Server Intrusion Process Flow

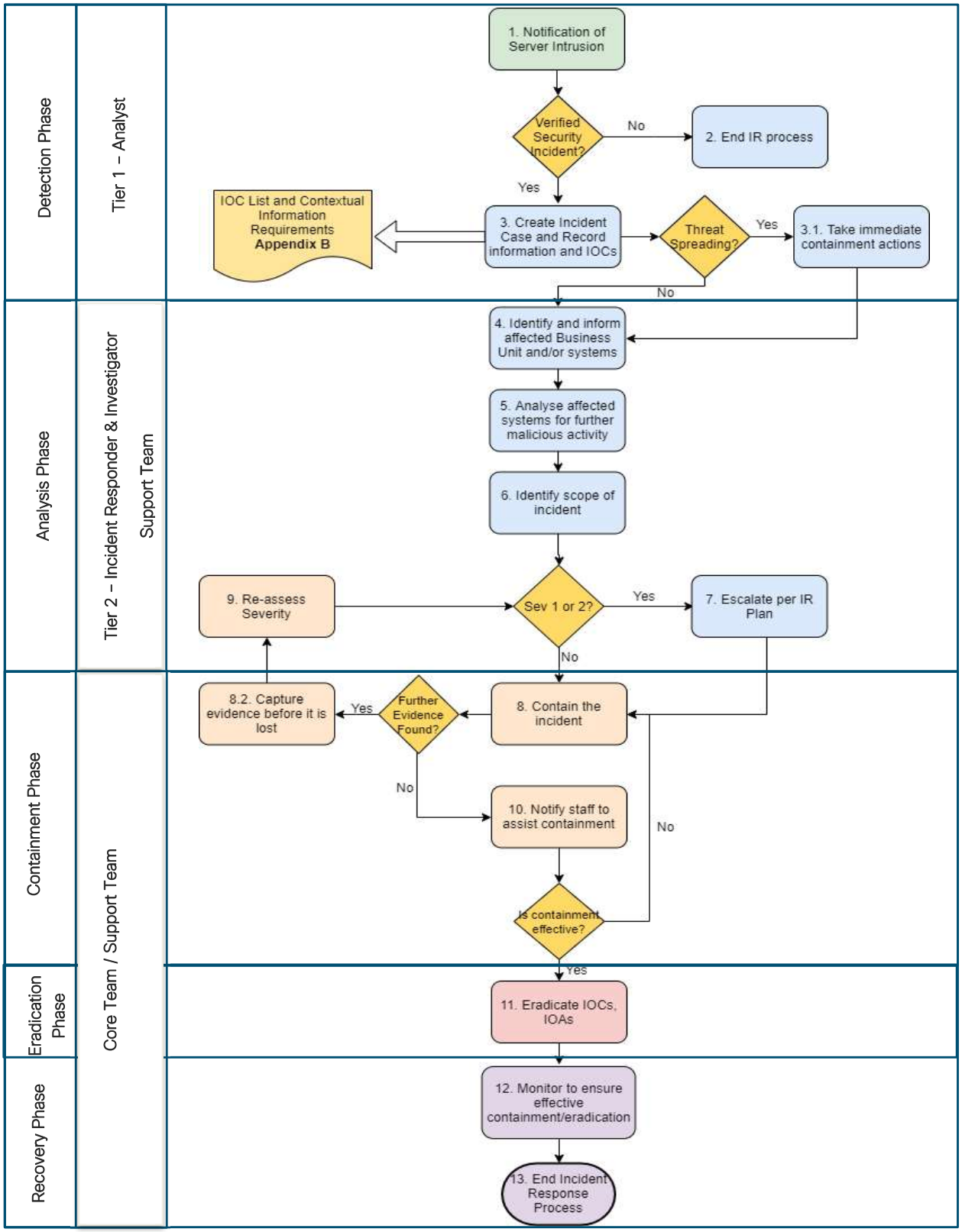
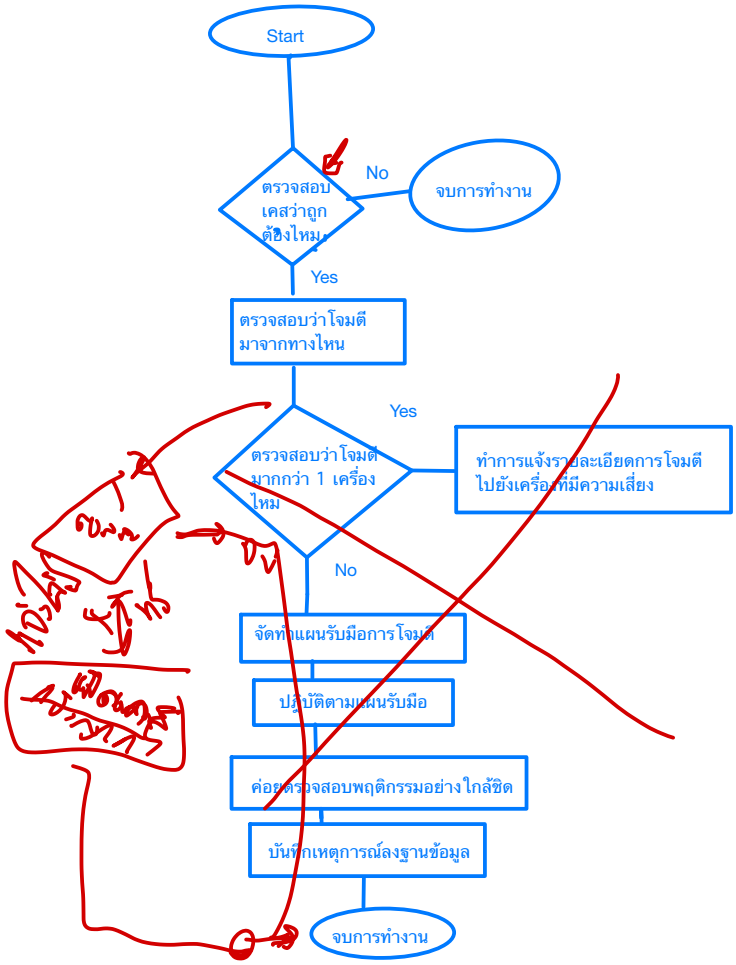
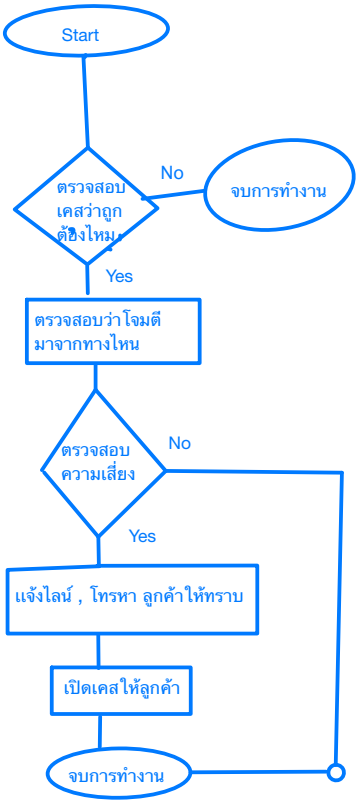


Figure 1: Server Intrusion Process Flow


Start
ตรวจสอบเคสว่าถูกต้องไหม
No
จบการทำงาน
Yes
ตรวจสอบว่าโจมตีมาจากทางไหน
ตรวจสอบว่าโจมตีมากกว่า 1 เครื่องไหม
Yes
ทำการแจ้งรายละเอียดการโจมตีไปยังเครื่องที่มีความเสี่ยง
No
จัดทำแผนรับมือการโจมตี
ปฏิบัติตามแผนรับมือ
ค่อยตรวจสอบพฤติกรรมอย่างใกล้ชิด
บันทึกเหตุการณ์ลงฐานข้อมูล
จบการทำงาน


Start
ตรวจสอบ
เคสว่าถูก
ต้องไหม
No
จบการทำงาน
Yes
ตรวจสอบว่าโจมตี
มาจากทางไหน
ตรวจสอบ
ความเสี่ยง
No
Yes
แจ้งไลน์ , โทรหา ลูกค้าให้ทราบ
เปิดเคสให้ลูกค้า
จบการทำงาน

Step 1 ตรวจสอบว่า เคสที่เด้งเข้ามานั้นถูกต้องหรือไม่ หากใช่ให้ดำเนินการต่อใน Step 2 หากไม่ใช่ให้หยุดการทำงาน

Step 2 ควรตรวจสอบการโจมตี phishing ว่ามาจากที่ไหน ได้แก่ภายในบริษัท, ภายนอก, หรือจากผู้ใช้งานที่ได้รับอนุญาตหรือไม่ เพื่อเสริมสร้างความปลอดภัยและป้องกันการละเมิดข้อมูลของลูกค้าของคุณ นอกเหนือจากนี้, คุณควรตรวจสอบลิงก์ที่มีความสุขลักษณะเพื่อป้องกันการตกอยู่ในกล trap และแนะนำให้พนักงานทุกคนเข้าใจถึงความเสี่ยงและวิธีการป้องกัน phishing attacks อย่างสม่ำเสมอ

Step 3 ตรวจสอบว่ามีความเสี่ยงหรือไม่ หากตรวจสอบแล้วพบว่าไม่มีความเสี่ยงที่สูงมากก็ให้หยุดการทำงานได้เลย

Step 4 หากพบว่ามีความเสี่ยงจากการโจมตี, ควรทำการแจ้งเตือนทันทีผ่านช่องทางที่รวดเร็ว เช่น ไลน์ หรือโทรหาลูกค้า เพื่อให้ทราบถึงปัญหาและดำเนินการเพื่อป้องกันความเสี่ยงอย่างทันที

Step 5 ทำการเปิดเคสเพื่อแจ้งรายละเอียดกับลูกค้า เพื่อให้ลูกค้าตรวจสอบย้อนหลังถึงปัญหาที่เกิดขึ้น

Unauthorized Access Process Detail

Step	Action	Performer	Details	Notes
1	Notification of Server Intrusion	Tier 1 - Analyst	☐ Receive a notification of Server Intrusion ☐ USE CASE: INSIDER THREATS / PERSISTENCE / DATA EXFILTRATION / PHYSICAL UNAUTHORIZED ACCESS o If any of these above use cases are suspected, consult Appendix A ☐ Collect basic information about the incident o Time that the incident was reported o How the incident was reported o Current impact of incident o Systems involved o Any remediation actions taken ☐ Ensure access to incident ticket and incident log are granted ☐ 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 and record contextual data and IOCs. ☐ Review security logs of applicable devices ☐ Review identified user accounts for permissions, changes and recent activity ☐ Understand affected system(s) and the potential motive for unauthorized access ☐ Review network connectivity of affected systems and subsequent access available ☐ Log any of the IOC's that have previously been identified (or analysis has provided) to the Incident Log	IOC List at Appendix B
3.1	Take immediate containment actions	Tier 1 – Analyst	☐ If there is an immediate need and the threat is seeing spreading, block any connections related to the initial notification and analyse them for suspicious behaviour ☐ If there is an immediate need, enforce password resets for involved user accounts ☐ If there is an immediate need, consider internal network controls that may be used ☐ Log all actions within Incident Log	Blocking connections and containing an incident before it has been fully scoped can reveal information to the attacker, causing them to change their attacking strategies. This action may necessitate the assistance of various Departments, such as Network & Datacentres Team, Server Team, etc.
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	IPAM DHCP AD

			☐ Using identified usernames determine potentially impacted business units through active directory ☐ Identify the affected business unit by location of the device or by hostname mapping ☐ Inform the Business unit of the imminent threat, include only relevant information in the communication ☐ The **escalation procedure** defined in the **IR Plan** shall be followed.	Hostname Maps
5	Analyse affected systems for further malicious activity	Tier 2 – Incident Responder & Investigator	☐ Analyse network traffic, logs, etc. for any activity that could indicate traversal through the network ☐ Determine if the attacker has deployed any malicious code o Ensure that malicious code is detected by anti-virus systems ☐ Generate any IOCs that show unauthorized user activity ☐ Log actions in incident log	Review Appendix B for list of IOCs

6	Identify scope of incident	☐ Tier 2 – Incident Responder & Investigator ☐ Support Team	☐ Deploy known indicators to IDS/IPS systems ☐ Search the enterprise for similar activity utilizing the available IOCs. ☐ Add all available details of observed activity, affected systems and utilised tools to incident log ☐ Implement monitoring of systems being manipulated in an unauthorized fashion ☐ Search the enterprise for similar activity utilizing the available IOCs. ☐ Log actions in incident log.	Test new signatures before production deployment Multiple departments from the Support team (IT) might need to be engaged for assisting with this step.
7	Escalate Per IR Plan	Tier 2 – Incident Responder & Investigator	☐ In the case that the Severity of an Incident is classified as Severity 1 or Severity 2 follow the escalation process as part of the IR plan to involve the relevant parties to remediate the incident.	

8	Contain the Incident	Tier 2 – Incident Responder & Investigator Support Team	Disable network access at switches and routers on the systems or choke points that display IOCs or other malicious traffic Block identified malicious Domains and IPs being contacted. Block identified External IPs performing inbound communications. Block specific network traffic based on port / application Implement patches required to close lateral movement options Determine if similar systems have been accessed without authorization Check for similar behaviour from other user accounts / systems. Reduce access to systems through authentication mechanisms / active directory permissions. Log all actions to incident log	
8.2	Capture evidence before it is lost	Tier 2 – Incident Responder & Investigator	In the case that further evidence / artefacts (e.g. IOCs) are identified, they need to be captured and recorded before they are lost. Where specialist assistance is required consider calling out specialist Incident Response providers via Incident Manager Where appropriate preserve network log information	Artefacts: Web Proxy Logs VPN Logs Firewall Logs Memory dumps DNS requests Processes

			☐ Gather relevant files and artefacts that could assist the investigation ☐ Store artefacts within Incident Folder ☐ Log actions in incident log	Loaded drivers Executed Commands
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.	
10	Notify staff to assist containment	Tier 2 – Incident Responder & Investigator	☐ (Optional) Request Service Desk to inform staff of an increased risk and request reports of suspicious activity to be communicated back to the Service Desk ☐ The **escalation procedure** defined in the **IR Plan** shall be followed. ☐ Log notification to incident log	
11	Eradicate IOCs	Support Team	☐ In the case that the threat is successfully contained, the resolver group can proceed with the eradication of the threat / incident. ☐ Inform resolver group that systems are required to be rebuilt (e.g. Server team, Networks and Datacentre team, etc.) ☐ (Optional) Confirm to resolver group if rebuilt devices can be immediately re-introduced into the environment ☐ Recover data from backups where integrity is questioned	

			☐ Log notification in incident log	
12	Monitor to ensure effective containment/eradication	SOC Team	☐ Monitor any systems, user accounts, Servers being re-deployed for an appropriate period to ensure no indicators of intrusions return and to confirm the containment and eradication has been successful. ☐ If further suspicious activity is identified, implement further containment and remediation ☐ Log all actions in incident log	
13	End Incident Response Process	Tier 2 – Incident Responder & Investigator	☐ Log / store all remaining information and artefacts in the incident folder ☐ Notify Incident Manager of completion of Incident Response process ☐ If Post Incident Review (PIR) is required refer to PIR Playbook ○ Carry out a Post Incident Review if required ○ PIR is required where an incident is a Severity 1 or Severity 2	

Appendix A - Specific Use Case

Insider Threats

Insider Threats can be very damaging to an organisation. Methods of controlling and managing the damage insider threat can cause often lies with internal firewalls and access control devices. Insiders have more knowledge about the layout of a network and as a result can be a lot more targeted with their attacks. Depending on the level of access that an insider has, they may be more effective at covering their tracks, or employing social engineering techniques to further assist in their goals.

From an incident response perspective, managing an insider threat can be very challenging. As well as having knowledge of the network, an insider also has physical access to buildings, equipment, and other employees. They may be able to use this to their advantage to obtain other users' credentials to disguise their activities. As the insider has legitimate access to resources, it can be a lot harder to detect.

From a business perspective, there are considerations to be made in terms of notification of suspicious activity. Human Resource processes must be considered before accusations are made or removal of staff from systems / areas is acted upon.

Special Considerations

1. If the identity of the insider is unknown, be wary of any internal communications that could give the insider information.
2. Ensure all HR processes are adhered to.
3. Evidence collection should be conducted with a view that it may be used in employment dispute processes and must be admissible as evidence.
4. If the insider is located inside an organizational building, ensure that he cannot physically access any equipment or systems.
5. Pay special attention to the systems and activity of disgruntled employees as this may be an indicator of potential malicious activity. Employees have been known to leave "Logic Bombs" – malicious code that only executes after the employee leaves the organization.
6. Insiders may be more likely to try and physically remove data from an organization. Special attention should be paid to logs that indicate exfiltration of data onto removable media.

Persistence

An attacker who wishes to maintain access onto the network may utilize some method of persistence. This could range from specific malware that the attacker can remotely control, to creating new user accounts in VPN systems. Methods of persistence can be easy to miss in the initial response to an investigation, as they may not immediately be used. An attacker may wait days or even weeks before utilizing a persistence mechanism in order to try to remain undetected.

Special Considerations

1. Systems that the attacker has traversed through should be closely examined for any persistence mechanisms that may have been used. This may include things such as:
    a. New user accounts
    b. Scheduled Tasks / 'cronjobs'
    c. Malware / Unknown Software
    d. WMI subscriptions
    e. Registry Entries
    f. Outlook rules

Data Exfiltration

One of the goals of an attacker who has gained unauthorized access to an organisation's systems may be data exfiltration – the removal of data from the network. This can happen over the network (uploading to an external site) or physically (transferred to USB and removed from a [redacted] site). The exact method of data exfiltration will depend on the size of the files being transferred and how stealthy the attacker wishes to be.

Special Considerations

1. Be aware of common data exfiltration channels and monitor unusual requests using these methods:
    a. HTTP/S
    b. FTP/SFTP
    c. Email
    d. Cloud Services
    e. RDP
    f. WhatsApp / Signal / Telegram
    g. IRC
2. Consider using DNS Blacklisting / Whitelisting to prevent traffic reaching malicious domains
3. Establish a baseline of normal outbound traffic – this will allow you to more easily discover something that appears out of the ordinary and should be investigated

4. Although data may be encrypted, monitoring the size of data being transferred and any relevant metadata available it may be possible to establish if the traffic is suspicious or not.
5. Consider reviewing identified device logs / Data Loss Prevention (DLP) systems for suspicious activity

Physical Unauthorized Access

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 unauthorised access. Depending on the segregation that is present in the network, this may allow an attacker 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:

- Dates and Times of reported suspicious activity
- Affected persons views on the suspicious behaviour
- Actions taken immediately prior to the initial incident
- Actions taken immediately after the initial incident
- Affected systems roles
- Critical business data stored on or associated with affected systems
- Normal working behaviour of affected systems
- Normal working behaviour or affected business unit and personnel
- Other recent incidents affecting the same or similar systems
- Historical incidents similar to ongoing issue
- Time sensitivity / downtime issues likely to impact decision making