Investigation Notes

Contents

[Console/Log Analysis 1](#_Toc104467658)

[EDR 1](#_Toc104467659)

[SIEM 1](#_Toc104467660)

[Firewall 1](#_Toc104467661)

[[Console] 1](#_Toc104467662)

[Hosts 1](#_Toc104467663)

[HOST1 1](#_Toc104467664)

[HOST2 1](#_Toc104467665)

[HOST3 1](#_Toc104467666)

[Indicators 1](#_Toc104467667)

# Console/Log Analysis

## EDR

## SIEM

## Firewall

## [Console]

# Hosts

## HOST1

Operating System:

IP Address:

Function:

Primary User:

Additional Notes:

### Artifact

[Analysis Notes regarding the artifact]

#### Artifact2

[Analysis Notes regarding the artifact]

## HOST2

Operating System:

IP Address:

Function:

Primary User:

Additional Notes:

### 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]