Brand Protection Process Flow

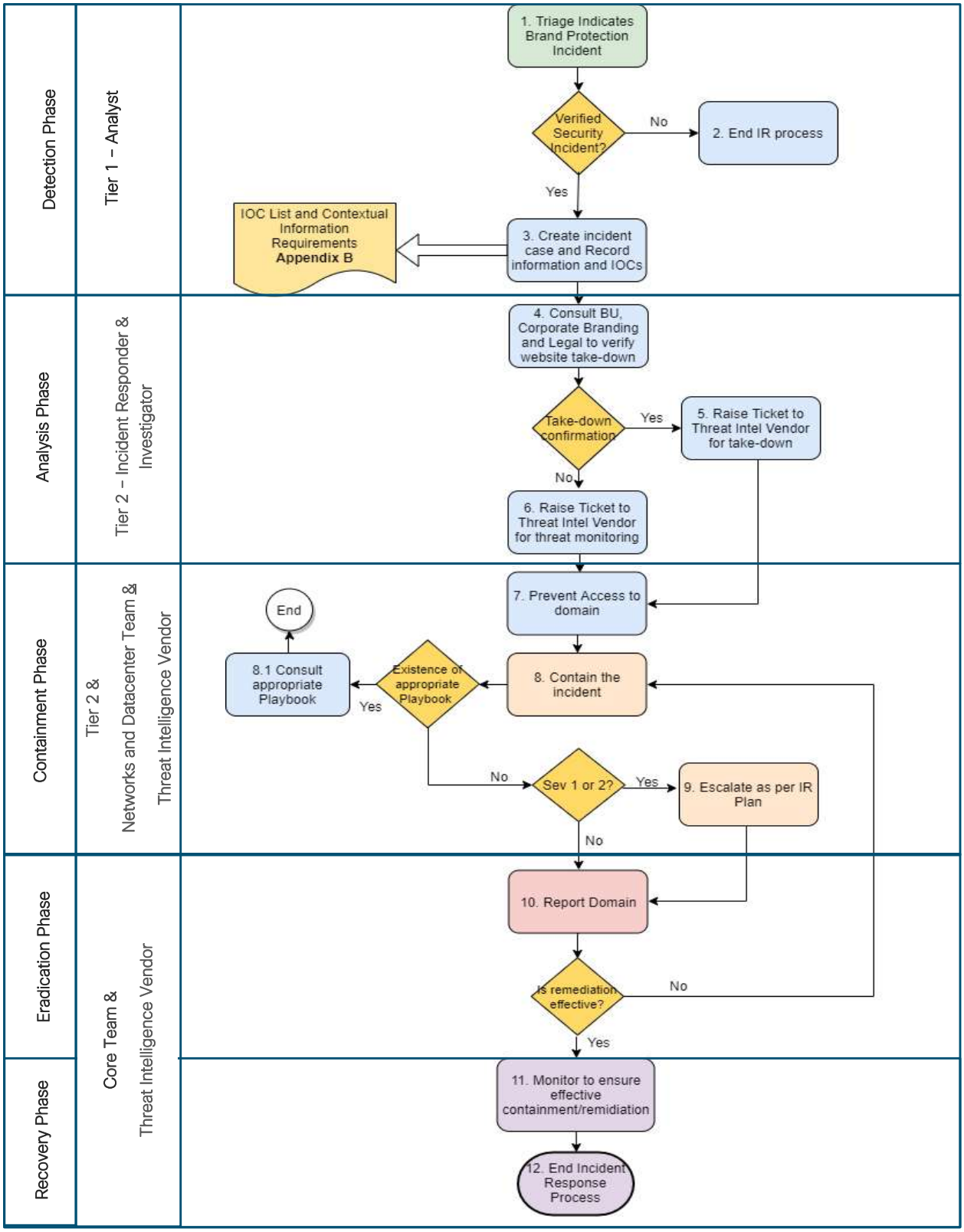
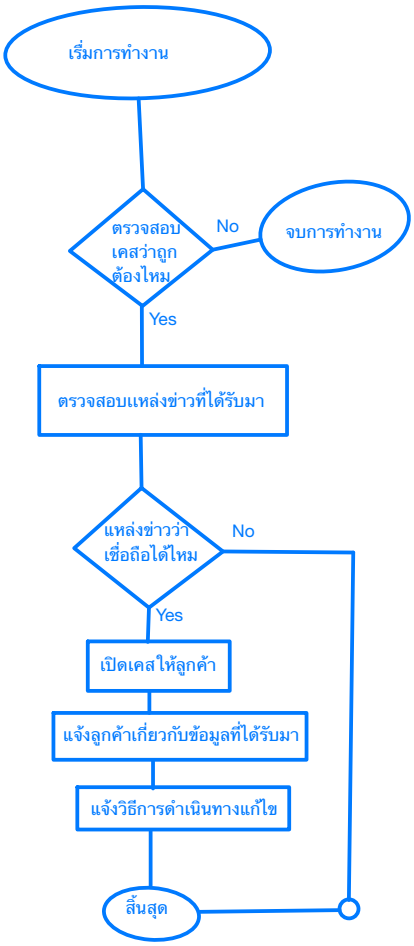


Figure 1: Brand Protection Process Flow


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

Brand Protection Process Detail

Step	Action	Performer	Details	Notes
1	Triage Indicates Brand Protection Incident	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 log are granted ☐ (Optional) Engage with Corporate Branding and communications for external communications ☐ USE CASE DOMAIN HIJACKING / DOMAIN SQUATTING / WEBSITE DEFACEMENT / ALTERATION / PHISHING CAMPAIGNS: o Consult Appendix A if any of the above scenarios are suspected ☐ Update Incident Log	
2	End IR Process	Tier1 - Analyst	☐ In the case that the incident is determined to not 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. ☐ Log any of the IOCs that have previously been identified (or analysis has provided) into the Incident case ☐ Investigate the domain and record the following in the incident log: o Results of a WhoIs lookup o Time domain has existed	IOC List at Appendix B

			○ Recent Activity ○ If the domain is part of any blacklists ○ The Top-Level Domain ○ Any registrant details ○ The status of the domain (active, parked, etc.) ○ Any MX records associated with the domain	
4	Consult BU, Corporate Branding and Legal Teams to verify unlawful website/data take-down	Tier 2 – Incident Responder & Investigator	☐ Pass any appropriate information to the Legal, corporate branding and appropriate business unit teams to receive advise on the possibility of initiating the take-down proceedings with the threat intelligence vendor. ☐ This action should be **approved** by the **SOC** and **CSIRT head.**	
5	Raise Ticket to Threat Intel Vendor for take-down	Tier 2 – Incident Responder & Investigator	☐ In the case that the BU, Corporate branding and Legal confirm the take down of the illicit website/data, raise a ticket to the CTI vendor to initiate proceedings for the take down ☐ This action should also be **approved** by the **SOC** and **CSIRT head.** Follow the escalation process in IR Plan.	Particular challenge can be posed by bulletproof hosting providers.
6	Raise Ticket to Threat Intel Vendor for threat monitoring	Tier 2 – Incident Responder & Investigator	☐ In the case that the BU, Corporate branding and Legal consults against the take down of the illicit website/data, raise a ticket to the CTI vendor for passive monitoring of the website/data in question for acquiring: ○ Actionable intelligence ○ Any changes in activity ☐ This action should also be **approved** by the **SOC** and **CSIRT head.** Follow the escalation process in IR Plan.	

7	Prevent access to domain	Tier 2 – Incident Responder & Investigator	☐ Prevent access to the site by blocking the URL at gateways and any associated IP addresses internally. ☐ Log actions to incident log	The assistance of support team might be required, e.g. Networks and Datacenter team.
8	Contain the Incident	☐ Tier 2 – Incident Responder & Investigator ☐ Networks and Datacenter Team ☐ Threat Intelligence Vendor	☐ Tier 2 should examine web proxy logs, firewall logs and perimeter devices to determine if anyone has accessed the malicious domain ☐ Tier 2 should examine email gateways to search for any email traffic that may have been sent from or to the offending domain ☐ Tier 2 should block any ongoing communications to the offending domain ☐ Server Team should block access / take down / recover from any attacks targeting KTB's servers leading to brand damage (e.g. website defacement, etc.) ☐ Group-IB should take-down any websites / data aiming at damaging the Brand of KTB in the case of third-party website involvement. ☐ Log all actions to incident log	
8.1	Consult appropriate Playbook	Tier 2 – Incident Responder & Investigator	☐ If the incident has developed to warrant consulting other Playbooks and these playbooks are readily available, ensure that this is done.	
9	Escalate as Per IR Plan	Tier 2 – Incident Responder & Investigator	☐ In the case of a severity 1 or severity 2 incident, escalate the incident to the appropriate stakeholders for action according to the IR Plan escalation procedure. If not, proceed into informing only the communications team.	

10	Report domain	Threat Intelligence Vendor	☐ Consider reporting the domain to law enforcement, ISP(s) and to Web browser vendors (e.g. Google). ☐ Report the domain to blacklists and other actions to reduce the reputation of the domain ○ See Appendix C for some common reporting locations ☐ Report the domain to the domain's registrar	
11	Monitor to ensure effective containment / remediation	☐ Threat Intelligence Vendor ☐ SOC Team	☐ In the case that the remediation steps were effective proceed to this step, otherwise go to step 8 for further containment. ☐ Group-IB to monitor the offending domain to ensure take-down was successful ○ If take-down was not possible, ensure that other remediating activity was taken ☐ SOC to alert resolver group(s) upon identifying further suspicious activity in order to implement further containment and remediation. Can include employees accessing the malicious website or other malicious websites are found online. ☐ Log all actions in incident log	
12	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	

			○ PIR is required where an incident is of Severity 1 or Severity 2	

Appendix A - Specific Use Case

Domain Hijacking / Domain Squatting

Domain Hijacking is the process of purchasing a domain that is owned b[redacted] when the domain expires. Domain Squatting involve the purchasing and holding of a domain in order to profit off[redacted] trademark. Although not illegal, these techniques can be dealt with as a violation o[redacted] trademark and the Profit Protection and Legal teams should be informed.

Special Considerations

1. Inform Profit Protection / Legal of the situation in order to recover the target domain as soon as possible.
2. Monitor any activity coming from the offending domain, as it may be part of a phishing campaign. Request that Group-IB add the domain(s) to their watch-list.

Website Defacement / Alteration

A defacement or alteration of[redacted] website is a high profile attack against[redacted] brand. Although protection of the brand is necessary, the immediate concern should be discovering how the website was changed as modification is indicative of unauthorised access or malicious code.

Special Considerations

1. Consult the Unauthorised Access Playbook to ensure that an attacker is not currently within[redacted] networks.
2. Inform the Profit Protection / Legal / Comms teams as soon as possible as they will likely want to respond to such a high profile attack.
3. After the immediate threat has been eradicated, the web server hosting the affected website should be restored from a safe backup.

Phishing Campaigns

Attackers may launch phishing campaigns that involve [redacted] brand. Although [redacted] may have nothing to do with any emails or mirror websites set up by an attacker, customers [redacted] may not necessarily be able to tell the difference between legitimate and fraudulent websites or emails.

Special Considerations

1. If [redacted] website has been fraudulently replicated, examine the webserver logs for any requests that may indicate spidering or copying activity.
2. Inform the relevant teams (Profit Protection / Legal / Comms) to take down the website/domain and inform customers about the risks of navigating to the fraudulent website/domain.
3. Examine any fraudulently mirrored sites for any unique features that would only be known to an internal employee – this may be indicative of an Insider Threat or other cases of unauthorised access.
4. Consult the Suspicious Email for any actions on how to respond to any suspicious emails that are sent [redacted] as part of the phishing campaign.
5. If emails are being spoofed to appear to be coming [redacted], try to ascertain the true source of the emails and take remediating action, such as blocking and reporting the source, and informing the Legal / Comms teams.

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 (IOCs) 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, timelining, 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

Appendix C – List of reporting sites and blacklists

Fraudulent Domain Reporting

ThaiCert is Thailand's national Computer Emergency Response team. The following link can be used to report a fraudulent domain:

https://www.thaicert.or.th/report-en.html

The domain registrar should always be contacted about instances of misuse or malicious activity. Check the registrar's website for instructions on how to submit an abuse report.

Blacklists

There are several online blacklists that a suspicious domain can be added to. Reporting a domain to these blacklists can lower the reputation of any email sent from the domain, increasing the likelihood that it will be blocked automatically by some commercial software. The following are some resources that can be used to report malicious domains/emails:

spamcop.net – This service can be used for reporting spam email.

uribl.com – uribl.com primarily deals with Unsolicited Bulk/Commercial Email (UBE/UCE).

Local ISPs

Web-Browser Vendors