# 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 Common Vulnerabilities and Exposures (CVEs)

There were %count% of OGCIO High Threat Security Alert in %month, year%.

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

## 

## 12.2 Follow-up on High Severity Level CVEs

There were %count% of Common Vulnerabilities and Exposures (CVE) Affected HKMA in %month, year%.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Severity Level | Jira Ticket No. | CVE number | Product | Affected System/ Server IP | Schedule patch/workaround date |
| High |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 12.3 Major Threat Intelligence Report Highlight

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

12.4 Executive Summary

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

# Threat Hunting

## 13.1 Indicators of Compromise (IOCs) Blocked

There were %count% of Threat Hunting cases in %month, year%. There are %count% of IPs, Domains

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | IP Blocked Count | Domain Blocked Count | Hash Blocked Count | Not blocked | Hits |
|  |  |  |  |  |  |  | N/A |
|  |  |  |  |  |  |  |  |
| Total | | |  |  |  |  |  |

## ~~13.2 IoCs from Threat Hunting found in HKMA~~

There were %count% of cases that the IoCs found via Threat Hunt found within the HKMA environment in %month, year%.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Hits | IoC Name | Description |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 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

Below is the overview of Phishing Email Alert handled in%month, year%.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unwanted | Spam | Phishing |
| Communications Division |  |  |  |
| Settlements Division |  |  |  |
| Total |  |  |  |