# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in August 2025

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Responsible Person |
| Cyber Threat Operations (CTO) | Last Modification of Latest Version (On 28 July 2025) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Security Operations Centre (SOC) | Last Modification of Latest Version (On 05 Nov 2024) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Threat Hunting | Last Modification of Latest Version (On 26 Mar 2025) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Incident Response (IR) | Last Modification of Latest Version (On 31 Jul 2024) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |

Remarks:

1 Since no further comment listed in July 2025 SOC Monthly Meeting on 25 Feb 2025, the latest version of SOP for Threat Intelligence – “HKMA Threat Intelligence SOP – 20250224” is endorsed.

# Cyber Threat Operations (CTO)

## 12.1 Monthly CVEs Summary

In July 2025, there were **2** critical& **6** high-severity-level Common Vulnerabilities and Exposures (CVEs).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Reply |
| High | PwC, DPO | 02/07/2025 | ITSSOC-10749 | CVE-2025-6554 | Google Chrome | Vulnerability in Google Chrome | N/A |
| High | PwC, DPO | 11/07/2025 | ITSSOC-10849 | CVE-2024-1086 | Palo Alto Networks products | Multiple Vulnerabilities in Palo Alto Products for subscribers | N/A |
| High | PwC, DPO | 22/07/2025 | ITSSOC-10955 | CVE-2025-6558 | Google Chrome | Vulnerability in Google Chrome for subscribers | N/A |
| High | PwC, DPO | 22/07/2025 | ITSSOC-10956 | CVE-2025-41236, CVE-2025-41237, CVE-2025-41238 | VMware products | Multiple Vulnerabilities in VMware Products for subscribers | Yes, Confirm affected |
| High | PwC, DPO | 22/07/2025 | ITSSOC-10957 | CVE-2025-20281, CVE-2025-20282, CVE-2025-20337 | Cisco products | Multiple Vulnerabilities in Cisco Products | N/A |
| Critical | PwC, DPO | 22/07/2025 | ITSSOC-10958 | CVE-2025-53770 | Microsoft SharePoint Server | Multiple Vulnerabilities in Microsoft SharePoint Server for subscribers | Yes, Confirm affected |
| Critical | PwC, DPO | 23/07/2025 | ITSSOC-10969 | CVE-2025-25257 | Fortinet products | Multiple Vulnerabilities in Fortinet Products | N/A |
| High | PwC | 30/07/2025 | ITSSOC-11060 | CVE-2025-52446 | Salesforce Tableau Server | Authorization Bypass Vulnerability in Salesforce Tableau Server | Yes, Confirm affected |

## 12.2 Monthly High Severity Level CVEs Tracking

In July 2025, there were **1** Critical & **2** High Severity Level CVEs affecting HKMA. The affected systems/servers and their scheduled patch dates were tracked by the respective system owners.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CVE number | Product | Response from System Owner | | | | Recommendations by PwC |
| Internet Facing | Affected System/ Server IP | Solution | Target Solution Apply Date |
| CVE-2025-53770 | SharePoint Server | N/A | SharePoint Server | Patch Deployment | 22 July 2025 | #1 We have observed active exploitation of these SharePoint vulnerabilities. Active exploitation of ToolShell vulnerabilities began mid-July 2025. We are urging organizations who are running vulnerable on-premises SharePoint to apply all relevant patches.  #2 Threat Hunt completed and request IOCs blocking in WAF, Firewall, and EDR. |
| CVE-2025-41236, CVE-2025-41237, CVE-2025-41238 | ESXi  VMware Tools | No | PAM-CPM-PD1  PAM-PSM-PD1  PAM-CPM-PD2  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  PAM-VAULT-TEST  PAM-CPM-TEST  PAM-PSM-TEST | Upgrade ESXi Server to 8.0 Update 3f  Upgrade VMware Tools to 12.5.3 | 14 Aug 2025 | To remediate the vulnerabilities, apply the patches listed in the 'Fixed Version' advised by Broadcom. |
| CVE-2025-52446 | Tableau Server | No | https://tableau2.intra.hkma.gov.hk | Upgrade Tableau Server Version from v2023.1.8 to v2025.1 latest version with the Tableau Planned Upgrade project | Feb 2026 | Update Tableau Server to the latest supported Maintenance Release, Given authorization Bypass Through User-Controlled Key vulnerability in Salesforce Tableau Server is critical. |

## Remark: Only the product running the affected version are shown.

## 12.3 Ongoing CVEs Remediation (Until 28 Aug 2025) 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Jira Ticket Number | CVE Number | Product Impacted | Severity | System Owner Name(s) | Date Raised by SOC | SOC Follow-up Attempts (1,2,3) | Date of Acknowledgement | Date of Last Follow-up | CVE Relevant to HKMA | Affected System/ Server IP | Target Remediation Completion Date | Actual Remediation Date | Time from Date Raised to Date Acknowledged (days) | Time from Date Acknowledged to Date Remediated (days) | Aging of Actual Remediation Date to Target Remediation Completion Date (days) | Source of Alert |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(DP)1 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025 | 3 | 26 Feb 2025 | 1st Follow-up: 3 Mar 2025 | Yes | JSM, IRIS | Pending by DP Team**2** | N/A | 7 | 150**1** | N/A | PwC |
| ITSSOC-9623 | CVE-2025-2783 | Google Chrome | Critical3 | AD(IT)(PSM)1 | 1st Attempt: 26 Mar 2025  2nd Attempt: 16 July 2025 | 2 | 16 July 2025 | N/A | Yes | N/A | Within 6 weeks | Pending | 0 | 71**1** | N/A | PwC, DPO |
| ITSSOC-10884 | CVE-2025-5419 | Palo Alto Firewall | High | A(SYS)(IT)(IS)10 | 1st Attempt: 11 Jul 2025  2nd Attempt: 14 Jul 2025 | 2 | 14 Jul 2025 | N/A | Yes | IFC OA  172.22.48.101  172.22.48.102  172.22.48.105  172.22.48.111  172.22.48.112  IFC SWT  172.22.148.51  172.22.148.52  172.22.148.55  KCC OA  172.22.49.101  172.22.49.102  172.22.49.105  172.22.49.111  172.22.49.112  KCC SWT  172.22.149.51  172.22.149.52  172.22.149.55 | 26/07 (KCC)  09/08 (IFC) | N/A | 4 | 12**1** | N/A | PwC, DPO |
| ITSSOC-10975 | CVE-2025-41236  CVE-2025-41237  CVE-2025-41238 | ESXi  VMware Tools(Windows) | High | D(IT)(ITS)2 | 1st Attempt: 16 Jul 2025 | 1 | 23 Jul 2025 | N/A | Yes | PAM-CPM-PD1  PAM-PSM-PD1  PAM-CPM-PD2  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  PAM-VAULT-TEST  PAM-CPM-TEST  PAM-PSM-TEST | 14 Aug 2025 | N/A | 8 | 3**1** | N/A | PwC |
| ITSSOC-10975 | CVE-2025-41236  CVE-2025-41237  CVE-2025-41238 | VMware Tools(Windows) | High | D(IT)(ITS)2 | 1st Attempt: 16 Jul 2025 | 1 | 23 Jul 2025 | N/A | Yes | PAM-CPM-PD1  PAM-PSM-PD1  PAM-CPM-PD2  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  PAM-VAULT-TEST  PAM-CPM-TEST  PAM-PSM-TEST | 28 Jul 2025 | N/A | 8 | 3**1** | N/A | PwC |

As of July 2025, there were **5** ongoing CVEs remediation efforts.

Remarks:

1st Follow-Up: SOC requested information from the system owner regarding the CVE.

2nd Follow-Up: SOC inquired about the system owner's patch status.

**1** The timeframe is calculated up to 28 Aug 2025; additional days will continue to be added until the patch is completed.

**2**Team is currently in the development and testing phase of the system. The user has agreed to provide an update once the impact analysis is complete.

## 12.4 Completed CVEs Remediation (Until 28 Aug 2025)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Jira Ticket Number | CVE Number | Product Impacted | Severity | System Owner Name(s) | Date Raised by SOC | SOC Follow-up Attempts (1,2,3) | Date of Acknowledgement | Date of Last Follow-up | CVE Relevant to HKMA | Affected System/ Server IP | Target Remediation Completion Date | Actual Remediation Date | Time from Date Raised to Date Acknowledged (days) | Time from Date Acknowledged to Date Remediated (days) | Aging of Actual Remediation Date to Target Remediation Completion Date (days) | Source of Alert |
| ITSSOC-7888 | CVE-2024-47575 | FortiManager | High | A(SYS)(IT)(IS)10 | 1st Attempt: 24 Oct 2024  2nd Attempt: 15 Nov 2024 | 2 | 15 Nov 2024 | 1st Follow-up: 29 Nov 2024  2nd Follow-up: 3 Jan 2025 | Yes | 172.20.22.23  172.20.141.23 | Dec 2024 | 12 Dec 2024 | 23 | 50 | 0 | PwC, GovCERT |
| ITSSOC-8780 | CVE-2024-55591, CVE-2025-24472 | FortiOS  FortiProxy | High | A(SYS)(IT)(IS)10 | 15 Jan 2025 | 1 | 15 Jan 2025 | 1st Follow-up: 16 Jan 2025; 20 Jan 2025  2nd Follow-up: 14 Feb 2025 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | KCC: 8 Feb 2025  IFC: 15 Feb 2025 | 1 | 31 | 0 | PwC, GovCERT, CISA |
| ITSSOC-7772 | CVE-2024-23113 | FortiOS  FortiPAM  FortiProxy  FortiWeb | High | A(SYS)(IT)(IS)10 | 15 Oct 2024 | 1 | 17 Oct 2024 | 1st Follow-up: 29 Nov 2024 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | 17 Feb 2025 | 3 | 125 | 0 | PwC, GovCERT |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(AS2)2 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025  4th Attempt: 03 Mar 2025 | >3 | 05 Mar 2025 | 1st Follow-up: 6 Mar 2025; 7 Mar 2025 | Yes | 172.31.234.105 | Before 12 Mar 2025 | 10 Mar 2025 | 15 | 5 | 0 | PwC |
| ITSSOC-8114 | CVE-2024-0012, CVE-2024-9474 | PAN-OS | High | Sr D(IT)(IS) | 15 Nov 2024 | 1 | 15 Nov 2024 | 1st Follow-up: 05 Dec 2024 | Yes | 172.22.48.101  172.22.48.102  172.22.48.105  172.22.48.111  172.22.48.112  172.22.49.101  172.22.49.102  172.22.49.105  172.22.49.111  172.22.49.112 | Q1 2025 | 31 Mar 2025 | 1 | 136 | 0 | PwC, GovCERT, CISA |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(PSM)1 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025  4th Attempt: 03 Mar 2025 | >3 | 04 Mar 2025 | 1st Follow-up: 5 Mar 2025; 11 Mar 2025 | Yes | 172.31.110.180  172.31.91.87  172.31.151.51  172.31.110.253  172.31.161.62 | Within 180 days | 03 July 2025 | 14 | 61 | 0 | PwC |
| ITSSOC-10536 | CVE-2025-5419 | Google Chrome | High | D(IT)(ITS)2 | 1st Attempt: 05 Jun 2025 | 1 | 11 Jun 2025 | N/A | Yes | PAM-CPM-PD1  PAM-CPM-PD2  PAM-PSM-PD1  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  spamprdcm101  spamprdcm102  spamprdpm101  spamprdpm102  spamprdcm201  spamprdcm202  spamprdpm201  spamprdpm202 | 2 Jul 2025 | 2 Jul 2025 | 6 | 21 | 0 | PwC, DPO |

As of July 2025, there were **7** completed CVEs remediation efforts.

Remarks:

1st Follow-Up: SOC requested information from the system owner regarding the CVE.

2nd Follow-Up: SOC inquired about the system owner's patch status

## 12.5 Major Threat Intelligence Report Highlight

This section shared major threat intelligence highlights for the past month.

1. xxxxx
2. xxxxxx

12.6 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
| 1. xxxxx | * TI on-site analyst conducts a threat hunt campaign against the LockBit Ransomware * No positive findings were observed in HKMA security solutions * All IoCs have been blocked |
| 1. xxxxx | * TI on-site analyst conducts a threat hunt campaign against the LockBit Ransomware * No positive findings were observed in HKMA security solutions * All IoCs have been blocked |

1. xxxxxx

In early July 2024, a security breach was detected following the exploitation of a critical Confluence remote code execution vulnerability (CVE-2023-22527) on an exposed Windows server.

**Impact and Analysis**

This exploitation allowed the attacker to gain unauthorized access, enabling them to install AnyDesk for persistent access and create a local administrative account, which facilitated further exploitation. They utilized Mimikatz to harvest credentials, disabled security measures, and cleared event logs to conceal their activities. Through reconnaissance and lateral movement, they positioned themselves to execute further attacks within the network.

The breach escalated quickly, with sensitive data exfiltrated using Rclone to transfer files to MEGA.io cloud storage approximately 71 minutes after initial access. Within two hours of the intrusion, the attacker deployed LockBitransomware, employing both manual execution on critical servers and automated distribution methods like PDQ Deploy. This rapid deployment led to widespread file encryption and the creation of ransom notes, highlighting the efficiency and coordination of the attack strategy. Despite LockBit’s slowdown in frequency of attacks, their latest LockBit 4.0 strain indicates their intention to regain their cadence of attacks.

**Recommendations**

TI on-site analyst conducts a threat hunt campaign against the LockBit Ransomware. No positive findings were observed in HKMA security solutions, and all IoCs have been blocked.

Source: PwC Cyber Threat Intelligence Weekly Report [22 July 2025 – 28 July 2025]

1. xxxxxx

In late 2024, researchers tracked activity by the threat actor Midnight Blizzard and discovered their phishing campaign involving the use of Remote Desktop Files.

**Impact and Analysis**

By further monitoring online antivirus scanners for similar files, a new campaign that begun in late January 2025 was revealed. The campaign is noted to target organisations in government and education sectors, and still active as of mid-July 2025. The aforementioned campaign has not been linked to any threat actor and as such has been tracked by PwC Global Threat Intelligence as White Dev 199.

White Dev 199 has been seen to impersonate Ukretelecom, a Ukrainan telephone company and Rheinmetall a German automotive and arms manufacturer, though based on analysis of the network traffic researchers deduce the campaign is likely targeting clients of Rheinmetall rather than the company itself. We continue to observe a rise in reports of threat actors leveraging RDP files in their phishing campaigns.

**Recommendations**

TI on-site analyst conducts a threat hunt campaign against the Remote Desktop Protocol (RDP) files. No positive findings were observed in HKMA security solutions, and all IoCs have been blocked.

Source: PwC Cyber Threat Intelligence Weekly Report [15 July 2025 – 21 July 2025]

# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In July 2025, a total of **8** threat hunting cases were handled. These included **6** government-targeted cases, **4** APAC-targeted cases, and **1** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 08/07/2025 | ITSSOC-10782 | Sophisticated RAT Delivered via Phishing Campaign Impersonating Government Entity | ✓ |  |  |
| 11/07/2025 | ITSSOC-10850 | Password Spray Against Exposed RDP Server Leads to RansomHub Deployment | ✓ |  |  |
| 14/07/2025 | ITSSOC-10854 | IOCs related to malicious activities (from DPO) | ✓ |  |  |
| 21/07/2025 | ITSSOC-10939 | SquidLoader malware activity targeting financial institutions in Hong Kong | ✓ | ✓ |  |
| 21/07/2025 | ITSSOC-10940 | (CVE-2025-49706 & CVE-2025-49704)/(CVE-2025-53770 and CVE-2025-53771) ToolShell Mass Exploitation | ✓ | ✓ | ✓ |
| 23/07/2025 | ITSSOC-10969 | New Salt Typhoon IOCs - Targeting Governmental Organizations | ✓ |  |  |
| 24/07/2025 | ITSSOC-10999 | Lumma Stealer Resurfaces After Takedown |  | ✓ |  |
| 30/07/2025 | ITSSOC-11044 | Cyber Stealer New Actively Developing Threat Creating Versatile Attack Platform |  | ✓ |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In July 2025, a total of **9** threat hunting cases were handled.

In addition, this effort resulted in the blocking of **41** hashes, **111** domains or URLs, and **132** IP addresses. All Indicators of Compromise (IoCs) were blocked, with **no** left unblocked.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Hits | Hash Blocked Count | Domain/URL Blocked Count | IP Blocked Count |
| 08/07/2025 | ITSSOC-10782 | Sophisticated RAT Delivered via Phishing Campaign Impersonating Government Entity | No | 1 | 2 | 1 |
| 11/07/2025 | ITSSOC-10850 | Password Spray Against Exposed RDP Server Leads to RansomHub Deployment | No | 5 | 0 | 4 |
| 14/07/2025 | ITSSOC-10854 | IOCs related to malicious activities (from DPO) | No | 4 | 73 | 5 |
| 21/07/2025 | ITSSOC-10939 | SquidLoader malware activity targeting financial institutions in Hong Kong | No | 7 | 6 | 93 |
| 21/07/2025 | ITSSOC-10940 | (CVE-2025-49706 & CVE-2025-49704)/(CVE-2025-53770 and CVE-2025-53771) ToolShell Mass Exploitation | No | 9 | 0 | 19 |
| 23/07/2025 | ITSSOC-10969 | New Salt Typhoon IOCs - Targeting Governmental Organizations | No | 0 | 0 | 6 |
| 24/07/2025 | ITSSOC-10999 | Lumma Stealer Resurfaces After Takedown | No | 3 | 26 | 0 |
| 30/07/2025 | ITSSOC-11044 | Cyber Stealer New Actively Developing Threat Creating Versatile Attack Platform | No | 12 | 4 | 4 |
| Total | | | | 41 | 111 | 132 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were **9** of reported emails from Communications Division in July 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 10/07/2025 | ITSPEIR-4238 | Spam |
| 17/07/2025 | ITSPEIR-4240 | Unwanted |
| 18/07/2025 | ITSPEIR-4242 | Phishing |
| 22/07/2025 | ITSPEIR-4246 | Phishing |
| 23/07/2025 | ITSPEIR-4250 | Spam |
| 24/07/2025 | ITSPEIR-4252 | Spam |
| 24/07/2025 | ITSPEIR-4254 | Spam |
| 28/07/2025 | ITSPEIR-4256 | Spam |
| 28/07/2025 | ITSPEIR-4257 | Spam |

## 14.2 Settlement Division

There were **7** of reported emails from Settlement Division in July 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 02/07/2025 | ITSPEIR-4229 | Phishing |
| 02/07/2025 | ITSPEIR-4230 | Phishing |
| 02/07/2025 | ITSPEIR-4231 | Phishing |
| 08/07/2025 | ITSPEIR-4233 | Spam |
| 10/07/2025 | ITSPEIR-4236 | Spam |
| 21/07/2025 | ITSPEIR-4244 | Phishing |
| 22/07/2025 | ITSPEIR-4248 | Spam |

## 14.3 Overview

In July 2025, TI has acknowledged **16** suspicious email reports by users, confirming that there are **9** spam emails, and **6** phishing emails. TI has sent out emails to the users who reported these emails, advising them to delete these emails and avoid clicking on any links or attachments within them. Additionally, instructions were provided on how to block future emails from the same sender to prevent further phishing attempts.

|  |  |  |
| --- | --- | --- |
|  | Spam | Phishing |
| Communications Division | 6 | 2 |
| Settlements Division | 3 | 4 |
| Total | 9 | 6 |