Incident Response Playbook: Dark Web Breaches

kaspersky

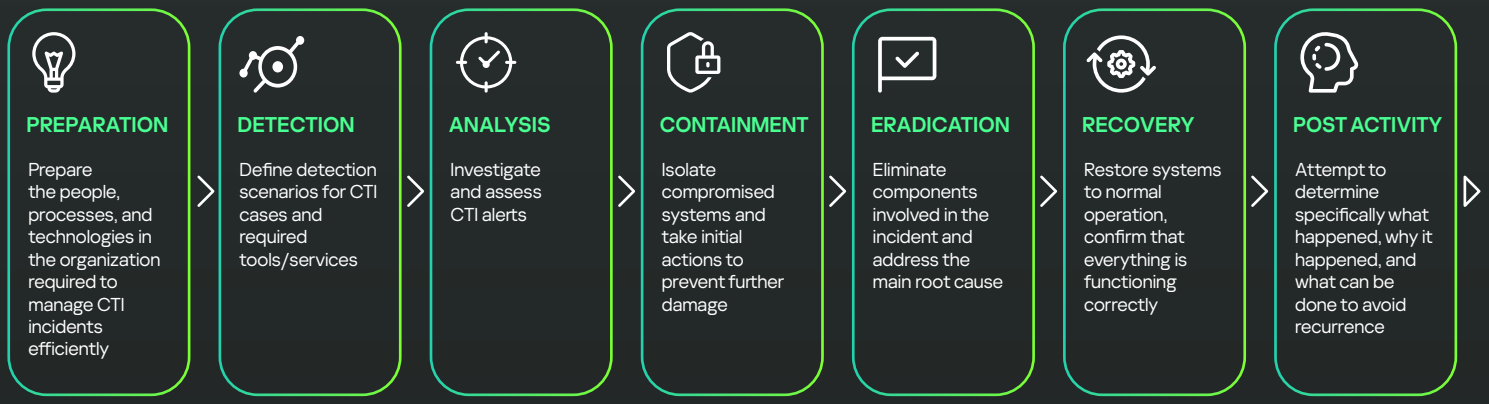
https://t.me/learningnets

Contents

https://t.me/learningnets

Introduction

Applying the widely-used approach to incident response from the NIST Framework, we can split the Dark Web monitoring lifecycle into seven stages, provided in the figure below.



In terms of incident management, Cyber Threat Intelligence (CTI) is considered to be a valuable source of information about potential incidents. Meanwhile, threat intelligence related to Dark Web findings includes additional steps for analyzing and verifying the found information, as well as evaluating the threat level.

After the incident is confirmed, the team can respond to the threat using the relevant IR playbooks. In this document, we will consider a Dark Web monitoring procedure involving these teams:

- CTI (Cyber Threat Intelligence)
- SOC (Security Operations Center)
- IR (Incident Response)

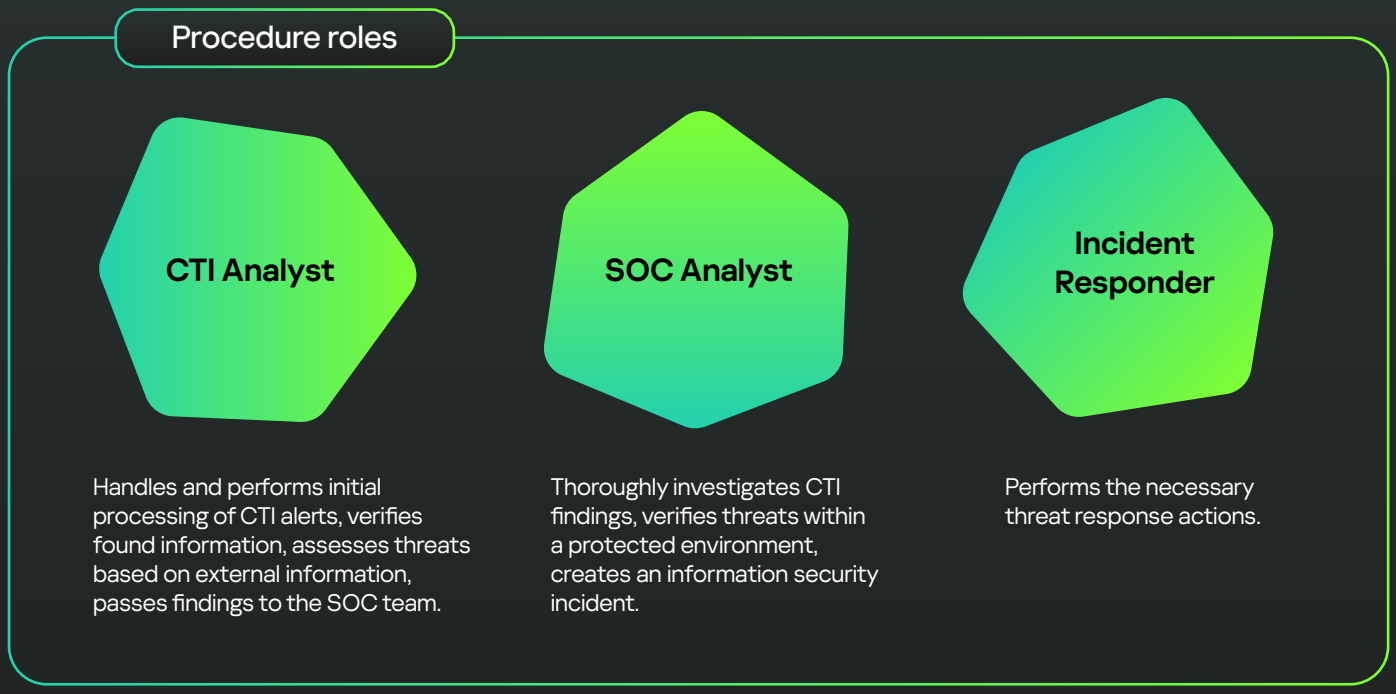
Depending on the structure of your cybersecurity team, these roles can be combined or split – but the overall procedure will stay the same.

When it comes to Dark Web monitoring, it's essential for companies to consult with legal experts and adhere to the laws and regulations applicable in their region. Additionally, transparent and ethical practices should guide the approach to cybersecurity and data protection. If you encounter any difficulties with a step, don't hesitate to reach out to experts specializing in Dark Web threats and incident response. You can continue progressing through the steps, but it's important to remember that seeking their assistance can help you address the threat more effectively.

https://t.me/learningnets

1. Roles and responsibilities

This procedure was developed as a reference for the following security roles:



RACI (Responsible, Accountable, Consulted, and Informed) matrix

Action	CTI	SOC	IR
Prepare and tune the detection mechanism	R	C	C
Handle and evaluate CTI alerts	R	I	I
Investigation	C	R	I
Containment	I	I	R
Eradication	I	I	R
Lessons learned	C	C	R

R — Responsible A — Accountable C — Consulted I — Informed

https://t.me/learningnets

2. Preparation

Set up monitoring of the Dark Web for information related to your company:

- Names of company/subsidiaries + partners/suppliers
- Shortened names/abbreviations
- Domains of the company/subsidiaries + partners/suppliers
- IP address ranges
- Industry/geolocation

Compile a list of relevant Dark Web resources where you will look for information.

Deploy infrastructure:

- VPN, Tor
- External virtual hosts for obtaining the data
- Register special accounts on forums for intelligence purposes, since some of the forums require an account, making it more difficult for law enforcement or researchers to access the resource and acting as an entry barrier to casual visitors

Or use solutions designed for such tasks, like Kaspersky Digital Footprint Intelligence.

https://t.me/learningnets

3. Detection

CTI detection usually involves sending an automatic alert when certain information is found on the Dark Web or in data dumps. The confidence of the alert can vary depending on its type.

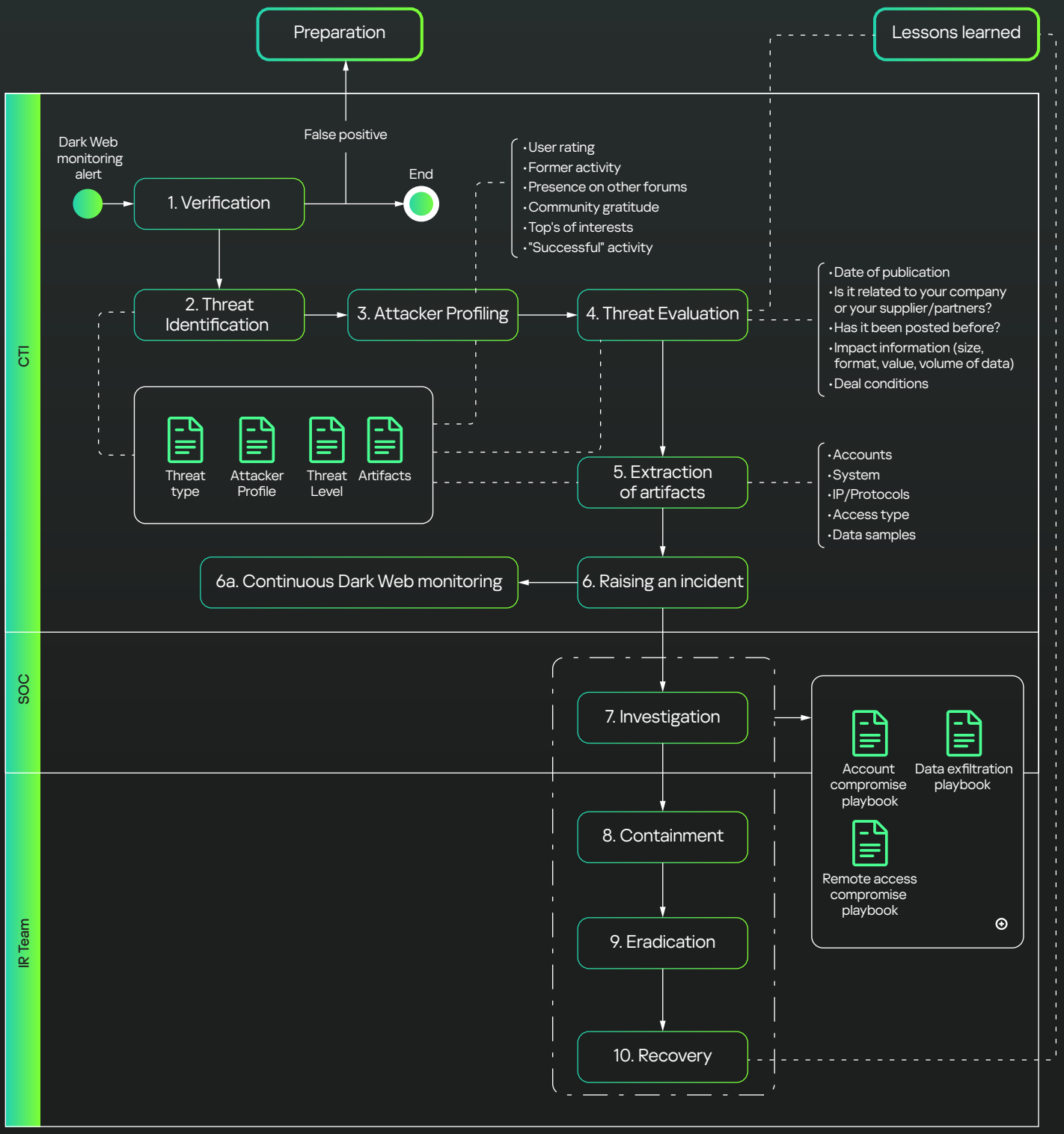
	Alert Type	Ways to Monitor Effectively
1	Company name mentioned on the Dark Web	Tracks mentions of the company name, abbreviations, or short names in target forums.
2	Company domain mentioned on the Dark Web	Tracks mentions of company domains in target forums.
3	Company domain mentioned in databases of compromised credentials	Tracks mentions of company account domains in dumps of compromised accounts.
4	Similar company profile mentioned on the Dark Web	Sometimes the malicious actor doesn't mention the exact name but rather gives some characteristics of the company (region/industry/size/revenue/system types) to hide their identity and activity.
5	Same as 1–4	Same set of alerts as above, but tracking your partners/suppliers/subcontractors/anyone else with access to your infrastructure.

Dedicated services for Dark Web monitoring, such as Kaspersky Digital Footprint Intelligence, can monitor all the alert types mentioned in the table.

https://t.me/learningnets

4. Procedure workflow

The procedure starts with the "Analysis" stage of incident response.



https://t.me/learningnets

Step	Description

1. Verification

The first step in processing a CTI alert is verifying the found information.

This especially concerns the data the relevance of which cannot be confirmed directly.

Points for verification:

- Direct mentions of the company with relevant proofs.
- If the company was not mentioned, assess indirect pieces of data (mentions of company geolocation, industry, size, revenue, list of systems).
- Find original posts – a lot of posts are reshared. If you know the resource where the data was initially mentioned but now the post cannot be found, it may have been deleted and the data sold.
- Compile a full list of mentions.

---

2. Threat identification

Identify the threat type described in the data. What information is being sold? It could be:

- Compromised accounts
- Remote access
- Company data

---

3. Attacker profiling

Build a new attacker profile – or update an existing one – with the following information:

- Author registration date.
- Author rating (if the forum supports such feature).
- Previous activity. Search for other messages of the author.
- Presence on other forums. Search for the same username on other resources.
- Community gratitude. Check the author's relationship with other members. Check reactions and comments to the author's posts.
- Topics of interests. Is the current topic related to the author's main area of interest?
- "Successful" activity. Try to find any evidence that previous offers were successfully sold.

Based on the collected data, build or update the **attacker profile**.

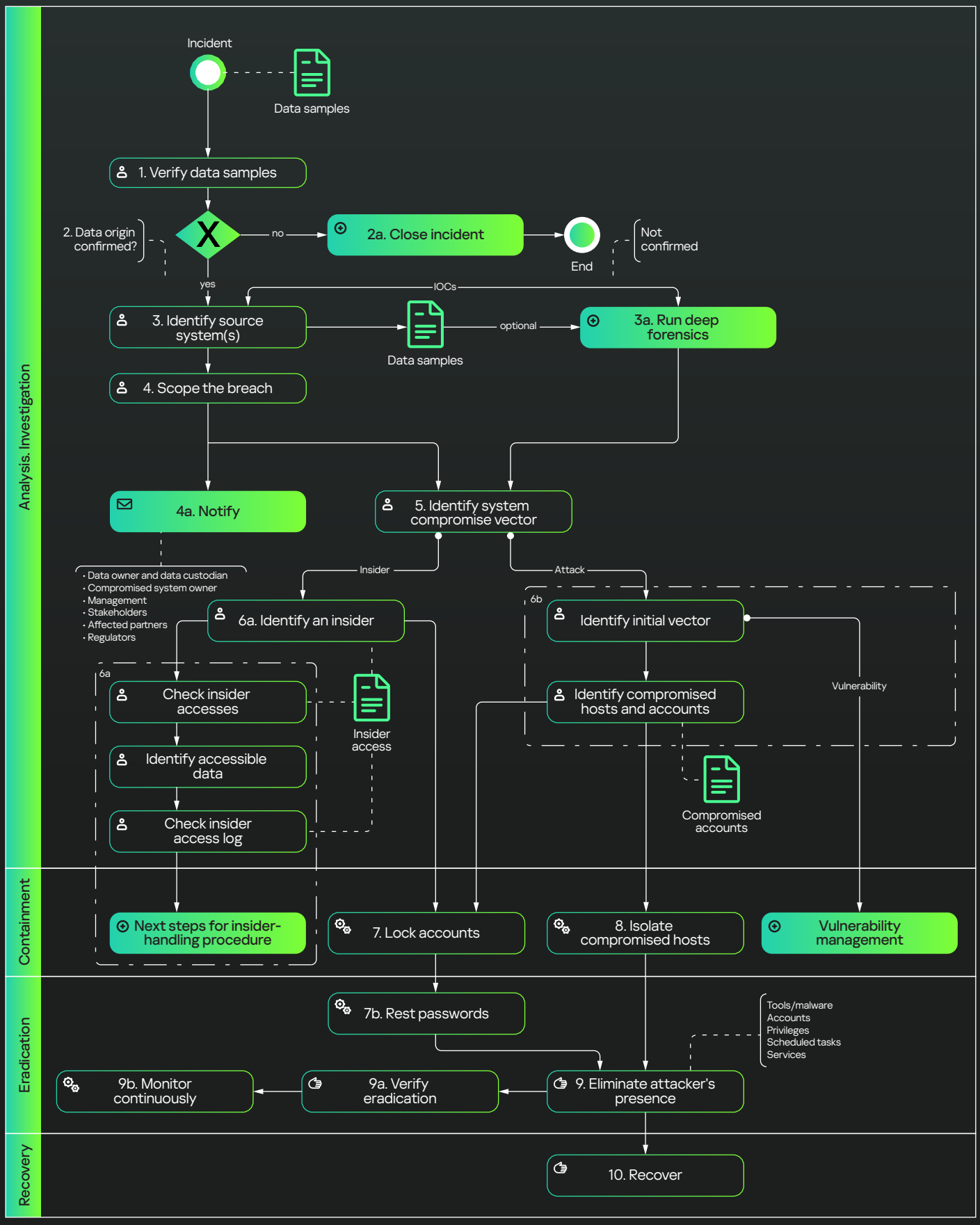
https://t.me/learningnets

Step	Description
4.	**Threat evaluation** Evaluate the risk associated with the threat: • Check the date of the offer. • Check if this information was published before. • Analyze the offer's price, data volume and value, and access or account types. • Deal conditions: is it for free or for sale, is it sold to one buyer only. Check if the information is related to your company or to third parties (partners/subcontractors/suppliers/etc.). Based on the collected data, identify the **threat level**.
5.	**Extraction of artifacts** Identify all the valuable information in the offer. Key artifacts to look for: • Account names • Systems and applications mentioned • IPs/protocols • Access type • Data samples
6.	**Raising an incident** Create an incident for the Security Operation Center (SOC) team to investigate further. From this point on, CTI findings are processed according to the SOC's standard incident response procedures.
7–10.	The next steps of the workflow (**Investigation, Containment, Eradication, Recovery**) are handled by the SOC and IR teams and determined by the relevant playbook according to the identified threat type: • Sale of compromised accounts → Account compromise • Sale of remote access → Remote access compromise • Sale of company data → Data exfiltration

https://t.me/learningnets

5. Response playbooks

5.1 Data exfiltration playbook



https://t.me/learningnets

Data exfiltration playbook steps

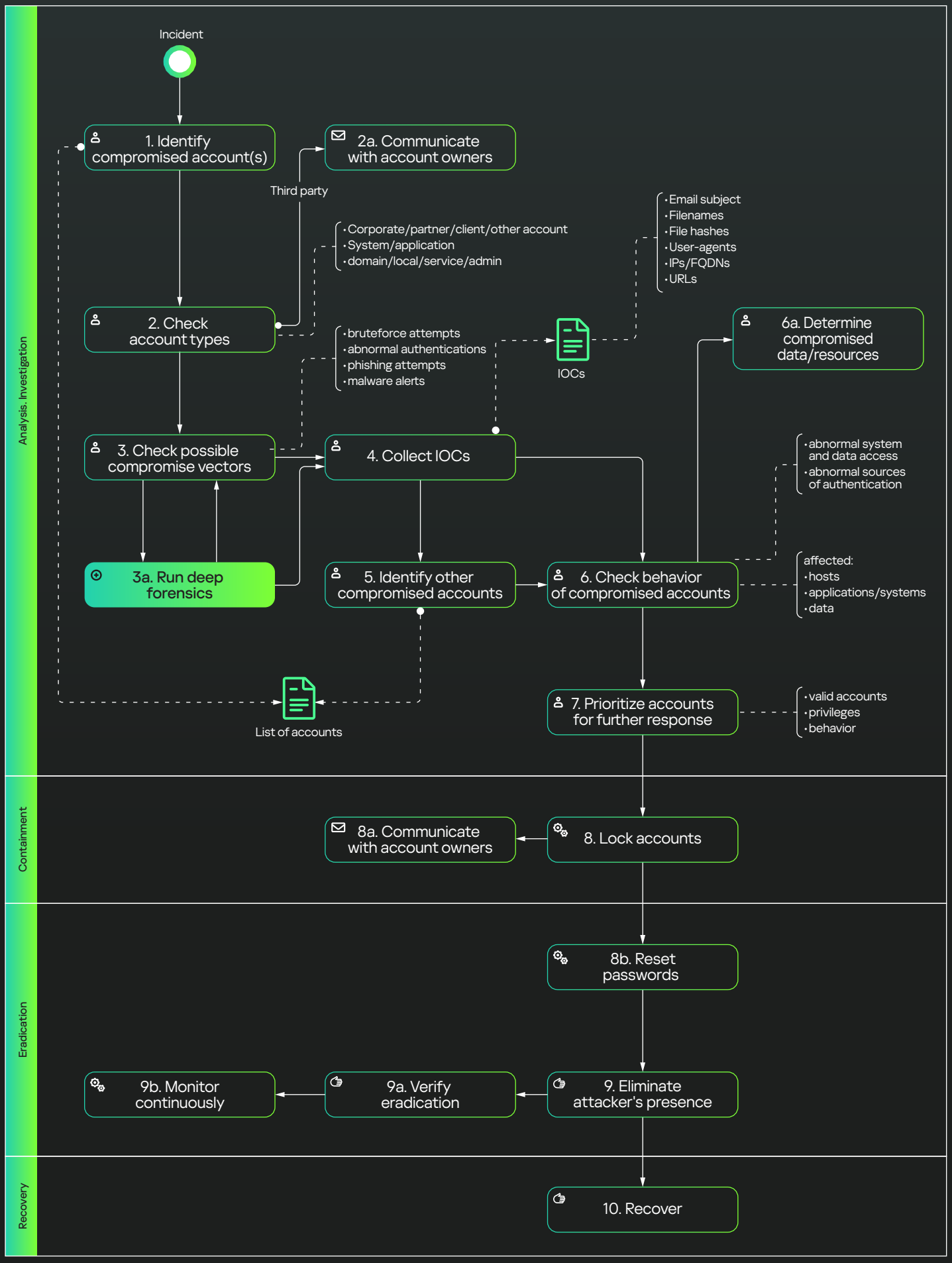
Step	Description
1.	**Verify data samples** Check the breached data samples to verify that the data belongs to your company.
2.	**Confirm data origin** If verification shows that the breached data does not belong to your company, the incident should be closed as a false positive.
3.	**Identify source system(s)** Based on the data samples, compile a list of systems that handle this data. Pay attention to the format, metadata, and technical fields if available (some systems can process the same data, but in different formats).
3a.	**Run deep forensics** If possible, initiate digital forensics procedures for the identified systems. This will help identify other systems compromised by the attacker.
4.	**Scope the breach** Identify the potential scope of compromise by analyzing the list of compromised systems and data processed there.
4a.	**Notify the responsible stakeholders** according to your communication matrix. Common audiences for data breach cases are: • System owners • Data owners or custodians • Management • Affected partners • Authorities, if the data falls under their regulations • Clients
5.	**Define the vector of system compromise** Conduct a thorough investigation to define the system(s) compromise vector. It can be either insider activity or an attack.

https://t.me/learningnets

Step	Description
6.	**Run the appropriate investigation procedures for the identified compromise vector** Based on the results of this investigation, compile a list of affected/compromised accounts and a list of compromised hosts.
6a.	**In case of insider activity:** • Identify the insider. • Identify their level of access for all company systems. • Identify all data potentially accessible for this person. • Check the insider's action logs to identify additional access rights and the type of information the person requested. • Carry out your company procedure for handling insider cases.
6b.	**In case of an attack,** identify the initial attack vector and attack path within your network. Compile a list of systems fully or partially controlled by the attacker. In case of exploited vulnerabilities, carry out the proper management procedures to prevent further exploitation.
7.	**Lock accounts** Regardless of the initial compromise vector, lock any compromised or insider accounts. Also, reset passwords for the accounts before unlocking them.
8.	**Isolate compromised hosts** In case of an attack, isolate any hosts under the attacker's control.
9.	**Eliminate the presence of the attacker in the infrastructure** Perform various eradication steps according to your findings. Verify eradication through continuous monitoring of identified IOCs. For an identified insider threat, set up monitoring of access attempts from all insider accounts.
10.	**Recover** Carry out recovery procedures.

https://t.me/learningnets

5.2 Account compromise playbook



https://t.me/learningnets

Account compromise playbook steps

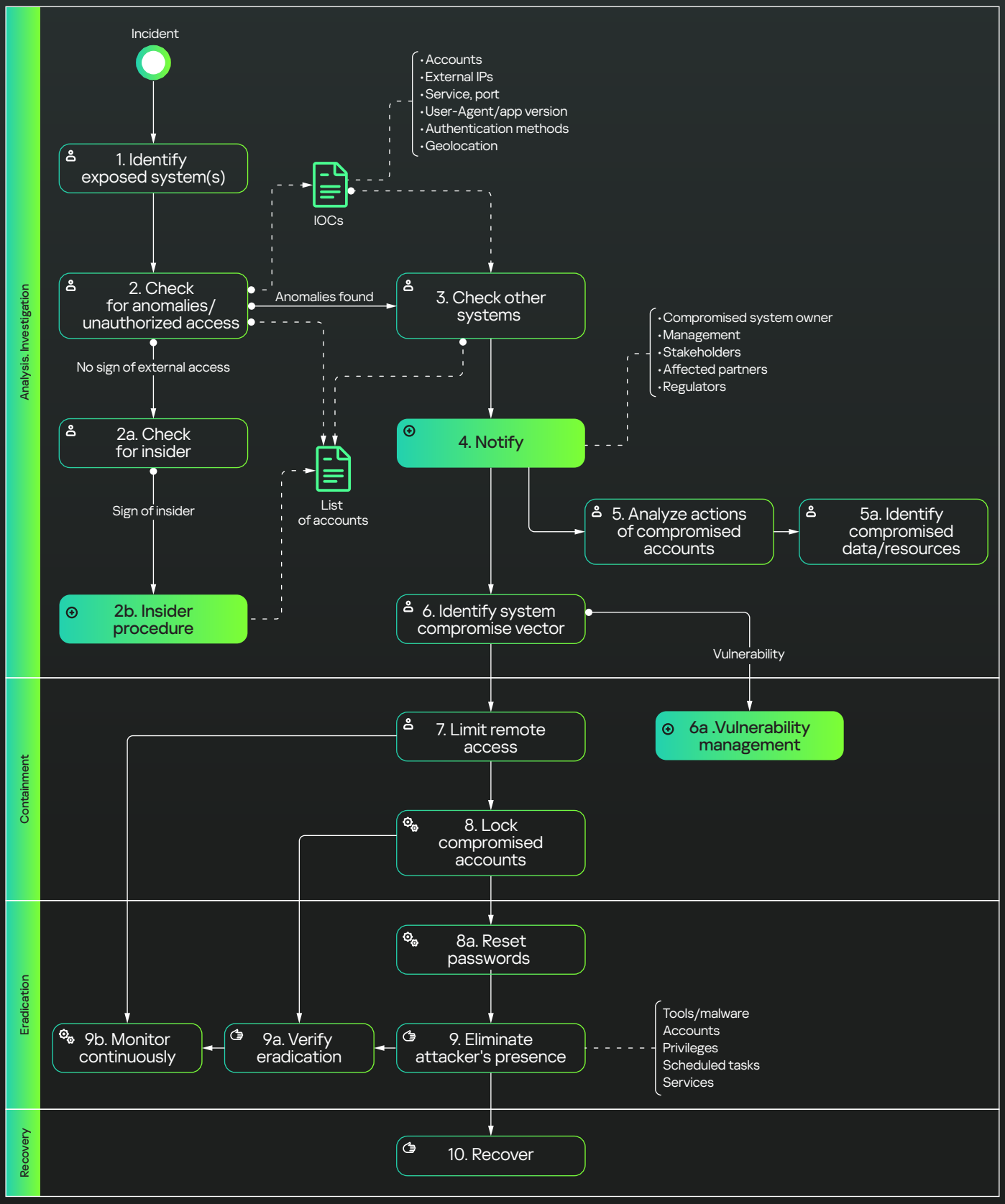
Step	Description
1.	**Identify compromised account(s)** Based on the provided information (access type, system), identify compromised accounts and/or systems.
2.	**Check account types** • Corporate/partner/client/other account • System/application • Domain/local/service/admin
3.	**Check possible compromise vectors** Analyze authentication logs of accounts for: • Bruteforce attempts • Authentication anomalies (non-typical hosts/systems, authentication methods, protocols, client applications, etc.) • Phishing attempts on affected users Check malware and EDR alerts for hosts associated with compromised accounts.
3a.	**Run deep forensics** In case accounts were compromised through system compromise, initiate forensics procedures for the compromised systems. This will help identify the initial attack vector and IOCs.
4.	**Collect IOCs** for identified compromised systems and accounts. IOCs can be: • Phishing email subjects • Malware filenames • File hashes of malware • User-Agent strings of web clients used by malware • IPs/FQDNs • URLs accessed by users

https://t.me/learningnets

Step	Description
5.	**Define other compromised accounts** based on the collected IOCs.
6.	**Check behavior and access history of compromised accounts** for anomalies in authentication methods and system or data access. Identify affected: • Hosts • Applications/systems • Data
7.	**Prioritize accounts for further response** based on: • Account validity • Account privileges • Signs of malicious behavior
8.	**Lock accounts** Lock the compromised accounts.
8a.	**Inform owners of accounts** about the compromise and any actions taken.
8b.	**Reset passwords** for the compromised accounts before unlocking them.
9.	**Eliminate the presence of the attacker in the infrastructure** Perform various eradication steps according to your findings. Verify eradication through continuous monitoring of identified IOCs.
10.	**Recover** Carry out recovery procedures.

https://t.me/learningnets

5.3 Remote access compromise playbook



https://t.me/learningnets

Remote Access playbook steps

Step	Description
1.	**Identify exposed systems** Based on the provided information (access type, prerequisites), identify systems for which access is being sold.
2.	**Check for anomalies/unauthorized access** For the identified systems, analyze access logs and look for anomalies. In case anomalies are detected, collect IOCs to check for access. Here's a list of typical indicators: • Account names • External IPs or IP pools • Services, ports, protocols • User-Agent strings, application fingerprints • Authentication methods • Geolocation profile
2a.	**Check for the possibility of an insider** If there are no signs of abnormal access to the system, conduct an investigation under the hypothesis that access is being sold by an insider. Identify personnel with the required level of access, and check their activities.
3.	**Check other systems** Look for the collected IOCs in the access logs of other systems.
4.	**Notify the relevant stakeholders** according to your communication matrix. Common audiences to notify about system compromise are: • System owners • Management • Affected partners • Authorities, if the affected system falls under their regulations

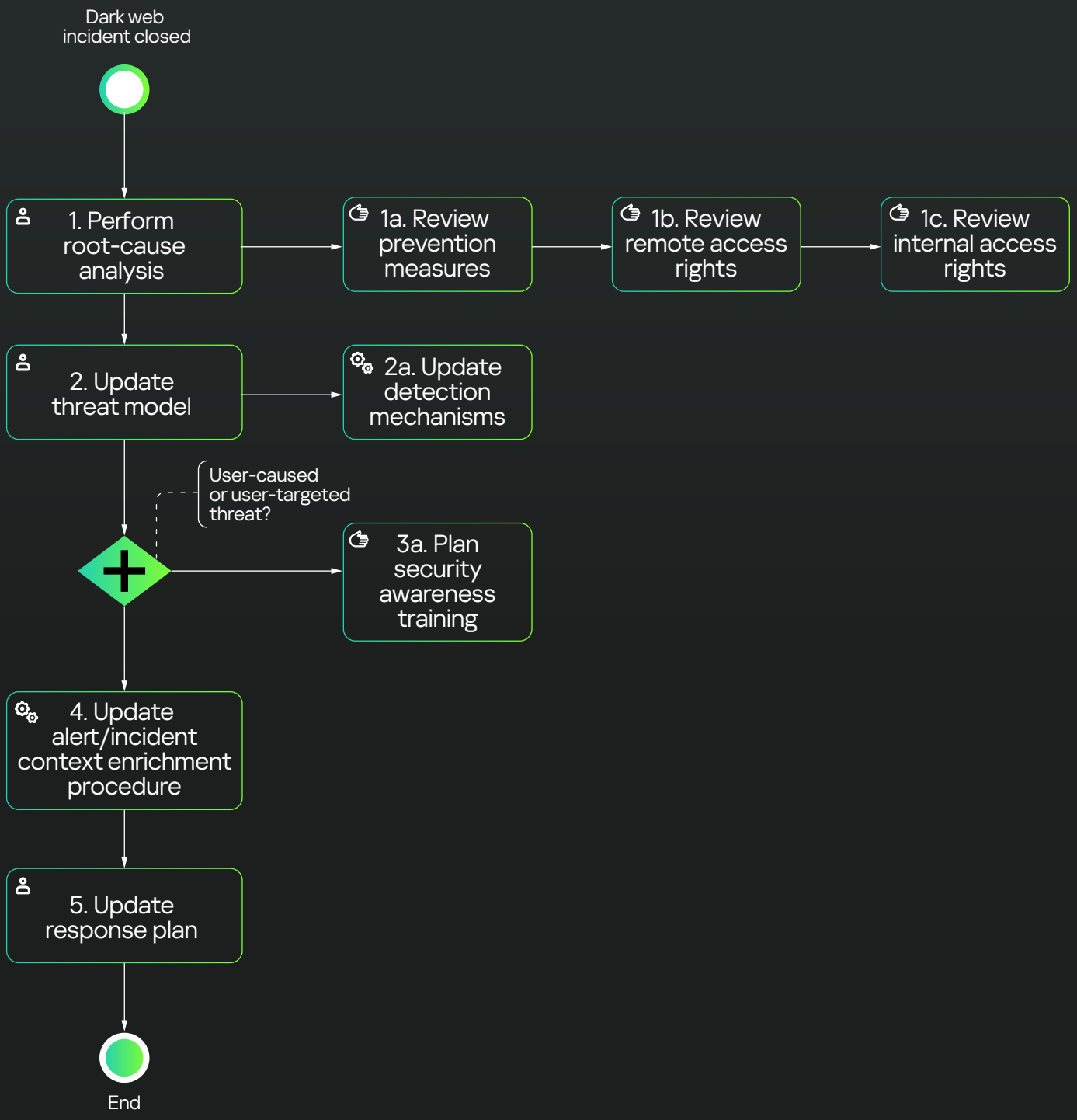
https://t.me/learningnets

Step	Description
5.	**Analyze the actions of compromised accounts** Analyze the actions and behavior of compromised accounts. Check if there are any signs that the accounts are already being used by the attackers. Compile a list of accessed resources, systems and data by the compromised account.
6.	**Identify the system compromise vector** Conduct a thorough investigation to define the system compromise vector. It can be either insider activity or an attack.
7.	**Limit remote access to compromised systems** Depending on the criticality of the system and access to it, different approaches can be applied for containing the attack: • Fully disable remote access. • Enable two-factor authentication. • Limit remote access by specific IPs/network segments/user groups.
8.	**Lock accounts** Lock the compromised accounts.
8a.	**Reset passwords** for the compromised accounts before unlocking them.
9.	**Eliminate the presence of the attacker in infrastructure** Perform various eradication steps according to your findings.
10.	**Recover** Carry out recovery procedures.

https://t.me/learningnets

6. Lessons learned from CTI findings

The "Post-incident activity" stage for CTI alerts includes standard "lessons learned" tasks based on the results of the incident investigation, but also some specific steps to update threat landscape information and adjust CTI alerts.



https://t.me/learningnets

Post-incident activity playbook steps

Step	Description
1.	**Perform root-cause analysis** of the circumstances that led to the incident. This step includes listing which measures and controls are missing and preparing an action plan to prevent similar incidents occurring in the future. Key elements: • Prevention measures • Remote access rights • Internal access rights
2.	**Update the threat model base** with new information. Update threat levels. This involves: • Updating severity levels for specific threat actors • Reviewing the threat profile for affected systems Also, this step often involves designing and implementing new detection mechanisms.
3.	Analyze the nature of the threat and whether it could be caused by an internal user error. If yes, plan an appropriate awareness training.
4.	**Update alert/incident context enrichment procedure** Analyze what data was missing at each step of the CTI alert and incident processing. Pay special attention to steps involving cross-team information exchange. Plan actions to provide the required context next time.
5.	**Update the response plan** Update the current procedure and playbooks according to identified flaws or required improvements.

https://t.me/learningnets

Appendix. Diagram guidelines

The following table provides a reference for the diagram elements used in the playbooks above.

Category	Element	Description
Event		Start event – indicates where a particular playbook starts.
Event		End event – indicates where the playbook ends.
Task		An integration task that can be automated.
Task		A manual action carried out by the T1/T2/T3 analyst according to some particular instructions.
Task		A task assigned to an analyst or other participant.
Gateway		Only one of the paths can be taken based on the workflow logic.
Gateway		Multiple paths can be taken without an order of priority.
Sub-procedure		A collapsed sub-procedure which is executed separately to assist the playbook flow.

www.kaspersky.com/
www.securelist.com

kaspersky

© 2023 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owners

https://t.me/learningnets