# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in September 2025

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Responsible Person |
| Cyber Threat Operations (CTO) | Last Modification of Latest Version (On 28 Jul 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 August 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 August 2025, there were **2** critical& **7** high-severity-level Common Vulnerabilities and Exposures (CVEs).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Reply |
| High | PwC, DPO | 01/08/2025 | ITSSOC-11084 | CVE-2025-6558 | Apple Products | Multiple Vulnerabilities in Apple Products | N/A |
| High | PwC | 04/08/2025 | ITSSOC-11095 | CVE-2025-40599 | SonicWall SMA100 | SonicWall SMA100 Post-authentication Arbitrary File Upload vulnerability | N/A |
| Critical | PwC | 06/08/2025 | ITSSOC-11097 | CVE-2025-6000 | HashiCorp Vault | Critical HashiCorp Vault Flaw Allowing Arbitrary Code Execution | N/A |
| High | PwC | 12/08/2025 | ITSSOC-11183 | CVE-2025-53652 | Jenkins | Command Injection in Jenkins via Git Parameter | N/A |
| High | PwC, DPO | 13/08/2025 | ITSSOC-11201 | CVE- 2025-53779 | Microsoft Products | Multiple Vulnerabilities in Microsoft Products (August 2025) for subscribers | N/A |
| High | PwC | 28/08/2025 | ITSSOC-11310 | CVE-2025-8088 | WinRAR | WinRAR 0-Day Path Traversal Vulnerability Allows Arbitrary Code Execution | N/A |
| High | PwC | 28/08/2025 | ITSSOC-11311 | CVE-2025-8714 & CVE-2025-8715 | PostgreSQL | PostgreSQL Allows Privileged Users Arbitrary Code Execution | N/A |
| High | PwC, DPO | 28/08/2025 | ITSSOC-11312 | CVE-2025-43300 | Apple Products | Vulnerability in Apple Products for subscribers | N/A |
| Critical | DPO | 28/08/2025 | ITSSOC-11313 | CVE-2018-0171 | Cisco IOS & IOS XE | Cisco IOS & IOS XE Remote Code Execution Vulnerability with Continued Exploitation Activity | N/A |

## 12.2 Monthly High Severity Level CVEs Tracking

In August 2025, there were **0** Critical & **0** 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 |
|  |  |  |  |  |  |  |

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

## 12.3 Ongoing CVEs Remediation (Until 26 Sep 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-9623 | CVE-2025-2783 | Google Chrome | Critical3 | AD(IT)(PSM)1 | 1st Attempt: 26 Mar 2025  2nd Attempt: 16 August 2025 | 2 | 16 August 2025 | N/A | Yes | N/A | Within 6 weeks | Pending | 0 | 71**1** | N/A | PwC, DPO |

As of August 2025, there were **1** 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 26 Sep 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 26 Sep 2025)

As of August 2025, there were **9** completed CVEs remediation efforts.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 August 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 |
| 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 | 14 Aug 2025 | 8 | 21 | 0 | 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 | 28 Aug 2025 | 8 | 35 | 0 | PwC |
| 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) | Before 09 August 2025 | 4 | 12**1** | N/A | PwC, DPO |

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. Fortinet SSL VPNs & FortiManager Hit by Global Brute-Force Wave Globally including Hong Kong, since 03 Aug 2025
2. Supply Chain Attack Salesforce Disclosed Data Breach via Social Engineering

12.6 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
| 1. Fortinet SSL VPNs & FortiManager Hit by Global Brute-Force Wave Globally including Hong Kong, since 03 Aug 2025 | * TI team continuously real-time monitor Fortinet advisories and TI-feeds like the NVDs for new vulnerabilities related to Fortinet SSL VPNs & FortiManager, to detect early signs of exploitation attempts that may precede CVE releases. No CVEs directly related in this case. * TI on-site analyst threat hunt campaign targeting malicious IP Addresses, and Indicators of Compromise (IoCs) associated with the brute-force attacks found no compromise within HKMA security solutions, and all known IoCs have been blocked |
| 1. Supply Chain Attack Salesforce Disclosed Data Breach via Social Engineering | * Confirm with AD(IT)(ITS)3, verified HKMA is unaffected as HKMA does not utilize Salesforce solutions. |

1. Fortinet SSL VPNs & FortiManager Hit by Global Brute-Force Wave Globally including Hong Kong, since 03 Aug 2025

Cybersecurity researchers warned of a significant spike in brute-force attacks targeting Fortinet SSL VPNs and FortiManagers, with notable activity observed on August 3, 2025, involving over 780 unique malicious IP addresses, and a shift in focus post-August 5.

**Impact and Analysis**

These attacks were deliberate, targeting the FortiOS profile for SSL VPNs initially and later pivoting to FortiManager systems, with two distinct waves: a steady, long-running campaign before August 5 and a concentrated burst with a different TCP signature afterward. The malicious IPs originated from countries like the United States, Canada, Russia, and the Netherlands, targeting systems in the United States, Hong Kong, Brazil, Spain, and Japan.

Historical data also revealed a June 2025 spike linked to a FortiGate device on a residential ISP (Pilot Fiber Inc.), suggesting possible attack testing or use of residential proxies. This pattern aligns with trends where spikes in malicious activity often precede the disclosure of new vulnerabilities (CVEs) in enterprise edge technologies like VPNs and firewalls within six weeks.

**Recommendations**

#1 TI team continuously real-time monitor Fortinet advisories and TI-feeds like the NVDs for new vulnerabilities related to Fortinet SSL VPNs & FortiManager, to detect early signs of exploitation attempts that may precede CVE releases. No CVEs directly related in this case.

#2 TI on-site analyst threat hunt campaign targeting malicious IP Addresses, and Indicators of Compromise (IoCs) associated with the brute-force attacks found no compromise within HKMA security solutions, and all known IoCs have been blocked.

Source: Coordinated Brute Force Campaign Targeting Fortinet SSL VPNs in Hong Kong, Early August 2025 (ITSSOC-11204)

1. Supply Chain Attack Salesforce Disclosed Data Breach via Social Engineering

In late 2024, threat actors initiated a widespread supply chain campaign targeting Salesforce environments, leveraging social engineering tactics such as voice phishing (vishing) to impersonate IT help desks and trick employees into granting unauthorized access.

The company provides services to over 11,000 organizations, including over 60% of Fortune 500 firms.

**Impact and Analysis**

The HR firm has disclosed a data breach after threat actors compromised a third-party customer relationship management (CRM) platform in a recent social engineering attack.

Compromised data was primarily commonly available business contact information, including names, email addresses, and phone numbers. The company warns that exposed data may potentially used by attackers to further their social engineering scams.

Detailed by Threat Intelligence, such affected over 700 organizations globally, including high-profile victims such as Google, Adidas, Cisco, Pandora, etc.

**Recommendations**

Confirm with AD(IT)(ITS)3, verified HKMA is unaffected as HKMA does not utilize Salesforce solutions.

Source: [Human resources firm Workday disclosed a data breach](https://securityaffairs.com/181271/data-breach/human-resources-firm-workday-disclosed-a-data-breach.html) – released by Security Affairs on August 18,2025

# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In August 2025, a total of **5** threat hunting cases were handled. These included **2** government-targeted cases, **3** APAC-targeted cases, and **3** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 06/08/2025 | ITSSOC-11096 | Soco404 Active Campaign Exploited Misconfigurations in PostgreSQL |  |  | ✓ |
| 11/08/2025 | ITSSOC-11166 | Google suffers data breach in ongoing Salesforce data theft attacks | ✓ | ✓ | ✓ |
| 12/08/2025 | ITSSOC-11195 | CastleBot Malware-as-a-Service (MaaS) Framework Fueling Info-Stealer & Ransomware Attacks |  | ✓ |  |
| 14/08/2025 | ITSSOC-11204 | Coordinated Brute Force Campaign Targeting Fortinet SSL VPNs in Hong Kong, Early August 2025 |  | ✓ | ✓ |
| 20/08/2025 | ITSSOC-11240 | New RAT 'GodRAT' targeting financial institutions | ✓ |  |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In August 2025, a total of **5** threat hunting cases were handled.

In addition, this effort resulted in the blocking of **50** hashes, **25** domains or URLs, **17** IP addresses, and **2** email 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 | Email Blocked Count |
| 06/08/2025 | ITSSOC-11096 | Soco404 Active Campaign Exploited Misconfigurations in PostgreSQL | No | 26 | 9 | 0 | 0 |
| 11/08/2025 | ITSSOC-11166 | Google suffers data breach in ongoing Salesforce data theft attacks | No | 0 | 0 | 0 | 2 |
| 12/08/2025 | ITSSOC-11195 | CastleBot Malware-as-a-Service (MaaS) Framework Fueling Info-Stealer & Ransomware Attacks | No | 18 | 15 | 1 | 0 |
| 14/08/2025 | ITSSOC-11204 | Coordinated Brute Force Campaign Targeting Fortinet SSL VPNs in Hong Kong, Early August 2025 | No | 0 | 0 | 10 | 0 |
| 20/08/2025 | ITSSOC-11240 | New RAT 'GodRAT' targeting financial institutions | No | 6 | 1 | 6 | 0 |
| Total | | | | 50 | 25 | 17 | 2 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were **12** of reported emails from Communications Division in August 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 01/08/2025 | ITSPEIR-4259 | Spam |
| 01/08/2025 | ITSPEIR-4260 | Spam |
| 04/08/2025 | ITSPEIR-4262 | Phishing |
| 04/08/2025 | ITSPEIR-4263 | Phishing |
| 04/08/2025 | ITSPEIR-4264 | Phishing |
| 04/08/2025 | ITSPEIR-4265 | Phishing |
| 04/08/2025 | ITSPEIR-4266 | Phishing |
| 04/08/2025 | ITSPEIR-4268 | Phishing |
| 19/08/2025 | ITSPEIR-4272 | Phishing |
| 20/08/2025 | ITSPEIR-4274 | Spam |
| 26/08/2025 | ITSPEIR-4278 | Phishing |
| 28/08/2025 | ITSPEIR-4280 | Phishing |

## 14.2 Settlement Division

There were **0** of reported emails from Settlement Division in August 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| N/A | N/A | N/A |

## 14.3 Overview

In August 2025, TI has acknowledged **12** suspicious email reports by users, confirming that there are **3** spam emails, and **9** 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 | 3 | 9 |
| Settlements Division | 0 | 0 |
| Total | 3 | 9 |