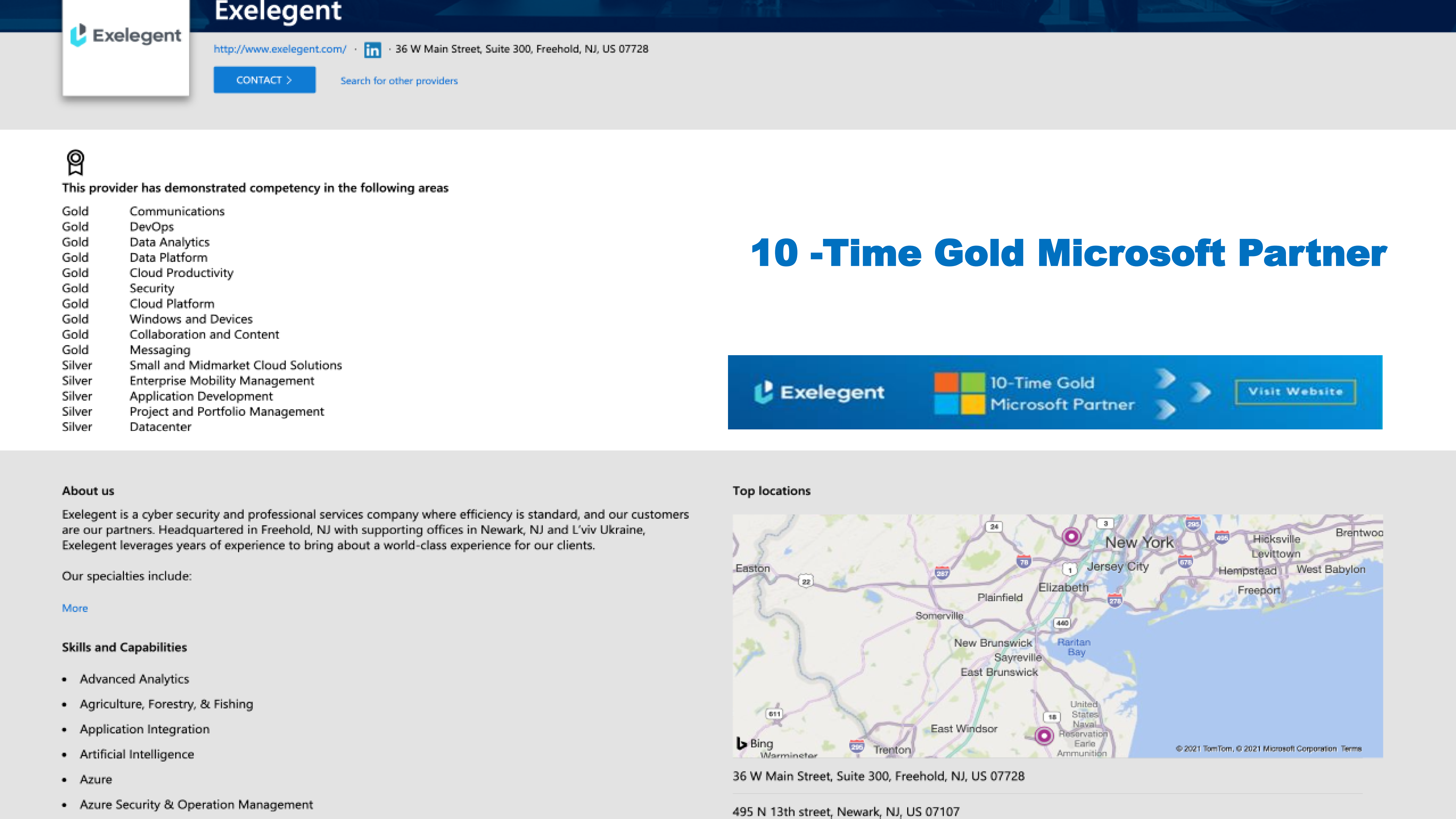
Defend Against Threats with SIEM Plus XDR (with Attack Simulation) 2W – Workshop by Exelegent & Microsoft



Exelegent

http://www.exelegent.com/ · in · 36 W Main Street, Suite 300, Freehold, NJ, US 07728

This provider has demonstrated competency in the following areas

Gold	Communications
Gold	DevOps
Gold	Data Analytics
Gold	Data Platform
Gold	Cloud Productivity
Gold	Security
Gold	Cloud Platform
Gold	Windows and Devices
Gold	Collaboration and Content
Gold	Messaging
Silver	Small and Midmarket Cloud Solutions
Silver	Enterprise Mobility Management
Silver	Application Development
Silver	Project and Portfolio Management
Silver	Datacenter

10 -Time Gold Microsoft Partner

Exelegent 10-Time Gold Microsoft Partner

About us

Exelegent is a cyber security and professional services company where efficiency is standard, and our customers are our partners. Headquartered in Freehold, NJ with supporting offices in Newark, NJ and L'viv Ukraine, Exelegent leverages years of experience to bring about a world-class experience for our clients.

Our specialties include:

Skills and Capabilities

- Advanced Analytics
- Agriculture, Forestry, & Fishing
- Application Integration
- Artificial Intelligence
- Azure
- Azure Security & Operation Management

Top locations

36 W Main Street, Suite 300, Freehold, NJ, US 07728

495 N 13th street, Newark, NJ, US 07107

What our clients say:

- "Exelegent helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. During the process, over 3,500 users continued to collaborate and run critical business functions seamlessly."

  Robert Florescu, CISO, CityMD

- "Switching to Exelegent has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity. Exelegent's IT Support has enabled our business to run as efficiently as possible."

  Bruce Lucarelli, CTO, DermOne

- "Exelegent has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency"

  Alexey Gololobov, CFO, Columbus Hospital LTACH

- "Exelegent has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security.«

  Kevin Hannigan, President, ACC Inc.

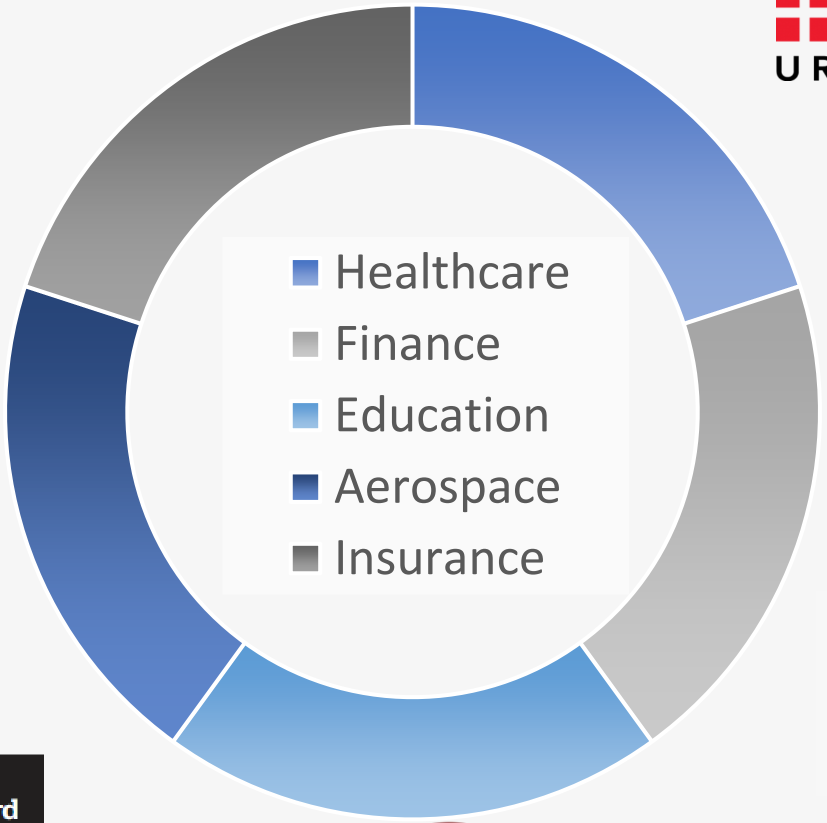
Exelegent

Clients

Industries we serve

WORLD INSURANCE

CITYMD URGENT CARE



SaintPeter's UNIVERSITY 1872

In-Phase Technologies, Inc.

OCEANFIRST BANK

CollegeBoard

ETS®

Defend Against Threats with SIEM Plus XDR Workshop

Focus on learning about your environment and methods you use to secure it.

Simulate attacks to the Trial tenant (based on your Production environment) across email, identity, and data.

Learn about Microsoft's approach to security with an immersive experience, centered around the simulation and analysis of threats.

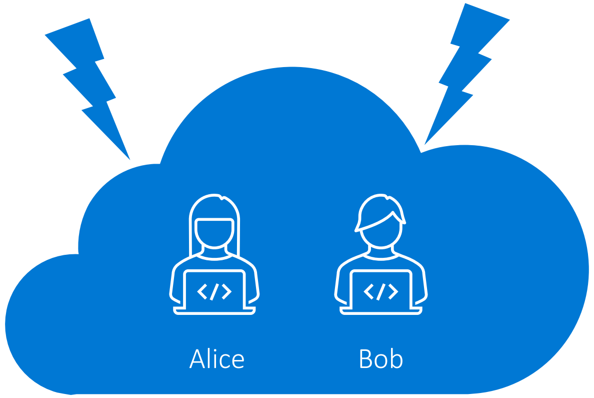
Plan next steps on how we can work together to improve your security posture.

Engagement Setup

Tenants: Production vs. Trial

Microsoft 365
and Azure

Contoso.com



Alice

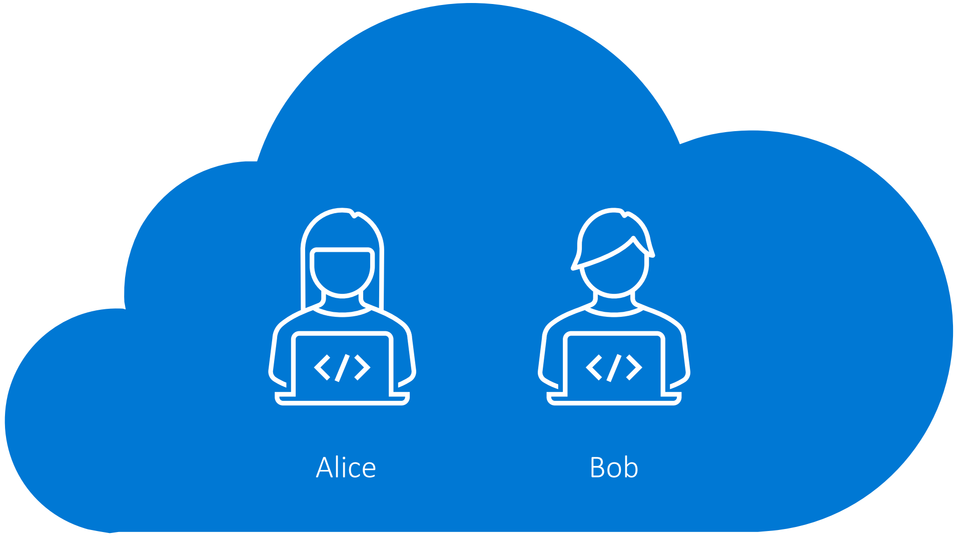
Bob

Contoso123456.onmicrosoft.com

- Your I Production enant.
- Your on-premises environment.
- Your users and their devices.
- NOT affected by any activity in this engagement.

- The Trial enant, created for this engagement.
- Should resemble your P Production vironment – the tenant, your users and their devices.
- User **Alice** is just like in your Pro Production ironment.
- User **Bob** is secured by the **Microsoft E5 Security** suite.
- Both Alice and Bob will be targeted by the Attack Simulation in this engagement.

The Trial tenant



Contoso123456.onmicrosoft.com

General characteristics

The Trial tenant is meant to represent customer’s Production environment.

Standard setup as per description below.

Custom setup agreed during the engagement.

Standard setup

Microsoft 365 E5 trial license

Azure subscription (based on Azure Pass)

Four virtual machines:

- Windows Server (AD DC, file server, etc.)
- Ubuntu Linux
- Two Windows 10 devices

Exelegent

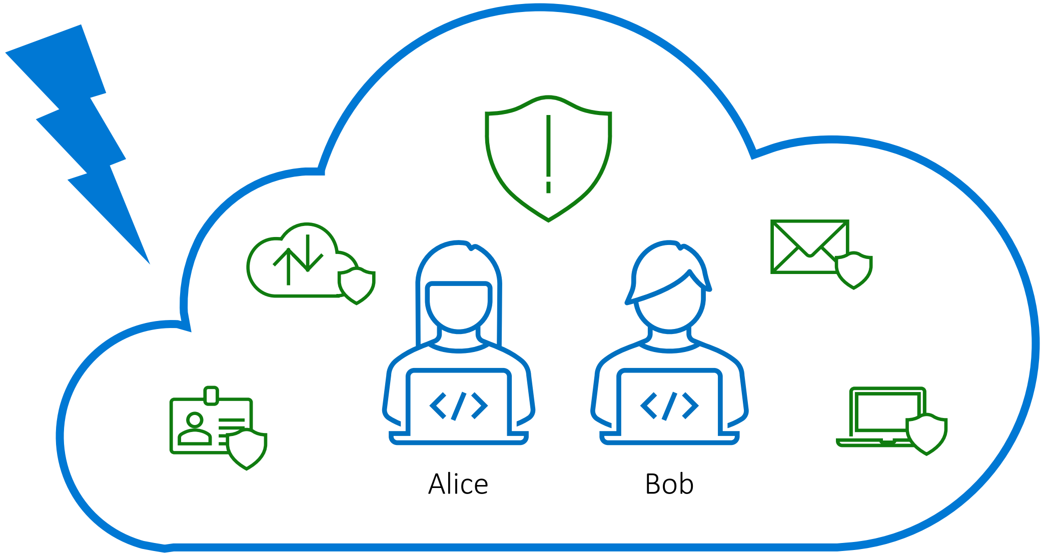
Microsoft Security tools

Microsoft Security tools

Use selected Microsoft Security tools in the Trial tenant and on the endpoints to gain visibility into threats.

- Microsoft Sentinel and Microsoft 365 Defender to understand the correlation between threats.
- Azure Active Directory Identity Protection, Microsoft Defender for Cloud Apps and Microsoft Defender for Identity to understand threats to identity.
- Microsoft Defender for Office 365 and Microsoft Defender for Cloud Apps to understand threats to email and data.
- Microsoft Defender for Endpoint to discover and analyze threats to endpoints.

Microsoft Security tools enablement



Contoso123456.onmicrosoft.com

Microsoft Security tools enablement

Enable selected Microsoft Security tools in the Trial tenant, but scope on user **Bob** and his device.

- Azure Active Directory Identity Protection with sign-in risk detection policies.
- Microsoft Defender for Cloud Apps.
- Microsoft Defender for Office 365 with safe attachments and safe links policies.
- Microsoft Defender for Endpoint.
- Microsoft Defender for Identity.

Attack Simulation

Use automatically generated, simulated attacks to assess your security posture.

Setup of Attack Simulation tool

The tool

AttackIQ https://attackiq.com/

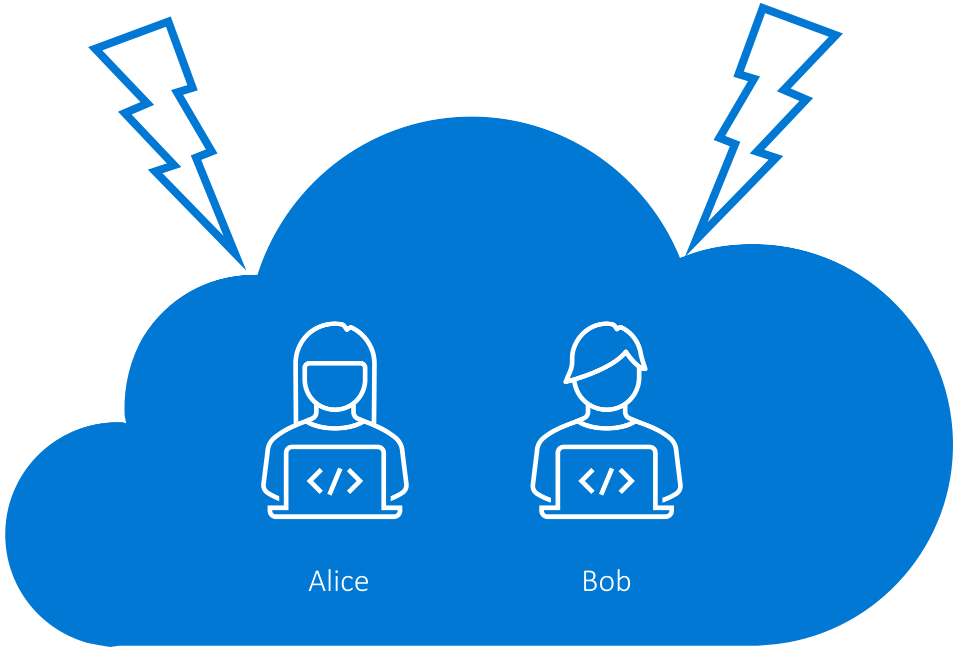
Principles

Target only the Trial tenant.

Targets include identity, email and data in Microsoft 365 and Azure.

Limited simulation of attacks to equivalent of on-premises infrastructure, devices, and users.

Attack Simulation



Contoso123456.onmicrosoft.com

Attack Simulation

Targets only the Trial tenant.

Users **Alice** and **Bob** targeted.

Attack Scenarios

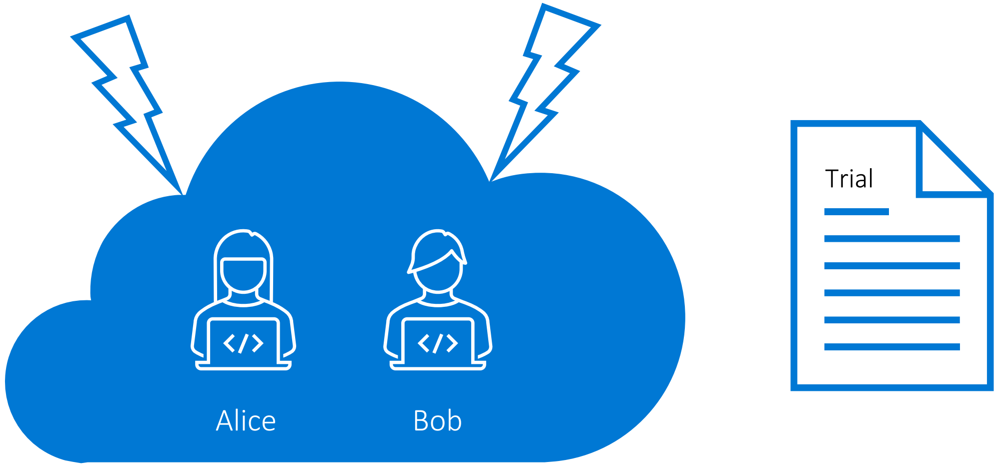
- Initial Access – Spearphishing attachment/link
- Defense Evasion – Stop Defender for Antivirus
- Command and Control – Setup C&C
- Persistence – DLL injection, Account/Service creation
- Discovery – Account, AD, endpoint discovery
- Credential Access – Credential dumping, Password Brute-Force
- Lateral Movement – Pass the ticket/hash, RDP
- Exfiltration – Exfiltration over alternative protocol/C2 channel
- Impact – Ransomware deployment

Exelegent

Attack Simulation & Threat Exploration

Explore results of Attack Simulations targeted at the Trial tenant towards users **Alice** and **Bob**.

Attack Simulation Exploration



Contoso123456.onmicrosoft.com

Reports

From the Attack Simulation targeted at the Trial tenant.

Approach

Explore the results of attack simulation, scenario by scenario.

Note cases where a scenario was:

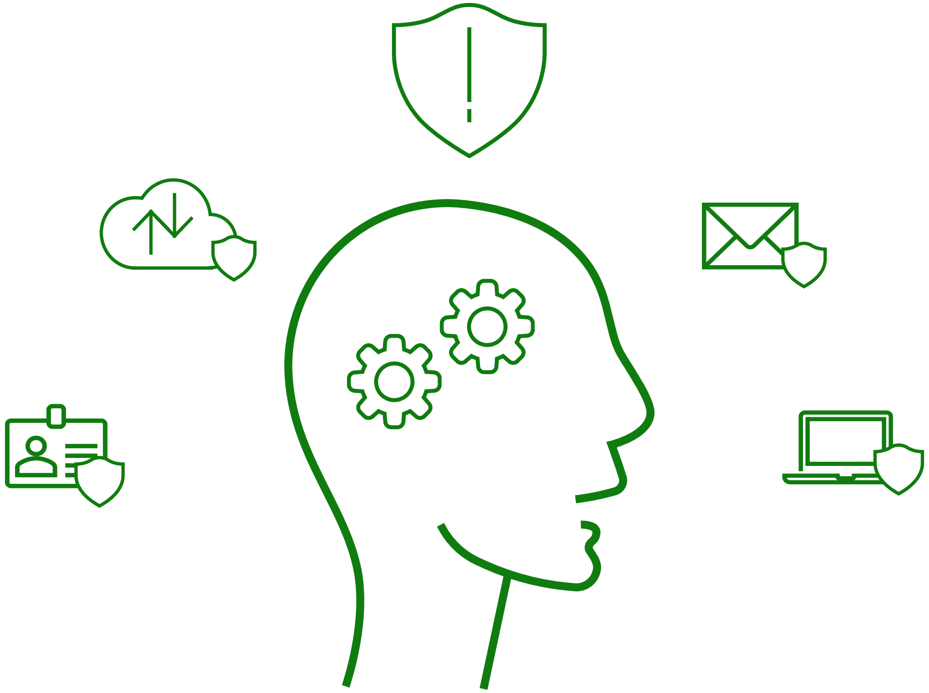
- successful for **Alice**,
- detected and prevented for **Bob**.

Extrapolate the result of the exploration

> “What would happen if such attack was targeted at resource X or user Y in your Production tenant…”

Exelegent

Threat Exploration



The tools

Microsoft Sentinel and Microsoft 365 Defender portal for high-level incidents and alerts from Microsoft security products.

Principles

Exploration of threats detected as result of simulated attacks in the Trial tenant.

Extrapolate the result of threat exploration

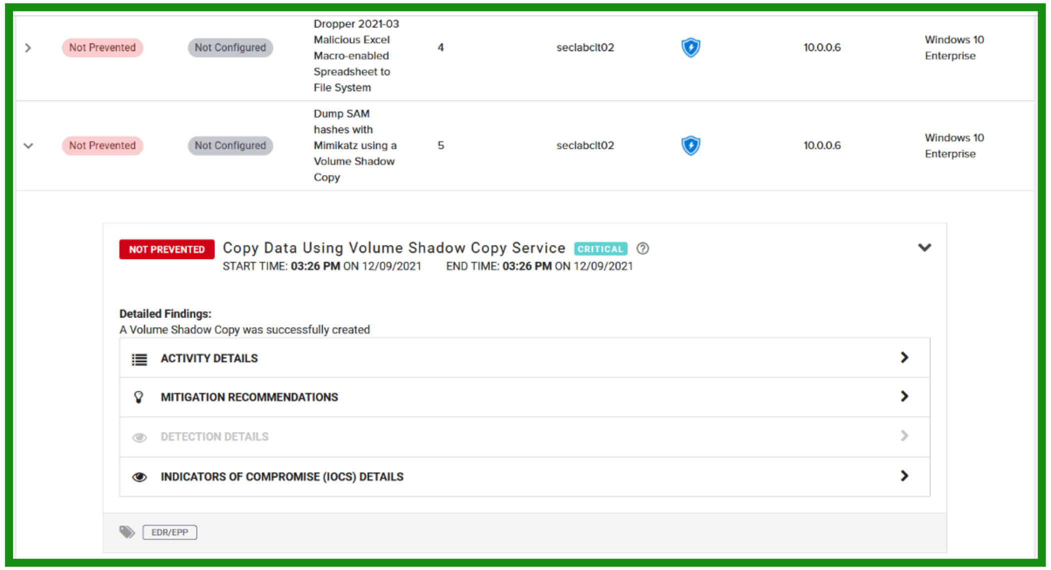
> "What would happen if such threat was targeted at resource X or user Y in your Production tenant..."

Exelegent

Results Presentation

Attack Simulation Exploration findings

- For each simulated attack scenario, note if it was successful or prevented in the Trial tenant.
- Dive deeper in each scenario to explain why it was successful or prevented.



Not Prevented	Not Configured	Dropper 2021-03 Malicious Excel Macro-enabled Spreadsheet to File System	4	seclabclt02		10.0.0.6	Windows 10 Enterprise
Not Prevented	Not Configured	Dump SAM hashes with Mimikatz using a Volume Shadow Copy	5	seclabclt02		10.0.0.6	Windows 10 Enterprise

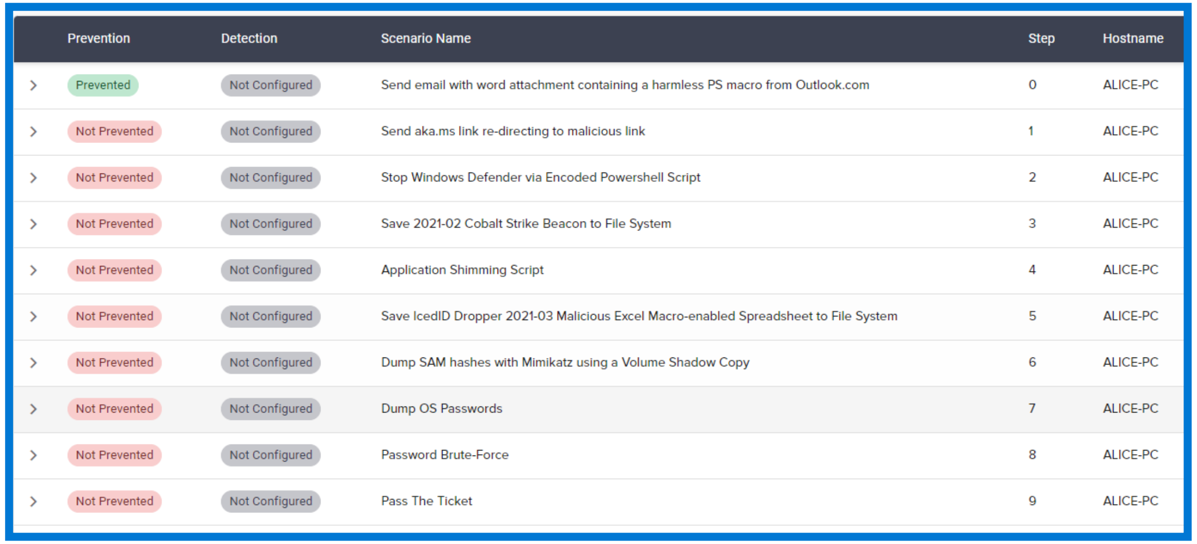
NOT PREVENTED Copy Data Using Volume Shadow Copy Service CRITICAL

START TIME: **03:26 PM** ON 12/09/2021 END TIME: **03:26 PM** ON 12/09/2021

Detailed Findings:
A Volume Shadow Copy was successfully created

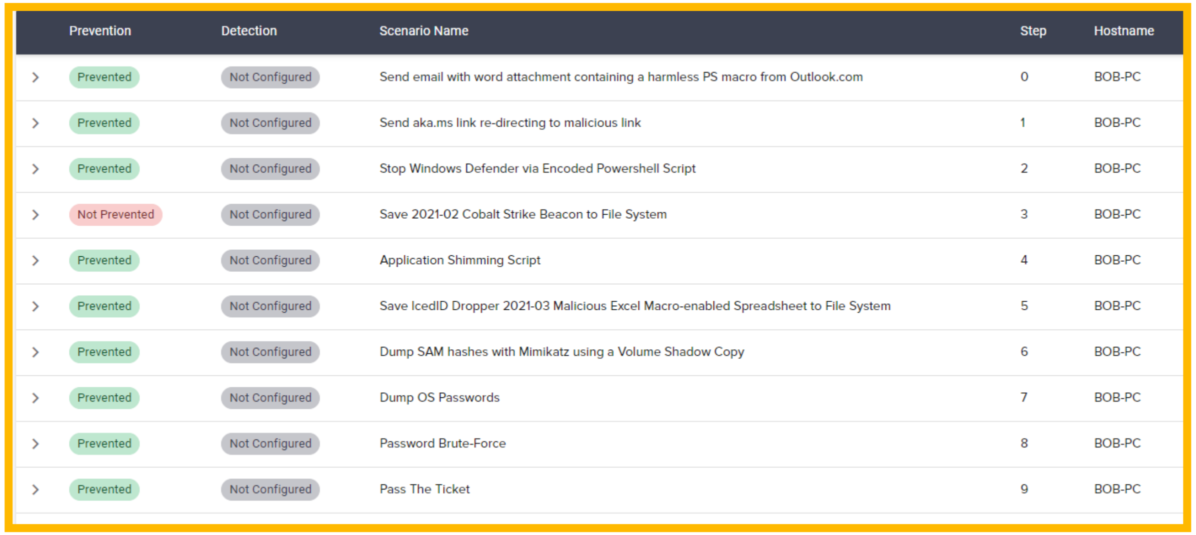
ACTIVITY DETAILS
MITIGATION RECOMMENDATIONS
DETECTION DETAILS
INDICATORS OF COMPROMISE (IOCS) DETAILS
EDR/EPP

User **Alice** results



Prevention	Detection	Scenario Name	Step	Hostname
Prevented	Not Configured	Send email with word attachment containing a harmless PS macro from Outlook.com	0	ALICE-PC
Not Prevented	Not Configured	Send aka.ms link re-directing to malicious link	1	ALICE-PC
Not Prevented	Not Configured	Stop Windows Defender via Encoded Powershell Script	2	ALICE-PC
Not Prevented	Not Configured	Save 2021-02 Cobalt Strike Beacon to File System	3	ALICE-PC
Not Prevented	Not Configured	Application Shimming Script	4	ALICE-PC
Not Prevented	Not Configured	Save IcedID Dropper 2021-03 Malicious Excel Macro-enabled Spreadsheet to File System	5	ALICE-PC
Not Prevented	Not Configured	Dump SAM hashes with Mimikatz using a Volume Shadow Copy	6	ALICE-PC
Not Prevented	Not Configured	Dump OS Passwords	7	ALICE-PC
Not Prevented	Not Configured	Password Brute-Force	8	ALICE-PC
Not Prevented	Not Configured	Pass The Ticket	9	ALICE-PC

User **Bob** results



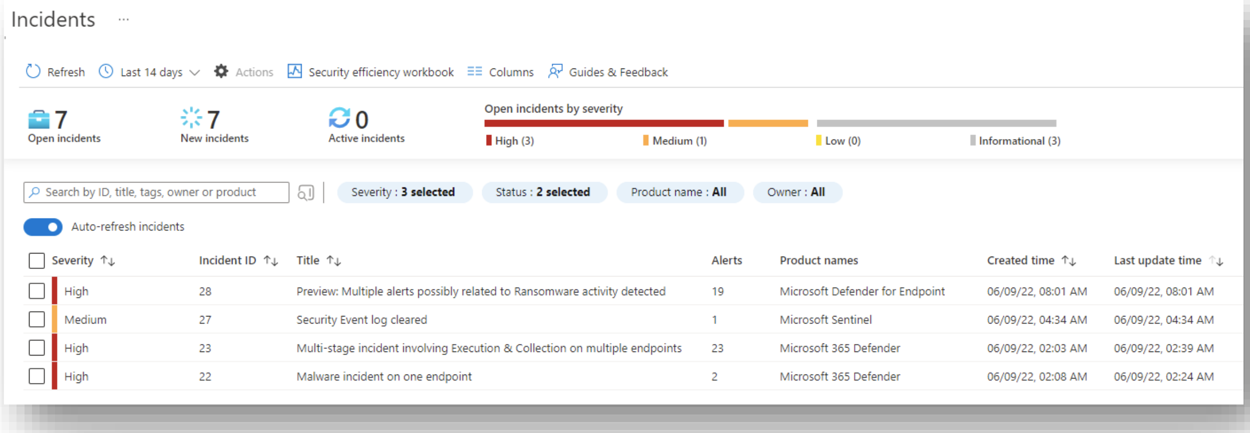
Prevention	Detection	Scenario Name	Step	Hostname
Prevented	Not Configured	Send email with word attachment containing a harmless PS macro from Outlook.com	0	BOB-PC
Prevented	Not Configured	Send aka.ms link re-directing to malicious link	1	BOB-PC
Prevented	Not Configured	Stop Windows Defender via Encoded Powershell Script	2	BOB-PC
Not Prevented	Not Configured	Save 2021-02 Cobalt Strike Beacon to File System	3	BOB-PC
Prevented	Not Configured	Application Shimming Script	4	BOB-PC
Prevented	Not Configured	Save IcedID Dropper 2021-03 Malicious Excel Macro-enabled Spreadsheet to File System	5	BOB-PC
Prevented	Not Configured	Dump SAM hashes with Mimikatz using a Volume Shadow Copy	6	BOB-PC
Prevented	Not Configured	Dump OS Passwords	7	BOB-PC
Prevented	Not Configured	Password Brute-Force	8	BOB-PC
Prevented	Not Configured	Pass The Ticket	9	BOB-PC

Exelegent

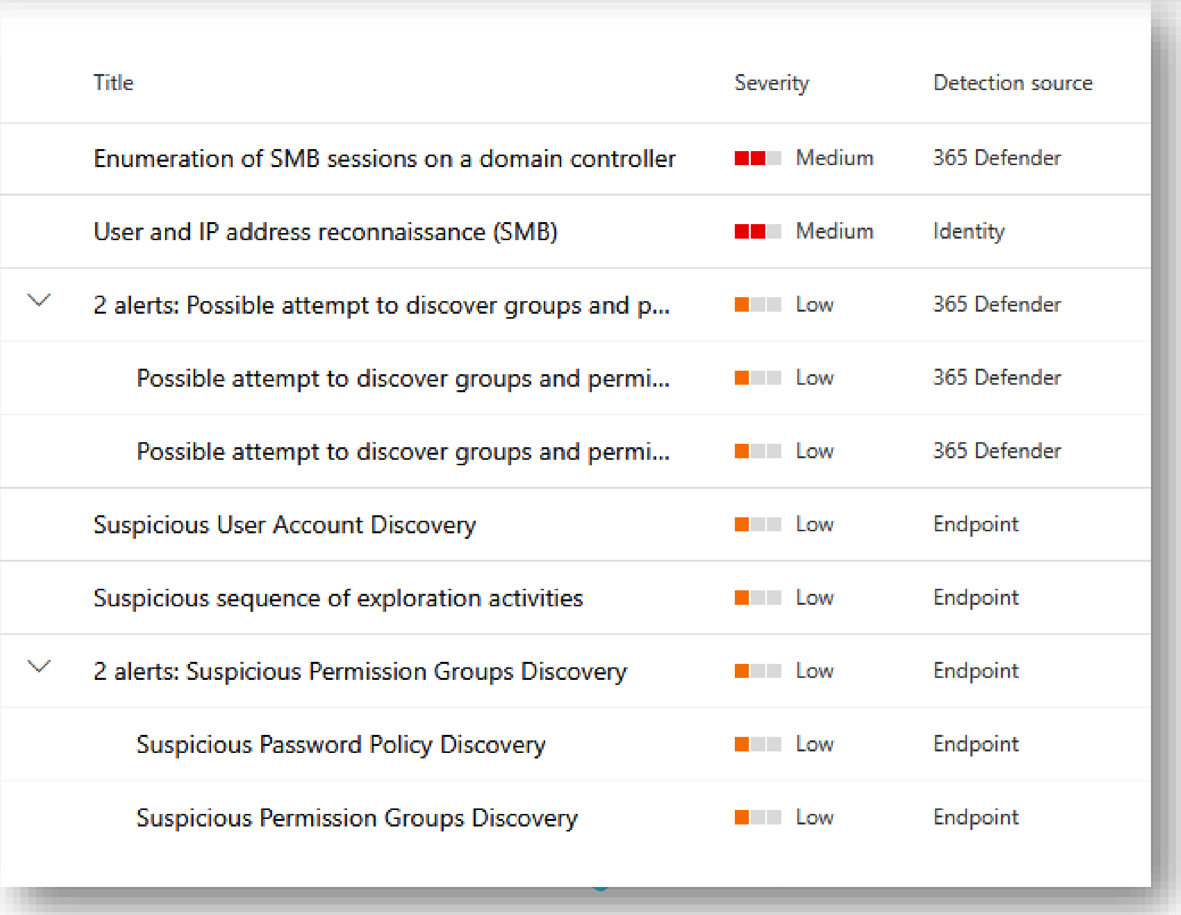
Threat Exploration findings

- Gain visibility into threats to cloud, on-premises environment obtained through Microsoft 365 security products in the Trial tena Trial

- Get recommendations from Microsoft experts on how to mitigate cyberattacks

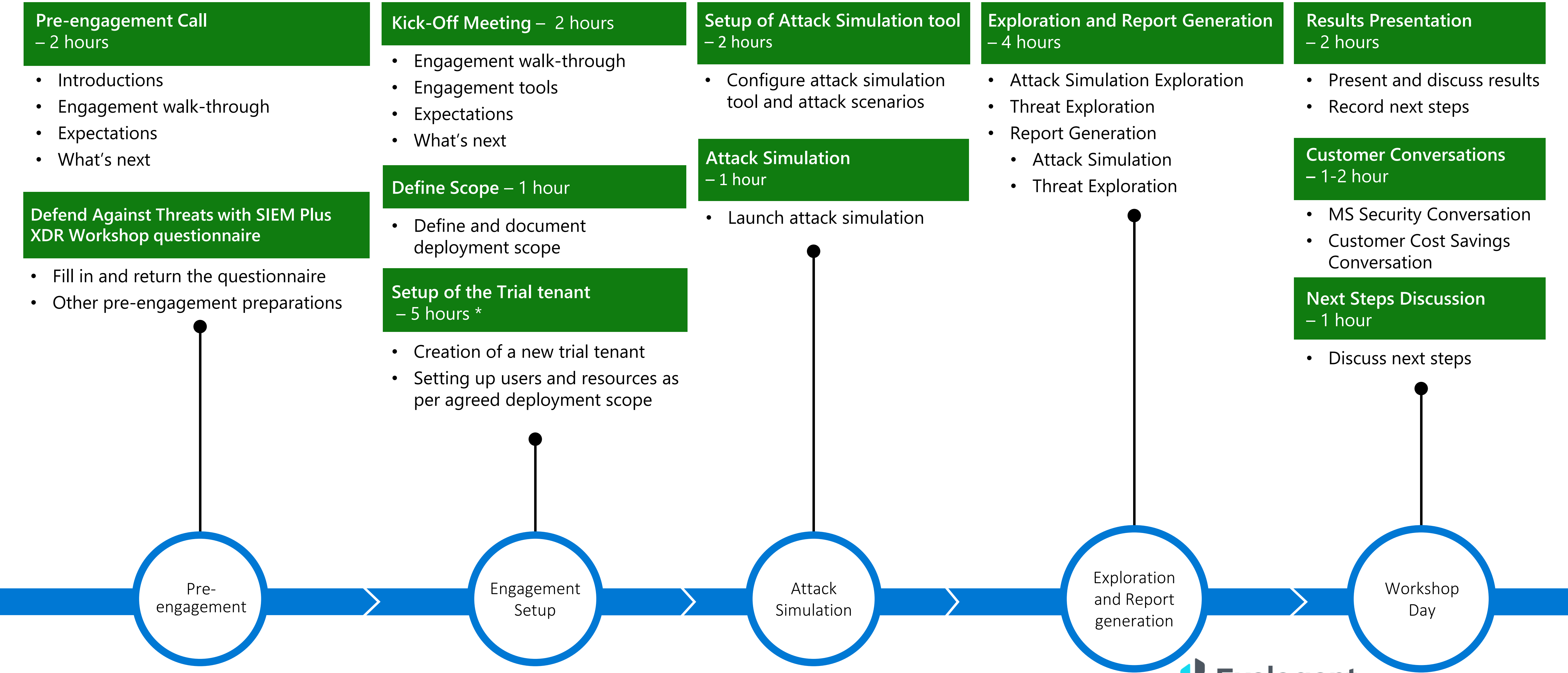


	Severity ↑↓	Incident ID ↑↓	Title ↑↓	Alerts	Product names	Created time ↑↓	Last update time ↑↓
□	High	28	Preview: Multiple alerts possibly related to Ransomware activity detected	19	Microsoft Defender for Endpoint	06/09/22, 08:01 AM	06/09/22, 08:01 AM
□	Medium	27	Security Event log cleared	1	Microsoft Sentinel	06/09/22, 04:34 AM	06/09/22, 04:34 AM
□	High	23	Multi-stage incident involving Execution & Collection on multiple endpoints	23	Microsoft 365 Defender	06/09/22, 02:03 AM	06/09/22, 02:39 AM
□	High	22	Malware incident on one endpoint	2	Microsoft 365 Defender	06/09/22, 02:08 AM	06/09/22, 02:24 AM



Title	Severity	Detection source
Enumeration of SMB sessions on a domain controller	Medium	365 Defender
User and IP address reconnaissance (SMB)	Medium	Identity
2 alerts: Possible attempt to discover groups and p...	Low	365 Defender
Possible attempt to discover groups and permi...	Low	365 Defender
Possible attempt to discover groups and permi...	Low	365 Defender
Suspicious User Account Discovery	Low	Endpoint
Suspicious sequence of exploration activities	Low	Endpoint
2 alerts: Suspicious Permission Groups Discovery	Low	Endpoint
Suspicious Password Policy Discovery	Low	Endpoint
Suspicious Permission Groups Discovery	Low	Endpoint

Defend Against Threats with SIEM Plus XDR Workshop (Attack Simulation) phases and activities



Pre-engagement Call – 2 hours

- Introductions
- Engagement walk-through
- Expectations
- What's next

Defend Against Threats with SIEM Plus XDR Workshop questionnaire

- Fill in and return the questionnaire
- Other pre-engagement preparations

Kick-Off Meeting – 2 hours

- Engagement walk-through
- Engagement tools
- Expectations
- What's next

Define Scope – 1 hour

- Define and document deployment scope

Setup of the Trial tenant – 5 hours *

- Creation of a new trial tenant
- Setting up users and resources as per agreed deployment scope

Setup of Attack Simulation tool – 2 hours

- Configure attack simulation tool and attack scenarios

Attack Simulation – 1 hour

- Launch attack simulation

Exploration and Report Generation – 4 hours

- Attack Simulation Exploration
- Threat Exploration
- Report Generation
  - Attack Simulation
  - Threat Exploration

Results Presentation – 2 hours

- Present and discuss results
- Record next steps

Customer Conversations – 1-2 hour

- MS Security Conversation
- Customer Cost Savings Conversation

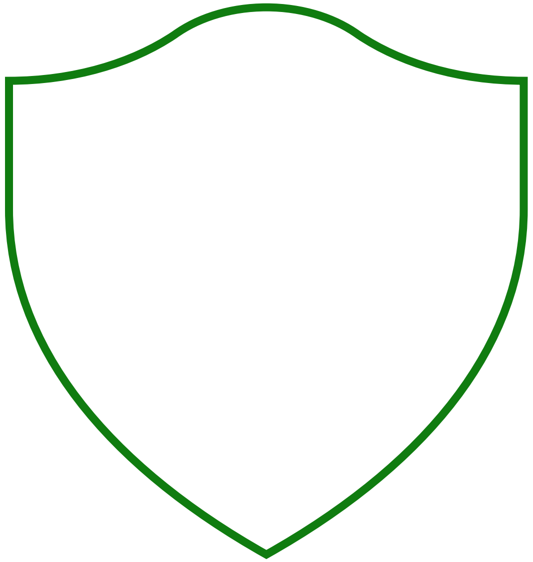
Next Steps Discussion – 1 hour

- Discuss next steps

* Effort depends on agreed scope

Appendix

Microsoft Security tools used in this engagement



What is Microsoft Sentinel?

Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Insights into threats

Get a birds-eye view across all data ingested and detect threats using Microsoft's analytics and threat intelligence. Investigate threats with artificial intelligence and hunt for suspicious activities.

In scope for this engagement.

Ability to automatically respond to detected threats

Out of scope for this engagement.

Requirements

Available to organizations with an Azure tenant.

Microsoft 365 Defender

What is Microsoft 365 Defender?

Unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

Detect threats and provide insights into them

In scope for this engagement.

Ability to prevent, investigate and respond to detected threats

Out of scope for this engagement.

Requirements

Available to organizations with Office 365 or Microsoft 365 enterprise, education or government subscriptions and with the tenant in the commercial (public) cloud or in any type of U.S. Government Community cloud.

Azure Active Directory Identity Protection

What is Azure Active Directory Identity Protection?

Identity threat detection system with proactive,
AI-enhanced automatic protection capabilities.

Insights into threats to identity

Detect threats to user’s identity such as compromised Azure Active Directory credentials or when someone other than the account owner is attempting to sign in using their identity.

In scope for this engagement.

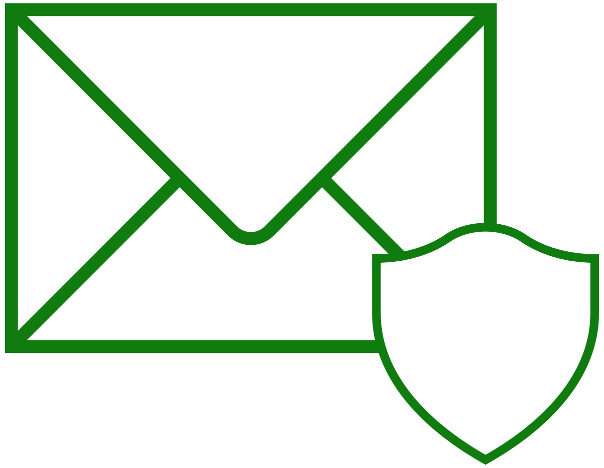
Ability to automatically respond to detected threats

In scope for this engagement.

Requirements

Available to organizations with Office 365 or Microsoft 365 enterprise, education or government subscriptions and with the tenant in the commercial (public) cloud or in any type of U.S. Government Community cloud.

Microsoft Defender for Office 365



What is Microsoft Defender for Office 365?

Detection and protection against sophisticated threats and ability to automatically investigate and remediate attacks against Office 365.

Insights into threats to email and data

Detect threats to email and data such as attempts of phishing and spreading of malware.

In scope for this engagement.

Ability to automatically respond to detected threats

In scope for this engagement.

Requirements

Available to organizations with Office 365 or Microsoft 365 enterprise, education or government subscriptions and with the tenant in the commercial (public) cloud or in any type of U.S. Government Community cloud.

Exelegent

Microsoft Defender for Cloud Apps

What is Microsoft Defender for Cloud Apps?

A multi-mode Cloud Access Security Broker.

Insights into threats to identity and data

Raise alerts on user or file behavior anomalies in cloud apps leveraging their API connectors.

In scope for this engagement (with Office 365 and Azure).

Discover the use of unsanctioned cloud application and services (aka “shadow IT”)

Out of scope for this engagement.

Ability to respond to detected threats, and configuration of application monitoring and control

Out of scope for this engagement.

Requirements

Available to organizations with Office 365 or Microsoft 365 enterprise, education or government subscriptions and with tenant in the commercial (public) cloud or in U.S. DoD or Government Community Cloud High (GCC High) clouds.

Microsoft Defender for Endpoint

What is Microsoft Defender for Endpoint?

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help organizations prevent, detect, investigate, and respond to advanced threats.

Insights into threats

Discover and analyze threats detected by Microsoft Defender for Endpoint. Learn how Microsoft Defender for Endpoint can reduce the volume of alerts using automatic investigation and remediation capabilities.

In scope for this engagement.

Discover endpoint weaknesses

Discover endpoint weaknesses and learn what can be done to harden the endpoint surface area.

Out of scope for this engagement.

Requirements

Available to organizations as a standalone offer (through a CSP partner) or as part of following enterprise or education subscriptions: Windows 10 Enterprise E5, Windows 10 Education A5, Microsoft 365 E5 (M365 E5), Microsoft 365 E5 Security and Microsoft 365 A5 (M365 A5).

Microsoft Defender for Identity

What is Microsoft Defender for Identity?

Microsoft Defender for Identity is a cloud-based security solution that leverages your Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Insights into threats

Discover and analyze threats detected by Microsoft Defender for Identity. Learn how Microsoft Defender for Identity can identify suspicious user activities and advanced attacks throughout the kill chain.

In scope for this engagement.

Discover Active Directory weaknesses

Discover Active Directory weaknesses and learn what can be done to harden its surface area.

Out of scope for this engagement.

Requirements

Available to organizations as a standalone Microsoft Defender for Identity offer or as part of following enterprise or education subscriptions: Microsoft 365 E5 or A5, Microsoft 365 E5 Security or A5 Security, Enterprise Mobility+Security E5 or A5.