Viva la Vita Online Incidence Response Playbook

Abstract

Incident Response Playbooks outlines specific procedures on how to handle cyber incidents. It also specifies members and roles of the Cyber Incident Response Team (CIRT) of the organization and their respective roles. This paper provides a general overview of the incident reponse playbook for “Viva la Vita Online” and provides a detailed incident Reponse Playbook for three (3) scenarios following the defined general procedure.

Contents

Background

“Viva la Vita Online”, an online store that sells mostly vitamins and food supplements to individuals and retailers. The company has the following existing security controls.

Network Controls

- Perimeter Firewall on the network egress points
- Intrusion Prevention Sensors on the internal network
- Email Gateway with Anti-malware Anti-Spam Protection
- Security Information and Event Management (SIEM - Correlates logs from all security control systems)

Host Controls

- Anti-malware Endpoint Protection (includes Host-based firewall and HIPS) on all devices.
- Full Disk Encryption on employee laptops only

Other Controls

- Vulnerability Patching program (30 days SLA for all patching)

Executive Summary

The “Viva la Vita Online” Incidence Response Playbook provides a general guideline on how the company will respond to incidents related to information technology outlining the right action, protocols, and right people to be involved when incidents occur.

This playbook will outline the general processes, procedures investigation, eradication, and recovery procedures from an incident. It also identifies that the general procedure on how the organization will engage the support of other government and private institutions to help perform incident analysis, mitigate, and communicate with other stakeholders such as customers when necessary.

Generally, this playbook identifies the Cyber Incident Response Team (CIRT) of the organization and their respective roles, identifies the contacts and the responses they should provide based on the contracts of the cybersecurity service providers of the organization, provides an outline of the incident reporting protocol with respective timelines, identify the response procedure that will be taken by the CIRT to conduct the necessary investigation, containment, eradication, and recover for the incident, and the strategic communication protocol to be followed.

Composition of the Cyber Incident Response Team (CIRT) and their Functions

Viva la Vita Online will have the following composition of the Incident Response Team (CIRT) and the corresponding responsibilities:

- Incident Response Manager - Directs the CSIRT team
- Security Analyst - Supports CSIRT Manager coordination tasks.
- CISO- Responsible to direct and maintain the company's information security vision to support enterprise objectives.
- CIO/CTO - Responsible to direct and maintain the company's information technology vision to support enterprise objectives.
- Technology and Operations Team Lead - Comprehensive and Authoritative knowledge of the IT infrastructure and Company Operations
- Senior Management - Highest management Level of the company
- Business Line Head of Departments - Directs and maintain company's business strategy.
- Human Resources - Employees' life-cycle manager
- Legal / General Counsel - Legal advisor
- Public Relations Officer - Company's public relations Manager

The team shall ensure availability 24/7. For positions considered are very critical such that its presence is needed in the office 24/7, the company needs to train a back-up since incidents can happen around the clock and the responses may be needed immediately. The lead and backup roles have to work in shifts to ensure 24-hour availability.

The company has the responsibility to provide necessary training to all the members of the team to ensure that they will be able to discharge their responsibilities excellently. Contacts to third-party consultants shall be maintained for ready reference when the need to contact them arises.

Aside from these, the authorities of each member of the CIRT should be provided to ensure that decisions are made by proper authorities. It should be explicitly indicated who has the authority to make rapid decisions such as determining whether to continue or discontinue a certain business process, who makes the critical decisions, who is authorized to request additional support, who has the authority to interface with another response partner, who is in authority to report the incident, who informs regulatory bodies, and who will do the paperwork.

The General Incident Response Plan

Viva la Vita Online will employ the general incident response plan when encountering incidents. The specific activities will be dependent on the specific incident to be faced. Responding to an incident shall have the following general steps.

a. Prepare

This is the initial phase where the necessary preparatory measures are done for the team to be ready with a response if and when incidents happen.

b. Detect

This phase involves the listing down of possible methods to detect that there's indeed an incident. This should be done in the shortest time possible to avoid further damage to be done. Early detection is always better.

The activities that may arise in this phase can be.

- System alert/treat alert/ employee report/or vendor alert is detected by the information/operations security.
- The first response team is activated to conduct an initial investigation.
- If the event was not confirmed that the actions conducted are documents or recorded and the raise the event as a resolved case.
- If the incident is confirmed, then the CIRT declared that there is an incident and activates the Cyber Internet Response Team

c. Analyze

The analysis involves the conduct of further investigations to get details of the incident. The answers to where did it all started and to what extent was the damage done should also be answered in this phase.

Specific activities that may arise in this phase include:

- Envolve CIRT team analyzes the situation.
- Investigation with proper documentation is done.

d. Contain and Eradicate.

Containment and eradication define ways on how to contain the incident to avoid further damage. However, by doing so, the team should have been a thing of how to completely eradicate the incident so that the organization can start moving forward.

In this phase the possible actions are:

- Initial containment actions are done by the right CIRT member.
- Require reporting is done.
- Eradication Plan is reviewed and implemented.
- Incident eradication is made.

e. Recover

Recover is the phase where plans on how to recover from the attack must be stated. If the company lost a million because of the attack, what should the company do? If the result of the incident resulted in the deletion or loss of the majority of the customer records, then who can the company retrieved the files.

In the recovery stage, the following activities may be done.

- Restore and verify the recovery.

f. Post-Incident Handling

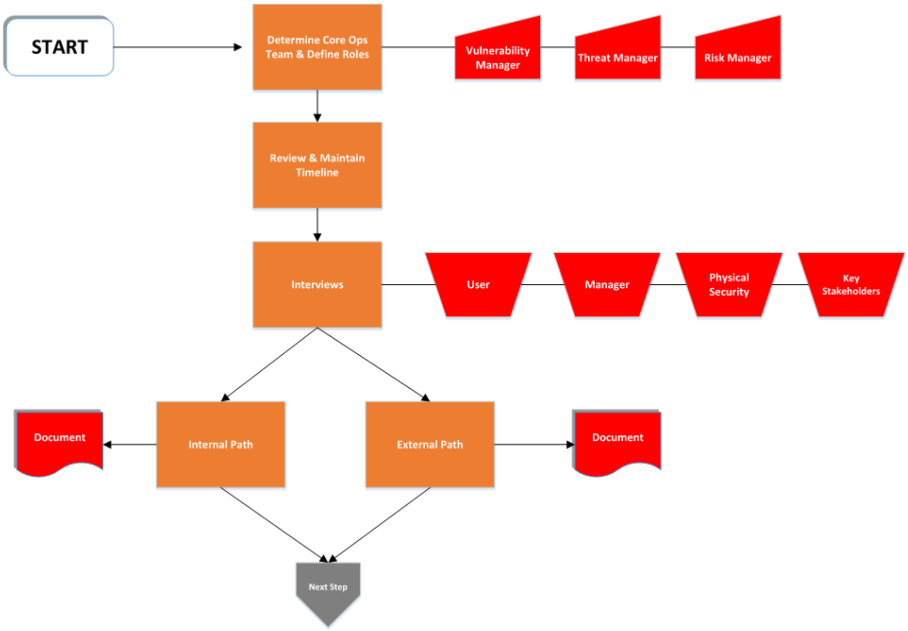
This will lay out what should the company implement after the event. There may be realizations like the company losing a million for example. What are the lessons learned? Will the company harden the system to provide additional security features?

In the post-handling activities, the following activities can be implemented.

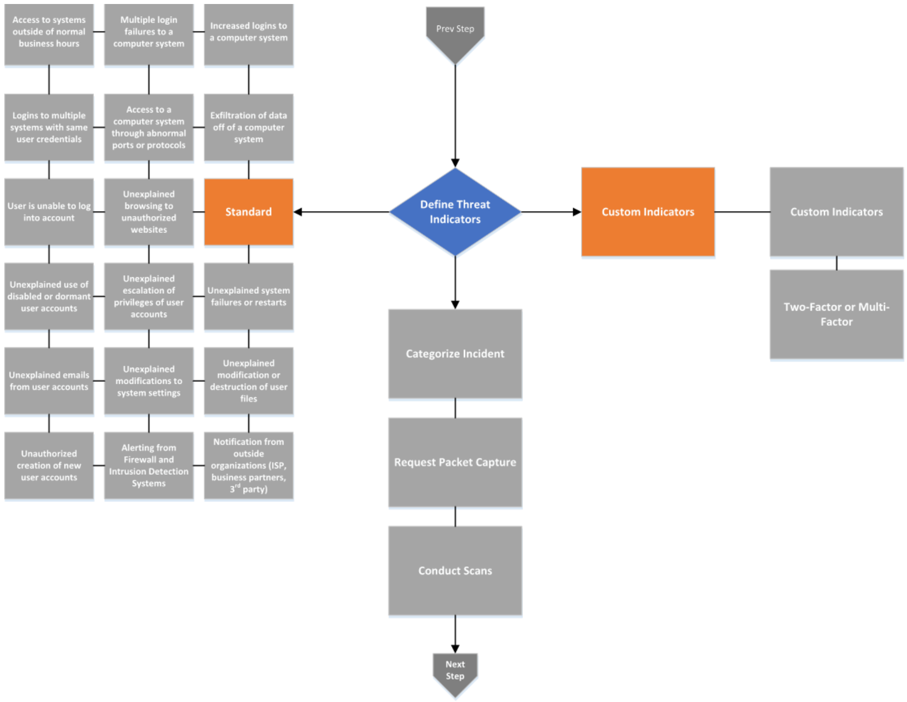
- Conduct after-action review.
- Update the incidence response plan if necessary and conduct necessary training.
- Assess for lessons learned and apply necessary preventive mechanisms.

The general flowchart is shown below:

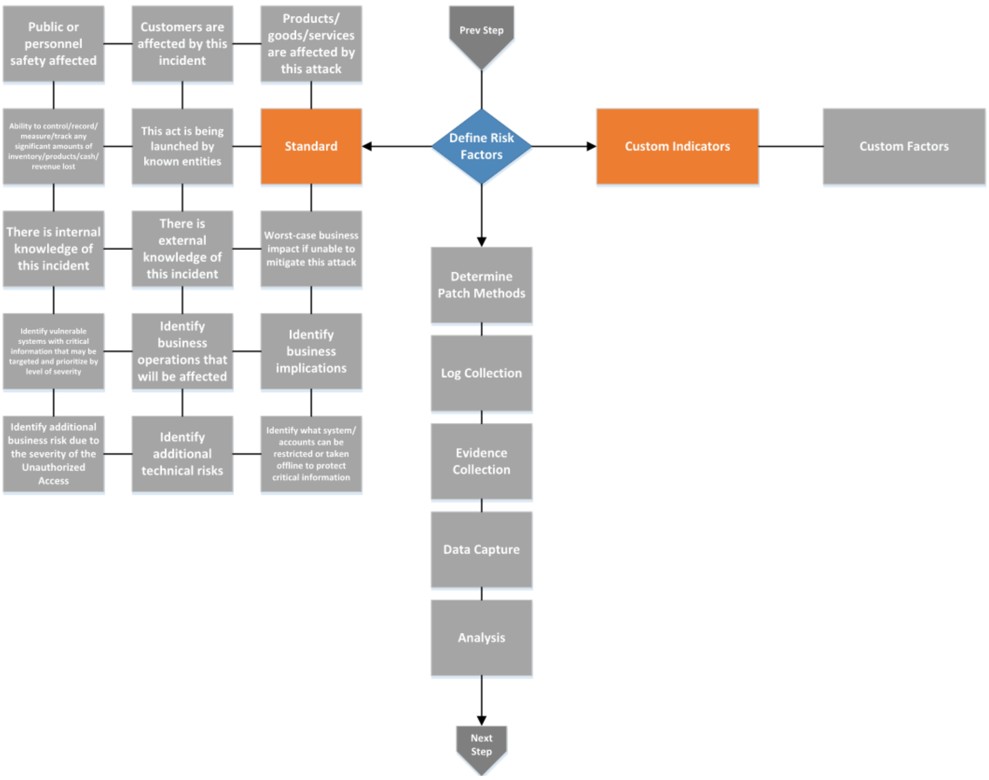
Prepare



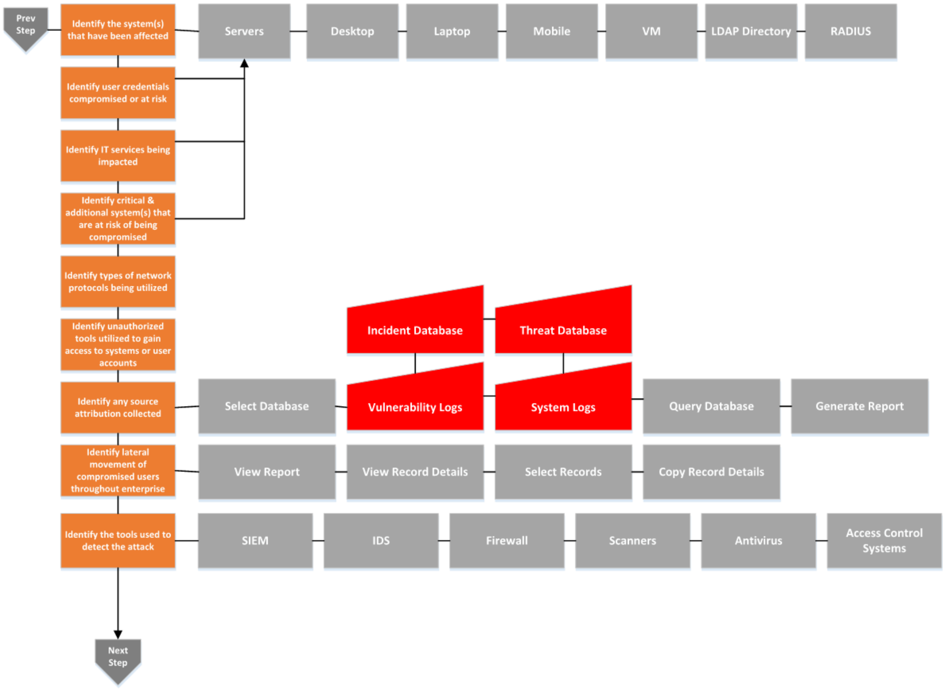
Detect


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

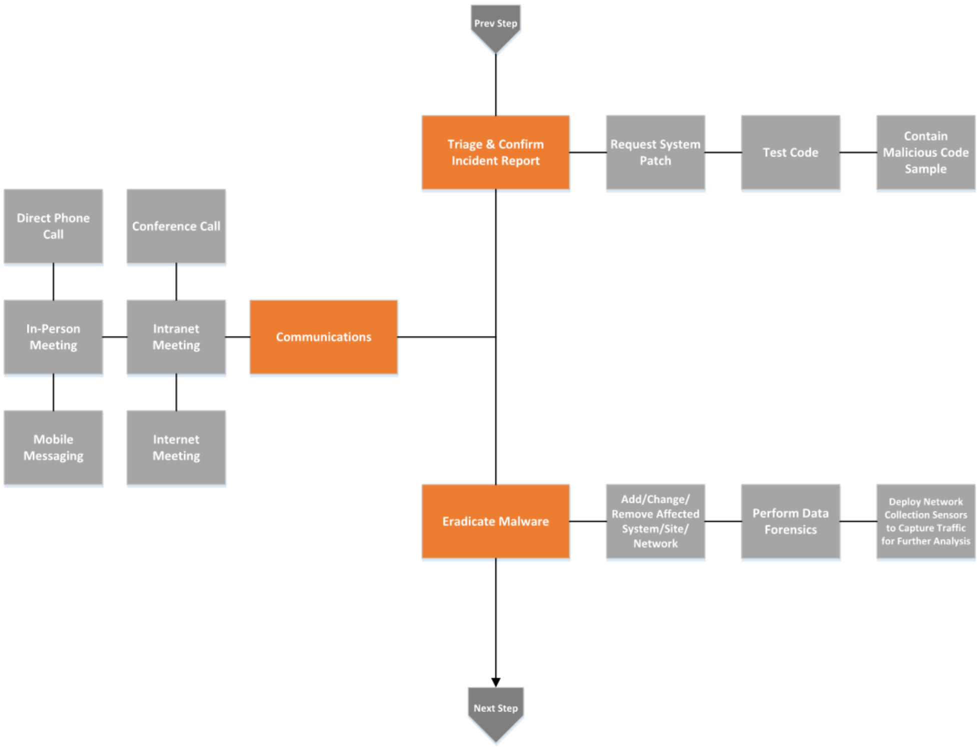
Analyze


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

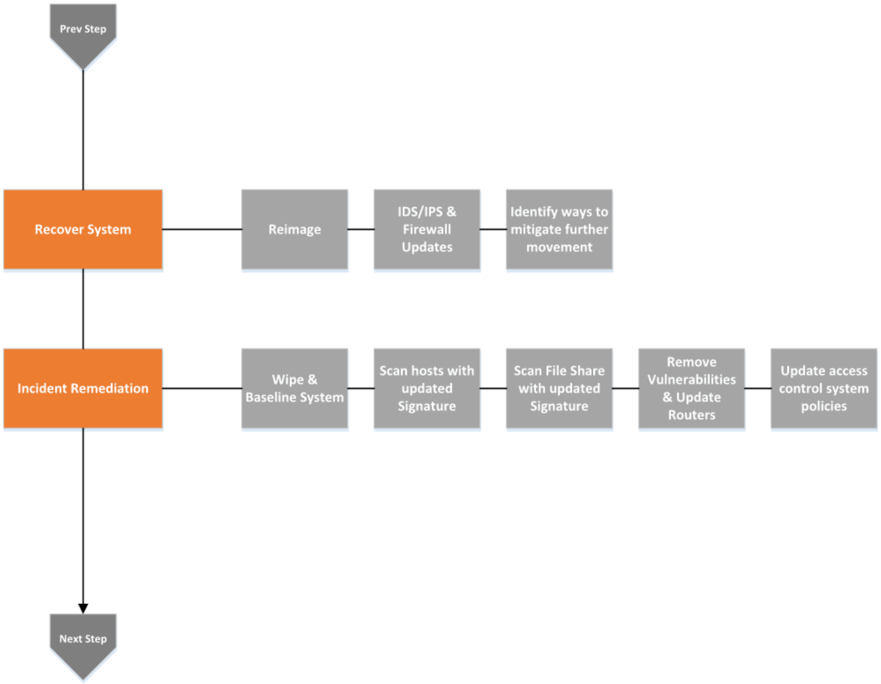
Contain


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
Incident Database
Threat Database
Identify unauthorized tools utilized to gain access to systems or user accounts
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

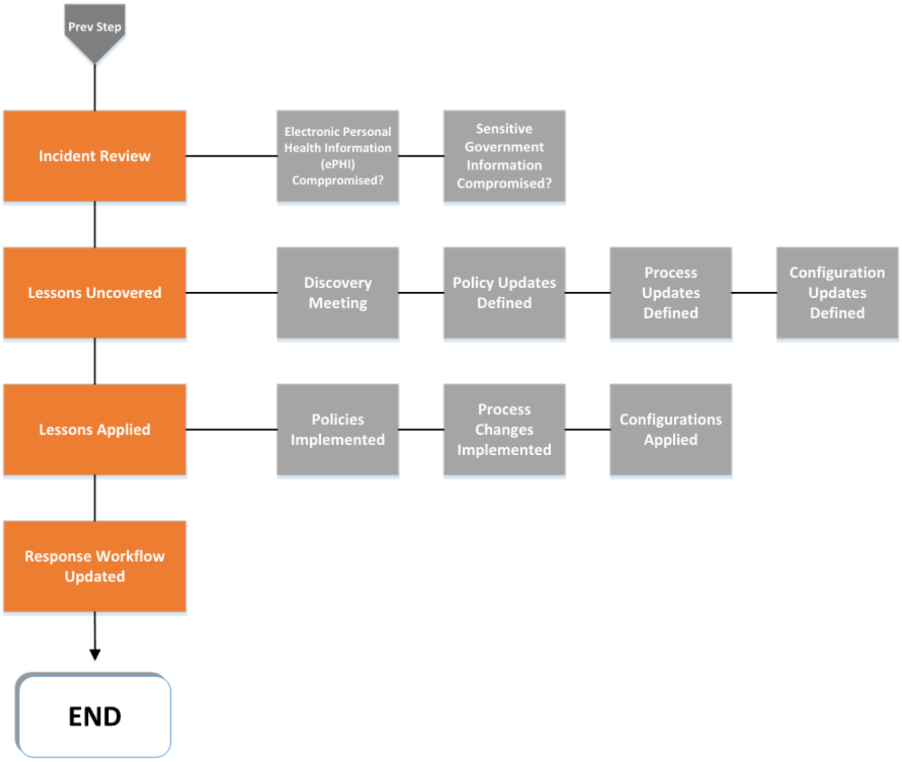
Eradicate



Recover


Prev Step
Recover System
Reimage
IDS/IPS & Firewall Updates
Identify ways to mitigate further movement
Incident Remediation
Wipe & Baseline System
Scan hosts with updated Signature
Scan File Share with updated Signature
Remove Vulnerabilities & Update Routers
Update access control system policies
Next Step

Post-incident


Prev Step
Incident Review
Electronic Personal Health Information (ePHI) Comppromised?
Sensitive Government Information Compromised?
Lessons Uncovered
Discovery Meeting
Policy Updates Defined
Process Updates Defined
Configuration Updates Defined
Lessons Applied
Policies Implemented
Process Changes Implemented
Configurations Applied
Response Workflow Updated
END

Scenario 1: Unauthorized attempt to access payroll records.

The SIEM has detected, attempt to access to payroll records of different employees. All attempts came from the same user account "j.saw", which is an account that belongs to a financial department employee John Saw. The Incident response team was able to identify that this account's password was recently reset due to a social engineering attack from somebody who called the helpdesk and provided the authentication information requested.

Detection and Notification

Incident	How to detect the occurrence of the incident	Responsible Person
Review of SIEM logs detects an attempt to access payroll records of different employees by j.saw user account	Review of SIEM logs indicate attempts of "j.saw" account to access records of employees	John Saw Database Manager

Immediately, the persons to be immediately notified should be the Incident Response Manager and the Technology and Operations Team Lead

Analysis:

The following steps would be taken to investigate the incident.

1. Report the incident to the Incident Response Team Manager and the Technology Operations Team Lead ad to provide initial findings. The content of the initial report

should include comprehensive details on when the attempt to access the payroll records of each employee was made and whose account was used in the attempt.

2. Since the account of John Saw of the Finance department reflected that it was the account who perform the attempt to access the files, investigate the history of the account of John Saw.
3. Determine the recent activities of the account, at least 5 days before the incident happened, and look for additional malicious behaviors or account patterns done by the account. Possible questions to ask and investigate include what usual activities were done using the account before the incident? Were there instances that the passwords were changed? From what address were the accesses made?
4. Having known that the password has changed due to a recent social engineering attack, check for possible loopholes on why the social engineering attack wasn't detected.
5. Determine who provided the authentication information from the helpdesk.

Containment:

For the containment, there is no actual data that was a loss in the payroll system because it was only attempted to be accessed. The problem that needs to be contained in the social engineering attack that enabled the password change. The initial containment step would be to change the password for John Saw's account.

Eradication:

To eradicate this threat, the following steps should be done.

1. Change the password for John Saw's account.

2. Change the authentication information requested.
3. Limit access to the authentication information.
4. Provide a security policy plan for the organization and define who has access to the security code authentication information of the company.
5. Provide training for the employees, emphasizing among others that information such as authentication information should not be divulged to anyone who asks them.

Recovery:

For the recovery, the main concern for recovery is the accounts of John Saw and authentication information. The recovery that affects the whole system is not appropriate since the system was not attacked yet.

Scenario 2: SQL injection vulnerability

Over a regular audit of your database applications, it was detected that one application uses an insecure code to construct SQL queries.

```
SELECT * FROM employees WHERE idemp='" + request.getParameter("idcode") + "’";
```

We do not have evidence of this vulnerability being exploited yet, but we know that the privileges of the application allow write, modify or delete data from *employees* table.

Detection and Notification

Incident	**How to detect the occurrence of the incident**	**Responsible Person**
Regular audit of database application detected the use of insecure code to construct SQL queries	Audtit of codes used in the construct of SQL queries	Database Manager Technology and Operations Team Leader

Upon detection of the vulnerability of the SQL codes, the Audit Team should notify and seeks the attention of the Database Manager and the Technology and Operations Team Leader.

Analysis:

Further investigation of the incident should be conducted which would focus on.

1. Determining the developers of the code.
2. Determine which applications makes use of the code.
3. Provide alternative codes.

4. Check whether the vulnerability detected has been exploited.

Containment:

For the immediate containment of the incident, the code to construct the SQL queries must immediately be deactivated while investigations are ongoing and necessary adjustments has not been made.

Eradication:

To eradicate this threat, the following steps should be done.

1. Change the code to create SQL statements in such a way that it will not allow the application to write, modify or delete data from employees table.
2. Ensure that only authorized users will have access to code that allows the modification of data contains in the database tables.
3. Conduct regular audit of the codes used and ensure that database priviliges are well organized.
4. Strengthened the database security specially in granting access rights to users.

Recovery:

For the recovery, if there has been proof that the vulnerabilities as been exploited, then tracing should be done. For a more permanent recovery mechanism, there must be backup and strengthening of the security for access to the database.

Scenario 3: Blacklisted IP is seen in the VPN connections.

Our intrusion prevention system has flagged an inbound connection originated from a blacklist IP address (http://ipqualityscore.com/ (Links to an external site.)). According to our logs, this IP has been used to connect our systems through our VPN Server. The employee account used, j.saw, was authenticated for the session and the name of the user associated with the user ID.

Detection and Notification

Incident	How to detect the occurrence of the incident	Responsible Person
A blacklisted IP Address was able to connect via inbound through the use of and employee account j.saw.	Intrusion detection system of the organization detected the attempt of the blacklisted Ip address	John Saw CISO

The operator of the instruction detection system should immediately report the incident to the incident report manager for necessary actions.

Analysis:

The following steps would be taken to investigate the incident.

1. Check the details the IP address was able to access the system and the owner of that IP address.
2. Check who authorized the access.
3. When it was seen that j.saw account was used authorized access, check the details when the authorization was made and the history of the account.
4. Determine the recent activities of the account, at least 5 days before the incident happened, and look for additional malicious behaviors or account patterns done by the account. Possible questions to ask and investigate include what usual activities were done using the account before the incident? Were there instances that the passwords were changed? From what address were the accesses made?
5. While the IP address have access, what were its activities? What was the extent of damage the access made?

Containment:

For the containment, immediately block access of the account of j.saw and the ip address.

Eradication:

To eradicate this threat, the following steps should be done.

1. Change the password for John Saw’s account.
2. Change the authentication information requested.

3. Limit access to the authentication information.
4. Provide a security policy plan for the organization and define who has access to the security code authentication information of the company.
5. Provide training for the employees, emphasizing among others that information such as authentication information should not be divulged to anyone who asks them.

Recovery:

For the recovery, the main concern for recovery is the accounts of John Saw and authentication information. Check the files of applications affected and restore.