James Graham

[Company name]

Incident report - [Document title]

Diagram

Description automatically generated

Contents

[Incident Information 2](#_Toc73881244)

[Incident Data 3](#_Toc73881245)

[Alert Information 4](#_Toc73881246)

[Associated Alerts 4](#_Toc73881247)

[Devices 5](#_Toc73881248)

[Entities 6](#_Toc73881249)

[Associated Entities 6](#_Toc73881250)

[User 6](#_Toc73881251)

[Process 6](#_Toc73881252)

[Registry 6](#_Toc73881253)

[File 6](#_Toc73881254)

[IP 6](#_Toc73881255)

[Mail Message 7](#_Toc73881256)

[Mailbox 7](#_Toc73881257)

[Mail Cluster 7](#_Toc73881258)

[MITRE Techniques 8](#_Toc73881259)

[Associated MITRE Techniques 8](#_Toc73881260)

# Incident Information

Microsoft Defender triggered an Alert (**Alert ID goes here**), this was triggered on:

**Click or tap here to enter text.**

The Alert is associated with the following Incident - Click or tap here to enter text.

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

Microsoft 365 services and apps create alerts when they detect a suspicious or malicious event or activity. Individual alerts provide valuable clues about a completed or ongoing attack. However, attacks typically employ various techniques against different types of entities, such as devices, users, and mailboxes. The result is multiple alerts for multiple entities in your tenant.

Because piecing the individual alerts together to gain insight into an attack can be challenging and time-consuming, Microsoft 365 Defender automatically aggregates the alerts and their associated information into an incident.

Word

Description automatically generated

[Incidents in Microsoft 365 Defender | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide)

## Incident Data

|  |  |
| --- | --- |
| Field Name | Value |
| Incident ID | Click or tap here to enter text. |
| Incident Name | Click or tap here to enter text. |
| Created Time | Click or tap here to enter text. |
| Last Update Time | Click or tap here to enter text. |
| Assigned To | Click or tap here to enter text. |
| Classification | Click or tap here to enter text. |
| Determination | Click or tap here to enter text. |
| Status | Click or tap here to enter text. |
| Severity | Click or tap here to enter text. |
| Comments | Click or tap here to enter text. |
| No. of associated Alerts | Click or tap here to enter text. |
| Link to Incident | Click or tap here to enter text. |

# Alert Information

Alerts are the basis of all incidents and indicate the occurrence of malicious or suspicious events in your environment. Alerts are typically part of a broader attack and provide clues about an incident.

In Microsoft 365 Defender, related alerts are aggregated together to form [incidents](https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide). Incidents will always provide the broader context of an attack, however, analysing alerts can be valuable when deeper analysis is required.

Microsoft 365 Defender alerts may come from solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft Cloud App Security. You may notice alerts with prepended characters in the alert. The following table provides guidance to help you understand the mapping of alert sources based on the prepended character on the alert.

[Investigate alerts in Microsoft 365 Defender | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide)

## Associated Alerts

|  |
| --- |
| Alert Details |
| **Click or tap here to enter text.** |

# Devices

The **Devices** lists all the devices related to the incident.

|  |
| --- |
| Device Details |
| Click or tap here to enter text. |

# Entities

Entities that have been identified to be part of, or related to, a given alert.  
The properties values are:

* User
* Ip
* Url
* File
* Process
* MailBox
* MailMessage
* MailCluster
* Registry

## Associated Entities

### User

|  |
| --- |
| User Details |
| Click or tap here to enter text. |

### Process

|  |
| --- |
| Process Details |
| Click or tap here to enter text. |

### Registry

|  |
| --- |
| Registry Details |
| Click or tap here to enter text. |

### File

|  |
| --- |
| File Details |
| Click or tap here to enter text. |

### IP

|  |
| --- |
| IP Details |
| Click or tap here to enter text. |

### Mail Message

|  |
| --- |
| Mail Message Details |
| Click or tap here to enter text. |

### Mailbox

|  |
| --- |
| Mailbox Details |
| Click or tap here to enter text. |

### Mail Cluster

|  |
| --- |
| Mail Cluster Details |
| Click or tap here to enter text. |

# MITRE Techniques

Techniques represent “how” an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. [Techniques - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/enterprise/)

[ATT&CK-Matrix-Only-09-03-2020-V3 (mitre.org)](https://attack.mitre.org/docs/attack_matrix_poster_2020_october.pdf)

Graphical user interface, application, table, Excel

Description automatically generated

## Associated MITRE Techniques

**Click or tap here to enter text.**