Related Document: Module 1

# Learning Objectives:

* What is a SIEM

# Overview:

Background Information

# Scenario:

Setting the stage for the case study

# 

# Threat Intelligence Report:

| **CATEGORY** | **DESCRIPTION** | **HINT** |
| --- | --- | --- |
| **Event** (general - what type of event occurred against your organization) |  | *Quick overview of the event. You can find this information in in the alerts pane of Enigma Glass and through your analysis* |
| **Target** |  | *You can find this information in the alerts pane of Enigma Glass* |
| **Attack Type** |  | *Internet Research; What type of campaign was this?* |
| **Remediation Actions** |  | *Read* the *following article to determine* [*remediation actions*](https://practical365.com/security/remediating-account-breaches-in-office-365/) |
| **Preventative Actions** (Lessons Learned) |  | *Internet Research: List some potential security measures that could prevent this type of event* |

|  |
| --- |