Incident Report

Contents

[INCIDENT SUMMARY 1](#_Toc109162598)

[TIMELINE 1](#_Toc109162599)

[ADVERSARY ACTIONS 1](#_Toc109162600)

[RECOMMENDATIONS 1](#_Toc109162601)

[TECHNICAL ANALYSIS 3](#_Toc109162602)

[Console/Log Analysis 3](#_Toc109162603)

[EDR 3](#_Toc109162604)

[SIEM 3](#_Toc109162605)

[Firewall 3](#_Toc109162606)

[[Console] 3](#_Toc109162607)

[Hosts 3](#_Toc109162608)

[HOST1 3](#_Toc109162609)

[HOST2 3](#_Toc109162610)

[Indicators 3](#_Toc109162611)

# INCIDENT SUMMARY

[Few paragraphs describing the incident, investigation, and analysis results]

# TIMELINE

[Refer to IncidentTracking.xlsx and the “TIMELINE” here when completed]

# ADVERSARY ACTIONS

[Include which MITRE TTPs were observed and details of how it matches]

#### [Tactic]:

**[Technique]:** [Correlating Incident details]

#### [Tactic]:

**[Technique]:** [Correlating Incident details]

# RECOMMENDATIONS

|  |  |  |
| --- | --- | --- |
| Priority | Title | Description |
| High |  |  |
| Medium |  |  |
| Low |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# TECHNICAL ANALYSIS

# Console/Log Analysis

## EDR

## SIEM

## Firewall

## [Console]

# Hosts

## HOST1

### Artifact

[Analysis Notes regarding the artifact]

#### Artifact2

[Analysis Notes regarding the artifact]

## HOST2

### Artifact

[Analysis Notes regarding the artifact]

### Artifact2

[Analysis Notes regarding the artifact]

# Indicators

### Network

[IP Address/DNS]

### File

[File Name/Hash]

### Users

[Domain and Username]