Advanced Threat Protection [ATP] Workshop

SYNERGY ADVISORS

Is your organization ready to protect against next-gen cybersecurity attacks?

More than 4,000 ransomware attacks have occurred every day since the beginning of 2016.

Ransomware can have a huge impact on business operations – in this workshop, learn how to protect, detect, and respond to threats using the latest Microsoft Cyber Security technologies from our security experts, who bring best practices and lessons from the field to help address your unique strategic requirements.

Workshop Overview

Learn how **Microsoft Advanced Threat Protection [ATP]** can provide you with end-to-end Cybersecurity to secure your:
- Collaboration/ Productivity **[O365]**
- End-Points **[Windows]**
- Identity services **[Active Directory]**
- Infrastructure **[Azure ATP]**

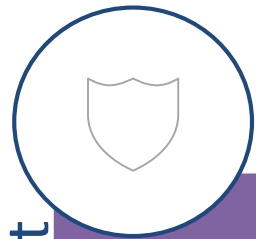## Workshop Scope

- **Who** Should Attend?
  - IT Security Personnel
  - Level **300**

- **Training Length?**
  - Up to **2** Days
  (flexible schedule)

- **Location**
  - Remote /
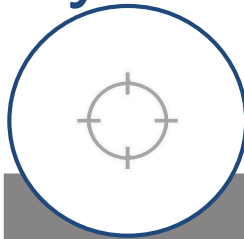 - On-Site

Deliverables

- Lecture Presentations **[PDF]**

- Hands-On-Lab extended access **[1 Week]**

Advanced Threat Protection [ATP] Workshop Details

Key Solutions Components

Protect

- Productivity
  - Anti-virus
  - Anti-spam
- EndPoint
  - AV
  - Device Guard
  - Cred Guard
- Identity
  - AAD Identity Protection
- Infrastructure
  - ATP Sensors for Domain Controllers

Detect

- General
  - Events correlation via Security Graph
- Productivity
  - Safe Links
  - Safe Attachments
  - URL Detonation
- EndPoint
  - Reflecting DLL
- Identity
  - Reconnaissance
  - Compromised Credentials
  - Anomalous Activities
  - Lateral Movement
  - Privilege scalation
  - Domain Dominance
- SaaS Applications
  - Anomalous Activities

Respond

- Productivity
  - Notifications
- EndPoint
  - Notifications
  - Controller folder Access
  - Automatic Investigation and Remediation
- Identity
  - Investigate a user
- Infrastructure
  - Network Machine Learning

Agenda

Session	Day I	Day II
I	**Lecture:** End to End Advanced Threat Protection Architecture **[90 Mins]**	**ATP Lab:** Exploring Windows ATP and how to use automated threat investigations **[90 Mins]**
II	**Lecture:** Protecting your collaboration resources using Office ATP **[90 Mins]**	**Lecture:** Real-time Identity Protection using Microsoft ATA / Azure ATP **[90 Mins]**
III	**ATP Lab:** Exploring Office ATP and seeing the near real time appearance of events in Azure ATP **[90 Mins]**	**ATP Lab:** Exploring ATA and Azure ATP by generating alerts with ATA and seeing how malicious activity appears **[90 Mins]**
IV	**Lecture:** Protecting your Endpoint devices using Windows ATP **[90 Mins]**	**Lecture:** Protecting your organization from Ransomware using Microsoft CAS, Azure ASC, AAD Identity Protection Architecture Overview **[90 Mins]**