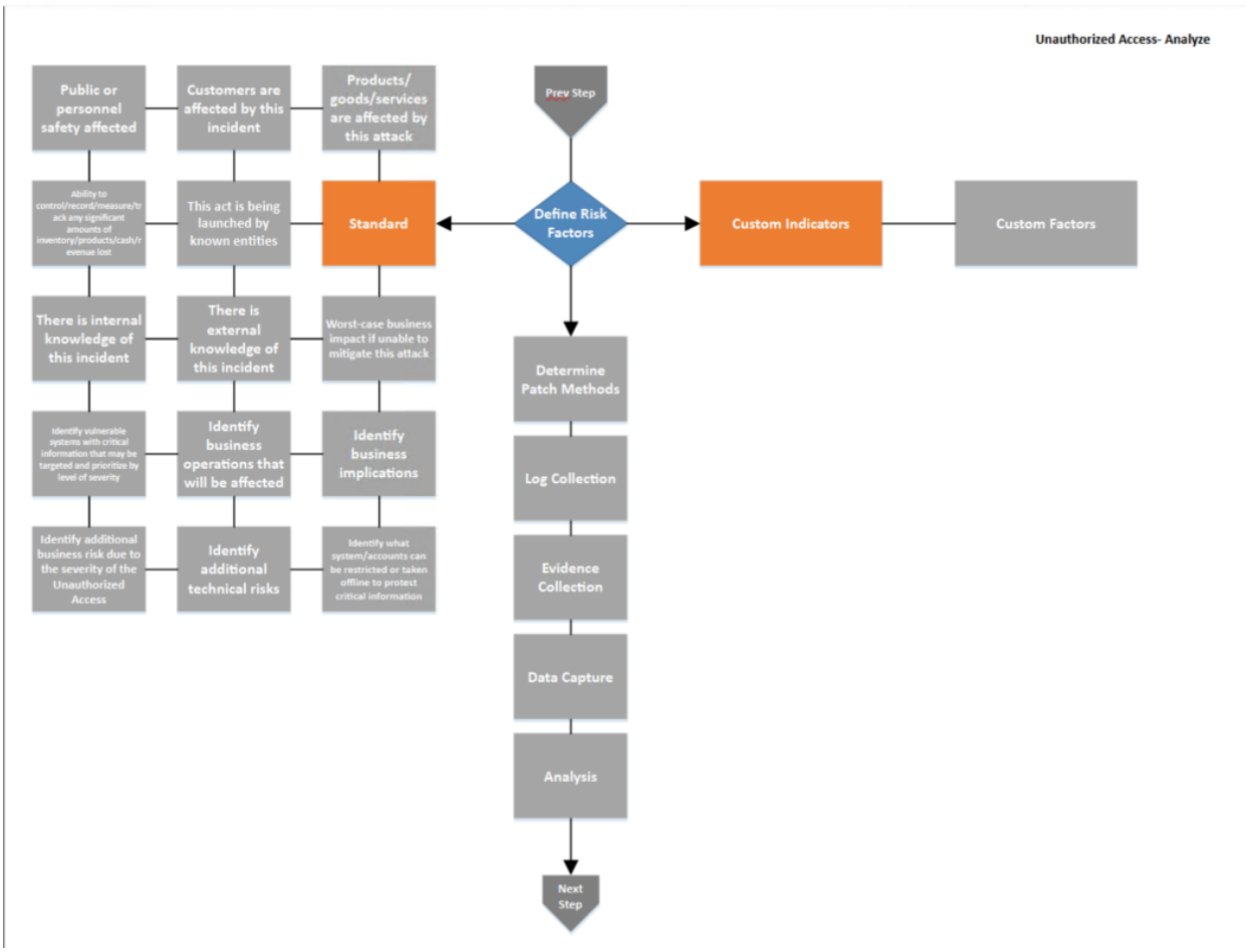
PREPARE:


Unauthorized Access- Prepare
START
Determine Core Ops Team & Define Roles
Vulnerability Manager
Threat Manager
Risk Manager
Review & Maintain Timeline
Interviews
User?
Manager
Physical Security
Key Stakeholders
Document
Internal Path
External Path
Document
Next Step

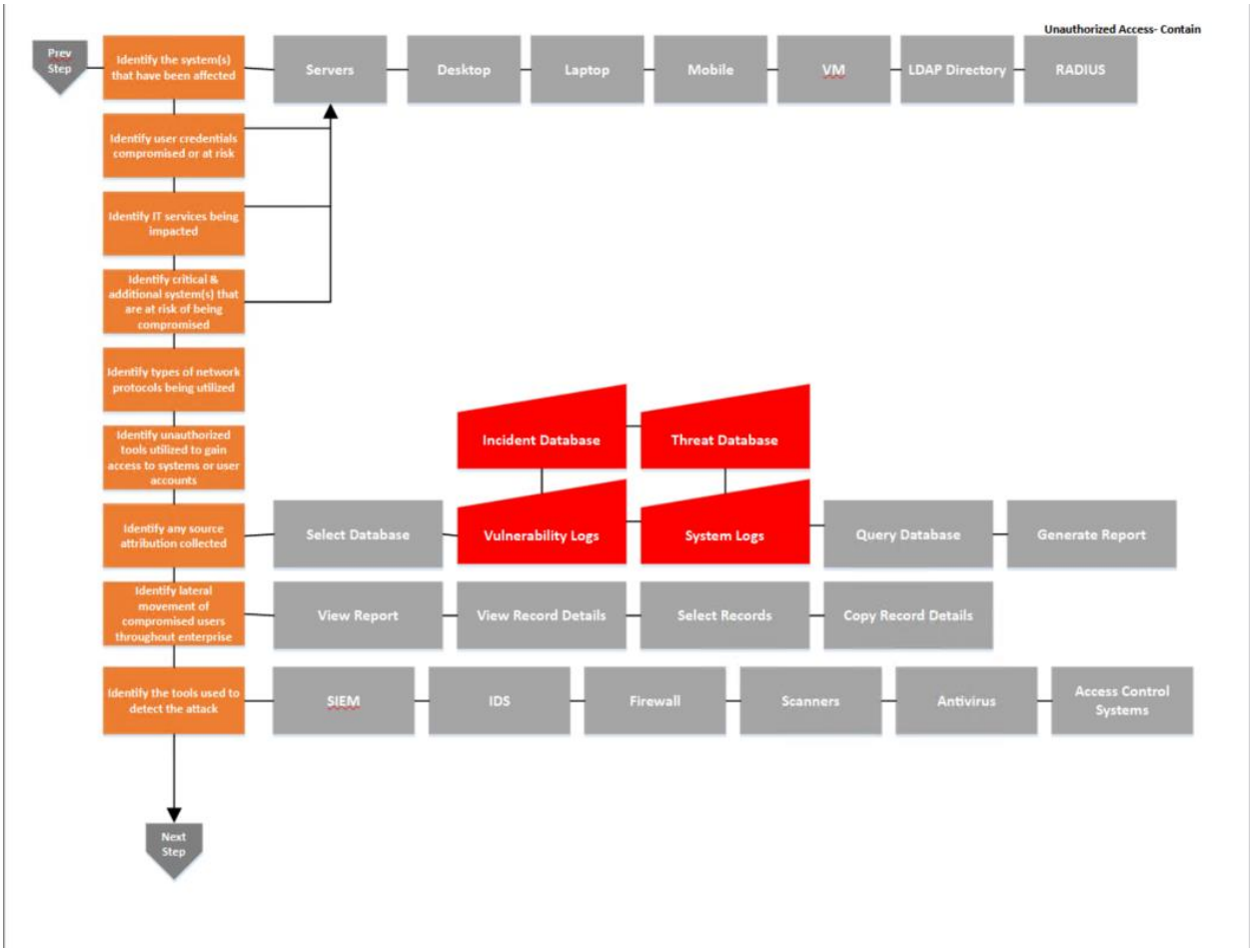
DETECT:


Unauthorized Access- Detect
Access to systems outside of normal business hours
Multiple login failures to a computer system
Increased logins to a computer system
Logins to multiple systems with same user credentials
Access to a computer system through abnormal ports or protocols
Exfiltration of data off of a computer system
User is unable to log into account
Unexplained browsing to unauthorized websites
Standard
Unexplained use of disabled or dormant user accounts
Unexplained escalation of privileges of user accounts
Unexplained system failures or restarts
Unexplained emails from user accounts
Unexplained modifications to system settings
Unexplained modification or destruction of user files
Unauthorized creation of new user accounts
Alerting from Firewall and Intrusion Detection Systems
Notification from outside organizations (ISP, business partners, 3rd party)
Prev Step
Define Threat Indicators
Custom Indicators
Custom Indicators
Two-Factor or Multi-Factor
Categorize Incident
Request Packet Capture
Conduct Scans
Next Step

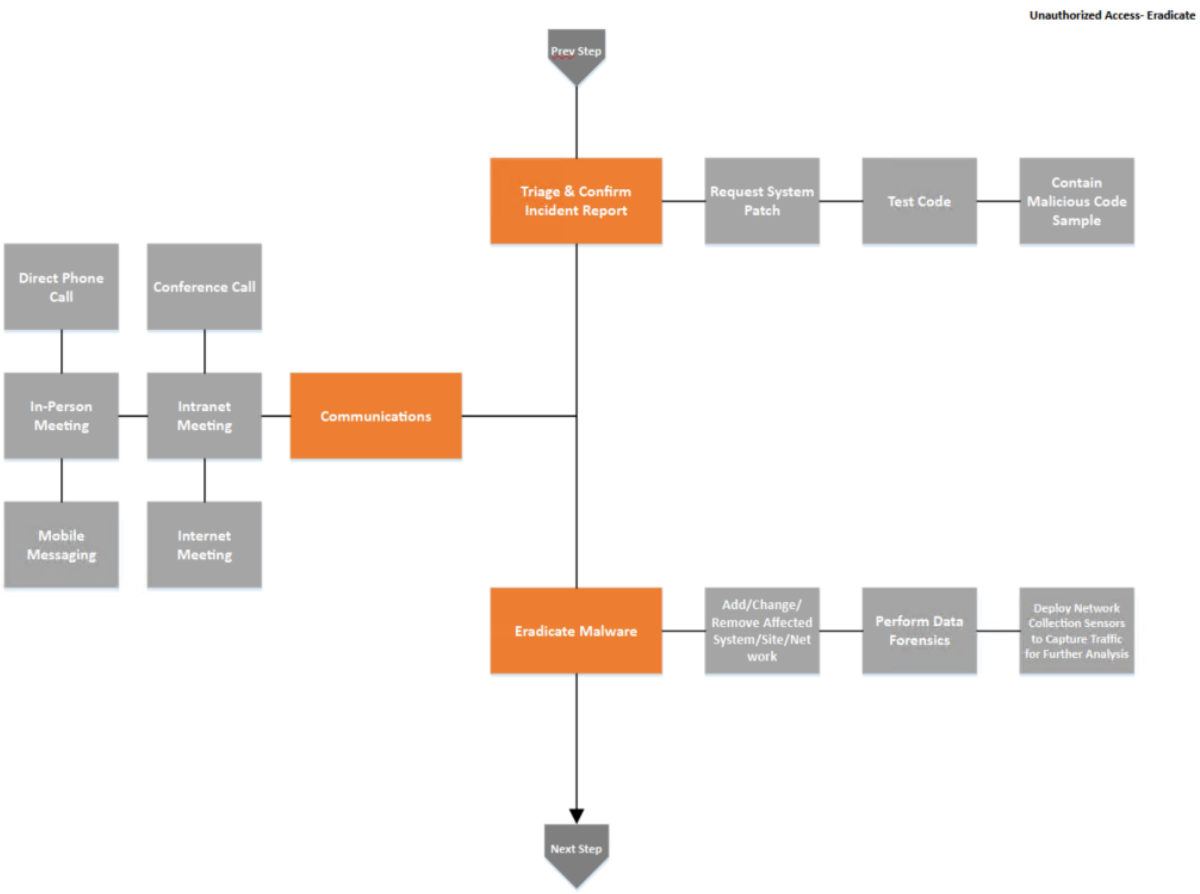
ANALYZE


Unauthorized Access- Analyze
Public or personnel safety affected
Customers are affected by this incident
Products/ goods/services are affected by this attack
Prev Step
Ability to control/record/measure/track any significant amounts of inventory/products/cash/revenue lost
This act is being launched by known entities
Standard
Define Risk Factors
Custom Indicators
Custom Factors
There is internal knowledge of this incident
There is external knowledge of this incident
Worst-case business impact if unable to mitigate this attack
Determine Patch Methods
Identify vulnerable systems with critical information that may be targeted and prioritize by level of severity
Identify business operations that will be affected
Identify business implications
Log Collection
Identify additional business risk due to the severity of the Unauthorized Access
Identify additional technical risks
Identify what system/accounts can be restricted or taken offline to protect critical information
Evidence Collection
Data Capture
Analysis
Next Step

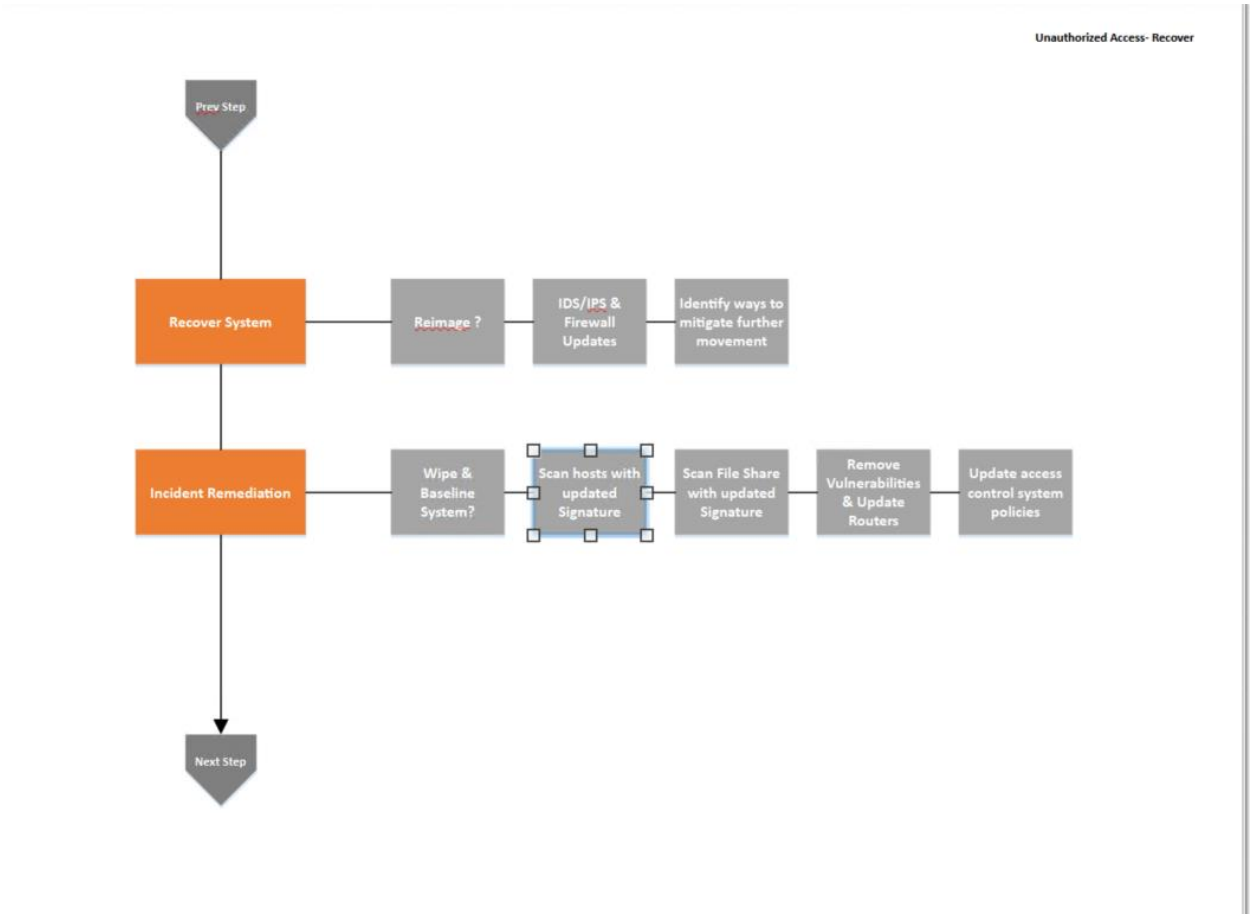
CONTAIN:


Unauthorized Access- Contain
Prev Step
Identify the system(s) that have been affected
Servers
Desktop
Laptop
Mobile
VM
LDAP Directory
RADIUS
Identify user credentials compromised or at risk
Identify IT services being impacted
Identify critical & additional system(s) that are at risk of being compromised
Identify types of network protocols being utilized
Identify unauthorized tools utilized to gain access to systems or user accounts
Incident Database
Threat Database
Identify any source attribution collected
Select Database
Vulnerability Logs
System Logs
Query Database
Generate Report
Identify lateral movement of compromised users throughout enterprise
View Report
View Record Details
Select Records
Copy Record Details
Identify the tools used to detect the attack
SIEM
IDS
Firewall
Scanners
Antivirus
Access Control Systems
Next Step

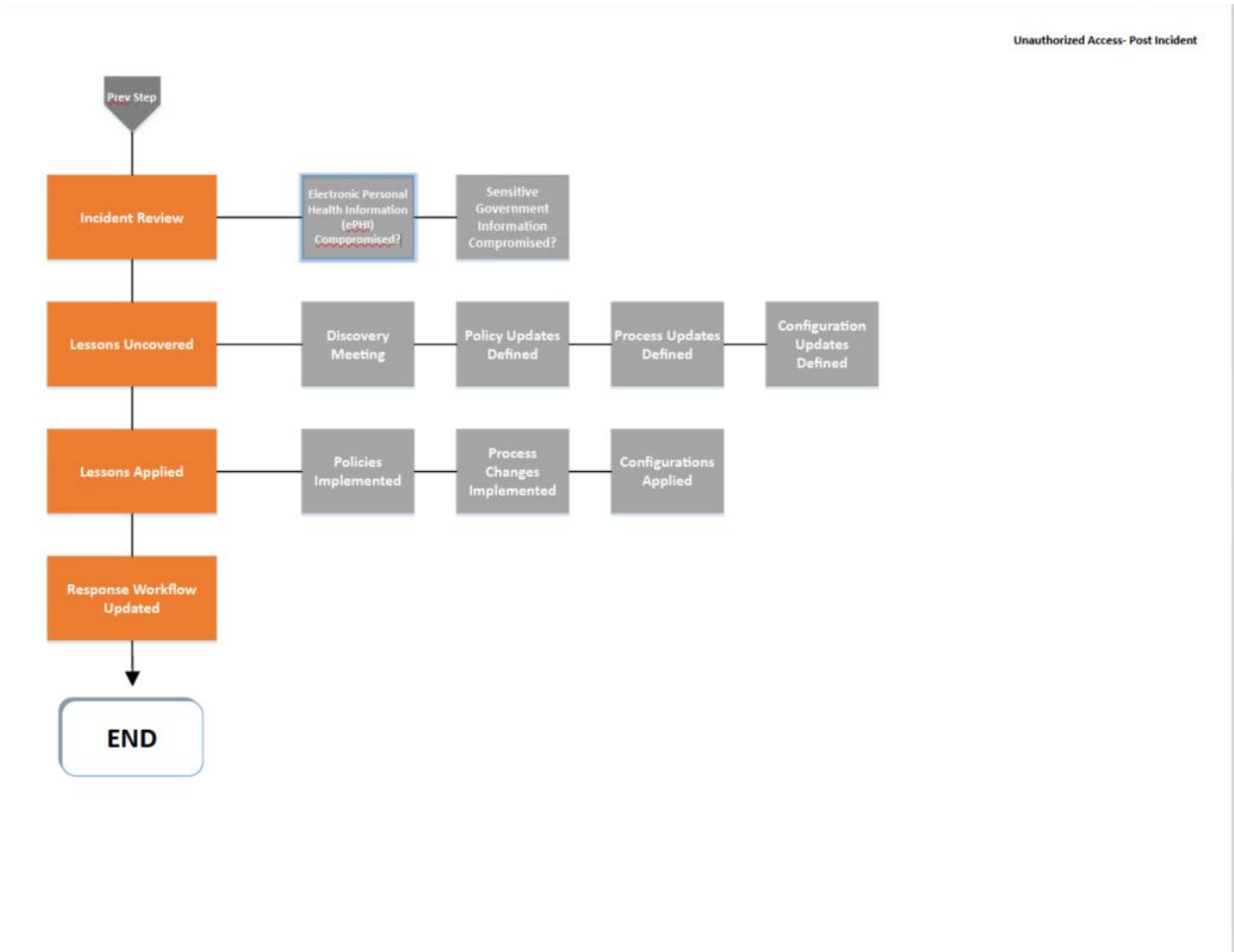
ERADICATE:


Unauthorized Access- Eradicate
Prev Step
Triage & Confirm Incident Report
Request System Patch
Test Code
Contain Malicious Code Sample
Direct Phone Call
Conference Call
In-Person Meeting
Intranet Meeting
Communications
Mobile Messaging
Internet Meeting
Eradicate Malware
Add/Change/ Remove Affected System/Site/Net work
Perform Data Forensics
Deploy Network Collection Sensors to Capture Traffic for Further Analysis
Next Step

RECOVER:



POST INCIDENT:



From the above playbook of unauthorized access incident happen in Canadian tire cooperation, I will discuss about five items where I need to escalate to senior IT team, internal and external stakeholders, those are:

1. In detect phase, when number of logins are increased from one or same ip address, this is the trigger point and need to escalate to SOC team to check if it is false positive or real threat by unauthorized users.
2. Affected Customers: After confirming the scope of the breach and identifying affected individuals, customers must be notified promptly to take necessary precautions and protect themselves from potential fraud.
3. Immediate Notification: When a product recall is initiated, the following stakeholders should be immediately notified: regulatory agencies and supply chain partners
4. In the event of a workplace accident, the following stakeholders should be immediately notified: emergency services and health and safety officer
5. Data breaches may trigger legal obligations under federal and provincial data protection laws, such as the Personal Information Protection and Electronic Documents Act (PIPEDA).

Incident Playbook Case Study Data Template

Data Name	Content	Rationale
Company Information	Retail company operating in the automotive, sports, leisure, and home improvement sectors.	
Company Name	Canadian Tire Corporation	

Contact Title (Position)	Chief information & technology Officer(CITO)	CITO is accountable for all aspects of technology including strategy, architecture, development, operations, and cybersecurity across the CTC family of companies.
Contact Availability	24*7 incident reporter and handler @111-111-1111	Incident reporter and handler available 24 *7 to detect the threat
Contact data permissions (TLP)	TLP: RED: Contact information marked as RED should only be shared with authorized personnel who have a specific need-to-know for critical business reasons. Unauthorized disclosure of RED contact information may lead to severe legal consequences and disciplinary actions. TLP: AMBER: Contact information marked as AMBER is for restricted distribution and should only be shared with relevant personnel involved in a specific project or business activity. Unauthorized disclosure may result in organizational harm and reputational damage. TLP: GREEN: Contact information marked as GREEN can be shared with all authorized personnel within the organization but should not be disclosed to external parties without proper authorization. TLP: WHITE: Contact information marked as WHITE can be shared freely within and outside the organization without restrictions.	All contact information must be classified based on its sensitivity and access permission
Incident Info:	The purpose of this information is to protect sensitive information, investigate breaches, and prevent future occurrences.	
Incident Name	Unauthorized access	
Incident Type	An event where an individual or entity gains unauthorized access to a system.	
C Effect	Loss of customer data, financial records, propriety information, any confidential data which leads to data breach and harm to reputation of the company	
I Effect	Data manipulation or tempering alters critical data which leads to inaccurate information, financial fraud or even sabotage.	Data integrity is essential for making informed business decision and maintains the accuracy of the records and transactions.
A Effect	It leads to unavailability of products and system to the stakeholders, downtime, loss of productivity and potential financial loss.	DoS attack impact the availability of services and system. Company system can be breached and may become unavailable to customers and stakeholders of the

		company.
Team Members (CSIRT)	CSIRT bringing together relevant stakeholder including IT team and security, Legal HR, senior management.	Whoever related to company is a stakeholder
Internal Stakeholders	Employees- who works with company have vested interest in its success and growth Management executives-leadership team and management of the company Board of directors- who oversees the company's management Shareholder- who has own shares in the company Suppliers- who supply goods and services to company Franchisees-who run their business under the Canadian tire brand	As a responsible corporate citizen, Canadian Tire strives to maintain positive relationships with its stakeholders, fulfilling its commitments to customer satisfaction, employee well-being, environmental sustainability, and ethical business practices
External Stakeholders	Customers- most significant stakeholder who's satisfaction and loyalty directly influence the business success. Investors- who have interest in the company financial performance Regulators and govt. agencies- who main the legal and ethical standards of various regulations and government policies Competitors- other retail companies Environmental and social advocacy groups- focused on environmental and social issues, influencing the company's sustainability and cooperate social responsibility practice. Health and safety officers	
Company data classifications & prioritizations	Canadian tire classifies and prioritizes the data bases on its sensitivity, criticality and level of protection required	
Categories of assets/devices that may be compromised	Customer data, retail platform, point of sales systems, supply chain system, inventory and management system, data center and cloud infrastructure, mobile applications, IT assets and endpoints	
Measurable metrics that would indicate the playbook has been completed and closed	Incident response time, user training and awareness, feedback from incident responder, post incident reviews	
Reports that would need to be written and to whom and when	To CSIRT, IT management, legal team, senior management, relevant stakeholders immediately after incident is detected or reported	

POLICIES:

1. Network Monitoring and Packet Capture

We will focus on implementing policies for network monitoring and packet capture to protect user information and sensitive data.

Packet Capture and Network Monitoring Policy

The purpose of this policy is to ensure the secure and ethical use of packet capture and network monitoring tools to protect user privacy and sensitive information.

- Packet capture and network monitoring tools may only be used by authorized personnel for legitimate security and operational purposes.
- All instances of packet capture and network monitoring must be approved by the Information Security team.
- Before initiating any packet capture or network monitoring, proper authorization and justification must be obtained and documented.
- The data captured or monitored must be protected and treated as sensitive information.
- Packet capture and network monitoring activities must comply with all relevant laws, regulations, and privacy policies.
- Any unauthorized use of packet capture or network monitoring tools will be considered a serious violation of company policies and may lead to disciplinary actions.

2. Protection of Personally Identifiable Information (PII)

In this, we focus on implementing policies to protect Personally Identifiable Information (PII) from unauthorized access, dissemination, or use.

PII Protection Policy

The purpose of this policy is to protect the confidentiality and integrity of Personally Identifiable Information (PII) and prevent its unauthorized access, use, or dissemination.

- Access to PII should be granted only to authorize personnel based on their role and job requirements.
- PII must be encrypted both in transit and at rest to maintain confidentiality.
- PII should be stored on secure, encrypted servers with access controls.
- PII must not be shared with third parties without explicit consent from the data subjects, unless legally required.
- Any suspected or confirmed unauthorized access to PII must be reported to the Information Security team immediately.
- Periodic access reviews should be conducted to ensure access rights are up to date and relevant.
- PII should be disposed of securely following the organization's data retention and destruction policies.

3. Handling of RED Information

In this, we focus on implementing policies to protect and handle information marked as RED according to the Traffic Light Protocol (TLP).

RED Information Handling Policy

The purpose of this policy is to define procedures for the proper handling, dissemination, and protection of information marked as RED according to the TLP.

- Any information marked as RED under the TLP must be treated as highly sensitive and confidential.
- Access to RED information should be restricted to personnel with a legitimate need-to-know and proper clearance.
- RED information must not be shared with parties outside the organization without explicit authorization.
- When disseminating RED information within the organization, it must be done securely and only to authorized recipients.
- RED information should not be stored on personal devices, and physical documents must be properly secured when not in use.
- Any suspected or confirmed unauthorized disclosure of RED information must be immediately reported to the Information Security team for investigation and remediation.

4. Data Retention and Destruction

In this, we focus on implementing policies for data retention and secure destruction to manage data effectively and minimize privacy risks.

Data Retention and Destruction Policy

The purpose of this policy is to establish guidelines for the retention and destruction of data to ensure compliance with legal requirements and protect sensitive information.

- All data collected and processed must have a defined retention period based on its nature and legal requirements.
- At the end of the data retention period, data must be securely destroyed using approved methods such as data wiping or physical destruction.
- Data owners and custodians are responsible for identifying and classifying data based on its sensitivity and retention requirements.
- The Information Security team will conduct periodic audits to ensure compliance with the data retention and destruction policy.
- Any data that is no longer required for business or legal purposes should be disposed of promptly and securely.

5. Log Retention and Incident Logs

In this, we focus on implementing policies for log retention, including incident logs, to aid in cybersecurity incident investigations and maintain accountability.

Log Retention and Incident Logging Policy

The purpose of this policy is to define procedures for the retention and management of logs, including those related to security incidents, to ensure their availability for investigations and compliance purposes.

- All logs related to security incidents must be retained for a minimum period for investigation and analysis.
- Logs should be stored securely to prevent unauthorized access, tampering, or deletion.
- Incident logs must include relevant details such as the time of occurrence, affected systems, actions taken, and the name of the personnel involved.
- The responsibility for log retention and management lies with the IT and Information Security teams.
- Regular reviews of log retention policies should be conducted to ensure they remain relevant and effective.
- Logs should be analyzed regularly to identify potential security incidents proactively.

Power point presentation: googledoc

https://docs.google.com/presentation/d/1lI-VW4UdlFiVU6EQqKYUovF1Tq7NEREf/edit#slide=id.p1