Enterprise Security Fundamentals

Instructor : Cristian Calinescu

Microsoft MTA, MCSA and MCSE certified
Microsoft Cybersecurity Proffesional certified
Comptia Security + certified

Attack Detection
Overview

Methods and tools used for attack detection:

- ✓ **Logging and monitoring**
- ✓ **SIEM systems**
- ✓ **Intrusion Detection Systems (IDS)**
- ✓ **Attack Detection and Machine Learning**

Attack Detection
Overview

Microsoft Attack Detection Products

- ✓ **Advanced Threat Analytics (Microsoft ATA)**
- ✓ **Azure Advanced Threat Protection (Azure ATP)**
- ✓ **Windows Defender Advanced Threat Protection (WDATP)**
- ✓ **Office 365 Advanced Threat Protection (O365 ATP)**

Microsoft Security Tools and Anomaly Detection

Machine Learning Benefits:

- **Ability to analyze very large volumes of system telemetry to identify anomalous activity related to attacks and intrusions**

Microsoft Security Tools and Anomaly Detection

Microsoft Security Graph:

- Collection of Microsoft's intelligence gathered from customers that opt-in and other sources
- Allows for recognition of anomalous behavior related to attacks across all integrated endpoints

Microsoft Security Tools and Anomaly Detection

Advanced Threat Analytics (ATA):

- On-premises solution for on-premises workloads
- Behavior based detection
- Flag anomalous behavior
- No cloud component

Microsoft Security Tools and Anomaly Detection

Azure Advanced Threat Protection (Azure ATP):

- Cloud based solution for on-premises workloads
- Console and telemetry detected in cloud
- Agents installed on on-premises workloads
- Behavior based detection
- Flag anomalous behavior

Microsoft Security Tools and Anomaly Detection

Windows Defender ATP:

- Solution for Windows 10 endpoints
- Cloud based console for analysis and reporting of security events

Microsoft Security Tools and Anomaly Detection

Azure Security Center:

- Azure based service
- Monitor Azure SaaS and IaaS workloads
- Monitor on-premises server configuration with agent

Microsoft Security Tools and Anomaly Detection

Analytics in the Cloud – the way going forward

- Cloud based analytics is likely the future
- Deep learning tasks performed against telemetry by vendor in the cloud to discover anomalous activity
- Vendor has vast access to telemetry
- Agents on on-premises and cloud workloads