Defend Against Threats with SIEM Plus XDR

HPT Vietnam Corporation

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.

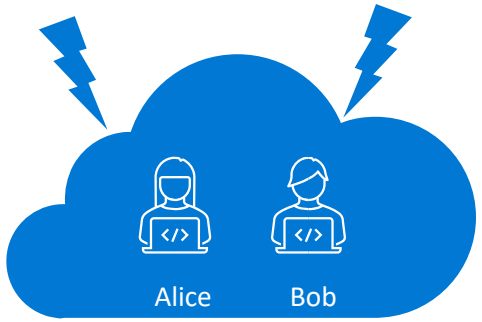
Plan next steps on how we can work together to improve your security posture.

hpt knowing IT

Engagement Setup

Tenants: Production vs.Trial

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



Contoso123456.onmicrosoft.com

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

hpt knowing IT

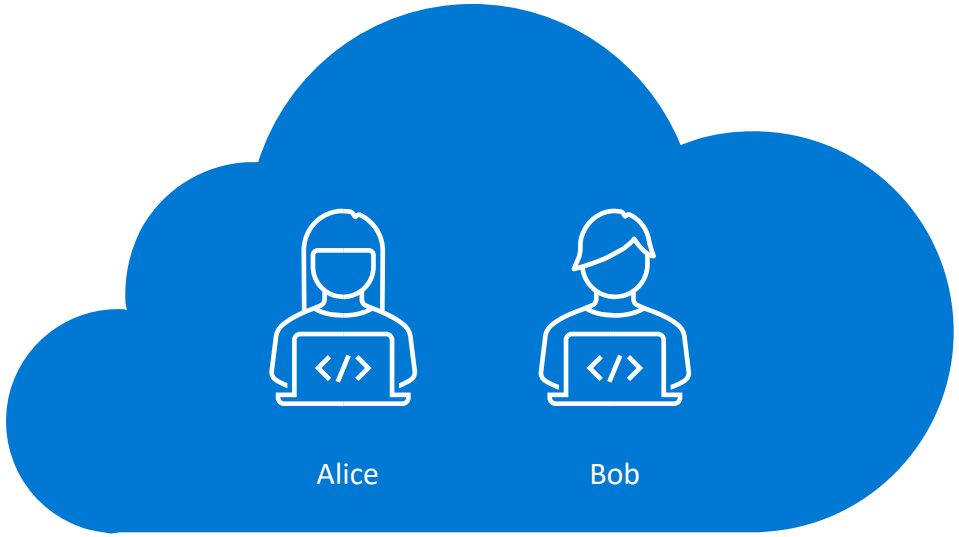
The Trial tenant

General characteristics

The tenant is meant to represent customer's Production environment.

Standard setup as per description below.

Custom setup agreed during the engagement.



Contoso123456.onmicrosoft.com

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

hpt knowing IT

Microsoft Security tools

Microsoft Security tools

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

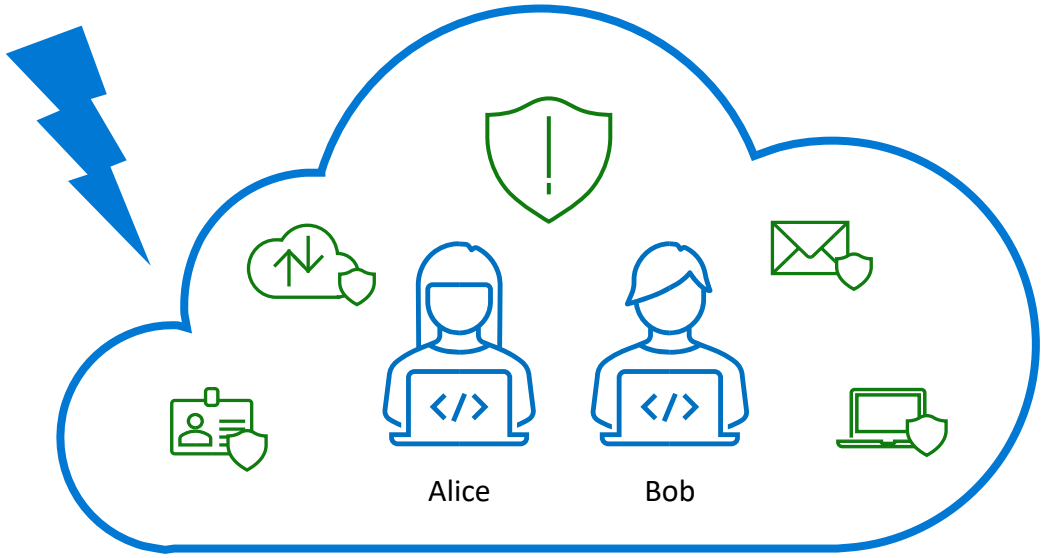
- Microsoft Sentinel and Microsoft 365 Defender to understand the correlation between threats.
- Azure Active Directory Identity Protection, Microsoft Defender for Cloud Apps and Microsoft Defender for Identity to understand threats to identity.
- Microsoft Defender for Office 365 and Microsoft Defender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

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



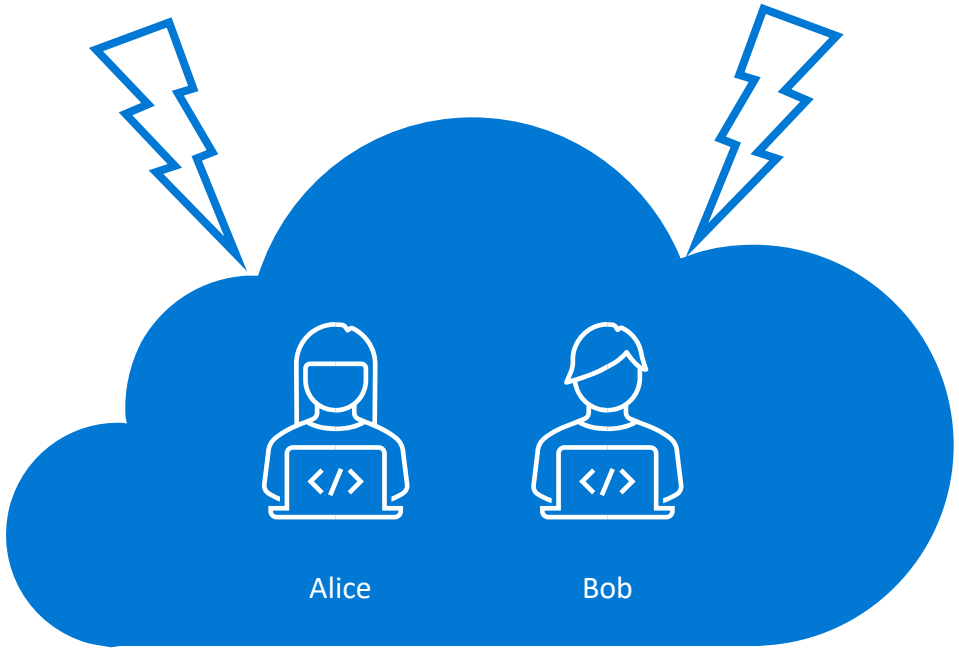
Contoso123456.onmicrosoft.com

Attack Simulation

Use automatically generated, simulated attacks to assess your security posture.
Setup of Attack Simulation Tool
Attack Simulation

Attack Simulation & Threat Exploration

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



Contoso123456.onmicrosoft.com

hpt knowing IT