Unauthorized Access Process Flow

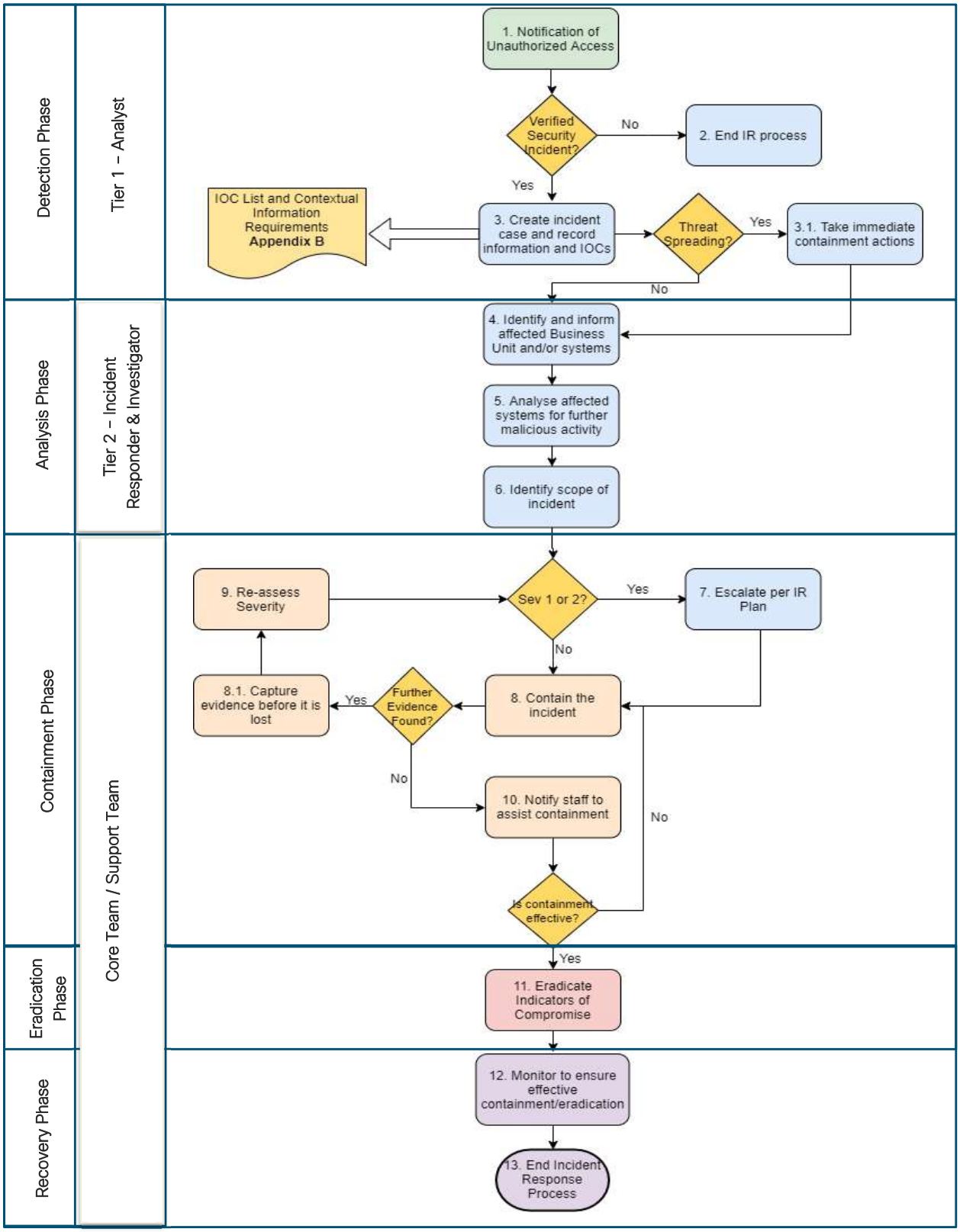
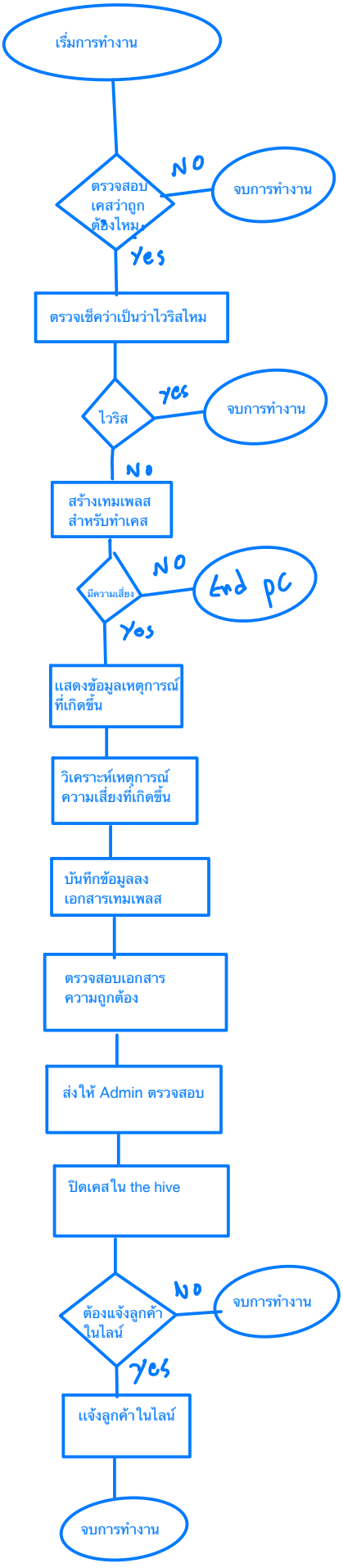


Figure 1: Unauthorized Access Process Flow


เริ่มการทำงาน
ตรวจสอบเคสว่าถูกต้องไหม
NO
จบการทำงาน
Yes
ตรวจเช็คว่าเป็นว่าไวริสไหม
ไวริส
yes
จบการทำงาน
NO
สร้างเทมเพลสสำหรับทำเคส
มีความเสี่ยง
NO
End pc
Yes
แสดงข้อมูลเหตุการณ์ที่เกิดขึ้น
วิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น
บันทึกข้อมูลลงเอกสารเทมเพลส
ตรวจสอบเอกสารความถูกต้อง
ส่งให้ Admin ตรวจสอบ
ปิดเคสใน the hive
ต้องแจ้งลูกค้าในไลน์
NO
จบการทำงาน
Yes
แจ้งลูกค้าในไลน์
จบการทำงาน

Step 1 ตรวจสอบว่า เคสที่เด้งเข้ามานั้นถูกต้องหรือไม่ หากใช่ให้ดำเนินการต่อใน Step 2 หากไม่ใช่ให้หยุดการทำงาน

Step 2 ตรวจสอบว่า Alert ที่เข้ามานั้นเป็นไวริสของลูกค้าหรือไม่ ตรวจเช็คจาก process update หรือ ไฟล์ Whilelist หากเป็นไวริสให้หยุดการทำงานหากไม่ใช่ให้ดำเนินการต่อ Step 3

Step 3 ตรวจสอบว่า พฤติกรรมที่ Alert เข้ามาเป็นการใช้งานปกติหรือไม่ หากปกติให้จบการทำงาน หากไม่ปกติให้ดำเนินการต่อใน Step 4

Step 4 สร้าง Template สำหรับเคสที่จะทำการเปิด

Step 5 นำข้อมูลที่ค้นมาจาก Splunk และรูปลงใน Template ตามช่องที่ให้ใส่ข้อมูลตามที่ได้กำหนดไว้

Step 6 ตรวจสอบความถูกต้องของข้อมูลและทำการส่งให้ Admin ตรวจสอบอีกรอบเพื่อทำการแจ้งให้ลูกค้าทราบ

Step 7 ทำการปิดเคสใน The Hive เมื่อทำการส่งให้ admin ตรวจสอบแล้วให้นำข้อมูลนี้ไปใส่ใน The Hive แล้วแจ้งว่าใครเป็นคนทำเคสนี้

Step 8 ตรวจเช็คว่าต้องแจ้งลูกค้าหรือไม่ หากเราเปิดไปแล้ว ถ้าต้องแจ้งลูกค้าให้ทำการแจ้งลูกค้า แต่หากไม่ต้องแจ้งให้รอการตอบกลับของลูกค้าเพื่อดำเนินการปิดเคสในภายหลัง

Unauthorized Access Process Detail

Step	Action	Performer	Details	Notes
1	Notification of Unauthorized Access	Tier 1 - Analyst	☐ Receive a notification of Unauthorised Access ☐ USE CASE: INSIDER THREATS / PERSISTENCE / DATA EXFILTRATION / LATERAL MOVEMENT / AUTOMATION/SCRIPTED ACTIVITY / FAILED LOGIN SPIKE / CREDENTIAL STUFFING / 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. ☐ Review security logs of applicable devices / user accounts ☐ 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) into the Incident case	IOC List at Appendix B
3.1	Take immediate containment actions	Tier 1 – Analyst	**External** ☐ If there is an immediate need (such as data exfiltration), 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 ☐ 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 how they are attacking.
			Internal ☐ If there is an immediate need, block any connections related to the initial notification and analyse them for suspicious behaviour ☐ If there is an immediate need, consider internal network controls that may be used	This action may necessitate the assistance of various Departments, such as Server Team, etc.

			☐ If there is an immediate need, temporarily disable any involved user accounts ☐ If unauthorised access was to a specific resource and there is an immediate need, ensure this has been disabled ☐ If the user is located inside [redacted] premises and there is an immediate need, ensure they cannot physically access systems ☐ Log all actions within Incident Log	
4	Identify and inform affected Business Unit and/or systems	Tier 1 - Analyst	☐ If an IP address is available search systems to identify device location ☐ 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 When informing Business Units in the case of external or internal attackers consider the following: **External** ☐ 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. **Internal** ☐ Be cautious that any internal communication does not give any information to an inside threat. ☐ This action should be **approved** by the **SOC** and **CSIRT head**.	IPAM DHCP AD Hostname Maps

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 ☐ Determine if the unauthorized user has deployed any malicious code (ensure that anti-virus system can detect the malicious code) ☐ Generate IOCs that show unauthorized 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	**<u>External</u>** ☐ 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 ☐ Log actions in incident log **<u>Internal</u>** ☐ 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 Severity 1 or Severity 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 ☐ Support Team	**<u>External</u>** ☐ 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 ☐ Log all actions to incident log	
			<u>Internal</u> ☐ Determine if similar systems have been accessed without authorization ☐ Check for similar behaviour from other user accounts ☐ Reduce access to systems through authentication mechanisms / active directory permissions ☐ If the user is located inside KTB premises, ensure they cannot physically access systems ☐ Log all actions to incident log	

			Internal ☐ Disable email access of user ☐ Review user's email for malicious content and/or suspicious activity ☐ Log actions in 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. ☐ Where specialist assistance is required consider calling out specialist Incident Response providers via Incident Manager ☐ Where appropriate preserve network log information ☐ Gather relevant files and artefacts that could assist the investigation ☐ Store artefacts within Incident Folder ☐ Log actions in incident log	Artefacts: Web Proxy Logs VPN Logs Firewall 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	**External** ☐ (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 ☐ Log notification to incident log ☐ The **escalation procedure** defined in the **IR Plan** shall be followed.	
			Internal ☐ Consider if social engineering is an aspect ☐ Be wary of informing users who may be colluding with each other	
11	Eradicate Indicators of Compromise	Support Team	**External** ☐ Utilize resolver groups to implement the rebuilds / replacement systems ☐ Reset any user accounts affected ☐ Block network connections ☐ Control deployment via IT-Ops to ensure effective monitoring can occur	
			Internal ☐ Utilise account team to ensure that account rights are revoked. ☐ Malicious users are revoked their physical and online access to KTB machines.	

12	Monitor to ensure effective containment/eradication	SOC Team	**External** ☐ Monitor systems being re-deployed for an appropriate period to ensure no indicators of Unauthorized Access 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	
			Internal ☐ Monitor re-activated user accounts for an appropriate period to ensure no indicators of Unauthorised Access return and confirm the containment and eradication has been successful ☐ Facility management to monitor for unauthorised access by the malicious insider. ☐ 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	☐ Notify Incident Manager of completion of Incident Response process ☐ Log / store all remaining information and artefacts in the incident folder ☐ If Post Incident Review (PIR) is required refer to PIR Playbook o 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 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

Lateral Movement

Lateral Movement involves an attacker traversing across a network as opposed to into a network. They may not get deeper access into the organization, however lateral movement can increase the spread of persistence mechanisms, make it harder to contain the malicious user and give the attacker access to other systems or information that would be deemed inappropriate.

Special Considerations

1. Perimeter network devices will not reveal lateral movement; look at intra-network devices instead.
2. Identify internal traffic that allows analysts to review internal activity and spot anomalous traffic patterns and high-volume data transfers.
3. Network Segmentation can help identify unauthorized access. For example, when source IPs from user device areas are entering into areas that are typically allocated to servers. This activity should be considered potentially suspicious.
4. Multiple authentication of a user onto multiple systems can be an indicator of lateral movement, being logged in to many devices would not be a standard activity for many employees.

Automation / Scripted Activity

Attackers may utilize automation during their attacks as a method of reducing mistakes and speeding up their activities. Automation and Scripts can also be a cause for concern if used by mistake on the network, leading to false signs of unauthorized access.

Special Considerations

1. Look for signs that indicate activity was not performed by a human. This may include things such as unfeasible response times, rapid commands / authentication attempts being executed in succession, and activity being repeated exactly on many systems.
2. Scripts that have been used may be left on a system. If these can be recovered, it may prove valuable to examine these.
3. Some attackers may use a "low and slow" approach to gain unauthorized access rather than high speed brute force. This is in order to provide a level of stealth, however these can still be identified through patterns in terms of usernames being used and distinct timing gaps (i.e. one event every 10 seconds). Just be aware however, these patterns are easily manipulated.

Credential Stuffing

The automated use of harvested credentials for log in attempts is also known as credential stuffing. This may take place over a short period of time or may be spread out over several weeks in order to reduce chance of detection as highlighted in the Automation / Scripted Activity scenario above. The main issue with Credential Stuffing is the use of legitimate credentials, which makes the activity harder to distinguish from normal activity.

Credential Stuffing will typically utilise tools to ensure the attack can leverage the large datasets at the pace required. These tools can be extremely customizable and allow changes to areas of the traffic that would typically provide IOCs such as User Agents. It is however, dependant on the attacker's motivation, skillset and operational security whether these settings are adjusted to provide the level of stealth required.

Identifying a pattern of any description that can identify suspicious traffic from normal traffic is the key to blocking credential stuffing attacks.

Special Considerations

1. Consider blocking traffic from a single source showing multiple failed log in attempts using multiple different usernames.
2. Investigate SSL handshakes to help identify abnormal behaviour in terms of handshake negotiation, tools used for credential stuffing can offer more available cipher suites for negotiation than standard browsers.
3. If the source of the credentials (i.e. a leaked third-party database) can be identified, consider instructing affected users to change their password as soon as possible. If the source of the credentials is unknown, it may be worth initiating this across all user accounts.
4. Credential stuffing will likely lead to a spike in failed login attempts due to users not being found. This can be a clear indicator of an attempt at credential stuffing.

Failed Login Spike

Detection of this attack is similar to credential stuffing above. Many failed log in attempts will be seen. This may originate from just one IP address as a lone attacker, or from many as a distributed brute force attack.

Special Considerations

1. Consider implementing controls that can throttle login attempts, for example:
    a. 1 failed attempt = 5 second delay
    b. 2 failed attempts = 15 second delay
    c. 3+ failed attempts = 45 second delay
2. Temporarily block any identified sources that have shown multiple failed logins.
3. Always consider the business impact of blocking traffic that could damage business.

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