# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in January 2025

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Responsible Person |
| Cyber Threat Operations (CTO) | 4th Modification of Latest Endorsement (Released on 21 Feb 2025)  Modified  •Phishing Email Handling   * Added “Neutral” into original classified types (“Unwanted”, “Spam”, “Phishing”) * Objective: Received feedback from HKMA Communications & Settlement Team, if reported emails do not contain any phishing indicators, plus mark as “Neutral” | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |
| Security Operations Centre (SOC) | Last Modification of Latest Version (in 05 Nov 2024) | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |
| Threat Hunting | 2nd Modification of Latest Version (Released on 21 Feb 2025)  Modified  •Conduct Threat Hunt Routinely against specific active Advanced Persistent Threat (APT) group  - Reason: Suggested by AD(IT)(ITS)3 as a lesson learnt, conduct threat hunt focus on an opportunistic threat actor, like base on Recent activity is active | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |
| Incident Response (IR) | Last Modification of Latest Version (in 31 Jul 2024) | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |

Remarks:

1 If no further comment listed in February 2025 SOC Monthly Meeting, the latest version of SOP for Threat Intelligence – “HKMA Threat Intelligence SOP – 20250221” is endorsed.

# Cyber Threat Operations (CTO)

## 12.1 Monthly CVEs Summary

In January 2025, there were **1** high-security-level Common Vulnerabilities and Exposures (CVE), **12** medium-security-level CVE, **2** low-security-level CVE.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Confirm Affected |
| High | PwC, GovCERT, CISA | 15/01/2025 | ITSSOC-8780 | CVE-2024-55591 | FortiOS and FortiProxy | Actively Exploited Authentication Bypass Zero-Day Vulnerability in FortiOS and FortiProxy | Yes |
| Medium | PwC | 07/01/2025 | ITSSOC-8705 | CVE-2024-46981 | Redis Server | Redis-Server System Manipulation Leads to Remote Code Execution | N/A |
| Medium | PwC, GovCERT | 09/01/2025 | ITSSOC-8731 | CVE-2025-0282 | Ivanti Products | Multiple Vulnerabilities in Ivanti Products for subscribers | N/A |
| Medium | PwC, GovCERT | 09/01/2025 | ITSSOC-8733 | CVE-2024-53704 | SonicWall | Multiple Vulnerabilities in SonicWall Products | N/A |
| Medium | PwC, GovCERT | 15/01/2025 | ITSSOC-8786 | CVE-2025-21333 | Microsoft Products | Multiple Vulnerabilities in Microsoft Products (January 2025) | N/A |
| Medium | PwC, GovCERT | 20/01/2025 | ITSSOC-8840 | CVE-2024-10811 | Ivanti Products | Multiple Vulnerabilities in Ivanti Products | N/A |
| Medium | PwC | 21/01/2025 | ITSSOC-8905 | CVE-2025-0411 | 7-Zip | 7-Zip Mark-of-the-Web Bypass Vulnerability | N/A |
| Medium | PwC | 21/01/2025 | ITSSOC-8906 | CVE-2025-23051 | HPE Aruba Networking | Authenticated Remote Arbitrary Code Execution in HPE Aruba Networking AOS Controllers and Gateways | N/A |
| Medium | PwC, GovCERT | 23/01/2025 | ITSSOC-8931 | CVE-2025-20128 | Cisco Products | Multiple Vulnerabilities in Cisco Products | N/A |
| Medium | PwC | 23/01/2025 | ITSSOC-8934 | CVE-2025-0611 / CVE-2025-0612 | Google Chrome | Google Chrome V8 Engine Vulnerability May Allow RCE | N/A |
| Medium | PwC | 23/01/2025 | ITSSOC-8939 | CVE-2025-21298 | Windows OLE | PoC Released for Windows OLE Remote Code Execution Vulnerability (CVE-2025-21298) | N/A |
| Medium | PwC, GovCERT | 24/01/2025 | ITSSOC-8949 | CVE-2025-23006 | SonicWall | Vulnerability in SonicWall SMA1000 Series Products for subscribers | N/A |
| Medium | PwC | 24/01/2025 | ITSSOC-8951 | CVE-2024-43468 | Microsoft Configuration Manager | PoC Released for Microsoft Configuration Manager Unauthenticated SQL Injection Vulnerability (CVE-2024-43468) | N/A |
| Low | PwC | 10/01/2025 | ITSSOC-8749 | CVE-2025-0194 | GitLab | Possible Access Token Exposure in GitLab Logs | N/A |
| Low | PwC | 22/01/2025 | ITSSOC-8915 | CVE-2025-23195 | Apache Ambari | Apache Ambari XXE Flaw Enables SSRF Attacks in Hadoop Management | N/A |

## 

## 12.2 Monthly High Severity Level CVEs Tracking

In January 2025, there were **1** 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-2024-55591 | FortiOS  FortiProxy | No (Admin Interface) | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Workaround as specified by advisory | 15/01/2025 (Applied) | The System Owner should apply the both patch and workaround.  Justifications  By allowing only specified IP addresses to access the administrative interface and blocking all others, the workaround reduces the attack surface. The patch prevents systems remain exposed to potential attacks that can lead to unauthorized access. |

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

## 12.3 Ongoing CVEs Remediation (Until 15 Feb 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-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 20241 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | N/A | 3 | 1243 | N/A | PwC, GovCERT |
| 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 20241 | 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 | N/A | 1 | 953 | N/A | PwC, GovCERT, CISA |

As of January 2025, there were **2** ongoing CVEs remediation efforts.

Remarks:

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

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

3 The timeframe is calculated up to 17 Feb 2025; additional days will continue to be added until the patch is completed.

## 12.4 Completed CVEs Remediation (Until 15 Feb 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 20241  2nd Follow-up: 3 Jan 20252 | 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 20251  2nd Follow-up: 14 Feb 20252 | 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 |

As of January 2025, there were **2** completed CVEs remediation efforts.

Remarks:

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

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

## 12.4 Major Threat Intelligence Report Highlight

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

1. Japan Airlines Under Cyberattack on 26 December, Flights Delayed
2. Actively Exploited Unauthenticated Denial of Service (DoS) Vulnerability in DNS Security Feature of Palo Alto Networks Firewall (CVE-2024-3393)

12.5 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
| 1. Japan Airlines Under Cyberattack on 26 December, Flights Delayed | * Monitor and gain insights from the news related to the Japan Airlines cyberattack, which may be relevant to HKMA. |
| 1. Actively Exploited Unauthenticated Denial of Service (DoS) Vulnerability in DNS Security Feature of Palo Alto Networks Firewall (CVE-2024-3393) | * Send an email to the network team to confirm if their current version of the PA Firewall is impacted. |

1. Public Bank Served by Capital Cell Global (CCG) Undergoes Data Breach on 11 February

On 11 Feb 2025, PwC’s Dark Lab observed that Capital Cell Global (CCG) has been claimed as a victim of Kill Security ransomware. We have noted that this company serves multiple bank clients, and based on the evidence provided by the threat actor, Public Bank’s documents were listed among the leaked data.

**Impact and Analysis**

KillSec (a.k.a. Kill Security) is a Ransomware-as-a-Service (RaaS) group, active since October 2023. Since the launch of their dedicated leak site in March 2024, KillSec has listed over 90 victims globally, with approximately 50% of victims based in Asia. The groups’ ransom demands range from thousands of dollars to 10,000 euros. KillSec primarily requests ransom in euros, which is considered uncommon amongst ransomware actors.

The group is observed to possess opportunistic targeting nature, though restricts targeting against CIS countries and critical infrastructure. Despite this, affiliates have been observed to compromise healthcare and government victims. The group is known to acquire access from initial access brokers or leaked credentials on the dark web to gain initial access.

In addition to their RaaS offerings, KillSec claims to provide penetration testing and open-source (OSINT) services to cybercriminals to assist with their reconnaissance and initial access stages of the attack.

**Recommendations**

TI on-site analyst conducts a threat hunt campaign against the Kill Security (KillSec) ransomware. No positive findings were observed in HKMA security solutions, and all IoCs have been blocked.

Source: [KILLSEC Ransomware IoCs](https://otx.alienvault.com/pulse/66e7e1d174ecff1abcd7a374)

1. OceanLotus APT Group Re-Active since November 2024 and Utilizes New Memory Technique in APAC Attacks

On 27 January 2025, Palo Alto Networks released a Security Advisory disclosing a new vulnerability impacting PAN-OS (CVE-2024-3393). The vulnerability enables an unauthenticated, remote attacker to achieve a Denial of Service (DoS) by sending a specially crafted packet through the firewall's data plane, disrupting firewall operations and forcing them into maintenance mode. Palo Alto Networks has confirmed active exploitation of this vulnerability in production environments.

**Impact and Analysis**

Palo Alto Networks is aware of customers experiencing this denial of service (DoS) when their firewall blocks malicious DNS packets that trigger this issue. However, it has not disclosed specific technical details regarding the mechanics of the vulnerability or the precise conditions under which it can be exploited.

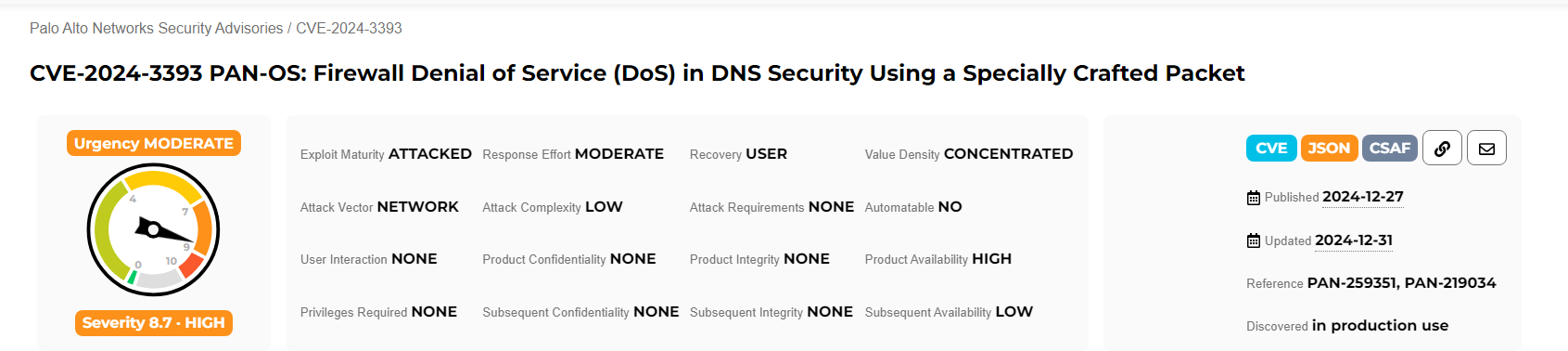
As of the time of writing, there are no indicators of compromise (IOCs) related to the CVE-2024-3393 vulnerability.

Affected Products:

* PAN-OS 11.2: Affected versions < 11.2.3
* PAN-OS 11.1: Affected versions < 11.1.5
* PAN-OS 10.2: Affected versions >= 10.2.8, < 10.2.10-h12, < 10.2.13-h2
* PAN-OS 10.1: Affected versions >= 10.1.14, < 10.1.14-h8
* Prisma Access: Affected versions >= 10.2.8 on PAN-OS< 11.2.3 on PAN-OS

\*Note: PAN-OS 11.0 reached the end of life (EOL), PA did not provide a fix for this release.

Source: [Palo Alto Network Security Advisory](https://security.paloaltonetworks.com/CVE-2024-3393)



# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In January 2025, a total of **9** threat hunting cases were handled. These included **6** government-targeted cases, **4** APAC-targeted cases, and **2** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 08/01/2025 | ITSSOC-8715 | EAGERBEE Targets Backdoor to Infiltrate Internet Service Providers (ISPs) and Governmental Institutions in APAC Region | ✓ |  |  |
| 10/01/2025 | ITSSOC-8755 | Play Ransomware Frequently Targeted the Flaws in FortiOS | ✓ | ✓ | ✓ |
| 13/01/2025 | ITSSOC-8762 | Lumma Stealer Infects Multiple Hong Kong-Based Victims |  | ✓ |  |
| 14/01/2025 | ITSSOC-8772 | APT28 Targets APAC Intelligence on Geopolitical and Economic Dynamics |  | ✓ |  |
| 15/01/2025 | ITSSOC-8787 | A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls |  |  | ✓ |
| 20/01/2025 | ITSSOC-8868 | Frequent Freeloader Part I: Secret Blizzard Compromising Storm-0156 Infrastructure for Espionage | ✓ |  |  |
| 21/01/2025 | ITSSOC-8880 | Frequent Freeloader Part II: Russian Actor Secret Blizzard Using Tools of Other Groups to Attack Ukraine | ✓ |  |  |
| 28/01/2025 | ITSSOC-8988 | Akira Ransomware Continues to Target Linux and VMware ESXi Servers | ✓ |  |  |
| 28/01/2025 | ITSSOC-8989 | Lazarus Group Deploys Electron-Based Malware to Target Cryptocurrency Enthusiasts | ✓ | ✓ |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

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

In addition, this effort resulted in the blocking of **78** hashes, **15** domains or URLs, and **40** 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 |
| 08/01/2025 | ITSSOC-8715 | EAGERBEE Targets Backdoor to Infiltrate Internet Service Providers (ISPs) and Governmental Institutions in APAC Region | No | 5 | 2 | 7 |
| 10/01/2025 | ITSSOC-8755 | Play Ransomware Frequently Targeted the Flaws in FortiOS | No | 21 | 0 | 0 |
| 13/01/2025 | ITSSOC-8762 | Lumma Stealer Infects Multiple Hong Kong-Based Victims | No | 5 | 0 | 0 |
| 14/01/2025 | ITSSOC-8772 | APT28 Targets APAC Intelligence on Geopolitical and Economic Dynamics | No | 9 | 3 | 0 |
| 15/01/2025 | ITSSOC-8787 | A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls | No | 0 | 0 | 12 |
| 20/01/2025 | ITSSOC-8868 | Frequent Freeloader Part I: Secret Blizzard Compromising Storm-0156 Infrastructure for Espionage | No | 8 | 2 | 21 |
| 21/01/2025 | ITSSOC-8880 | Frequent Freeloader Part II: Russian Actor Secret Blizzard Using Tools of Other Groups to Attack Ukraine | No | 6 | 8 | 0 |
| 28/01/2025 | ITSSOC-8988 | Akira Ransomware Continues to Target Linux and VMware ESXi Servers | No | 15 | 0 | 0 |
| 28/01/2025 | ITSSOC-8989 | Lazarus Group Deploys Electron-Based Malware to Target Cryptocurrency Enthusiasts | No | 9 | 0 | 0 |
| Total | | | | 78 | 15 | 40 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were 4 of reported emails from Communications Division in January 2025.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
| 10/01/2025 | ITSPEIR-3623 | Request for Reply | Spam |
| 14/01/2025 | ITSPEIR-3627 | Request for Reply | Spam |
| 14/01/2025 | ITSPEIR-3629 | Request for Reply | Spam |
| 16/01/2025 | ITSPEIR-3631 | Financial Scam | Spam |

## 14.2 Settlement Division

There were 4 of reported emails from Settlement Division in January 2025.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
| 13/01/2025 | ITSPEIR-3625 | Request for Reply | Spam |
| 27/01/2025 | ITSPEIR-3635 | Spam Attachment | Spam |
| 27/01/2025 | ITSPEIR-3636 | Spam Attachment | Spam |
| 27/01/2025 | ITSPEIR-3638 | Request for Reply | Spam |

## 14.3 Overview

In January 2025, TI has acknowledged **8** suspicious email reports by users, confirming that there are **0** unwanted emails, **8** spam emails, and **0** 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.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unwanted | Spam | Phishing |
| Communications Division | 0 | 4 | 0 |
| Settlements Division | 0 | 4 | 0 |
| Total | 0 | 8 | 0 |