Post-Incident Review Process Flow

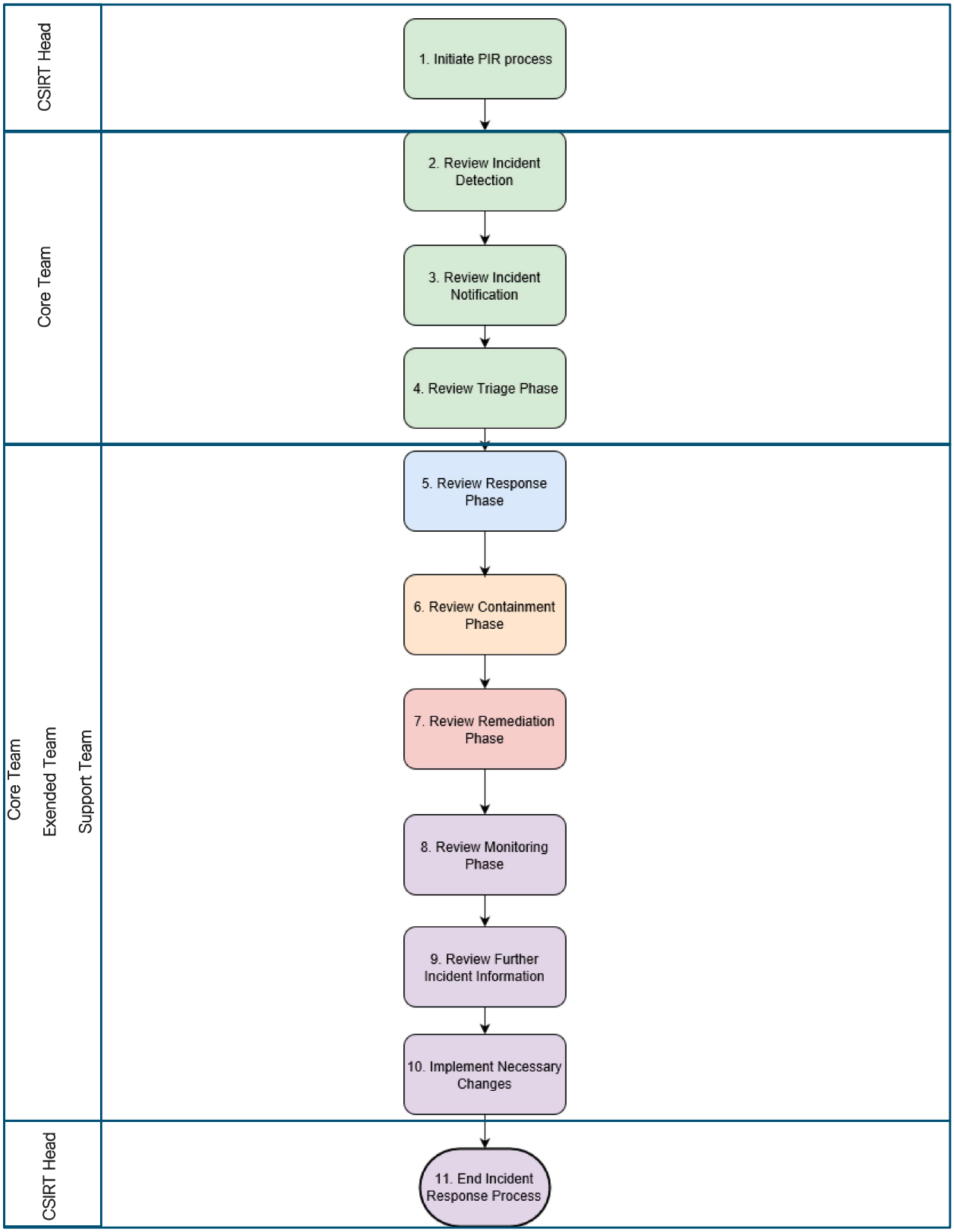
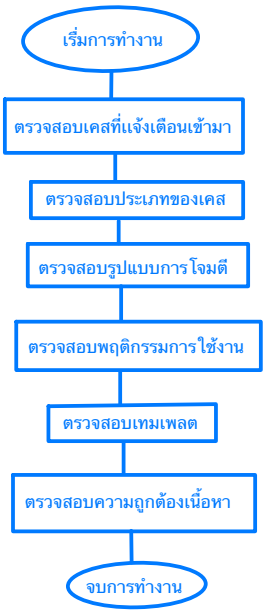


Figure 1: Post-Incident Review Process Flow


เริ่มการทำงาน
ตรวจสอบเคสที่แจ้งเตือนเข้ามา
ตรวจสอบประเภทของเคส
ตรวจสอบรูปแบบการโจมตี
ตรวจสอบพฤติกรรมการใช้งาน
ตรวจสอบเทมเพลต
ตรวจสอบความถูกต้องเนื้อหา
จบการทำงาน

Step 1 ตรวจสอบ Alert ที่เข้ามาว่ามีข้อมูลที่ครบถ้วนถูกต้องหรือไม่ เช่น มี Src Dst Port User Device_Product หากไม่มีให้ทำการแจ้ง L2 เพื่อตรวจสอบว่าผิดพลาด

Step 2 ตรวจสอบว่า Alert ที่เข้าอยู่ในประเภทใด เป็นรูปแบบใดเช่น การเชื่อมต่อไปยังพอร์ตสำคัญ การโจมตี DDOS DOS Bruteforce

Step 3 ตรวจสอบรูปแบบการโจมตี นั้นเข้ามาในรูปแบบใด เช่น จากภายใน จากภายนอก และตรวจเช็คมีความเสี่ยงมากหรือไม่

Step 4 ตรวจเช็คว่าพฤติกรรมการใช้งานของผู้ใช้งานนั้น มีความผิดปกติหรือไม่ หากมีความผิดปกติที่ไม่สามารถทำเองได้ให้แจ้ง L2 ให้ตรวจสอบเพิ่มช่วย

Step 5 ตรวจสอบ Template ที่จะใช้ถูกต้องตามประเภทของการโจมตีหรือไม่ ถูกต้องตามที่บริษัทลูกค้า กำหนด ขอ หรือไม่

Step 6 ตรวจสอบว่าข้อมูลที่ใส่เข้าไปใน Template นั้นมีความถูกต้องครบถ้วนหรือไม่ ก่อนส่งให้ลูกค้าตีสจสอบ

Post-Incident Review Process Detail

Step	Action	Performer	Details	Notes
1	Initiate PIR process	☐ CSIRT Head	☐ Resolve the incident and determine that a PIR is required ☐ Ensure all necessary documentation is created ☐ Determine PIR attendees (necessary engineers from SOC, Incident Coordinators, and required persons from resolver groups) ☐ Inform attendees of the upcoming PIR and provide a short briefing and any necessary input required	
2	Review Incident Detection	☐ Core Team	☐ Who detected the incident? ☐ How was the incident detected? ☐ What was the time to detection (time between incident occurring and incident being detected by systems)? ☐ Could it have been detected earlier?	Possible outcomes may be: • Modifications to incident detection systems
3	Review Incident Notification	☐ Core Team	☐ If SOC did not detect the incident: ○ Were SOC notified in an appropriate timeframe? ○ How were SOC notified? ○ Should SOC be able to detect these incidents in the future?	

4	Review Triage Phase	☐ Core Team	☐ Was all of the information that was needed gathered in the triage stage? ☐ Was the incident correctly or incorrectly identified as a false positive? ☐ Was the incident given the correct expected business impact / priority? ☐ Was the correct Playbook chosen?	Possible outcomes may be: • Guidelines on how to report an incident • Modifications to example business impact/priority tables • Guidance on how to reduce false positives • Training to improve the Triage process
5	Review Response Phase	☐ Core Team ☐ Extended Team (if needed) ☐ Support Team (Relevant parties, e.g. Server Team, onsite team, etc.)	☐ Was the initial attack vector quickly contained and stopped? ☐ Were any external vendors utilised and if yes, did they provide added value? ☐ Were other affected systems quickly identified? ☐ Did resolver groups (e.g. Server Team, onsite team, etc.) respond quickly to notifications and instructions?	Possible outcomes may be: • Training on how to quickly stop attacks • Feedback to third parties • Guidance on how to use identified IOCs effectively • Feedback to resolver groups

6	Review Containment Phase	☐ Core Team ☐ Support Team (Relevant parties, e.g. Server Team, onsite team, etc.)	☐ Was the incident quickly contained? ☐ Was containment effective? ○ Were there any impacts as a result of containment? ○ Were these expected? ☐ Was evidence able to be gathered for analysis? ○ Were all industry best practice guidelines followed during evidence acquisition and analysis?	Possible outcomes may be: • Restrictions on network devices to prevent the spread of an attack • Guidance on how to preserve evidence
7	Review Remediation Phase	☐ CSIRT Head ☐ Support Team (Relevant parties, e.g. Server Team, onsite team, etc.)	☐ Were there any problems with rebuilding and re-introducing systems back into the network? ○ Are there any rebuild activities outstanding? ☐ Was the root cause able to be established (People, Process, Technology)? ○ Can this root cause be resolved? ○ Was the incident caused by a network/system change? ☐ Was the source or threat actor of the incident identified? ☐ Was the incident successfully remediated? ○ Were there any accepted risks and have these been recorded?	Possible outcomes may be: • Improvements to the rebuild process
8	Review Monitoring Phase	☐ CSIRT Head	☐ Are the systems involved undergoing increased monitoring, if necessary?	Possible outcomes may be:

		☐ Support Team (Relevant parties, e.g. Server Team, onsite team, etc.)	☐ Have appropriate people been informed on how to respond to further incidents? ☐ Was the monitoring effective? o If monitoring is ongoing - is there a process to ensure the effectiveness of any monitoring that is taking place?	• Improvements to system monitoring
9	Review Further Incident Information	☐ Core Team ☐ Extended Team (if needed) ☐ Support Team (Relevant parties, e.g. Server Team, onsite team, etc.)	☐ Were all of the utilised Playbooks followed? o Are there any improvements needed to any of the Playbooks? ☐ Were all tools used effective? ☐ Were all communications made during the incident appropriate and timely? ☐ Did all actions taken during the incident have appropriate authorisation – in particular when there were substantial impacts to people or systems? ☐ What was the time to resolve the incident? o Were all phases completed in a reasonable time? ☐ Were there any key successes achieved as a result of responding to this incident? o What was the business impact that was prevented? ☐ What were the financial/reputational/legal impact to KTB?	Possible outcomes may be: • Improvements to the SecOps Playbooks • Improvements or changes to tools used

			☐ Was all relevant information passed to the necessary teams (Legal, Profit Protection, Data Privacy, Information Security, IT Security Architecture) to take action as necessary?	
10	Implement any necessary changes	☐ Core Team ☐ Extended Team ☐ Support Team (Relevant parties, e.g. Server Team, onsite team, etc.)	☐ Any outcomes identified in the previous steps should be recorded in the PIR Action Tracker	
11	End Post Incident Review Process	☐ CSIRT Head	☐ Distribute the PIR document to attendees and Security Operations team ○ Conform to any information handling restrictions	