

Hong Kong Monetary Authority (HKMA)

Threat Intelligence (TI) Playbook



Version Control

No.	Date	Author	Description
0.1	07 Jun 2024	PwC (Herbert Kwok)	1st draft
0.2	31 Jul 2024	PwC (Herbert Kwok)	<p>2nd draft</p> <p>1) CTO – About Completion Phase</p> <p><u>New</u></p> <ul style="list-style-type: none"> • Expected Turnaround of Incident / CVE • Monthly Statistics & Report <p><u>Modified</u></p> <ul style="list-style-type: none"> • Incident Escalation for HKMA Evaluation <p><u>Enhancement</u></p> <ul style="list-style-type: none"> • Follow-up Actions for CVE Escalation <ul style="list-style-type: none"> - Communication with System Owner(s) • Follow-up Actions for Incident Escalation <ul style="list-style-type: none"> - Analysis Template - IOCs Blocking <p>2) Threat Hunting – Initiating Phase</p> <p><u>New</u></p> <ul style="list-style-type: none"> • Threat Actor Profiling • Weekly Review and Update of IOCs in HKMA Internal TI Source • Evaluating IOC Impact and Initiating Incident Response (IR) <p>3) SOC – About Completion Phase</p> <p><u>New</u></p> <ul style="list-style-type: none"> • Supporting SOC Operations • Delivering Threat Hunting Analysis to SOC <p>4) Incident Response (IR) – Initiating Phase</p> <p><u>New</u></p> <ul style="list-style-type: none"> • IR Initiation and Notifications Phase • Investigation Phase • Drilling & Reporting Phase

0.3	25 Sept 2024	PwC (Herbert Kwok)	<p>3rd Draft</p> <p>1) CTO – About Completion Phase</p> <p><u>Note</u></p> <ul style="list-style-type: none"> • HKMA: <ul style="list-style-type: none"> - Released the latest version of “SOC_TI_Workflow_20240902” (updated on 2024-09-02). • PwC: <ul style="list-style-type: none"> - In Progress: drafting the 3rd draft of the TI SOP, which aligns with the workflow of the cross-functional flowchart. <p><u>Enhancement</u></p> <ul style="list-style-type: none"> • Communication with System Owner(s) <ul style="list-style-type: none"> - Email Template <p><u>Modified</u></p> <ul style="list-style-type: none"> • High / Critical Case <ul style="list-style-type: none"> - Route JIRA ticket to affected stakeholders - Users creates sub-ticket, update sub-task with evidence when patching completed • Medium / Low Case <ul style="list-style-type: none"> - Send out notification emails via Outlook, asking users remediate the vulnerability • Patching Confirmation <ul style="list-style-type: none"> - Confirm remediation with the evidence of screenshot • CVE Escalation for HKMA Evaluation <ul style="list-style-type: none"> - Added “Check with users via Outlook email, asking potentially affected parties explicitly if they are using the affected system and its version” • Non-office Hour Workflow for Critical Case <p><u>New</u></p> <ul style="list-style-type: none"> • Threat Classification <ul style="list-style-type: none"> - CVA Criteria Table - Define Critical / High / Medium / Low severity levels for CVEs - Initiate corresponding follow-up actions
0.4	05 Nov 2024	PwC (Herbert Kwok)	<p>Latest Endorsement</p> <p>1) CTO</p>

			<p><u>Modified</u></p> <ul style="list-style-type: none"> • High / Critical Case <ul style="list-style-type: none"> - Add a step “Email to System Owner confirm if system is affected” before routing JIRA sub-ticket to System Owner - TI on-site analyst creates sub-ticket to fill in the response from System Owner’s email reply, instead of System Owner creating sub-ticket and filling in the information themselves - Set the component of JIRA sub-ticket to “TI follow up” instead of “TI alert escalation” • Add Case Categorization <ul style="list-style-type: none"> - Requested by HKMA to align OGCIO Threat Handling Practice <ul style="list-style-type: none"> ○ Social threats (e.g., social engineering attacks, phishing) ○ Technical Threats (e.g., Malware, zero-day exploits) ○ Environmental Threats (e.g., hardware failures, outage) ○ Others (e.g., threat landscape) • Day-to-day duties for CVEs sweeping <ul style="list-style-type: none"> - As requested by HKMA, if the threat is issued by OGCIO or PwC Proprietary Critical Vulnerability Alert, the TI on-site analyst should create a JIRA ticket for every threat follow-up. • Monthly Statistics Report <ul style="list-style-type: none"> - As requested by HKMA, upcoming following statistics will be included: <ul style="list-style-type: none"> ○ Communications/Settlement Phishing Email ○ Threat Hunt ○ OGCIO High Threat Security Alert ○ PwC Proprietary Critical Vulnerability Alert <p>2) Threat Hunt</p> <p><u>Add</u></p> <ul style="list-style-type: none"> • Objectives of Threat Hunting <ul style="list-style-type: none"> - Add an outcome “Ensure whether users had run the unblocked malware in HKMA computer by Threat Hunting in Splunk, and other EDR Solutions” • Scope of Threat Hunting <ul style="list-style-type: none"> - Add Threat Hunting Scope, agreed with HKMA <ul style="list-style-type: none"> ○ HKMA Related ○ Regional Focus ○ CVE / Vulnerabilities ○ Technology Related
--	--	--	--

			<ul style="list-style-type: none"> ○ PwC Proprietary Cyber Threat Intelligence Weekly Report • Coverage of finding Indicators of Compromise (IoCs) for threat hunting in security solutions <ul style="list-style-type: none"> - Mapping table is added • Validate the findings of IoCs <ul style="list-style-type: none"> - Add the method of validating the following hits: <ul style="list-style-type: none"> ○ False Positive ○ True Positive with low/medium confidence ○ True Positive with high confidence <p><u>Modified</u></p> <ul style="list-style-type: none"> • Threat Actor Profiling <ul style="list-style-type: none"> - The following details should be included, if available (if not, fill in N/A): <ul style="list-style-type: none"> ○ Aliases ○ Country of Origin ○ Known Targets ○ Active Since ○ Target Sectors ○ Primary Objectives ○ Techniques <p><u>Remove</u></p> <ul style="list-style-type: none"> • Review and Consolidation HKMA Internal TI Source <ul style="list-style-type: none"> - The IOC consolidation is inefficient after trial run, we proposed to remove this part due to no any integration in place, there is no impact on current threat hunting tasks. <p>3) SOC</p> <p><u>Modified</u></p> <ul style="list-style-type: none"> • TI Analysis Coordination with SOC <ul style="list-style-type: none"> - Add a case study: "Hash Value of File Analysis in JIRA ticket provided by SOC" <p><u>Remove</u></p> <ul style="list-style-type: none"> • Delivering Threat Hunting Analysis to SOC <ul style="list-style-type: none"> - Reason - Since TI will conduct threat hunting itself, there is no need to deliver to SOC afterwards <p>4) Incident Response (IR)</p> <p><u>Modified</u></p> <ul style="list-style-type: none"> • IR Initiation and Notifications Phase
--	--	--	--

			<ul style="list-style-type: none"> - If a ticket/incident is related to TI, AD(IT)(ITS)3 will kick off IR to the PwC TI Team. If the ticket is related to SOC, kick off IR to the PwC SOC Team.
0.5	27 Nov 2024	PwC (Herbert Kwok)	<p>1) CTO (1st Modification of Latest Endorsement)</p> <p><u>Add</u></p> <ul style="list-style-type: none"> • Dark Web Monitoring Alerts Handling <ul style="list-style-type: none"> - On working days at 10:00 AM and 4:00 PM, the TI on-site analyst will monitor alerts from Dark Web Monitoring (DWM) in the PwC JIRA Platform - Created dark web monitoring alert ticket in JIRA ticket with title, component, status <p><u>Modified</u></p> <ul style="list-style-type: none"> • High / Critical Case Follow Up <ul style="list-style-type: none"> - Requested by AD(IT)(ITS)3, set the component of JIRA sub-ticket to “TI alert escalation” instead of “TI follow up” to track progress of system owner for further follow up
0.5	20 Dec 2024	PwC (Herbert Kwok)	<p>1) CTO (2nd Modification of Latest Endorsement)</p> <p><u>Modified</u></p> <ul style="list-style-type: none"> • Medium / Low Severity CVE Processing <ul style="list-style-type: none"> - Requested by AD(IT)(ITS)3, the following actions should be taken based on the Final Severity Level of vulnerability being ‘Low’: <ul style="list-style-type: none"> ○ Perform Further Investigation and Document Findings in JIRA ○ (New Addition) No need to send out a notification email to the system owner <p>3) Security Operation Centre (SOC) (1st Modification of Latest Endorsement)</p> <p><u>Add</u></p> <ul style="list-style-type: none"> • TI Requests Findings by SOC <ul style="list-style-type: none"> - Requested by AD(IT)(ITS)3, if the TI on-site analyst identifies Indicators of Compromise (IoCs) using HKMA security tools (e.g., Splunk, Sentinel One) during a threat hunt, the case should be passed to the SOC on-site analyst for further action.

			<ul style="list-style-type: none"> ○ TI on-site analyst will create a Jira sub-ticket under the threat hunt parent ticket for the passing case to SOC. ○ SOC on-site analyst will perform analysis on HKMA security solutions, gather and provide observations in the sub-ticket accordingly where necessary.
0.6	21 Jan 2025	PwC (Herbert Kwok)	<p>1) CTO (3rd Modification of Latest Endorsement)</p> <p><u>Add</u></p> <ul style="list-style-type: none"> • HKMA Domain Monitoring (Trial-Run) <ul style="list-style-type: none"> - Agreed by AD(IT)(ITS)3 and PwC, it is to expand the existing TI coverage process to regularly search reputable feeds for keywords (e.g., “HKMA” or “hkma.gov.hk”) to cover social media monitoring. - AD(IT)(ITS)3 agreed to trial-run and if suitable. - During trial-run, explore (a) automation and (b) additional use cases. <p><u>Modify</u></p> <ul style="list-style-type: none"> • Template for documenting CVEs in the Outlook Email <ul style="list-style-type: none"> - Requested by AD(IT)(ITS)3, place the indicator “Exploited in the Wild” as the first row under the attribute “Exploitation Metrics” since it has a greater impact to the vulnerability severity level compared to the indicators “Exploitable”, “Remotely Exploitable”, and “Exploitable by Non-Privileged Accounts.” <p>2) Threat Hunting (1st Modification of Latest Endorsement)</p> <p><u>Modify</u></p> <ul style="list-style-type: none"> • Validate the findings of IoCs <ul style="list-style-type: none"> - Below is the detailed process for handling the security hits: <ol style="list-style-type: none"> 1) Research IP Purpose, Pass to SOC 2) Confirm if APT Targeting 3) Update Severity Level to ‘Critical’ if APT Targeting 4) Request blocking IoCs within one business day if APT Targeting <p>3) SOC (2nd Modification of Latest Endorsement)</p> <p><u>Modify</u></p> <ul style="list-style-type: none"> • TI Requests Findings from SOC <ul style="list-style-type: none"> - TI provide the ticket content to SOC

			<ul style="list-style-type: none"> ○ Include Threat Hunting findings (i.e., the purpose of the IP leveraged by the threat actor) - SOC will provide the following observations if the IoCs are IP addresses: <ul style="list-style-type: none"> ○ Identify any malicious inbound and outbound traffic ○ Confirm whether such activity has been denied ○ Observe whether there is any callback (for C2 IP address only)
0.6	24 Feb 2025	PwC (Herbert Kwok)	<p>1) CTO (4th Modification of Latest Endorsement)</p> <p><u>Modified</u></p> <ul style="list-style-type: none"> • Phishing Email Handling <ul style="list-style-type: none"> - Added “Neutral” into original classified types (“Unwanted”, “Spam”, “Phishing”) - As obtaining feedback from the HKMA Communications & Settlement Team and agreed by AD(IT)(ITS)3, emails reported without any phishing indicators will now be marked as “Neutral”. • Submit Block IP Request to HKMA System Owner <ul style="list-style-type: none"> - As requested by the HKMA Infrastructure Team System Owner A(SYS)(IT)(IS)10, when a TI on-site analyst creates a ticket including an IP Address request for blocking, the brackets between the dots will be removed for smoother operation (i.e., making it more convenient for the system owner to input the malicious IP Address into the NIPS block list. <p>2) Threat Hunting (2nd Modification of Latest Endorsement)</p> <p><u>Modify</u></p> <ul style="list-style-type: none"> • Conduct Threat Hunt against Specific Active Advanced Persistent Threat (APT) Group <ul style="list-style-type: none"> - Suggested by AD(IT)(ITS)3 as a lesson learned, to conduct threat hunts focusing on opportunistic threat actors based on their recent activity.
0.7	26 Mar 2025	PwC (Herbert Kwok)	<p>Latest Endorsement on 25 Feb 2025</p> <p>1) CTO (1st Modification of Latest Endorsement)</p> <p><u>Modified</u></p> <ul style="list-style-type: none"> • Phishing Email Handling

			<ul style="list-style-type: none"> - As requested by AD(IT)(ITS)3, the categories "Unwanted" and "Neutral" have been removed. The new categories are "Spam" or "Phishing". - Justification: To unify the outcome of analyzing the reported email and prevent subjective conclusions. <p>2) Threat Hunting (1st Modification of Latest Endorsement)</p> <p><u>Enhance</u></p> <ul style="list-style-type: none"> • Scope of Threat Hunting <ul style="list-style-type: none"> - Expand the scope of threat hunting - Trend-Related Threats (Not limited but include the following): <ul style="list-style-type: none"> ○ Remote Access Tools ○ InfoStealers - Provide a mapping of Remote Access Tools with corresponding threat actor groups for reference
--	--	--	---

Estimated TI SOP Progress (snapshot from 26 Mar 2025)

Content of SOP	PwC follow up action on Version Control									SOP Trial Run	Lesson Learnt (25 Feb 2025 to 26 Mar 2025)
	2 June	2 Aug	25 Sep	5 Nov	27 Nov	20 Dec	21 Jan	24 Feb	26 Mar		
Cyber Threat Operations (CTO)	1 st Draft	2 nd Draft	3 rd Draft	First Endorsement	1 st Modification of First Endorsement	2 nd Modification of First Endorsement	3 rd Modification of First Endorsement	Latest Endorsement	1 st Modification of Latest Endorsement	Since 2 June	1) Phishing Email Handling - As requested by AD(IT)(ITS)3, the categories "Unwanted" and "Neutral" have been removed. The new categories are "Spam" or "Phishing". - Justification: To unify the outcome of analyzing the reported email and prevent subjective conclusions.
Threat Hunting	Not yet released	1 st Draft	No Modification	First Endorsement	No Modification	No Modification	1 st Modification of First Endorsement	Latest Endorsement	1 st Modification of Latest Endorsement	Since 2 Aug	1) Scope of Threat Hunting - Expand the scope of threat hunting - Trend-Related Threats (Not limited but include the following): O Remote Access Tools O InfoStealers - Provide a mapping of Remote Access Tools with corresponding threat actor groups for reference
Security Operations Centre (SOC)	1 st Draft	2 nd Draft	No Modification	First Endorsement	No Modification	1 st Modification of First Endorsement	2 nd Modification of First Endorsement	No Modification	No Modification	Since 2 June	Nil
Incident Response (IR)	Not yet released	1 st Draft	No Modification	First Endorsement	No Modification	No Modification	No Modification	No Modification	No Modification	Since 2 Aug ¹	Nil

- Legend
- Reviewed by HKMA
 - Not yet reviewed by HKMA
 - Not yet released
 - No Modification compared with previous version

Footnote

¹ Not yet Triggered

Estimated TI on-site analyst workload per month (snapshot from November 2024)

Task	Outcome	Estimated Time Per Task	Estimated Frequency	Estimated FTE
CVE and Security Incidents escalation (Create Jira ticket, Provide Analysis, Provide Recommendation) <ul style="list-style-type: none">• Create JIRA ticket• Provide in-depth analysis• Provide Recommendations by PwC	Follow standard procedures for documentation and reference.	1 hours (4 incidents per day on average)	Daily	0.125
Threat Research <ul style="list-style-type: none">• Perform OSINT & PwC proprietary source sweeping• Create proprietary Critical Vulnerability Alert (CVA) analysis for critical threat (Summary, in-depth impact & technical analysis, conclusion)• Process Malware Alert of Police Force• Process Security Alert of OGCIO	1) Obtain threat-related information, such as attacker tactics, strategic information, disseminated from different TI platforms, for threat landscape. 2) Act appropriately based on the information gathered. 3) Cover a prompt response plan to IT security threats.	4 hours	Daily	0.5
Threat Hunting <ul style="list-style-type: none">• Perform Threat Actor Profiling• Perform Threat Hunting on Splunk, JIRA, Sentinel One, Trellix APT, and other security solutions	1) Determine appropriate actions to mitigate the risks by identifying the threat, such as impersonation incidents. 2) Establish monitoring mechanism for system log records. ¹	2 hours	Daily	0.25
Threat Intelligence Feed Enrichment <ul style="list-style-type: none">• Consolidate and request blocking the found IOCs for Threat Hunting via OSINT in HKMA environment	1) Establish on-going threat intelligence with updated IOCs in TI feed. 2) Cover a prompt response plan to IT security threats detected by the TI feed. ¹	0.5 hour	Daily	0.063
Phishing email reported by Comm/Settlement Team - need to leverage TI tools and check with SOC	Leverage TI tools and consult with SOC to classify the reported email by users and determine if it is a malicious event.	2 hours	Daily	0.25
Ad-hoc request from HKMA <ul style="list-style-type: none">• Process validation check to determine if HKMA has a vulnerable version of product• Update JIRA ticket with findings and route it to the potentially impacted system owners• Draft and send out notification email with findings to potentially impacted system owners• Follow-up on Users’ Patching Status• Check remediation results by system owners• Work on the in-depth investigation regarding publicly reported incidents upon request by HKMA• Work on the ad-hoc request on TI given by PwC SOC	1) Take appropriate follow-up actions to mitigate risks and enhance the security posture of HKMA if a potentially vulnerable product in HKMA is identified. 2) Agree on turnaround times with HKMA on a case-by-case basis for (urgent) requests related to specific Threat Intelligence.	3 hours	Ad hoc – Average 3 per week	0.225
TI SOP update	Enhance operational tasks, modify if necessary.	2 hour each	Ad hoc – Average 1 per week	0.022
Monthly statistics - High Threat Security Alert Monitoring	Present in the Threat Intelligence section of the HKMA SOC Monthly Report during the monthly meeting with HKMA.	2 hours	Monthly	0.011
Monthly overview of SOP status update by section		2 hours	Monthly	0.011
Monthly Major Threat Intelligence Report Highlight		2 highlight per report, 2 hours each, 4 hours total	Monthly	0.022
Monthly meeting action items follow up		1 hour	Monthly	0.006
Monthly report preparation, Pre-Monthly Meeting & Monthly Meeting		4 hours	Monthly	0.022
Total				Total: 1.507

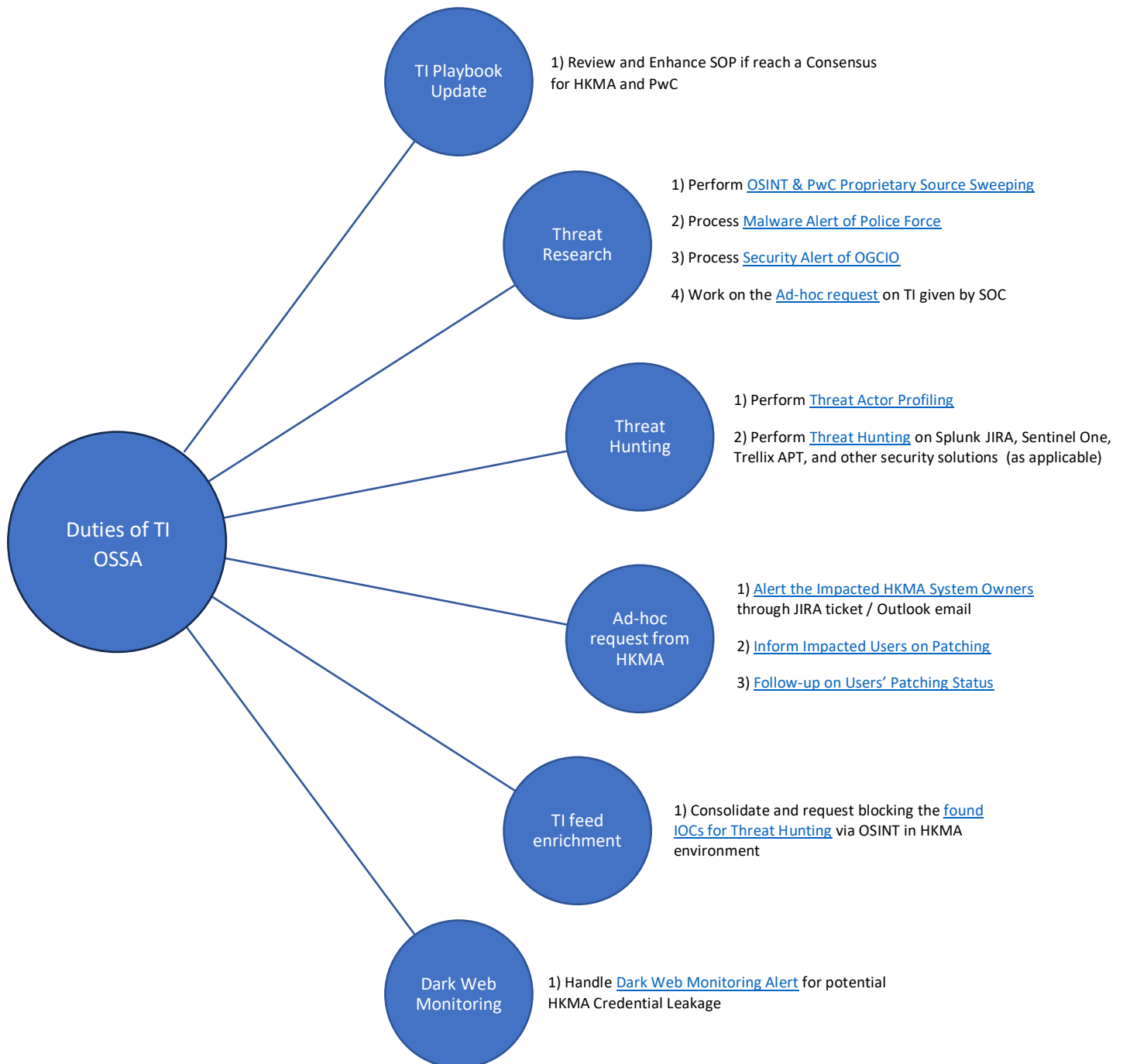
¹ The Government of the Hong Kong Special Administrative Region of the People’s Republic of China. (2024, April). Practice Guide for IT Security Threat Management. OGCI0. https://www.govcert.gov.hk/doc/PG_for_IT_Security_Threat_Management-v1.0_EN.pdf

Table of Contents

Duties of Threat Intelligence (TI) On-Site Security Analyst (OSSA)	14
1) Cyber Threat Operations (CTO)	15
a) Police Force TI Management	15
Day-to-day duties for Police Force	15
b) Threat Intelligence Alert to HKMA for HKMA-related CVEs and Incidents	15
Day-to-day duties for CVEs sweeping (Collect Data)	19
Day-to-day duties for Incidents sweeping (Collect Data)	20
Perform Threat Research	21
Confirming Relevancy of CVE with HKMA	22
Confirming Relevancy of Security Incident with HKMA	24
Case Categorization	26
Case Classification	27
Critical / High Severity CVE Processing	30
Perform Further Investigation and Document Findings in JIRA	31
Email HKMA System Owners via Outlook to Confirm System is Affected	33
Route the JIRA ticket to HKMA System Owners	35
Verify Remediation Result	36
Medium / Low Severity CVE Processing	37
Perform Further Investigation and Document Findings in JIRA	38
Sends out notification emails to HKMA system owners	39
Update JIRA Ticket	41
Security Incident Processing	42
Perform Further Investigation and Document Findings of Security Incident in the Jira ticket	42
i) Preliminary Findings Summary by TI On-Site Analyst	42
ii) In-Depth Investigation by TI On-Site Analyst	43
Request Blocking IoCs	44
c) Monthly Statistics & Report for OGCIO Security Alerts	48
HKMA Monthly Report	48
OGCIO Security Alerts	49
d) Dark Web Monitoring (DWM) Alerts Handling	52
e) HKMA Domain Monitoring (Trial-Run)	55

f) Phishing Email Handling	57
2) Threat Hunting	58
Objectives of Threat Hunting	59
Scope of Threat Hunting	60
2.1) Ticket Creation for Threat Hunting	62
2.2) Evaluation of Threat Hunting	62
2.3) Threat Actor Summary	62
2.4) Collect Findings – Key Takeaways and IoCs – Utilize in JIRA ticket.....	63
2.5) Perform Threat Hunting on Splunk, Cisco AMP, and Sentinel One	63
2.6) Validate the findings of IoCs.....	64
2.7) Create sub-ticket to request blocking the IoCs found via Threat Hunting.....	65
2.8) Close the Jira Ticket	65
3) Security Operation Centre (SOC).....	66
3.1) TI Analysis Coordination with SOC.....	66
3.2) TI Requests Findings from SOC	68
4) Incident Response (IR)	69
4.1) IR Initiation and Notifications Phase.....	69
4.1.1) Triggering IR.....	69
4.1.2) Email Notifications by HKMA and PwC	70
4.1.3) Additional Action Items.....	71
4.2) Investigation Phase.....	72
4.2.1) Collaboration with PwC DFIR team.....	72
4.3) Reporting Phase.....	72
4.3.1) Contribute Threat Intelligence Perspective in IR Report	72
4.3.2) Ongoing Monitoring of Threat Actors	73
Appendix.....	74
TI Investigation Tools.....	74
Other Sources.....	74
Incident Escalation for HKMA Evaluation	74

Duties of Threat Intelligence (TI) On-Site Security Analyst (OSSA)



1) Cyber Threat Operations (CTO)

a) Police Force TI Management

Day-to-day duties for Police Force

- 1) The PwC on-site Threat Intelligence Analyst should download 1) the Hong Kong Police email, and 2) zipped "Alert on Malicious Phishing Domains" excel file and unzip it.
- 2) Add the columns for information gathering such as "ISP", "Country", "URL exist in Previous Police alert", and "IP exist in Previous Police alert"
- 3) Go to "colab.ipynb" website, upload the csv file with the IPs in the "Alert on Malicious Phishing Domains" to get the information of "ISP", "UsageType" and "Country"
- 4) Check whether the URL/IP is existing in previous police alerts by refer to downloaded "Police all previous phishing domain_<date>.xlsx".
- 5) Create Jira Ticket with the component "TI Update" to upload the police email and the excel files for record.
- 6) Additionally, two sub-tickets should be created under the parent ticket for the proxy and SIEM updates. The first sub-ticket should be assigned the component "TI Update for Proxy" and escalated to HKMA staff Wong Kwok-hung, Gary. The second sub-ticket should be assigned the component "TI Update for SIEM" and escalated to HKMA staff Wong Sai-ming, Josh.

For more details, please refer to the separate document "Alert on Malicious Phishing Domains / Malware Alert of Police – Processing Guideline".

b) Threat Intelligence Alert to HKMA for HKMA-related CVEs and Incidents

Discover &
Research on
Threats

During working hours, **TI on-site analyst**:

- 1) Continuously monitor Threat Sources on CVEs (Common Vulnerabilities and Exposures) and Security Incidents.
- 2) Research conducted via OSINT and PwC proprietary sources, collect and analyse the research information.

Confirm Relevancy
of Threat against
HKMA

- 3) **TI on-site analyst** confirms the relevancy of threat with HKMA based on the criteria defined in Section 3 below,
 - 3.1) If the threat meets the criteria,
 - Create JIRA ticket ("ITSSOC"), perform Investigation, update JIRA ticket with findings, proceed to next workflow state.
 - 3.2) Otherwise,
 - Inform AD(IT)(ITS)3, provide supporting reason for low relevancy, and terminate at this step.

Threat Processing

- 4) **TI on-site analyst** undergo the case categorization and case classification to determine the severity level (Critical/High/Medium/Low).

- 5) **TI on-site analyst** conducts a thorough analysis, documents the threat evaluation in the JIRA ticket.

Meanwhile, the following procedures are applied based on the severity of the threat:

- 5.1) **Critical/High** Severity CVEs:

(For Critical ONLY)

- **AD(IT)(ITS)3** immediately communicates with responsible parties
- **D(IT)(ITS)1** informs relevant stakeholders, including CIO, if needed

(For both Critical/High)

- Change the assignee of the JIRA sub-ticket to **System Owner**
- **TI on-site analyst** emails System Owners via Outlook to confirm system is affected
- **System Owner** confirms if system is affected by replying email

- 5.1.1) If affected,

- **TI on-site analyst** creates sub-ticket in JIRA for remediation, **System Owner** initiates remediation, updates the sub-ticket with evidence of remediation (e.g., screenshot).
- **TI on-site analyst** verifies the remediation evidence by **System Owner** in sub-ticket.

- 5.1.2) Otherwise,

- **TI on-site analyst** creates sub-ticket in JIRA, and update it with supporting information by **System Owner**.

- 5.2) **Medium/Low** Severity CVEs:

- **TI on-site analyst** sends out notification emails to HKMA system owners, including recommendations to remediate the vulnerability.
- **TI on-site analyst** updates the JIRA ticket, attaching with screenshot of the sent notification email.

- 5.3) Security Incidents:

- **TI on-site analyst** documents the details in the Jira ticket.

Threat Resolution

- 6) **TI on-site analyst** obtains AD(IT)(ITS)3 approval, to request blocking validated IOCs if any, found through OSINT or proprietary sources.
- 7) **TI on-site analyst** escalates the ticket to HKMA AD(IT)(ITS)3, concludes that the above actions have been taken regarding the threat.
- 8) **AD(IT)(ITS)3** reviews ticket and confirm completion, closes the ticket.

NOTE: At times where HKMA makes urgent requests for specific TI, PwC will initially agree the associated turnaround time with HKMA on a case-by-case basis.

In such a scenario, the following are the steps required for both parties accordingly:

PwC

- TI / SOC on-site analyst should immediately inform the Cyber Threat Operations Leads (Jason Lee, Michael Ching) about the request.
- TI on-site analyst analyses the request with TI Team, provide a preliminary response with the agreed SLA upon HKMA's request.
- TI on-site analyst creates a JIRA ticket ("ITSSOC") upon returning to office hours.

HKMA

- AD(IT)(ITS)3 provides relevant information on the identified threat to the PwC Cyber Threat Operations Lead (Michael Ching), who will deliver the investigation results at the earliest opportunity.
- AD(IT)(ITS)3 then collects findings from the PwC Cyber Threat Operations Lead and uses these findings to communicate with the affected System Owner(s).

Reference

There are six major stages in IT security threat management. An overview of these stages is provided below, with reference to the framework in section 3.2 “IT Security Threat Management Framework” for managing IT security threat in “Practice Guide for IT Security Threat Management” version 1.0² published by OGCIO in April 2024.

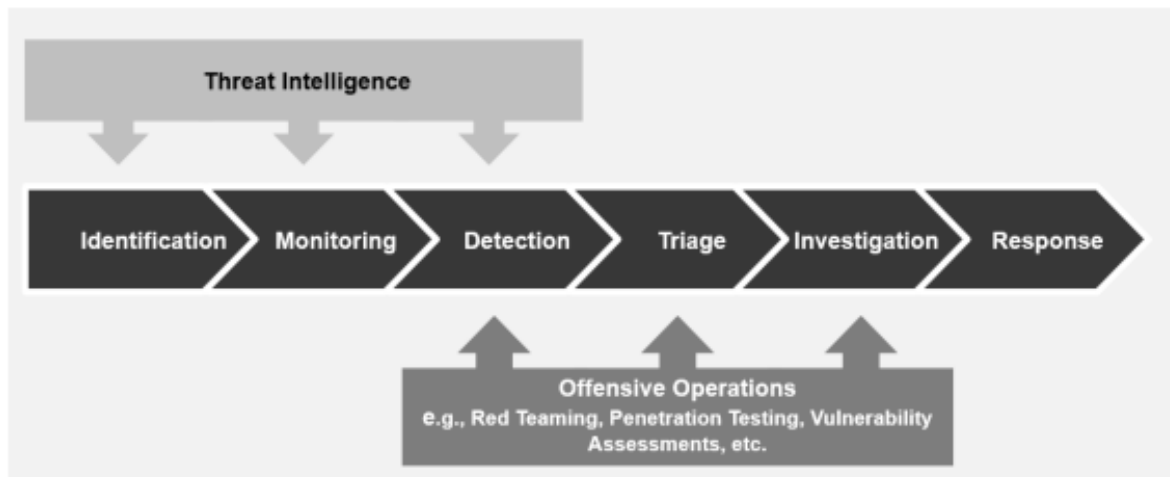


Figure 2.3 Major Stages in IT Security Threat Management Framework

² The Government of the Hong Kong Special Administrative Region of the People’s Republic of China. (2024, April). Practice Guide for IT Security Threat Management. OGCIO. https://www.govcert.gov.hk/doc/PG_for_IT_Security_Threat_Management-v1.0_EN.pdf

Step 1)

On working days from 9am to 6pm, the PwC TI on-site analyst will perform continuous monitoring on CVEs and Security Incidents from the Threat Sources.

Day-to-day duties for CVEs sweeping (Collect Data)

i) For CVEs:

Threat Sources to be monitored

- Continuously monitor the PwC mailbox for Critical Vulnerability Alerts (CVAs) sent from "Darklab Threat Intelligence" with the email address darklab.cti@hk.pwc.com.
- Additionally, monitor the HKMA provisioned device for OGCIO CVEs sent from "GovCERT Subscription/OGCIO" with the email address cert@govcert.gov.hk.

How to monitor Threat Sources

- Inspect incoming emails in these mailboxes to identify any CVE notifications. For PwC CVAs, the CVE number (e.g., CVE-2024-<number>) is located at the end of the email subject.

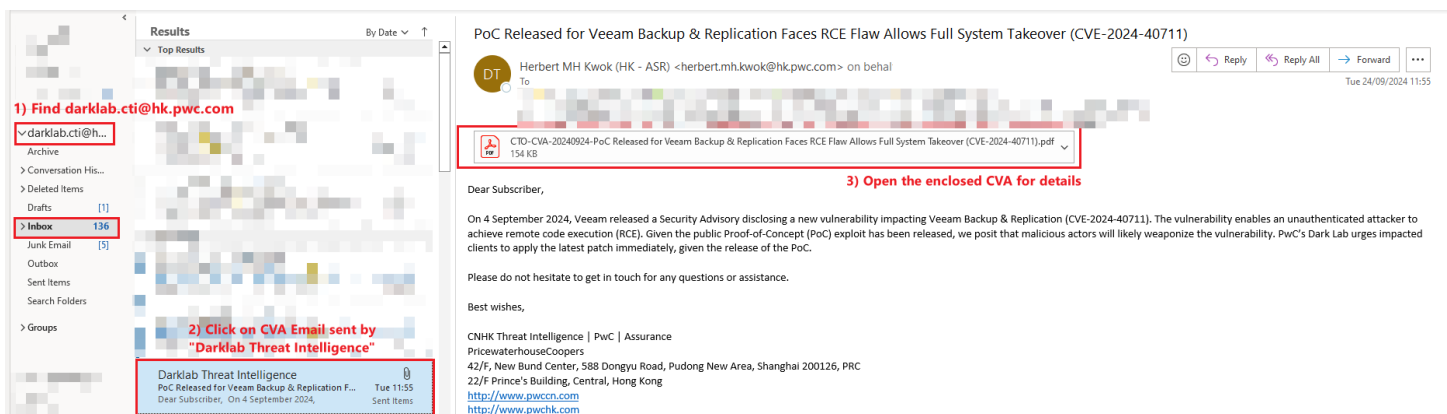


Figure 1: Sample CVAs in PwC's Outlook mailbox

- For OGCIO CVEs, the email subject begins with "Security Alert <Date>" or "High Threat Security Alert <Date>", with the inclusion of the CVA keyword in the title or summary of the email.

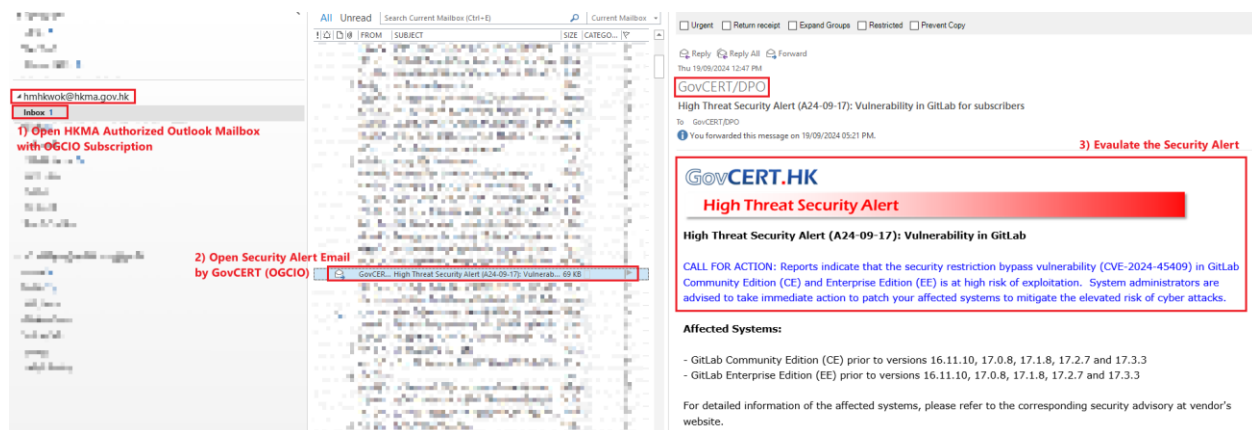


Figure 2: Sample OGCIO Security Threat Alert in HKMA's outlook's mailbox

ii) For Incidents:

Day-to-day duties for Incidents sweeping (Collect Data)

The TI on-site analyst will perform the following Incident Sweeping including but not limited to "Other Sources" listed in the Appendix:

Intelligence Sweeping	Description
Intelligence from PwC News and Threat Intelligence Portal	<p>1) The TI on-site analyst should review the PwC News and Threat Intelligence Portal to follow security vendors' updates, social media trends, as well as intelligence from reputable cybersecurity sources e.g. BleepingComputer, The Register, CyberScoop, etc.</p> <p>2) The TI on-site analyst should also <u>perform regular monitoring (e.g. hourly)</u> during a business day. The analysis will be based on reports generated <u>within the past 24 hours</u> and their relevance to HKMA in terms of potential threats.</p>
Other Newly Raised Information from PwC's internal cyber threat operations	Example such as open source, dark web, and proprietary source

Step 2)

Perform Threat Research

The TI on-site analyst should conduct preliminary research based on the discovered CVE / Incident using OSINT and PwC proprietary sources, collect and analyse the research information.

Step 3)

The TI on-site analyst should confirm the relevancy of threat with HKMA by consolidating the researched information, then maps it to the proprietary CVA Criteria: “Capability”, “Intent”, and “Opportunity” as shown below.

3.1) If the threat meets pre-defined criteria (see below) - [“Confirming Relevancy of CVE with HKMA”](#) or [“Confirming Relevancy of Security Incident with HKMA”](#) section, it is considered to be relevant. The **TI on-site analyst** should:

- Create (“ITSSOC”) ticket in JIRA Confluence with the component "TI Alert".
- Change the assignee name be AD(IT)(ITS)3 - HKMA primary contact point of Threat Intelligence.
- Perform Investigation of the threat.
- Update JIRA ticket with findings.
- Proceed to the next step (Step 4).

3.2) Otherwise, the **TI on-site analyst** should:

- Inform AD(IT)(ITS)3 with supporting reason for low relevancy of threat with HKMA.
- If agreed by AD(IT)(ITS)3, terminate at this step.

NOTE:

1) As requested by HKMA, if the **“High Threat Security Alert”** is issued by **OGCIO** or **Proprietary Critical Vulnerability Alert** is issued by **PwC**, the TI on-site analyst should create a JIRA ticket for every threat follow-up.

2) The TI on-site analyst should evaluate the relevancy of CVEs / Incidents based on the following pre-defined criteria (see below), which include but are not limited to:

i) For CVEs:

Confirming Relevancy of CVE with HKMA

a. Capability

- Attack Vector (e.g., Considering the level of access is required to exploit the vulnerability)
- Attack Complexity (e.g., Considering the ease for attackers to exploit the vulnerability)
- User Interaction (e.g., Whether exploitation require user execution)

b. Intent

- Active exploitation in the wild (i.e., The vulnerability has been observed to be exploited by threat actors)
- Relevant reporting in the source that PwC TI on-site analyst to check regarding to CVEs

Source Checking	Purpose
OSINT	When multiple researchers report a CVE, it suggests a higher likelihood of it being a critical vulnerability and more prone to exploitation.
Dark Web	Checking for any references to the CVE (e.g., Threat actors selling Proof of Concept (PoC) or requesting exploit codes)
Social Media	Monitoring discussions on platforms like Twitter helps assess public perception, indicating the criticality the vulnerability.

c. Opportunity

- CvSS v3 score
- Whether it is Actively Exploited in the Wild
- PwC Client Product Coverage – Known use by other SOC client
- Possibility of matching to one of the reference
 - 1) "HKMA_Technology_stack_Reference.xlsx"
 - 2) Tenable Vulnerability Management
 - 3) Check with users via Outlook email, asking potentially affected parties explicitly if they are using the affected system and its version

Category	Status	Technology	Domain	Subcat	Hosting
(A) Data Science	GREEN	Apache Spark	Data/ Infrastructure	Data Compute	On-Premises
(A) Data Science	GREEN	Jupyter	Data	Data Science Studio / Notebook	On-Premises
(A) Data Science	GREEN	MatLab	Data	Advanced Analytics	On-Premises
(A) Data Science	GREEN	R studio	Data	Data Science Studio / Notebook	On-Premises
(A) Data Science	GREEN	Tableau	Data	Data Visualisation	On-Premises
(A) Data Science	AMBER	Anaconda	Data/ Application Development	Advanced Analytics	On-Premises
(A) Data Science	AMBER	DataRobot	Data	Data Science Studio / AutoML	On-Premises
(A) Data Science	AMBER	Eviews	Data	Advanced Analytics	On-Premises
(A) Data Science	AMBER	FLA	Data	Network Analysis	On-Premises

Figure 3: HKMA_Technology_stack_Reference.xlsx

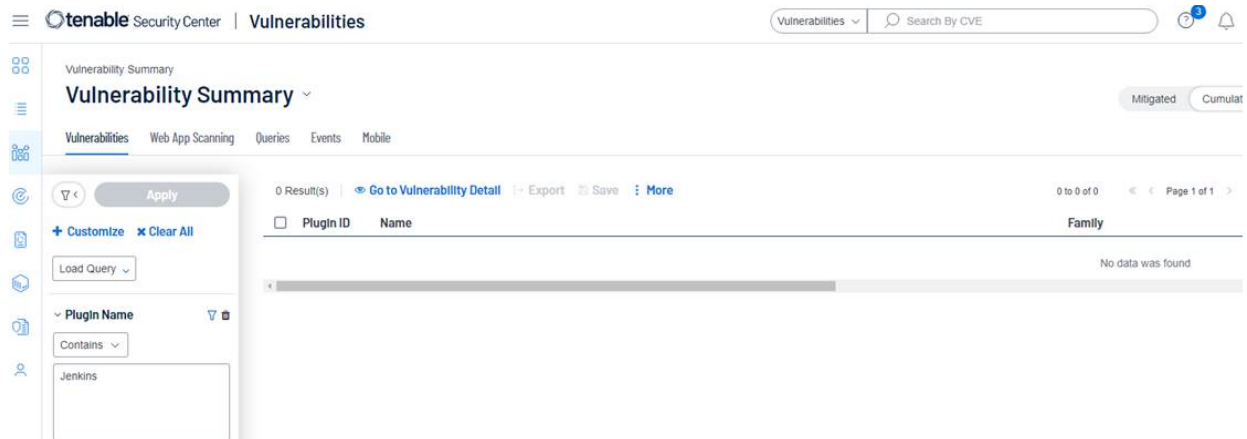


Figure 4: Continuous Vulnerability Management (CVM) using Tenable

If there is no match, the TI on-site analyst should write the following as a Jira comment.

Type	Content of Request for Ticket Closure in Jira
Ticket	"Ticket is closed. Based on the result from Tenable, none of the above listed CVEs are found in our asset list."

ii) For Incidents:

Confirming Relevancy of Security Incident with HKMA

- a. Assessing the relevance of the incident against HKMA (e.g., Potential match with HKMA's basic Inventory List on technology)
- b. Assessing the relevance of the incident to Hong Kong
- c. Assessing the relevance of the incident with respect to whether the industry is typically recognized globally and/or locally as a critical infrastructure operator (e.g., Singapore Cyber Security Act may have a list of Essential Services³)
- d. Assessing the relevance of the incident to specific industries that are relevant to HKMA (e.g., Global Central Banks, Fintech, Financial Services, and Property Development⁴, etc.)
- e. If PwC cannot find any publicly available information regarding the incident or if the incident has not been publicly disclosed, PwC will provide the findings of their analysis (if any) to HKMA via email including relevant case studies of incident experiences, where applicable
- f. HKMA provides the information on IOC to PwC TI / SOC on-site analyst for further investigation
- g. Upon request by HKMA, PwC will provide a summary regarding publicly reported incidents based on their understanding from OSINT, and the expected turnaround is as follows:

³ Cybersecurity act. Default. (2024, June). <https://www.csa.gov.sg/faq/cybersecurity-act>

⁴ Hong Kong Monetary Authority (2024, June). Regulatory Resources. <https://www.hkma.gov.hk/eng/regulatory-resources/regulatory-guides/by-subject-current/>

Time Range	Description	Expected Turnaround
During office hours	Monday to Friday, 9 AM to 6 PM	1) PwC on-site analyst should analyze the request with the TI Team, provide a preliminary response <u>within 1 business day</u> upon HKMA's request.
During non-office hours	The time outside of office hours	2) Provide timely updates on HKMA's request, if necessary.

NOTE: At times where HKMA makes urgent requests for specific TI, PwC will initially agree the associated turnaround time with HKMA on a case-by-case basis.

In such a scenario, the following are the steps required:

1. PwC TI / SOC on-site analyst should immediately inform the Cyber Threat Operations Leads (Jason Lee, Michael Ching) about the request.
2. Analyze the request with the TI Team, provide a preliminary response with the agreed SLA upon HKMA's request.

Step 4)

The TI on-site analyst will perform Case Categorization and Case Classification (both detailed below) and include the findings in JIRA.

Case Categorization

The TI on-site analyst categorizes the threat into relevant categories:

- Social threats (e.g., social engineering attacks, phishing)
- Technical Threats (e.g., Malware, zero-day exploits)
- Environmental Threats (e.g., hardware failures, outage)
- Others (e.g., threat landscape)

Within each category, the analyst should define specific threat types as comprehensively as possible.

Case Classification

The TI on-site analyst should reference multiple sources to and use the Threat Classification Matrix (see below) determine the **Final Severity Level (Critical / High / Medium / Low) of vulnerability**. The following criteria should be considered to determine the threat severity:

- Internet Facing System
- CvSS v3 Impact Score
- *PwC Client Product Coverage (Known use by various SOC client)
- Exploited in the Wild

*It is a proprietary source by PwC

NOTE: At times where HKMA makes manual override of **Final Severity Level** for specific TI, PwC will initially agree on the associated **Final Severity Level** with HKMA on a case-by-case basis.

System Type	CVSS V3 Impact Score	PwC Client Product Coverage	Exploited in the Wild	Final Severity Level
Internet Facing System / Critical System				
	9.0-10.0	Yes	Yes	Critical
	7.0-8.9	Yes	Yes	High
	4.0-6.9	Yes	Yes	Medium
	0.1-3.9	Yes	Yes	Low
	9.0-10.0	Yes	No	High
	7.0-8.9	Yes	No	Medium
	4.0-6.9	Yes	No	Medium
	0.1-3.9	Yes	No	Low
	9.0-10.0	No	Yes	High
	7.0-8.9	No	Yes	Medium
	4.0-6.9	No	Yes	Medium
	0.1-3.9	No	Yes	Low
	9.0-10.0	No	No	High
	7.0-8.9	No	No	Medium
	4.0-6.9	No	No	Low
	0.1-3.9	No	No	Low
Non-Internet Facing System				
	9.0-10.0	Yes	Yes	Medium
	7.0-8.9	Yes	Yes	Medium
	4.0-6.9	Yes	Yes	Medium
	0.1-3.9	Yes	Yes	Low
	9.0-10.0	Yes	No	Medium
	7.0-8.9	Yes	No	Medium
	4.0-6.9	Yes	No	Low
	0.1-3.9	Yes	No	Low
	9.0-10.0	No	Yes	Medium
	7.0-8.9	No	Yes	Medium
	4.0-6.9	No	Yes	Low
	0.1-3.9	No	Yes	Low
	9.0-10.0	No	No	Medium
	7.0-8.9	No	No	Low
	4.0-6.9	No	No	Low
	0.1-3.9	No	No	Low

Figure 5: Threat Classification Matrix

Step 5)

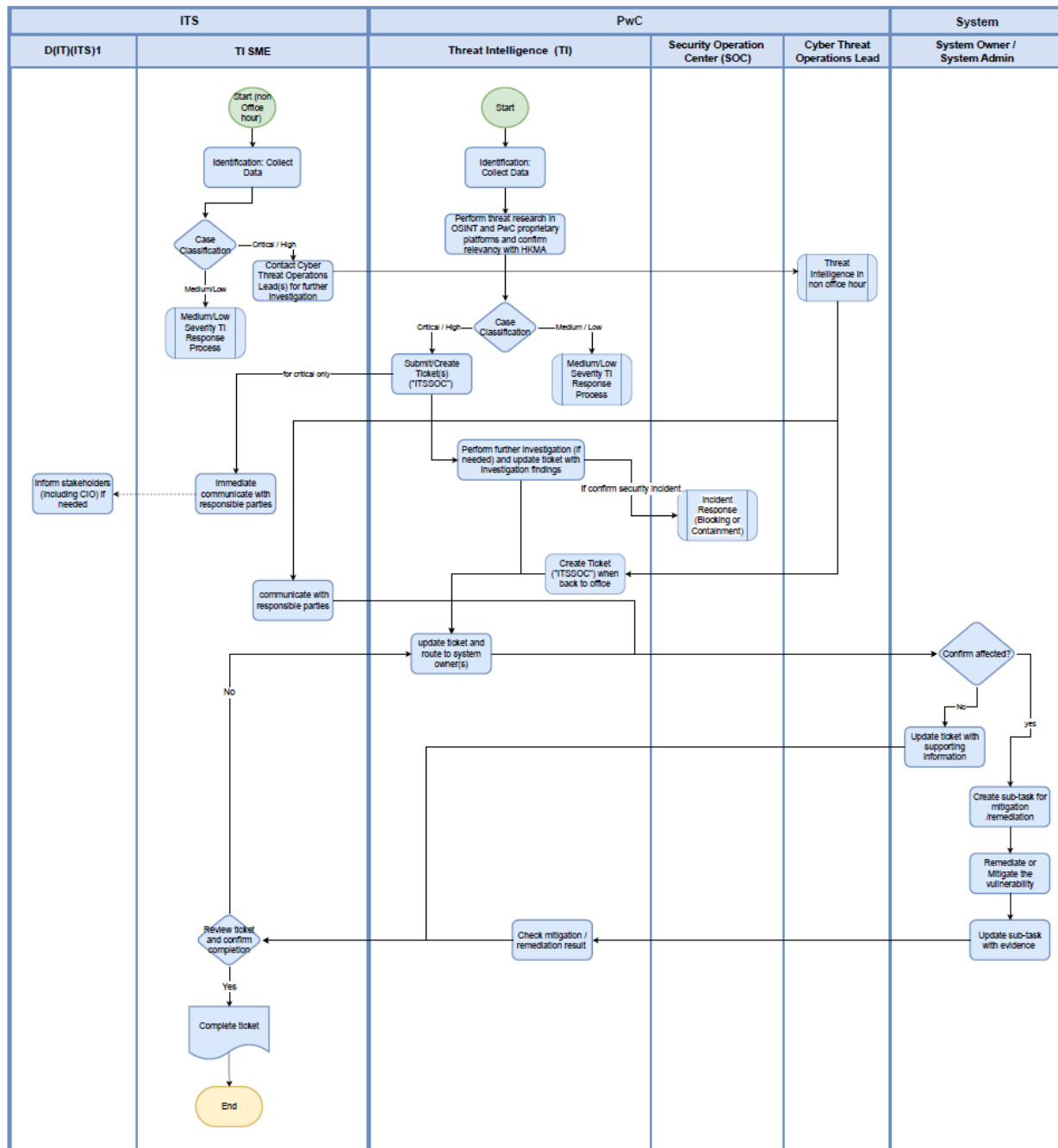
The TI on-site analyst obtains the Final Severity Level of the CVE in **step 4)** above. Then, the following actions should be taken based on the Final Severity Level of vulnerability (**Critical / High / Medium / Low**)

Final Severity Level of CVE	Critical	High	Medium	Low
Follow-up Actions by PwC TI on-site analyst				
Perform Further Investigation and Document Findings in JIRA	✓	✓	✓	✓
Email HKMA System Owners via Outlook to Confirm System is Affected				
If Confirm Affected: - Route the JIRA ticket to HKMA system owners - Verify Remediation Result	✓	✓		
Sends out notification emails to HKMA system owners Updates the JIRA ticket			✓	
Follow-up Actions by HKMA				
AD(IT)(ITS)3 immediately communicates with responsible parties D(IT)(ITS)1 informs relevant stakeholders, including CIO, if needed	✓			
System Owner confirms if system is affected, remediate the system if necessary, update sub-ticket with evidence	✓	✓		
System Owner confirms if system is affected, remediate the system if necessary, no need to update sub-ticket			✓	

Figure 6: Follow-up Actions Based on Final Severity Level of CVE

TI on-site analysts and HKMA should take follow-up actions accordingly, referencing the table above. Detailed follow-up actions are as follows:

Critical / High Severity CVE Processing




Perform Further Investigation and Document Findings in JIRA

The TI on-site analyst should enclose the attachment(s) if any, then document the findings to update the ticket in JIRA (See following steps).

- a) Enclosed OGCIO Threat Alert Email if any
- b) Enclosed PwC proprietary Critical Vulnerability Alert (CVA) source issued by PwC's Threat Intelligence team if any (See below)

Critical Vulnerability Alert

24 September 2024



TLP: AMBER
No third party distribution
Tags: Technology Stack-Related

PoC Released for Veeam Backup & Replication Faces RCE Flaw Allows Full System Takeover (CVE-2024-40711)

Introduction

On 4 September 2024, Veeam released a Security Advisory disclosing a new vulnerability impacting Veeam Backup & Replication (CVE-2024-40711). The vulnerability enables an unauthenticated attacker to achieve remote code execution (RCE). Given the public Proof-of-Concept (PoC) exploit has been released¹, we posit that malicious actors will likely weaponize the vulnerability. The following report is issued as it satisfies our criteria for the release of a critical vulnerability alert.

PwC's Dark Lab urges impacted clients to apply the latest patch immediately, given the release of the PoC. The following report is issued as it satisfies our criteria for the release of a critical vulnerability alert.

PwC's Dark Lab summarises the known information regarding this vulnerability below:

CVE(s)	CVE-2024-40711
CVE Published Date	4 September 2024
CVSS v3	9.8 ²
Affected Products	<ul style="list-style-type: none">Veeam Backup & Replication - Version 12.1.2.172 and all earlier version 12 builds
Description	Deserialization of Untrusted Data Vulnerability
Potential Impact	Remote Code Execution
Proof of Concept (PoC) Available	Yes ³
Exploited in the Wild	No
Patch Available	Yes ⁴
Workaround Available	No

Figure 7: Critical Vulnerability Alert (CVA)

c) Background of the CVE

Include an identification number CVE-yyyy-xxxx, where yyyy stands for the year and xxxx is a unique identifier.

d) Summary of the CVE

Provide a brief overview of the vulnerability.

e) Potential Impact of the CVE

Evaluate the potential impact the vulnerability brings.

f) Affected Product and Its Version

Specify the affected product and its version as indicated by each CVE entry.

g) Recommendations / Suggestions Provided by PwC

Mainly suggest patch management.

Template for documenting CVEs in the JIRA ticket

Template

Subject: [Patch Request] High Threat Security Alert: **%Multiple Vulnerabilities/Vulnerability%** in **%Application name%**

Dear all,

%Vendor Name% has released **%Month, Year%** Security Updates, please apply the patch accordingly.

For **%CVE ID% (%CVE Name%)**, the CVSS score is **%CVSS Score%** and **%could be exploitable/is not exploitable%**.
The vulnerability enables **%What Threat Actor can Achieve%**.

Affected Version(s):

%Affected Version(s)%

Actions:

We strongly suggest administrator to **%Action Taken (i.e., upgrade the version to (name of Fixed Version) or after)%**.
Based on the Threat Classification Matrix, the vulnerability is **%Severity Level%** and should be patched within **%SLA to Patch%** if the servers you owned are affected.

If you confirm that your systems are affected, please create a sub-ticket for notification and remediation. Additionally, please provide a screenshot as evidence once the patching process is completed.

References:

%Reference Link%

Email HKMA System Owners via Outlook to Confirm System is Affected

The TI on-site analyst should email HKMA System Owner(s) via Outlook who is/are adapting the potentially affected system:

Template for Email

Template

Subject: **[Urgent]** [%CVE Identifier%] %CVE Title%

Dear all,

This is to notify you that %Vendor Name% has released an official advisory and patches to remediate %CVE Identifier% for potentially affected %Affected Product Name% Instances.

Attribute		Details
Name		[%CVE Identifier%] %CVE Title%
CVSS v3 Score		%CVSS v3 Score%
Exploitation Metrics	Exploited in the Wild (Attackers are already leveraging the vulnerability)	%Yes or No?%
	Exploitable	%Yes or No?%
	Remotely Exploitable	%Yes or No?%
	Exploitable by Non-Privileged Accounts	%Yes or No?%
System Known to be Widely Used		%Yes or No?%
Affected Version(s)		%Versions of Products%
Impact		%Type of Vulnerability% enables attacker to %Consequence%.
Final Severity Level		High
Action(s)		Please reply to this email if you confirm your system(s) are affected. We suggest following the Fortinet Advisory to apply the patch or workaround.
Reference(s)		Vendor Security Advisory (with hyperlink) Tenable for CVE (with hyperlink)

Based on the System Owner(s)' reply, TI on-site analyst take the following actions:

5.1.1) If the System Owner(s) confirm the system is affected:

- TI on-site analyst creates sub-ticket in JIRA for remediation purpose.
- System Owner initiates remediation, updates the sub-ticket with evidence of remediation (e.g., screenshot).

5.1.2) Otherwise:

- TI on-site analyst creates sub-ticket in JIRA, and update it with supporting information provided by System Owners in email (if any).

Route the JIRA ticket to HKMA System Owners

The TI on-site analyst should change the Assignee to be the name of HKMA System Owner(s) who is/are adapting the potentially affected system, then the ticket will be created with the following points:

- Add "[TI alert escalation]" to the front of the ticket title.
- Set the ticket component as "TI alert escalation."
- Set the assignee to be the according stakeholder.
- Set the status of the sub-ticket as "In progress."
- Attach the supporting information to the ticket, or OGCIO Email Alert where applicable.

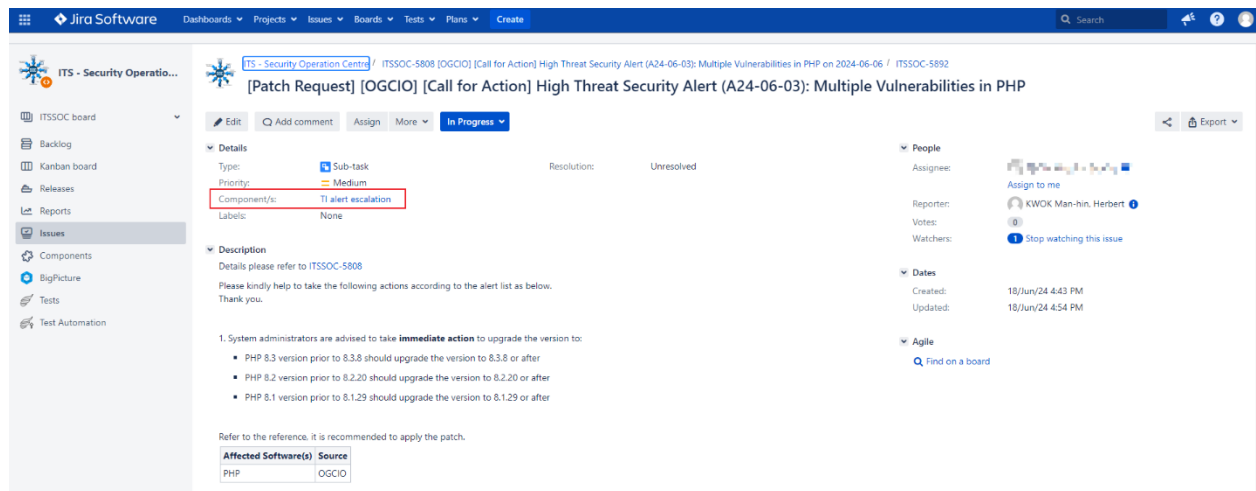


Figure 8: Sample template of assigning JIRA ticket to stakeholder(s)

Verify Remediation Result

TI on-site analyst verifies the remediation evidence by System Owner in sub-ticket, ensuring the patched version has remediated the vulnerability.

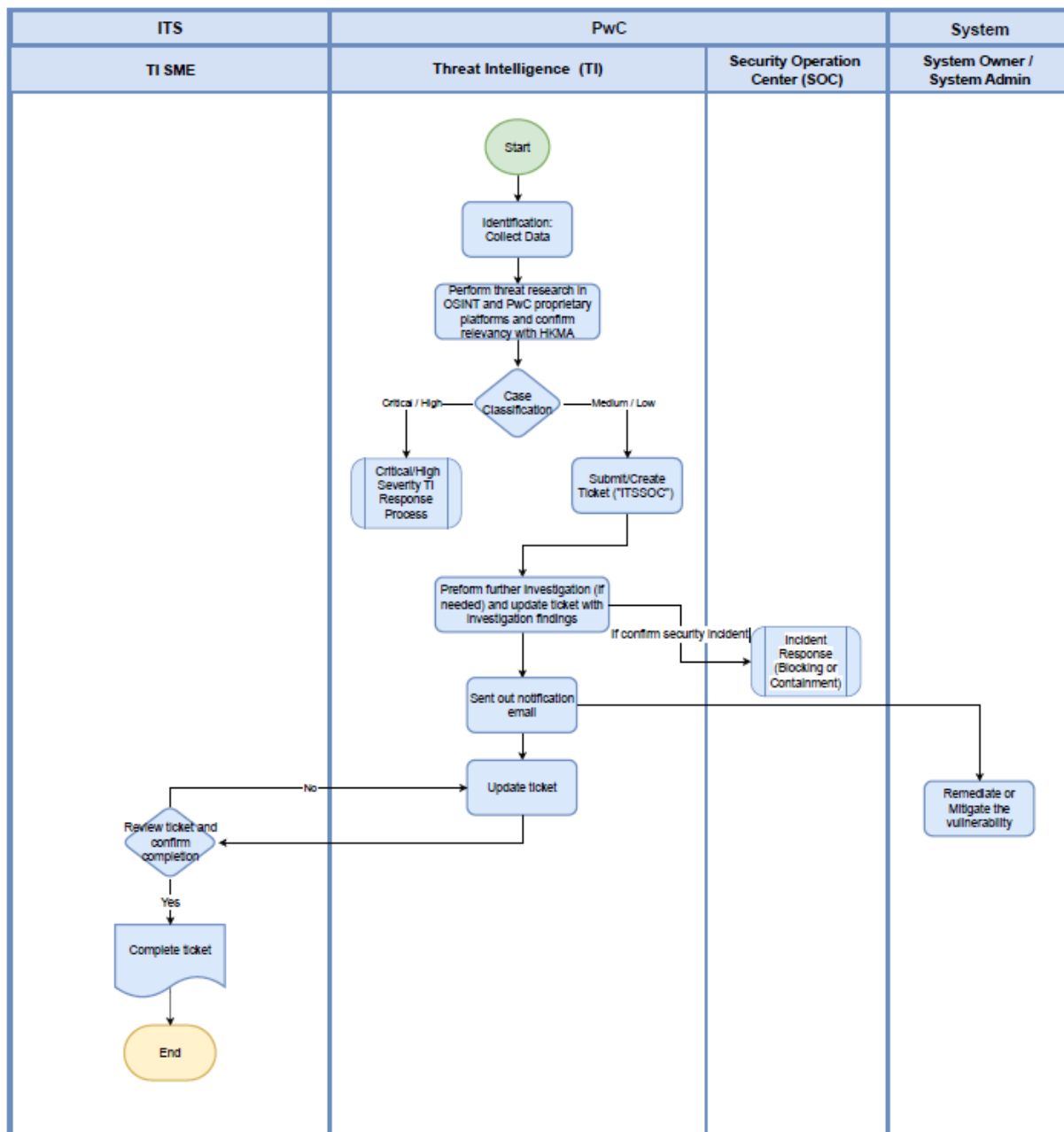
The TI on-site analyst then marks the sub-ticket's status as "Done," includes a justification in the sub-ticket, and seeks approval for sub-ticket closure from AD(IT)(ITS)3.

The following is a reference for comments in the JIRA ticket/sub-ticket. Additional details can be added if applicable:

[Jira Template] Ticket / Sub-ticket Closure Comment

Type	Content of Request
Ticket	"The ticket is closed as confirmed there is no system owner leveraging the affected version of the system for past two weeks." OR "The ticket is closed as confirmed all system owner leveraging the affected version of the system has completed the patch for past %Patching duration% ."
Sub-ticket	"The ticket is closed as confirmed %System owner name% has completed the patch."

Medium / Low Severity CVE Processing



Perform Further Investigation and Document Findings in JIRA

Please refer to the above "[Perform Further Investigation and Document Findings in JIRA](#)" in "Critical / High Severity CVE Processing".

Sends out notification emails to HKMA system owners

The TI on-site analyst should enclose the attachment(s) if any, then document the findings to update the ticket in JIRA (See following steps).

a) Background of the CVE

Include an identification number CVE-yyyy-xxxx, where yyyy stands for the year and xxxx is a unique identifier.

b) Summary of the CVE

Provide a brief overview of the vulnerability.

c) Potential Impact of the CVE

Evaluate the potential impact the vulnerability brings.

d) Affected Product and Its Version

Specify the affected product and its version as indicated by each CVE entry.

e) Recommendations / Suggestions Provided by PwC

Mainly suggest patch management.

Template for documenting CVEs in the Outlook Email

Template

Subject: **[Urgent]** [%CVE Identifier%] %CVE Title%

Dear all,

This is to notify you that %Vendor Name% has released an official advisory and patches to remediate %CVE Identifier% for potentially affected %Affected Product Name% Instances.

Attribute		Details
Name		[%CVE Identifier%] %CVE Title%
CVSS v3 Score		%CVSS v3 Score%
Exploitation Metrics	Exploited in the Wild (Attackers are already leveraging the vulnerability)	%Yes or No?%
	Exploitable	%Yes or No?%
	Remotely Exploitable	%Yes or No?%
	Exploitable by Non-Privileged Accounts	%Yes or No?%
System Known to be Widely Used		%Yes or No?%
Affected Version(s)		%Versions of Products%
Impact		%Type of Vulnerability% enables attacker to %Consequence%.
Final Severity Level		High
Action(s)		Please reply to this email if you confirm your system(s) are affected. We suggest following the Fortinet Advisory to apply the patch or workaround.
Reference(s)		Vendor Security Advisory (with hyperlink) Tenable for CVE (with hyperlink)

Update JIRA Ticket

TI on-site analyst then update JIRA ticket by commenting with attaching the screenshot of the sent notification email.

The screenshot shows the Jira Software interface for a ticket titled "IT Security/HKMA". The ticket is in the "Issues" section. A comment by "KWOK Man-hin, Herbert" is highlighted with a red box. The comment contains a screenshot of a VMware security alert for CVE-2024-38812, which is a heap overflow vulnerability in vCenter Server. The alert includes details about the vulnerability, affected versions, and recommended actions. The JIRA interface shows the "Activity" tab with the comment history.

Activity

All Comments Work Log History Activity

Newest first 15

You can now pin up to five comments to highlight important information. Pinned comments will appear above all other comments, so they're easy to find.
[Got It](#) • [Learn more about pinned comments](#)

✓ KWOK Man-hin, Herbert added a comment - 5 hours ago

Mon 23/09/2024 02:17 PM

IT Security/HKMA

Fw: High Threat Security Alert (A24-09-16): Multiple Vulnerabilities in VMware Products for subscribers

From: DE CHONG@HKMA, Leo LAM@HKMA, Ron KY@HKMA, Sara HY@HKMA, Tammy SLEUNG@HKMA, Bernard LI@HKMA, Ryan CH@HKMA, Simon CH@HKMA, Amy CH@HKMA, Susan CH@HKMA, Susan CH@HKMA, Edward CH@HKMA, Susan CH@HKMA, Jerry YK@HKMA, Ching@HKMA, Raymond HS@HKMA, Andy HO@HKMA, Stephen YC@HKMA, Jade TH@HKMA, Benny ML@HKMA

Dear all,

VMware has released an official advisory and patches to remediate the vulnerabilities. Regarding this, we advise you to patch as soon as possible to eliminate the potential threat of exploitation.

For CVE-2024-38812 (vCenter Server Heap-Overflow Vulnerability), the CVSS score is 9.8 and it is exploitable.

Summary:
The vCenter Server contains a heap-overflow flaw. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet, potentially leading to remote code execution.

Affected Version(s):

- VMware vCenter Server
- VMware Cloud Foundation

Actions:
We strongly suggest administrators apply the released patch [here](#) immediately.

References:

- [Broadcom Security Advisory](#)
- [Tenable CVE-2024-38812](#)

Kind regards,
IT Security

Edit • Delete • Pin • ⌵

✓ KWOK Man-hin, Herbert added a comment - 5 hours ago

We have notified the responsible parties via email about the CVE and recommend immediate patching to mitigate the risk.

Edit • Delete • Pin • ⌵

Add a comment...

Figure 9: Sample of attaching the screenshot of the sent notification email

Security Incident Processing

Perform Further Investigation and Document Findings of Security Incident in the Jira ticket

i) Preliminary Findings Summary by TI On-Site Analyst

The TI on-site analyst compiles preliminary findings from OSINT, social media, and security data sources (e.g., VirusTotal, URLscan.io, AbuseIPDB) using the following proprietary template:

[Analysis Template] OSINT Sweeping

Name	Description
IP/Domain/URL to be investigated	N/A
Confidence	Confidence level
Traffic Light Protocol (TLP)	<p>%Red/Amber/Green/White%</p> <p>Each colour represents for how the information should be handled.:</p> <p>i) Red: The most sensitive and should only be shared within the organization on a need-to-know basis.</p> <p>ii) Amber: information that should be shared within the organization and with trusted partners.</p> <p>iii) Green: information that can be shared more widely</p> <p>iv) White: information that can be publicly shared</p>
Target Sector	Sector/Industry that involved
Target Country	N/A
Identified Threat Actor (TA)	Individuals or groups that intentionally cause harm to digital devices or systems
Threat Actor Type	Industry of Threat Actor, if applicable
Tactics, Techniques & Procedures (TTP)	Search for the name and the ID of attack technique which are involved in the incident in MITRE ATT&CK framework.
Indicators of Attack (IOAs)	<p>Example:</p> <p>Unexpected login attempts</p> <p>Unusual network traffic</p> <p>Suspicious file downloads</p>
Indicators of Compromise (IOCs)	<p>Example:</p> <p>Malicious IP/Domain/URL/signature/hash</p>

[Analysis Sample] OSINT Sweeping

Sample

Source: OSINT

Confidence: High

TLP: AMBER

Target Sector: Supply Chain

Target Country: Worldwide

Identified TA: China-based CDN company "Fnull"

Threat Actor Type: Information technology

TTP: T1059 - Command and Scripting Interpreter

IOA: N/A

IOC: %IP/URL/Domain/Signature/Hash%

ii) In-Depth Investigation by TI On-Site Analyst

The TI on-site analyst collaborates with the TI team for a comprehensive investigation to identify any malicious IP(s) or domain(s) and assess their potential indication of a targeted attack. The following factors should be considered, where applicable:

- Pivoting on fingerprints / thumbprints of other malicious domains that may be impersonated by the same threat actor
- Determine if the malicious domain shares the same IP address
- Assess if the domain registration is recent / young
- Conduct source code analysis, particularly for domains applicable to webpages (e.g., Look for redirected pages and assess their purpose)
- Determine the intention of the threat actor behind the identified activity
- If applicable, include relevant case studies of incident experiences where there is insufficient public and PwC source information, such as cases without IOCs or identified threat actors.

Request Blocking IoCs

The TI on-site analyst should obtain AD(IT)(ITS)3 approval, to request blocking validated IOCs, if any, based on their types indicating below.

Blocking IoCs with Domains

- a) The TI on-site analyst should block the domain in proxy by creating a sub-ticket with the title prefixed by "[Block request for proxy]."
- b) Set the ticket component as "Block request for proxy."
- c) Set the status of the sub-ticket as "In progress."
- d) Use the sample template provided below for the sub-ticket in Jira.

[Jira Template] Request on blocking IoCs with Domains in Proxy

Template

This request is requested by Alex Li. Details please refer to ITSSOC-xxxx

Please kindly help to take the following actions according to the alert list as below.
Thank you.

Block the mentioned URL in **Proxy**

Refer to the reference, it is recommended to block below domain in **Proxy**

Domain(s)	Source
Domain name	TI

Blocking IoCs with Hash Values

- a) TI on-site analyst should block the hashes in Sentinel 1 and Cisco AMP by creating sub-tickets. Add "[Block request for S1]" or "[Block request for Cisco AMP]" respectively to the front of the sub-ticket titles.
- b) Set the ticket component as "Block request for S1" and "Block request for Cisco AMP" respectively.
- c) Set the status of the sub-ticket as "In progress."
- d) Use the sample template provided below for the sub-ticket in Jira.

[Jira Template] Request on blocking IoCs with Hash Values in Sentinel 1 (S1) or Cisco AMP

Template

This request is requested by Alex Li. Details please refer to ITSSOC-xxxx

Please kindly help to take the following actions according to the alert list as below.
Thank you.

Update the anti-virus definition/blacklist (**Sentinel 1 / Cisco AMP**) with the mentioned hash values

Hash

Description	MD5	SHA1	SHA256
Hash Value			

NOTE: If the IoC contains a partial signature (e.g., only SHA256), TI on-site analyst should search for the corresponding SHA1 and MD5 hashes as well, where applicable.

Blocking IoCs with IP Addresses

- a) TI on-site analyst should block the hashes in proxy by creating two sub-tickets. Add "[Block request for NIPS]" to the front of the sub-ticket titles.
- b) Set the ticket component as "[Block request for NIPS]".
- c) Set the status of the sub-ticket as "In progress."
- d) Use the sample template provided below for the sub-ticket in Jira.

[Jira Template] Request on blocking IoCs with Hash Values in Proxy

Template

This request is requested by Alex Li. Details please refer to **ITSSOC-xxxx**

Please kindly help to take the following actions according to the alert list as below.
Thank you.

Update the anti-virus definition/blacklist (**NIPS**) with the mentioned IP

IP

Type	Value	VT Score	Usage Type	Reference
IP Address				

Remark: As requested by HKMA, when a TI on-site analyst creates a ticket including an IP Address request for blocking, the brackets between the dots of the IP Address will be removed in Jira ticket, for smoother operation.

Step 6)

TI on-site analyst escalates the ticket to HKMA AD(IT)(ITS)3, concludes that the above actions have been taken regarding the threat.

Step 7)

AD(IT)(ITS)3 reviews ticket and confirm completion, closes the ticket.

c) Monthly Statistics & Report for OGCI Security Alerts

HKMA Monthly Report

For the HKMA Monthly Report, the following statistics will be included:

- Communications/Settlement Phishing Emails
- Threat Hunts
- OGCI High Threat Security Alerts
- PwC Proprietary Critical Vulnerability Alerts
- SOP Status of Operational Intelligence
- Major Threat Intelligence Report Highlight & Executive Summary
- Threat Intelligence Report List

OGCIO Security Alerts

- 1) Access the HKMA internal Sharepoint named [SOC Filing Database](#).
- 2) Click on “3.1 High Threat Security Alert Monitoring (2024 March Start) – New”.

SharePoint

SOC Filing Database

new item

By Category By Author By Subject Officer Find an item

Doc Type	Title	Subject Officer	Source Doc Date	Filing Date	Last Modified	By Last Editor	Author	Notes ID
Normal Text	3.1 High Threat Security Alert Monitoring (2024 March Start) - New	CHOW Tin-ik, Timmy	30/04/2024	30/04/2024 16:24	17/07/2024 15:22	KWOK Man-ho, Herbert	CHOW Tin-ik, Timmy	
Normal Text	APT EX email campaign (Monthly)	CHOW Tin-ik, Timmy		21/03/2024 18:02	25/06/2024 11:32	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Normal Text	Monthly impersonation statistic	CHOW Tin-ik, Timmy		21/03/2024 15:58	03/06/2024 12:04	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Excel	Phishing email reported by ED or above (Detail information for DCE or above)	CHOW Tin-ik, Timmy		28/12/2023 16:15	02/05/2024 10:39	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Normal Text	3.4c APT (Web) - Virus Trend Analysis	LEE Cheuk-yin, Justin	06/09/2017	31/08/2023 11:59	05/06/2024 14:09	CHOW Tin-ik, Timmy	LAM Tin-hang, Andy	
Normal Text	3.4e Virus Report By User (Follow up cases) - after 202311	CHOW Tin-ik, Timmy		31/01/2024 14:14	05/06/2024 12:39	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Image	Network Diagram of CMU & HKTR	CHOW Tin-ik, Timmy	29/08/2023	29/08/2023 09:15	29/08/2023 09:19	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Normal Text	DSSA shared document	CHOW Tin-ik, Timmy		08/03/2024 12:09	29/04/2024 14:33	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Normal Text	External SBA notification procedure	CHOW Tin-ik, Timmy		28/03/2024 16:06	11/04/2024 14:48	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	
Normal Text	Email notification/reminder/inquiry template	CHOW Tin-ik, Timmy		16/01/2024 09:25	17/05/2024 17:54	CHOW Tin-ik, Timmy	CHOW Tin-ik, Timmy	

- 3.1) Fill in the total number of cases for OGCIO security alerts that require "Call for returns", "Call for actions", and immediate review.

SharePoint

3.1 High Threat Security Alert Monitoring (2024 March Start) - New

Subject Officer: CHOW Tin-ik, Timmy

Source Doc Date: 30/04/2024

Doc Type: Normal Text

Document

Reference link:
<https://info.cgo.hksg/content/itsecure/secalert/archive.shtml>

	Jan	Feb (Till 27 Feb)	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
1. requiring "Call for returns"	0	1	1	0	1	0	12						
2. requiring "Call for actions"	2	2	2	4	3	5	2						
3. requiring immediate review	10	1	4	9	6	8	1						
Total	12	5	7	13	10	13	15						

- 3.2) Fill in the information for each security alert in the corresponding columns.

Report Date	Security Alerts / High Threat Security Alerts	Action	Related to HKMA?	Affected Systems, Summary, and Impact	Follow-up Action(s)
15-Jul-2024	Security Alert (A24-07-14) Multiple Vulnerabilities in Juniper Networks Junos OS and Junos OS Evolved	Call for Return	N		
15-Jul-2024	High Threat Security Alert (A24-07-13) Vulnerability in Cisco Products	Call For Action	Y		
12-Jul-2024	High Threat Security Alert (A24-07-12) Multiple Vulnerabilities Palo Alto Products	Call For Action	Y		Action item(s): 1) Email notifications to potential affected system owner on whether the system is affected 2) Create Jira ticket for tracking the progress and status of system patching Potential Affected System Owner: Jacko Tang Confirmed Affected System Owner: N/A Affected System Name(s): A24-07-12

Suggested Template for Threat Monitoring Table

Template

Report Date	Security Alerts / High Threat Security Alerts	Action	Related to HKMA?	Affected Systems, Summary, and Impact	Follow-up Actions
%dd-mm-yyyy%	%Security alert title%	%Call For Action / Call For Return / Immediate Review%	%Y / N%		(If applicable) Action item(s): 1) Email notifications to potential affected system owner on whether the system is affected 2) Create Jira ticket for tracking the progress and status of system patching Potential Affected System Owner: %Name / N/A% Confirmed Affected System Owner: %Name / N/A% Affected System Name(s): %Name / N/A% Patched? %Y / N% Jira Ticket Status: %Done / In progress / N/A%

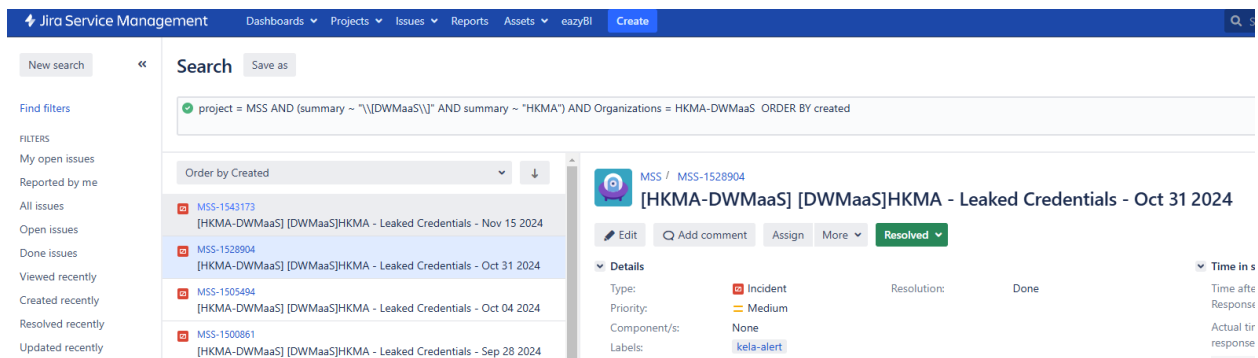
4) For information on OGCI0 security alerts or high threat security alerts, please refer to the [IT Security Theme](#) by the Government Information Station. The below screenshot is for reference.

Published	Updated	Action	Alert
12-Jun-2024	12-Jun-2024		Security Alert (A24-06-20): Multiple Vulnerabilities in Google Chrome
12-Jun-2024	12-Jun-2024	▼	High Threat Security Alert (A24-06-04): Multiple Vulnerabilities in Microsoft Products (June 2024)
11-Jun-2024	11-Jun-2024	▼	High Threat Security Alert (A24-06-02): Multiple Vulnerabilities in PHP
6-Jun-2024	6-Jun-2024		Security Alert (A24-06-07): Multiple Vulnerabilities in Android
4-Jun-2024	4-Jun-2024		Security Alert (A24-06-01): Multiple Vulnerabilities in Microsoft Edge
31-May-2024	31-May-2024		Security Alert (A24-06-24): Multiple Vulnerabilities in Google Chrome
27-May-2024	27-May-2024	▼	High Threat Security Alert (A24-05-23): Multiple Vulnerabilities in Microsoft Edge
24-May-2024	24-May-2024	▼	High Threat Security Alert (A24-05-22): Vulnerability in Google Chrome
23-May-2024	23-May-2024	▼	High Threat Security Alert (A24-05-21): Multiple Vulnerabilities in Git
23-May-2024	23-May-2024	▼	High Threat Security Alert (A24-05-20): Multiple Vulnerabilities in Intel Products
23-May-2024	23-May-2024		Security Alert (A24-06-19): Multiple Vulnerabilities in Cisco Products
22-May-2024	22-May-2024		Security Alert (A24-05-18): Multiple Vulnerabilities in QNAP Products
22-May-2024	22-May-2024		Security Alert (A24-06-17): Multiple Vulnerabilities in Google Chrome

d) Dark Web Monitoring (DWM) Alerts Handling

i) Alert Monitoring

On working days at 10:00 AM and 4:00 PM, the TI on-site analyst will monitor “HKMA - Leaked Credentials” alerts from Dark Web Monitoring (DWM) in the PwC JIRA Platform, as shown in the screenshot.



ii) Ticket Creation

If a dark web monitoring alert ticket is found in the PwC JIRA Platform, the TI on-site analyst will create a corresponding JIRA ticket in the HKMA platform with the following details:

- Title: Add "[TI Dark Web]" to the front of the ticket title.
- Component: Set the ticket component as "TI Alert".
- Status: Set the status of the sub-ticket as "In progress".

iii) Findings by TI on-site analyst

The TI on-site analyst should copy the content of the relevant ticket from the PwC JIRA Platform and paste it into the HKMA JIRA Platform. Below is an example template:

Template

==Background==

Our Cyber Threat Intelligence investigated the incident and found **%Count%** Leaked Credential related to your organisation exposed in dark web. The credentials are listed below:

As per our open-source investigation through passive means, we observe that:

EMAIL	DOMAIN	PASSWORD	SOURCE	POSTED DATE	SERVICE

%Source Name% Credentials automatically extracted from various Telegram channels.

We recommend confirming that the service coverage is to customers only, or whether it also includes staff and/or third-party, and evaluate if accounts with administrative privileges require a password change. We also recommend to heighten monitoring of customer login to indicate anomalies in location or timing, and review password policies and evaluate if there is a need to strengthen (e.g., mandate password rotation regularly). A further recommendation is to reach out to these account holders if the accounts are still active, and request that they change their passwords.

iv) Further follow-up by TI on-site analyst, if applicable

- **Scenario: No update in the ticket within 1 business day**
 - The TI on-site analyst will comment in the JIRA ticket follow the template below, and contact AD(IT)(ITS)3, using the template below.

Template

Dear Customer,

May we know if you have an update regarding this case? We look forward to hearing from you. Thank you.

This is a reminder. If you have already responded to this alert, please ignore this reminder and sorry for the inconvenience caused.

Best Regards,

TI on-site analyst

- **Scenario: AD(IT)(ITS)3 has any concerns or ad-hoc requests**
 - The TI on-site analyst will coordinate with Tier 2 PwC Threat Intelligence (TI) colleagues, and update AD(IT)(ITS)3 once new information is available.

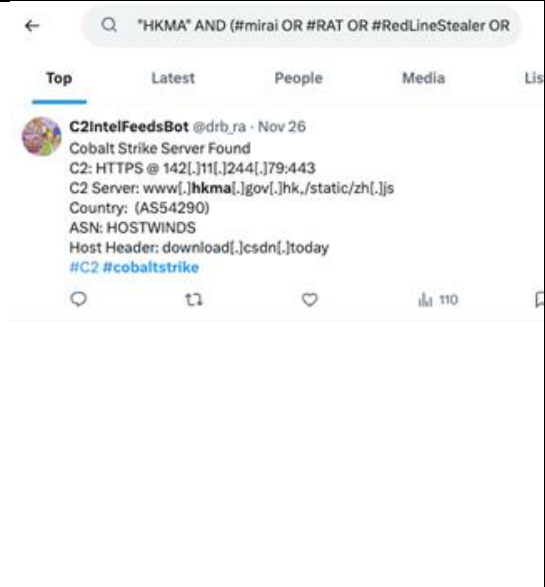
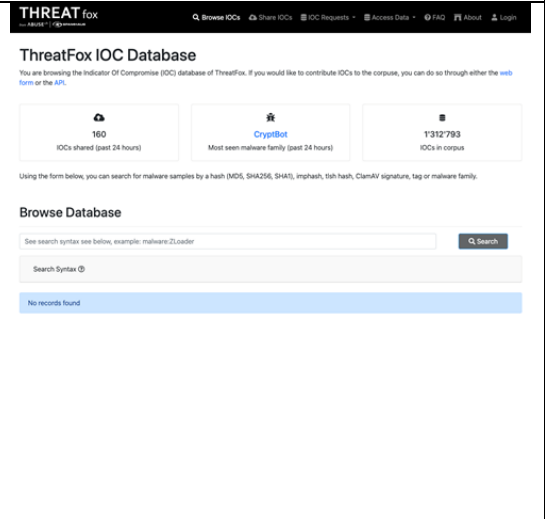
v) Ticket Closure

AD(IT)(ITS)3 reviews ticket and confirm completion, closes the ticket.

e) HKMA Domain Monitoring (Trial-Run)

i) Alert Monitoring

On working days at 10:00 AM and 4:00 PM, the TI on-site analyst will monitor the HKMA domain (hkma.gov.hk) using search feeds on social media and a malware database to cover social media monitoring, as shown in the table below.

Use case	Source	Frequency	Search Query	Output sample
Search feeds on social media	https://x.com/	Daily (10am, 4pm)	<p>Example: "HKMA" AND (#mirai OR #RAT OR #RedLineStealer OR #cobaltstrike OR #NjRAT OR #qakbot OR #asynrat OR #DCRat OR #Guildma OR #geo)</p> <p>Then Click "Latest" to make sure the information is the latest.</p> <p>Note: The selected tags are the top 10 malware families from threatfox.abuse.ch. We will include more malware families as required, but this approach allows us to be focused while also reducing large volume of false positives.</p>	 <p>The screenshot shows a tweet from @C2IntelFeedsBot dated Nov 26. The text of the tweet reads: "Cobalt Strike Server Found C2: HTTPS @ 142[.]11[.]244[.]79:443 C2 Server: www[.]hkma[.]gov[.]hk./static/zh[.]js Country: (AS54290) ASN: HOSTWINDS Host Header: download[.]csdn[.]today #C2 #cobaltstrike". The tweet has 110 likes.</p>
Search feeds on malware database	https://threatfox.abuse.ch/	Daily (10am, 4pm)	<p>Example: ioc: hkma.gov.hk</p> <p>Note: While this includes the user drb_ra which we assessed was how HSBC identified and notified BSD, we observed that the abuse.ch integration is not always accurate. As a result, this is also required to work together with use case no.1. https://threatfox.abuse.ch/user/11122/</p>	 <p>The screenshot shows the ThreatFox IOC Database interface. It includes a search bar with the text "See search syntax see below, example: malware:ZLoader". Below the search bar, it says "No records found". The interface also displays statistics: 160 IOCs shared (past 24 hours), Most seen malware family (past 24 hours) is CryptBot, and 1312793 IOCs in corpus.</p>

ii) Ticket Creation

If search feeds for keywords are found, the TI on-site analyst will create a corresponding JIRA ticket in the HKMA platform with the following details:

- Title: Add "[HKMA Domain Alert]" to the front of the ticket title.
- Priority: Set as "High".
- Component: Set the ticket component as "TI Alert".
- Status: Set the status of the sub-ticket as "In progress".

If there are any new findings, the TI on-site analyst will document them in the JIRA ticket, escalate it to HKMA AD(IT)(ITS)3, PwC Michael, Jason, and Wendy to determine if Incident Response (IR) is necessary.

f) Phishing Email Handling

i) Reported Email Analysis

On working days, the TI on-site analyst will initiate the investigation on the email reported by the HKMA Communications & Settlement Team. This email is sent from the HKMA IT Helpdesk via the HKMA IT Security Mailbox (i.e., its-operations@hkma.gov.hk).

ii) Reported Email Category

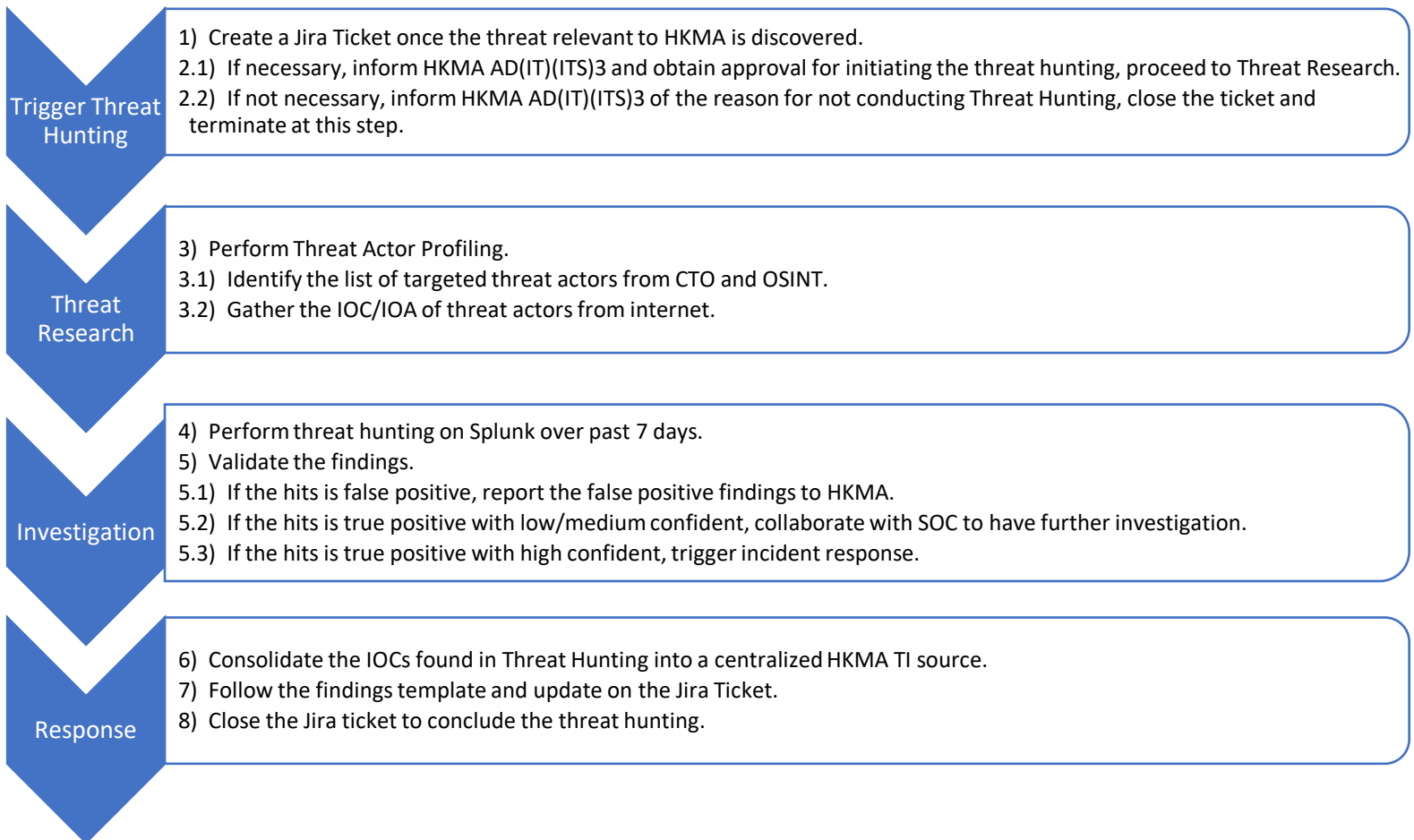
The major classified types are as follows:

- **Spam:** Appears to be promotional/advertising/financial purpose or lures the user for an instant reply.
- **Phishing:** Involves credential harvesting or malware.

For detailed procedures, please refer to the Phishing Email Handling Guideline titled “**User Guide on creating Jira ticket for handling phishing email incident (Settlement and Communications) case.docx**”. This document is available in the SOC Filing Database hosted internally at HKMA⁵.

⁵ <https://masp.hkma.gov.hk/sites/SOCFilingDB/Lists/SOC%20Filing20Database/By%20Category.aspx?web=1>

2) Threat Hunting



Objectives of Threat Hunting

Below are the examples of objectives mapped with Threat Hunting Scenario:

Outcome(s)	Threat Hunting Scenarios	Source(s)
Determine if the email poses a threat to HKMA or its stakeholders.	Malicious Emails	Security incidents
Determine appropriate actions to mitigate the risks associated with impersonation incidents. Evaluate the potential impact of the impersonation attempts.	Impersonation of HKMA	PwC CTO output, CVEs
Consider outcomes of discussions with HKMA, that require the threat hunting activities.	Requirements based on discussion agree with HKMA	Case-by-case, per discussions with HKMA
Ensure whether users had run the unblocked malware in HKMA computer by Threat Hunting in Splunk, and other EDR Solutions	User Interactions - Identification of HKMA users run malware	JIRA Ticket provided by PwC SOC

Scope of Threat Hunting

Below is the Threat Hunting Scope, agreed with HKMA, including but not limited to:

HKMA Related:

- Malware in malicious emails (ED or above, Communications, Settlement Team)
- Malware found on any HKMA device provided by SOC, which is responsible for creating a ticket and assigning a sub-ticket to TI

Regional Focus:

- China / HK / Macau Related

CVE / Vulnerabilities:

- CVE / Vulnerabilities targeting HKMA technology-related tools

Technology Related:

- HKMA Technology (e.g., Payload / malware download compromising HKMA tools)

PwC Proprietary Cyber Threat Intelligence Weekly Report:

- Included any IoCs

Opportunistic Advanced Persistent Threat (APT) Group:

- Included the IoCs in APT Groups' latest campaign based on their latest activities

Trend-Related Threats (Not limited but include the following):

- Remote Access Tools
- InfoStealers

[illegible]

2.1) Ticket Creation for Threat Hunting

In the HKMA JIRA environment, TI on-site analyst will create a Jira ticket for the threat hunting process.

- Ticket component: "TI Threat Hunt"
- Ticket title: [TI] [Threat Hunt] [Name of Affected Product, if any] **%CVE / Incident Name%**
- Ticket content: Include but not limited to the findings of threat and IoCs (See below steps)

2.2) Evaluation of Threat Hunting

The TI on-site analysts should refer to the following sources to assess the threat hunt:

- Open-source security research blogs (pre-defined by PwC)
- OGCI0 High Threat Security Alert Email
- CVAs received in PwC's Darklab Threat Intelligence Mailbox, OR
- Other PwC's proprietary source

The evaluation should be conducted in accordance with the "[Scope of Threat Hunting](#)" as above outlined.

2.3) Threat Actor Summary

In the event of identifying a threat actor during a threat hunting case, the TI on-site analyst should conduct a **Threat Actor Summary** to gather and reference potential threat actors for further information. The following details should be included, if available (if not, fill in N/A):

- **Aliases**
- **Country of Origin**
- **Known Targets**
- **Active Since**
- **Target Sectors**
- **Primary Objectives**
- **Techniques**

2.4) Collect Findings – Key Takeaways and IoCs – Utilize in JIRA ticket

Key Takeaways: Key points or summaries listed in OSINT sources, selected by the TI on-site analyst.

Indicators of Compromise (IoCs): Collect IoCs from credible sources in OSINT, VirusTotal, social media, etc.

2.5) Perform Threat Hunting on Splunk, Cisco AMP, and Sentinel One

The coverage of finding Indicators of Compromise (IoCs) for threat hunting in security solutions, as originally intended for SOC monitoring log sources in HKMA, is as follows:

Threat Hunt Security Solutions	Index	Description	IoCs			
			IP	Domain	URL	Hash
Splunk	soc_forcepoint	Proxy	✓	✓	✓	
	soc_fireeye		✓	✓	✓	
	soc_darktrace		✓	✓		
	soc_cisco_fp	NIPS	✓			✓
	soc_paloalto		✓			
	soc_cisco_asa		✓			
	soc_fortinet	NIPS	✓			
	soc_axway		✓			
	soc_imperva	WAF	✓			
	soc_f5		✓			
	soc_symantec					✓
	hkma_infoblox					
	hkma_windows					
Cisco AMP	N/A					✓
Sentinel 1	N/A					✓

2.6) Validate the findings of IoCs

If an Indicator of Compromise (IOC) is discovered during a threat hunt and matches an IOC found within the HKMA internal systems, it indicates the presence of an identified threat.

The TI on-site analyst should next determine whether the hit is a **False Positive / True Positive with low/medium severity / True Positive with high severity**. Appropriate actions for investigation and mitigation will then be initiated, as outlined in the following table:

Hits	Condition(s)	Inform AD(IT)(ITS)3?	Further follow-up	Descriptions
False Positive	Legitimate File or Domain	Yes	Explain the reason why the hit is a false positive in the JIRA ticket.	Determine if the user has the permission allow to use the legitimate file / access legitimate domain.
True Positive with low/medium severity	1) TI Feed reported suspicious activity 2) The collected evidence is not correlated to Threat Actor or a C2 Server	Yes	Collaborate with SOC on-site analyst to perform searches in the source for further analysis and detection.	TI on-site analyst shares the Threat Hunting case listed in Jira ticket to SOC on-site analyst.
True Positive with high severity	1) Already Compromised 2) The collected evidence is correlated to Threat Actor and/or a C2 Server Common case Example: Web Shell	Yes	Discuss with HKMA if necessitate to trigger Incident Response.	Please refer to the section 4 Incident Response.

Below is the detailed process for handling the security hits:

1. **Research IP Purpose:** TI should investigate the purpose of the IP (e.g., Command and Control (C2), Distributed Denial-of-Service (DDoS), Malware Distribution, Phishing, etc.) and relay this information to the SOC.
2. **Confirm APT Targeting:**
 - Verify the attack period by the threat actor using HKMA security solutions.
 - Determine if the Indicators of Compromise (IoCs) are associated with an Advanced Persistent Threat (APT) group, as documented in reputable researchers' blog posts.
 - Review reports on the IP address obtained through OSINT and social media.
3. **Update Severity Level:** TI should escalate the JIRA ticket's severity level to 'critical' if confirm APT Targeting.

2.7) Create sub-ticket to request blocking the IoCs found via Threat Hunting

Generate sub-tickets to request the blocking of the IoCs.

Ensure the severity level of each sub-ticket is flagged as 'critical' if confirm APT Targeting.

Note: As agreed by AD(IT)(ITS)3, for critical cases, the IoCs should be blocked within one business day.

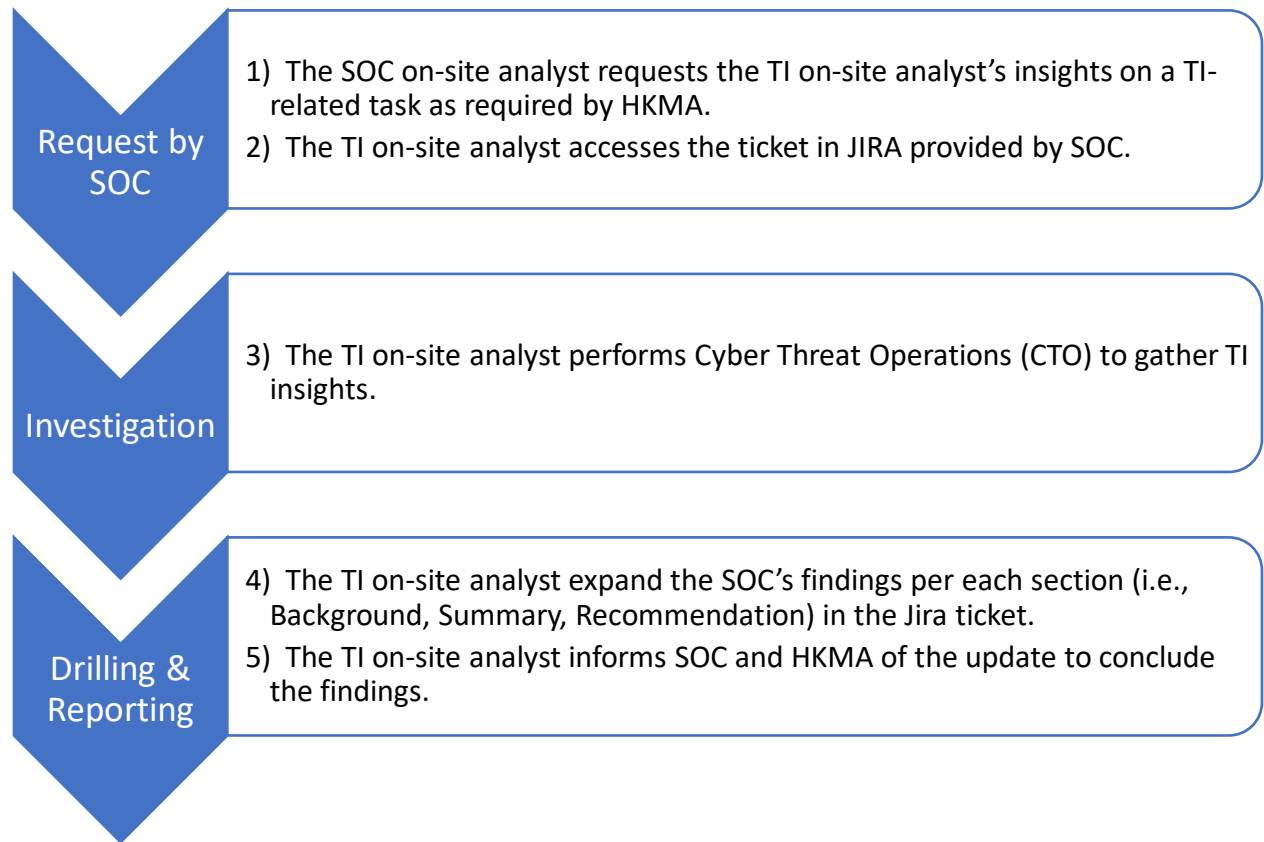
Please refer to “[Request Blocking IoCs](#)” in the above CTO section.

2.8) Close the Jira Ticket

Close the Jira Ticket with AD(IT)(ITS)3's approval to conclude the threat hunting.

3) Security Operation Centre (SOC)

3.1) TI Analysis Coordination with SOC



The following criteria will be defined for TI analysis coordination for a specific incident by the TI on-site analyst with SOC on-site analyst:

- i. The SOC on-site analyst will assign the TI analysis request to the TI on-site analyst. The below shows case studies of such requests:

Example Case Study : Malware Analysis in JIRA ticket provided by SOC

The SOC on-site analyst will create and route a sub-ticket to the TI on-site analyst for Threat Hunt purpose, prefixed with [Threat Hunt] in the title.

For more comprehensive guidelines and procedures, please refer to Section 2 "Threat Hunting."

Example Case Study : Malicious Inbound IOCs Investigation

The SOC on-site analyst will identify and provide malicious IP(s) / Domain(s) / URL(s) based on their assessment, such as focusing on with numerous hits on HKMA websites plus exhibiting malicious events.

Example Case Study : Web Server IIS Log Analysis

The SOC and TI on-site analyst will receive the logs named "[Date] IIS log.zip" in zip format via email from HKMA's AD(IT)(ITS)3 to the HKMA SOC/TI on-site analyst mailbox. The logs are in Excel format.

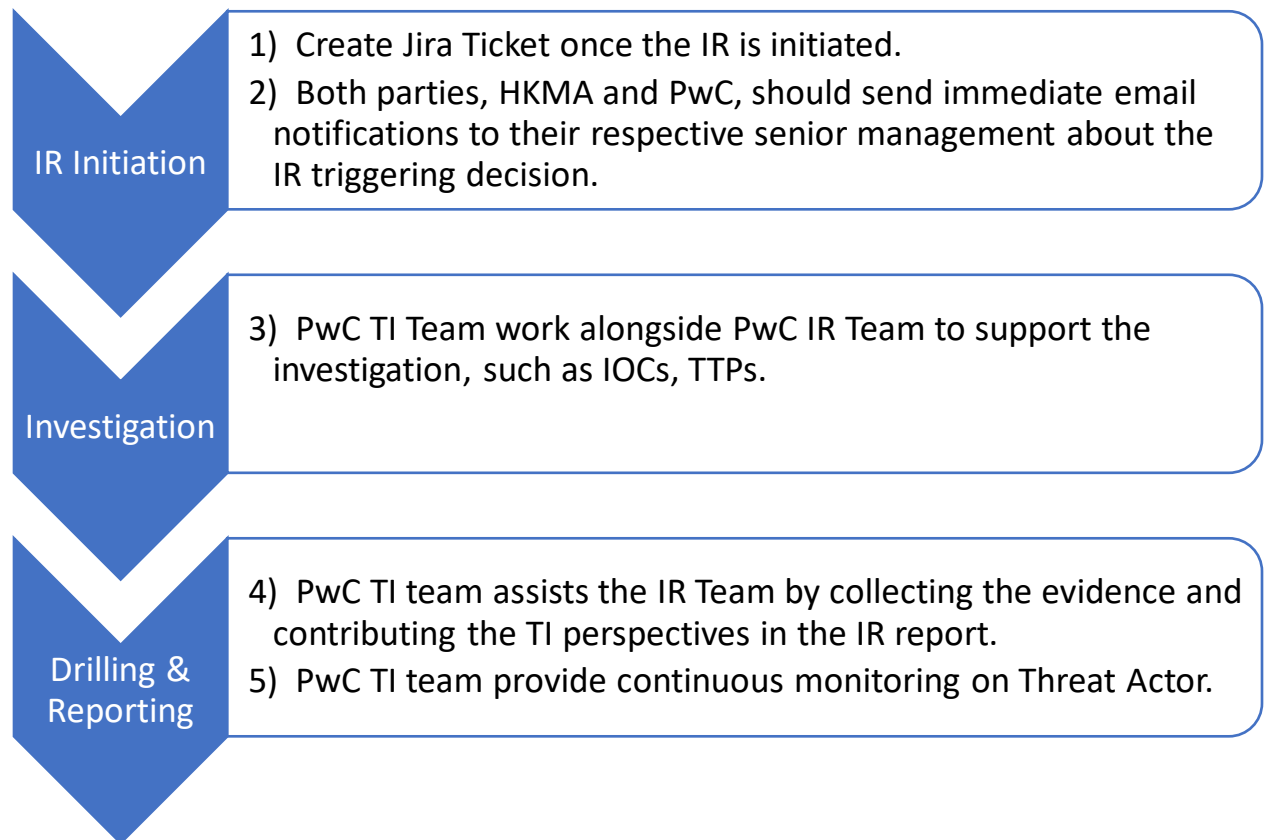
The SOC on-site analyst will extract the prioritized IPs (based on the highest event count) forwarded to the TI on-site analyst for further investigation, with the following indicators, where applicable:

- IPs with the most hits
- IPs triggering 404 responses
- IPs associated with specific user agents

- ii. The TI on-site Analyst will access the corresponding incident with the link provided by SOC.
- iii. The TI on-site analyst will perform Cyber Threat Operations (CTO).
- iv. The TI on-site analyst will collaborate with TI team to consolidate the insights, and expand the findings per each section (i.e., Background, Summary, Recommendation).
- v. The TI on-site analyst expand the SOC's findings per each section (i.e., Background, Summary, Recommendation) in the Jira ticket.
- vi. Once the TI on-site analyst finishes follow-up, set the assignee of the ticket be AD(IT)(ITS)3.
- vii. The TI on-site analyst reports in person to AD(IT)(ITS)3. AD(IT)(ITS)3 will close the ticket after verifying that all follow-up actions have been completed.

- Check the specific recipients of the malware to determine the scope of impacted individual

4) Incident Response (IR)



4.1) IR Initiation and Notifications Phase

4.1.1) Triggering IR

If both the SOC and TI on-site analyst escalate the incident to HKMA's AD(IT)(ITS)3 and necessary to initiate an Incident Response (IR), a corresponding Jira ticket will be created in advance.

If a ticket/incident is related to TI, AD(IT)(ITS)3 will initiate IR to the PwC TI Team. For SOC-related tickets, AD(IT)(ITS)3 will initiate IR to the PwC SOC Team.

4.1.2) Email Notifications by HKMA and PwC

Both HKMA and PwC should send immediate email notifications to their respective senior management to inform them about the decision to trigger the Incident Response (IR) for awareness. The following table outlines the actions taken by each party:

Party	Description
HKMA	AD(IT)(ITS)3 will report to HKMA's Andrew Tam and obtain approval through email, Nexchat, or Jira ticket, as per the established communication channels.
PwC	The TI on-site analyst will report to PwC Threat Intelligence Team Leader Michael Ching via Outlook email and obtain email approval.

The following template is for TI on-site analyst to notify PwC IR Team via email, as applicable.

[Email Template] Notification to IR Team Lead (i.e., Michael Ching)

Suggested Email Template – Notification to IR Team Lead (i.e., Michael Ching)

Subject: [HKMA] Critical **%Incident/CVE%** Notification - **%Incident/CVE Name%**

Dear Michael,

As requested by HKMA, there is a critical issue bringing severe impact on **%Vulnerability Name%, which %Reason for triggering IR/Impact details%** and plus IR is triggered.

Below is the information of the **%Incident/CVE Name%**. Thank you.

%Incident/CVE% Details:

Incident ID: **%Incident ID%**

Timestamp: **%Timestamp%**

Severity: **%Severity%**

Incident Count: **%Incident Count%**

Rule Name: **%Rule Name%**

Rule Description: **%Rule Description%**

Target host IP: **%Target host IP%**

Target host Name: **%Target host Name%**

Details: **%Details%**

IOAs: **%IOAs%**

IOCs: **%IOCs%**

Others: **%Others%**

Our Threat Intelligence team will provide immediate updates if there are further findings or updated IOCs related to this **%Incident/CVE Name%**.

Please let me know if you require any further assistance or information.

Best Regards,

%OSSA Name%

TI On-site Security Analyst

4.1.3) Additional Action Items

- PwC TI on-site analyst will collaborate with PwC DFIR Team for the associated artefacts (e.g. ransom note), where applicable
- Analyze associated data sources (e.g. leak site, forums, where applicable) to understand the context and intelligence on the incident and the threat actor
- Any other stakeholder/party need to be informed as needed

4.2) Investigation Phase

4.2.1) Collaboration with PwC DFIR team

PwC TI Team will work with DFIR team along the incident, with objectives to enrich IOCs, TTPs, and knowledge on the threat actor based on the incident and provide support in threat hunting and investigation procedures.

- a. Identify possible points of initial access (i.e., initial access broker, vulnerable servers, administrative ports, etc.):
- b. Assist DFIR in the process to collect several forensic artefacts, including the tools used by the threat actor;
- c. Collaborate with DFIR team to assess Indicators of Attacks (IOAs), including Unusual Login Attempts and Suspicious File Downloads;
- d. Perform necessary analysis with PwC's tools, including but not limited to digital footprint intelligence, dark web search, leak sites;
- e. Set up proactive dark web monitoring of the relevant context keywords.

4.3) Reporting Phase

4.3.1) Contribute Threat Intelligence Perspective in IR Report

The following sections outline how the TI team collaborates with the IR team and contributes to the IR report:

- Executive Summary
- Key Facts (e.g., purpose of the attack, tools used)
- Recommendations / Lessons Learnt
- Sharing a list of artefacts associated e.g. list of Indicators of Compromise (IoC)
- Forensic artifacts in the appendices of the IR report, including details such as:
 - Tool name
 - Description / Purpose
 - Observations
 - MITRE

4.3.2) Ongoing Monitoring of Threat Actors

The PwC Threat Intelligence team will engage in continuous monitoring of Threat Actors, including events, timings, and types of malicious actions taken (e.g., Unauthorized sale of HKMA data.)

Appendix

TI Investigation Tools

Tools that may be leveraged for PwC TI team to perform analysis include (but not limited to):

Type of Tools	Examples	Usage
Forensics	Shodan.io, Censys.io, VirusTotal, Urlscan.io, Pulsedive.com, Whois	Identify current and historical ports observed to be open, potential vulnerability, SSL certificates, etc
Community-based	Abuseipdb.com, VirusTotal	Ascertain if IP address or domain was reported as malicious
Dark Web Search Engine	Duckduckgo, Torch, Ahmia	Helps find, understand, and deal with online threats that come from hidden parts of the internet

Other Sources

The PwC Threat Intelligence Team may utilize various sources before and during the incident, including but not limited to the following:

- 百度: www.baidu.com
- 微步在线: x.threatbook.cn
- 腾讯哈勃: habo.qq.com
- Virscan: virusscan.jotti.org
- Freebuf: www.freebuf.com
- Jotti: virusscan.jotti.org
- Scandir: www.scandir.com
- Alexa 排名: www.alexa.com
- 备案查询: beian.cndns.com
- 深信服安全中心: sec.sangfor.com.cn
- 深信服威胁分析平台: wiki.sec.sangfor.com.cn
- 深信服 EDR 安全软件中心: edr.sangfor.com.cn

Incident Escalation for HKMA Evaluation

- a. Assessing the relevance of the incident against HKMA (e.g., Potential match with HKMA's basic Inventory List on technology)

- b. Assessing the relevance of the incident to Hong Kong
- c. Assessing the relevance of the incident with respect to whether the industry is typically recognized globally and/or locally as a critical infrastructure operator (e.g., Singapore Cyber Security Act may have a list of Essential Services⁶)
- d. Assessing the relevance of the incident to specific industries that are relevant to HKMA (e.g., Global Central Banks, Fintech, Financial Services, and Property Development⁷, etc.)
- e. If PwC cannot find any publicly available information regarding the incident or if the incident has not been publicly disclosed, PwC will provide the findings of their analysis (if any) to HKMA via email including relevant case studies of incident experiences, where applicable
- f. HKMA provides the information on IOC to PwC TI / SOC on-site analyst for further investigation
- g. Upon request by HKMA, PwC will provide a summary regarding publicly reported incidents based on their understanding from OSINT, and the expected turnaround is as follows:

Time Range	Description	Expected Turnaround
During office hours	Monday to Friday, 9 AM to 6 PM	1) PwC on-site analyst should analyze the request with the TI Team, provide a preliminary response <u>within a business day</u> upon HKMA's request.
During non-office hours	The time outside of office hours	2) Provide timely updates on HKMA's request, if necessary.

NOTE: At times where HKMA makes urgent requests for specific TI, PwC will initially agree the associated turnaround time with HKMA on a case-by-case basis.

⁶ Cybersecurity act. Default. (2024, June). <https://www.csa.gov.sg/faq/cybersecurity-act>

⁷ Hong Kong Monetary Authority (2024, June). Regulatory Resources. <https://www.hkma.gov.hk/eng/regulatory-resources/regulatory-guides/by-subject-current/>

In such a scenario, the following are the steps required:

- 1) PwC TI / SOC on-site analyst should immediately inform the Cyber Threat Operations Leads (Jason Lee, Michael Ching) about the request.
- 2) Analyze the request with the TI Team, provide a preliminary response with the agreed SLA upon HKMA's request.

Finding the Names of HKMA System Owners

To identify relevant HKMA staff members to notify and locate the names of system owners within HKMA, TI on-site analysts should:

- a) Access the HKMA authorized computer
- b) Open the USO Client application.
- c) Launch Lotus Notes 9 on HKMA computer.
- d) Within Lotus Notes, navigate to the "HKMA Phone List" section.
- e) Perform keyword search using relevant keywords such as "AD(IT)" for the Information Technology Associate Director.
- 6) If uncertain about the specific roles or unable to find the relevant system owner, contact AD(IT)(ITS)3 for further assistance.