Data Leakage Process Flow

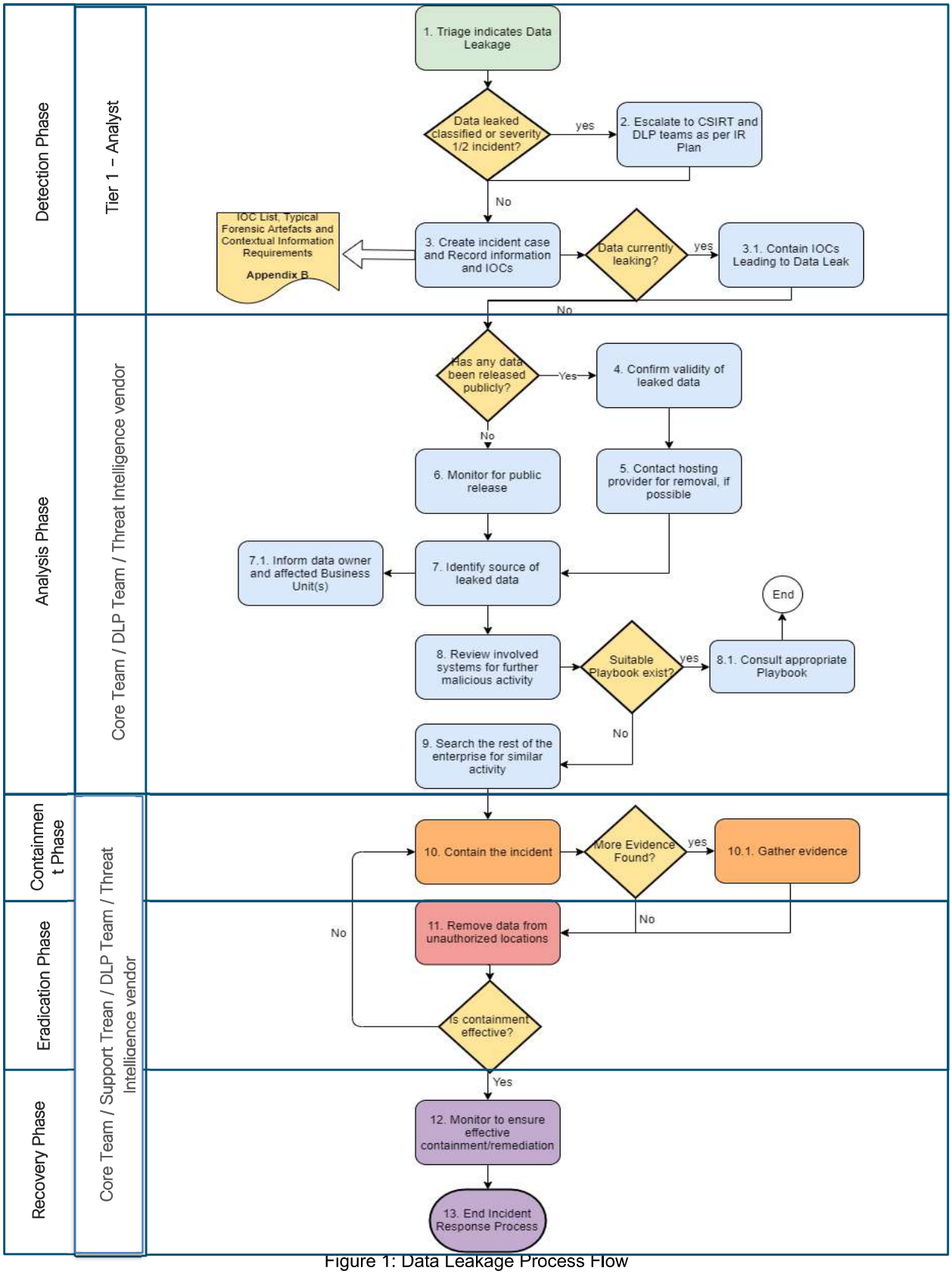
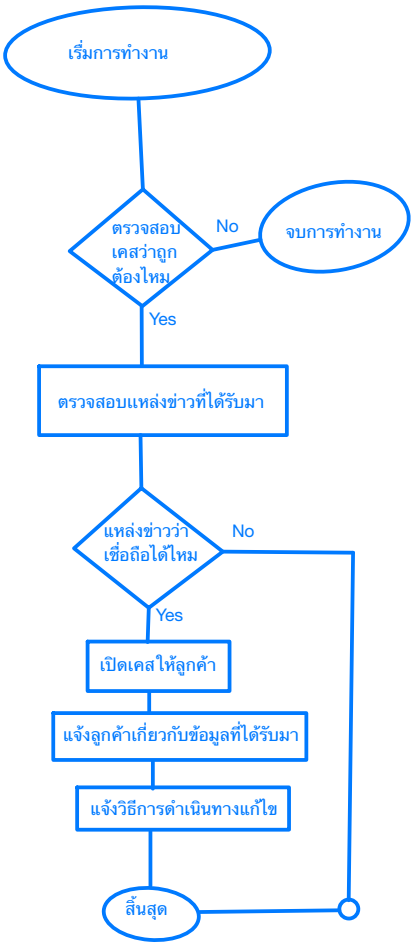


Figure 1: Data Leakage Process Flow


เริ่มการทำงาน
ตรวจสอบเคสว่าถูกต้องไหม
No
จบการทำงาน
Yes
ตรวจสอบแหล่งข่าวที่ได้รับมา
แหล่งข่าวว่าเชื่อถือได้ไหม
No
Yes
เปิดเคสให้ลูกค้า
แจ้งลูกค้าเกี่ยวกับข้อมูลที่ได้รับมา
แจ้งวิธีการดำเนินทางแก้ไข
สิ้นสุด

Step 1 ตรวจสอบว่า เคสที่เด้งเข้ามานั้นถูกต้องหรือไม่ หากใช่ให้ดำเนินการต่อใน Step 2 หากไม่ใช่ให้หยุดการทำงาน

Step 2 ตรวจสอบจากแหล่งข่าวที่ได้รับมาว่ามากจากไหน เช่น Website Facebook Telegram

Step 3 ตรวจสอบว่าแหล่งข่าวที่ได้รับมานั้น มีความน่าเชื่อถือ มากแค่ไหน เช่น เป็นแหล่งข่าวจากเว็บไซต์ที่มีความน่าเชื่อถือ ข้อมูลของข่าวนั้นมีความถูกต้องมากแค่ไหน วันเวลาที่ข่าวนั้นได้แพร่กระจายออกมา หากแหล่งข่าวนั้นไม่มีความน่าเชื่อถือให้หยุดการทำงาน

Step 4 ให้ทำการเปิดเคสเพื่อแจ้งลูกค้าให้ทราบถึงข้อมูลที่ได้รับมา และ แจ้งลูกค้าเกี่ยวกับที่อาจเป็นความเสี่ยงต่อลูกค้า

Step 5 แนะนำเสนอแนวทางการตรวจสอบและแก้ไขปัญหา หากลูกค้ามีความเสี่ยง และ ค่อยตรวจสอบพฤติกรรมอย่างใกล้ชิด

Data Leakage Process Detail

Step	Action	Performer	Details	Notes
1	Triage Indicates Data Leakage	Tier 1 - Analyst	☐ Become familiar with the background and context of the incident by ingesting the detail within the triage report ☐ Ensure access to incident ticket and incident folder are granted ☐ USE CASE - LOST OR STOLEN DEVICE, PHYSICAL DATA LEAKAGE, THIRD PARTY DATA LEAK, SENSITIVE DATA IN INAPPROPRIATE LOCATIONS: ○ Consult Appendix A if any of the above scenarios are suspected ☐ Update Incident Ticket	
2	Escalate to CSIRT and DLP teams as per IR Plan	Tier 1 - Analyst	☐ In the case that the data leaked is believed to be classified or the severity of the incident is 1 or 2, imiddiately inform the DLP and CSIRT team to verify and identify the source of the data leaked. Assistance from the affected BU(s) might be needed. ☐ Update the incident details including the reasons and conclusion on why this is classified information.	
3	Create incident case and Record information and IOCs	Tier 1 - Analyst	☐ Create a security incident case and record contextual data and IOCs. ☐ Collect and analyse all information currently availabe including background context and IOCs ☐ 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	Contain IOCs Leading to Data leakage	Tier 1 – Analyst	☐ If it is determined that classified information is currently being exfiltrated out of the organisation, ensure that any suspicious network connections are blocked immediately ○ Look for unique indicators that can be used to block traffic, such as: ▪ Port ▪ Protocol ▪ IP address ▪ URI ▪ Application ▪ Source/Destination domain ▪ Geolocation ☐ Examine DLP System configuration and logs. ☐ Change DLP detetion and enforcement policies if needed on the DLP System. ☐ Log details in incident ticket	The assistance of the members of the support team can be crucial on this stage. Such members are the onsite team, Server team and Networks and Datacenter team. Depending on the needs of the intial containment the appropriate team should be engaged.
4	Confirm validity of leaked data	• DLP Team • Tier 2 – Incident Responder & Investigator • Affected BU(s)	☐ Examine the data that has been leaked to confirm and verify if it came [redacted] and is of concern. ☐ In the case that the investigator is unsure whether the leaked data are of sensitive nature, the affected BU handling the leaked data should be consulted.	
5	Contact hosting provider for removal, if possible	• Threat Intelligence Vendor • DLP Team	☐ Where possible and appropriate, request a takedown of the leaked material / data via CSIRT and threat intelligence vendor, Group-IB.	Obtain advice from the Compliance and Legal Department for appropriate actions.

		• Tier 2 – Incident Responder & Investigator	☐ As per the **IR Plan** follow the **incident escalation procedure** when necessary.	
6	Monitor for public release	Threat Intelligence Vendor	☐ Contact external threat intelligence sources (e.g. Group-IB) to determine if any data has been posted publicly. The TI vendor should keep monitoring for any possible leaked data. ☐ Check common sites data leak sites (i.e. PasteBin, Twitter, etc.) for any suspected leaked data ☐ Inform external threat intelligence (e.g. Group-IB) of the data leak to search for any uploads of any leaked data	Once data has been posted publicly, even if it is removed, you should adopt the mind-set that all of that data is compromised.
7	Identify source of leaked data	• DLP Team • Tier 2 – Incident Responder & Investigator • CSIRT Forensic Investigator (if needed)	☐ If you can view the leaked data examine the structure and any unique traits that are present to identify the system involved ☐ Consider duplicate storage locations of leaked data, for example, backup locations ☐ If an IP address or hostname is available search systems to identify device location ☐ Identify the originating business unit by location of the device or by hostname mapping	IPAM DHCP AD Hostname Maps
7.1	Inform data owner and affected Business Unit(s)	• DLP Team • Tier 2 – Incident Responder & Investigator	☐ Inform the Business unit of the leaked data, include only relevant information in the communication ☐ Inform the team that deals with external communication so they can prepare a statement if necessary ☐ As per the **IR Plan** follow the **incident escalation procedure** when necessary.	Information to include: • Immediate Action they should take • Actions they should not take • Restrictions they may suffer

				because of the investigation • Point of contact within the Incident Team to report further concerns
8	Review involved systems for further malicious activity	• Tier 2 – Incident Responder & Investigator • CSIRT Forensic Investigator (if needed)	☐ Any systems that have been involved in the data leak should be examined for further malicious activity ☐ Where appropriate, ensure that the CSIRT head is updated ☐ Log all findings and actions to Incident Ticket	
8.1	Consult appropriate playbook	Tier 2 – Incident Responder & Investigator	☐ If is determined that there is further malicious activity occurring and a more suitable playbook exists consult that playbook for guidance ○ Of interest may be Unauthorised Access or Malicious Code	
9	Search the rest of the enterprise for involved systems	• DLP Team • Tier 2 – Incident Responder & Investigator	☐ Search the enterprise for involved systems utilising the available IOCs. ☐ Review communications and logs of systems involved to assist with determining the user that leaked the data ☐ Search for systems where the exfiltrated data may have been stored without authorisation before removal from the network ☐ Add all available details of identified systems to incident ticket ☐ Utilise process at section 4.1 to inform affected BU's where this differs from current situation.	• Consider both external attackers and insider threats

			☐ Where appropriate, ensure CSIRT team is updated ☐ Log all findings and actions to Incident ticket	

10	Contain the Incident	• DLP Team
		• Support team
			☐ Depending on the type of incident notify the appropriate department to assist with containment. Departments include, the Server team, Networks team, Applications team, on-site team, etc.
			☐ Ensure that the source of the data leak (user/system) has been isolated and access has been disabled
			  ○ This may be done by temporarily blocking user accounts, forcing a password reset, etc.
			☐ Physically remove any users from equipment that may be leaking information
			☐ Ensure that any unauthorised storage locations of sensitive data are no longer accessible
			☐ Block malicious/offending traffic based on specific attributes, such as:
			  ▪ Port
			  ▪ Protocol
			  ▪ IP address
			  ▪ URI
			  ▪ Application
			  ▪ Source/Destination domain
			  ▪ Geolocation
			☐ Inform relevant teams for responsible disclosure of leaked information
			☐ Where appropriate, ensure CSIRT team is updated	

			☐ Log all actions to incident ticket	
10.1	Gather evidence	☐ CSIRT Forensic Investigator ☐ Tier 2 – Incident Responder & Investigator ☐ Support team	☐ In the case that further evidence is found during the containment of the incident, ensure that are all well captured and recorded in a forensic sound manner. ☐ Tier 2 with the CSIRT Forensic investigator (where applicable) should be the primary lead of gathering the required evidence with the assistance of the relevant department(s) within the support team (on-site, Networks department, etc.). Where specialist assistance is required consider calling out specialist Incident Response providers via Incident Coordinator. ☐ Where specialist assistance is required consider calling out specialist Incident Response providers via Incident Coordinator ☐ 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 ticket	
11	Remove data from unauthorised locations	• Threat Intelligence Vendor • Support team	☐ In the case that the data is already leaked, the threat intelligence vendor (Group-IB) should take action to assist in taking it down, whereas if it is hosted on an internal system the appropriate support team should be invoked (e.g. onsite, Server team, Application team, etc.) ☐ Any locations that have been used to store any data without authorisation should be wiped of said data ☐ Where appropriate, ensure that the CSIRT team is updated ☐ Log actions in incident ticket	

12	Monitor to ensure effective containment / remediation	SOC Team	▯ In the case that containment was effective proceed to this step (recovery), otherwise go back to step 10 for further containment actions . ▯ The relevant support team(s) (e.g. onsite, Server team, Application team, etc.) involved in containment /remediation of the incident should monitor to ensure the complete eradication of the threat / incident. ▯ Monitor systems that were involved in the incident for an appropriate period to confirm that the containment has been successful. ▯ Alert resolver group(s) upon identifying further suspicious activity in order to implement further containment and remediation ▯ Log all actions in incident ticket	
13	End Incident Response Process	▯ Tier 2 – Incident Responder & Investigator	▯ Notify Incident Coordinator of completion of Incident Response process ▯ Log / store all remaining information and artefacts in the incident folder. This information shall be revised from the Incident Coordinator for approval. ▯ 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

Lost or Stolen Device

There is little an organisation can do to recover a device that is no longer in the physical control of the organisation. Lost devices may be easily found using location tracking technology and then recovered, however recovery is less likely in the case of stolen devices. The loss or theft should be reported to the local police – they will have a higher chance of recovering and returning a stolen device.

Special Considerations

1. If they are not already aware, report lost devices to the Service Desk.
2. Ensure device is reported to the authorities - if the device is recovered it may be returned.
3. If the device is running software that allows for location tracking, ensure that this is activated and information is passed to the relevant teams.
4. Monitor for attempted connections back to the organisation through compromised accounts.
5. Ensure that remote wiping software has been activated to remove any potentially sensitive data. Be aware that this will also prevent any future location tracking attempts.
6. Determine the details of what state the device was in when it was lost or stolen:
    - Was the device switched on or fully powered off (not in sleep/standby)?
    - Does the device utilise some form of encryption?
    - Was the device locked or unlocked?
7. Ensure that all passwords associated with the device and users of the device have been changed.
8. Determine the sensitivity of any information held on the device and increase awareness over potential incidents that may be caused as a result.

Physical Data Leakage

Data being leaked or exfiltrated physically is one of the primary methods that an insider will use to remove data from the organisation. Storage devices are getting increasingly smaller and can hold more data. These can easily be concealed when leaving an organisation and then accessed from another location. Personal devices such as mobile phones can also be used to exfiltrate data.

Special Considerations

1. Monitor controls that are in place that can detect transfer of data to removable media.
2. Identify where the user is that is exfiltrating data and remove any access as appropriate.
3. When the employee is located ensure that all removable media devices are seized - consult legal/HR throughout this process as personal devices may be involved that are outside the remit
4. Ensure that the chain of custody is maintained throughout the seizure process.

Third Party Data Leak

A third-party data leak occurs when a third party that is handling data experiences a breach and as a result, ata becomes compromised. Other than contractual requirements, there is little influence that have over how data is secured by the third party.

Special Considerations

1. Ensure that good communication is maintained between and third parties, such as the correct communication channels during incidents. If there are any breaches that could affec , notice should be provided as soon as possible however this is dependent on the third party notifying KTB.
2. Communications from third parties about suspected data breaches may come via unexpected routes such as Telegram, etc.
3. Advise third parties on appropriate security handling of data.
4. Conduct reviews or audits of third parties to ensure that they are handling and protecting data in a secure manner.
5. Work with the third party during a data breach – it is possible that they may be able to provide detail about the data that was at risk, allowing to take appropriate action.
6. Ensure that the appropriate containment steps on systems are taken as appropriate, such as password resets.
7. Third Party Intelligence sources are aware of critical supplier relationships however discuss with them the current situation to establish whether the third party in question are being monitored. Generate a watch list if this is not the case.

Sensitive Data in Inappropriate Locations

There are occasions when data may be leaked through non-malicious means. Data could be uploaded to cloud services by mistake or saved to inappropriate locations within the enterprise that may have weaker security controls. Although not malicious in nature, these incidents can put data at risk and highlight a failure in current processes to mitigate such actions.

Special Considerations

1. Review the location to identify access that is afforded by the current security controls.
2. Review access and who could access the inappropriately placed data.
3. Review access / audit logs to identify any users that may have interacted with the data.
4. Consider the placement of the data as potentially malicious. Data may be being aggregated to compress and extract from the organisation.
5. Does the new location of the data have any High Availability / Back Up systems that may have duplicated the data? If so, ensure these areas have the data removed.
6. Be aware that data may be moved to areas of "Shadow IT", systems that are not managed or maintained by administrators. This may introduce considerably larger concerns and risks.

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.)
- URL's
- URI's
- Domain Name
- Domain Registrant Information
- Virus Signatures
- File Name
- Autonomous System Number (ASN)
- User Defined Input (usernames, passwords etc.)
- User Agents (UA's)
- 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