# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in %Month%

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Status | Responsible Person |
| Cyber Threat Operations (CTO) |  |  |  |  |
| Security Operations Centre (SOC) |  |  |  |  |
| Threat Hunting |  |  |  |  |
| Incident Response (IR) |  |  |  |  |

# Cyber Threat Operations (CTO)

## 12.1 Monthly CVEs Summary

In %month, year%, there were **%count%** high-security-level Common Vulnerabilities and Exposures (CVE), **%count%** medium-security-level CVE, and **%count%** low-security-level CVE.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Confirm Affected |
| High |  |  |  |  |  |  |  |
| Medium |  |  |  |  |  |  |  |
| Low |  |  |  |  |  |  |  |

## 

## 12.2 Monthly High Severity Level CVEs Tracking

In %month, year%, there were **%count%** 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 |
|  |  |  |  |  |  |  |

## 12.3 Ongoing CVEs Remediation

As of %month, year%, there were %count% ongoing 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 Last Follow-up | Date of Acknowledgement | CVE Relevant to HKMA | Affected System/ Server IP | Target Remediation Completion Date | Affected System/ Server IP | Target Remediation Completion 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 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## 12.4 Major Threat Intelligence Report Highlight

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

12.5 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
|  |  |
|  |  |

# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In %month, year%, a total of **%count%** threat hunting cases were handled. These included **%count%** government-targeted cases, **%count%** APAC-targeted cases, and **%count%** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
|  |  |  |  |  |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In %month, year%, a total of **%count%** threat hunting cases were handled

In addition, this effort resulted in the blocking of **%count%** hashes, **%count%** domains or URLs, and **%count%** IP addresses. All **%count%** Indicators of Compromise (IoCs) were blocked, with **%count%** left unblocked.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Hits | Hash Blocked Count | Domain/URL Blocked Count | IP Blocked Count |
|  |  |  |  |  |  |  |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were %count% of Phishing Email from Communications Division in %month, year%.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
|  |  |  |  |
|  |  |  |  |

## 14.2 Settlement Division

There were %count% of Phishing Email from Settlement Division in %month, year%.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
|  |  |  |  |
|  |  |  |  |

## 14.3 Overview

In %month, year%, TI has acknowledged **%count%** suspicious email reports by users, confirming that there are **%count%** unwanted emails, **%count%** spam emails, and **%count%** 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 |  |  |  |
| Settlements Division |  |  |  |
| Total |  |  |  |