# Unauthorized Elevation of Privilege Process Flow

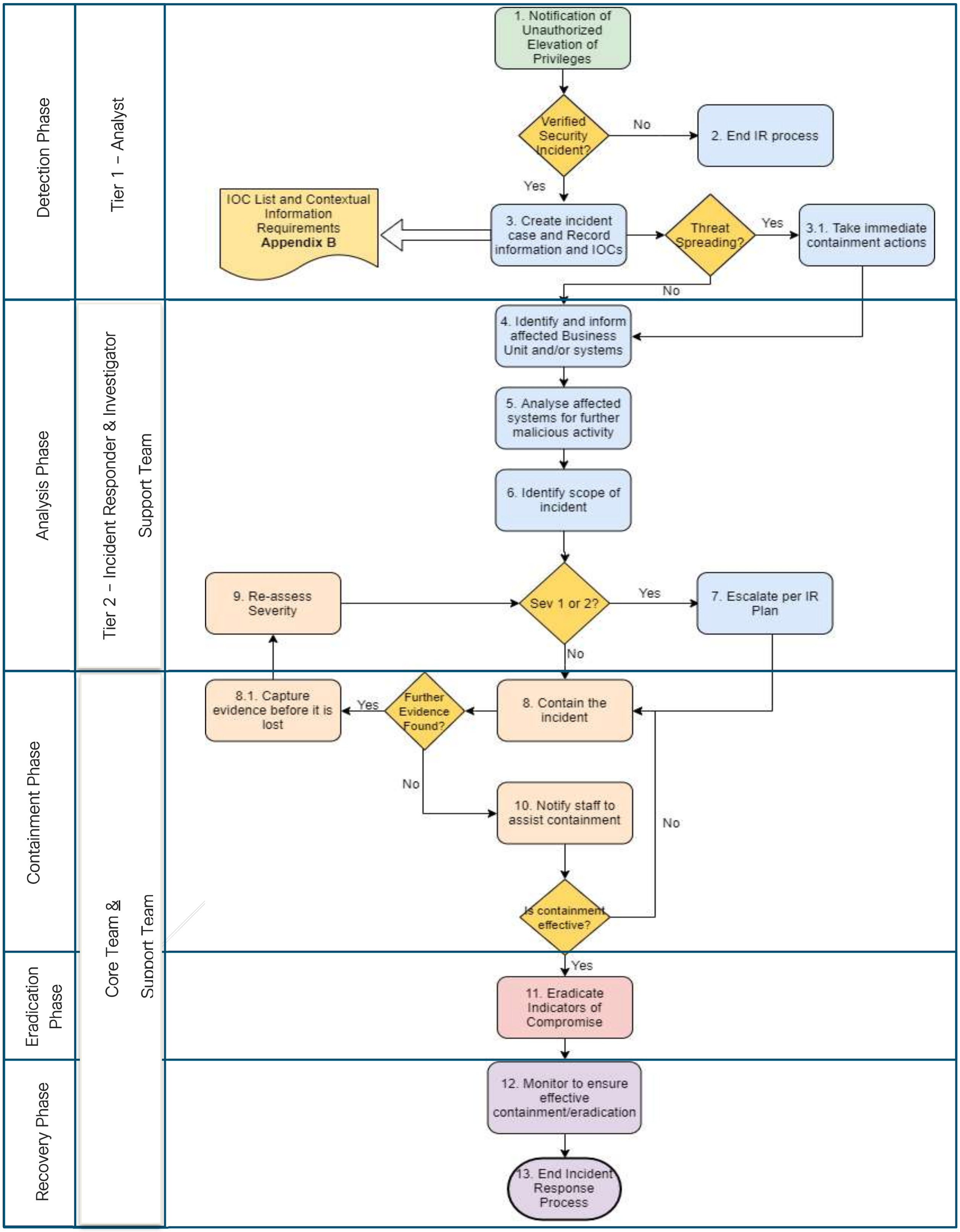
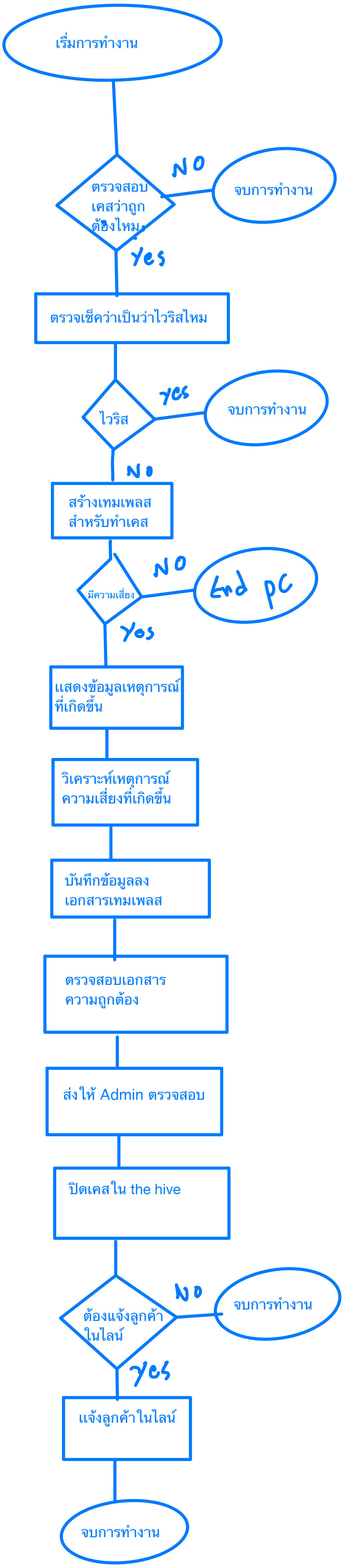

Detection Phase
Tier 1 – Analyst
1. Notification of Unauthorized Elevation of Privileges
Verified Security Incident?
No
2. End IR process
Yes
IOC List and Contextual Information Requirements
Appendix B
3. Create incident case and Record information and IOCs
Threat Spreading?
Yes
3.1. Take immediate containment actions
No
Analysis Phase
Tier 2 – Incident Responder & Investigator
Support Team
4. Identify and inform affected Business Unit and/or systems
5. Analyse affected systems for further malicious activity
6. Identify scope of incident
9. Re-assess Severity
Sev 1 or 2?
Yes
7. Escalate per IR Plan
No
Containment Phase
Core Team &
Support Team
8.1. Capture evidence before it is lost
Yes
Further Evidence Found?
8. Contain the incident
No
10. Notify staff to assist containment
No
Is containment effective?
Yes
Eradication Phase
11. Eradicate Indicators of Compromise
Recovery Phase
12. Monitor to ensure effective containment/eradication
13. End Incident Response Process

Figure 1: Unauthorized Elevation of Privilege Process Flo


เริ่มการทำงาน
ตรวจสอบ เคสว่าถูก ต้องไหม
NO
จบการทำงาน
Yes
ตรวจเช็คว่าเป็นว่าไวริสไหม
ไวริส
yes
จบการทำงาน
No
สร้างเทมเพลส สำหรับทำเคส
มีความเสี่ยง
NO
End pc
Yes
แสดงข้อมูลเหตุการณ์ ที่เกิดขึ้น
วิเคราะห์เหตุการณ์ ความเสี่ยงที่เกิดขึ้น
บันทึกข้อมูลลง เอกสารเทมเพลส
ตรวจสอบเอกสาร ความถูกต้อง
ส่งให้ Admin ตรวจสอบ
ปิดเคสใน the hive
ต้องแจ้งลูกค้า ในไลน์
No
จบการทำงาน
yes
แจ้งลูกค้าในไลน์
จบการทำงาน

## Unauthorized Elevation of Privilege Process Detail

| Step | Action | Performer | Details | Notes |
|---|---|---|---|---|
| **1** | Notification of Unauthorized Elevation of Privilege | Tier 1 - Analyst | □ Receive a notification of Unauthorized Elevation of Privilege<br>□ USE CASE: PHYSICAL UNAUTHORIZED ELEVATION OF PRIVILEGE<br>○ If the above use case is suspected, consult Appendix A<br>□ Collect basic information about the incident<br>○ Time that the incident was reported<br>○ How the incident was reported<br>○ Current impact of incident<br>○ Systems / user accounts involved<br>○ Authorized service accounts and other server credentials<br>○ Asset role (such as whether it is used for key business or administrative tasks)<br>○ Any remediation actions taken<br>□ Ensure access to incident ticket and incident log are granted<br>□ Update Incident Log | Use the “Incident Reporting Form” to ensure that all the basic information is captured. |
| **2** | End IR process | Tier 1 - Analyst | □ In the case that this is not verified to be a security incident, end the IR process. | |

| | | | | |
|---|---|---|---|---|
| **3** | Create incident case and Record information and IOCs | Tier 1 - Analyst | □ Create a security incident case.<br>□ Review security logs of affected devices<br>□ Review identified user accounts for permission changes and recent activity<br>□ Understand affected system(s) and the potential motive for Unauthorized Elevation of Privilege<br>□ Review network connectivity of affected systems and subsequent access available<br>□ Log any of the IOC's that have previously been identified (or analysis has provided) into the created incident case. | IOC List at Appendix B<br>Interview unauthorised user / custodian to gather additional information to identify if it was an error or social engineering attack. |
| **3.1** | Take immediate containment actions | Tier 1 – Analyst | □ Revoke unauthorised elevated privileges. Block any connections related to the initial notification and analyse them for suspicious behaviour<br>□ If there is an immediate need, consider internal network controls that may be used<br>□ If there is an immediate need, temporarily disable any involved user accounts<br>□ Log all actions within Incident Log | This action may necessitate the assistance of various Departments, such as Server and onsite team. |

| | | | | |
|---|---|---|---|---|
| **4** | Identify and inform affected Business Unit and/or system administrators | Tier 1 - Analyst | □ If an IP address is available search systems to identify device location<br>□ Using identified usernames determine potentially impacted business units through active directory<br>□ Identify the affected business unit by location of the device or by hostname mapping<br>□ Be cautious that any internal communication does not give any information to an inside threat.<br>□ This action should be **approved** by the **SOC** and **CSIRT head**. | Information to include:<br>• Immediate Action they should take<br>• Actions they should not take<br>• Restrictions they may suffer as a consequence of the investigation<br>• Point of contact within the IR |
| **5** | Analyse affected system for further malicious activity | Tier 2 – Incident Responder & Investigator | □ Analyse network traffic, logs, etc. for any activity that could indicate traversal through the network<br>□ Determine if the unauthorized user has accidentally deployed any malicious code<br>□ Generate IOCs that show unauthorized activity<br>□ Log actions in incident log | Review Appendix B for list of IOCs |
| **6** | Identify the scope of incident | □ Tier 2 – Incident Responder & Investigator<br>□ Support Team | □ Implement monitoring of affected systems<br>□ Search the enterprise for similar activity using available IOCs.<br>□ Identify the root cause of the unauthorised elevation. Possible causes can be: system vulnerabilities / errors, lack of security controls.<br>□ Log actions in incident log | |
| **7** | Escalate Per IR Plan | Tier 2 – Incident Responder & Investigator | □ If an Incident is Severity 1 or 2 follow the escalation process in the IR plan to involve the relevant parties to remediate the incident. | |

|  |  |  |  |  |
|---|---|---|---|---|
| **8** | Contain the Incident | □ Tier 2 – Incident Responder & Investigator<br>□ Support Team | □ Determine if other systems are affected<br>□ Check for similar behaviour from other user accounts<br>□ Reduce access to systems through authentication mechanisms / active directory permissions<br>□ Reset User accounts, if needed<br>□ Revoke additional unauthorised privileges<br>□ Implement patches to stop unauthorised elevation<br>□ Log all actions to incident log |  |
| **8.1** | Capture evidence before it is lost | Tier 2 – Incident Responder & Investigator | □ In the case that further evidence / artefacts (e.g. IOCs) are identified during containment, they need to be captured and recorded before they are lost.<br>□ Where specialist assistance is required consider calling out IR providers via Incident Manager<br>□ Preserve network log information<br>□ Gather relevant files and artefacts that could assist the investigation<br>□ Store artefacts within Incident Folder<br>□ Log actions in incident log | Artefacts:<br>System Logs<br>Security Logs |
| **9** | Re-assess Severity | Tier 2 – Incident Responder & Investigator | □ Based on the evidence captured / identified during the containment phase (if any) the severity of the incident needs to be revised and go to step 7 if needed. |  |

|  |  |  |  |  |
|---|---|---|---|---|
| **10** | Notify staff to assist containment | Tier 2 – Incident Responder & Investigator | □ Consider if social engineering is an aspect<br>□ Be wary of informing users who may be colluding with each other<br>□ The **escalation procedure** defined in the **IR Plan** shall be followed. |  |
| **11** | Eradicate Indicators of Compromise | Support Team | □ In the occasions that the containment was effective, initiate recovery. If the containment was not effective, more containment actions are needed.<br>□ Inform resolver group (on-site team) that systems are required to be rebuilt<br>□ (Optional) Confirm to resolver group if rebuilt devices can be immediately re-introduced into the environment<br>□ Recover data from backups where integrity is questioned<br>□ Log notification in incident log | Rebuilding systems in this occasion can be as simple as resetting an account or resetting the privileges of an account.<br>To make sure that containment was effective revise the logs of systems that have been utilized to implement containment actions and confirm there is no more malicious activity |
| **12** | Monitor to ensure effective containment/eradication | SOC Team | □ Monitor re-activated user accounts for an appropriate period to ensure no indicators of Unauthorized Elevation of Privilege resurges to confirm the containment and eradication has been successful<br>□ If further suspicious activity is identified, implement further containment and remediation<br>□ Log all actions in incident log |  |

| | | | | |
|---|---|---|---|---|
| **13** | End Incident Response Process | Tier 2 – Incident Responder & Investigator | □ Notify Incident Manager of completion of Incident Response process<br>□ Log / store all remaining information and artefacts in the incident folder<br>□ If Post Incident Review (PIR) is required refer to PIR Playbook<br>○ Carry out a Post Incident Review if required<br>○ PIR is required where an incident is a Severity 1 or Severity 2 | |

# Appendix A - Specific Use Case

## Physical Unauthorized Elevation of Privilege

Due to the nature of the events that [redacted] deals with, there may be scenarios where sensitive assets must be left in public places where there is a chance of physical Unauthorized Elevation of Privilege. Depending on the segregation that is present in the network, this may allow unsuspected employees to bypass the main defences on the perimeter of the network and provide access to sensitive resources within the network.

### Special Considerations

1. Ensure that sensitive equipment is protected adequately. The criticality of the asset should match the level of protection given. Protection mechanisms may include things such as padlocks, fenced off areas, and security guards. Assets should also be monitored using CCTV to assist with investigation.
2. Ensure that there is a well-defined list of what each asset is responsible for. This will ensure that if an asset is compromised, there is an understanding of where an attacker could reach and the impact that they may have.
3. If possible, segregate any publicly accessible assets to a secure part of the network with increased monitoring.
4. If an asset is deemed to be compromised, physical teams should move to secure the asset and assess the asset for signs of any physical tampering.
5. If the attacker has not been caught, protection over other physical assets in the area should be increased.
6. Outgoing connections from the compromised asset should be monitored and contained until the asset can be restored to a "known good" state.
7. Once the above steps have been considered, the main flow should be followed, and appropriate steps taken.

# Appendix B - IOC List, Typical Forensic Artefacts and Contextual Information Requirements

## Indicators of Compromise

Indicators convey specific observable patterns combined with contextual information intended to represent artefacts and/or behaviours of interest within a cyber-security context. They consist of one or more observable patterns potentially mapped to a related Tactic, Technique or Procedure (TTP).

The following is a non-exhaustive list of Indicators of Compromise (IOC's) to be leveraged during Incident Response (IR) investigations:

- IP Addresses
- File Hashes (MD5, SHA1, SHA256 etc.)
- URLs
- URIs
- Domain Name
- Domain Registrant Information
- Virus Signatures
- File Name
- Autonomous System Number (ASN)
- User Defined Input (usernames, passwords etc.)
- User Agents (UAs)
- Unique / Identifiable Strings
- Network Traffic patterns
- Any item of intelligence that can directly indicate suspicious activity

## Typical Forensic Artefacts

The following list details typical forensic artefacts that may be of interest during an investigation:

- Operating System Logs (Windows Event Logs, syslog, etc.)
- Application Specific Logs
- Application Configuration Files
- Operating System configuration files
- Windows Registry Files
- Deleted Files / Recycle Bin Contents

- User Specific folder files
- Internet History Databases
- Email storage files (ost, mbox etc.)
- Application Data folder
- Temporary folders
- Hibernation files
- Page files
- Crash Dumps
- Server Management Logs
- Networking Details

## Contextual Information Requirements

During any incident, analysts should aim to identify the following background information. This will assist with ongoing investigation, analysis, time lining, containment and remediation:

- Asset location (if a fixed location or virtual host)
- Asset owner / custodians
- Operating system version and patch levels
- Asset role (such as whether it is used for key business or administrative tasks)
- Related assets (such as other partners in clusters, upstream and downstream servers in common application deployment, etc.)
- Authorized service accounts and other server credentials
- Network and system configurations
- Installed applications
- Running processes
- Known vulnerabilities
- Current incident and problem tickets
- Recent changes as well as approved current and future changes

Using the directory platform, gather additional information about the affected asset owners, custodians and/or user(s). This should include:

- Roles
- IDs and other credentials
- Privileges
- Locations