# Defend Against Threats with SIEM Plus XDR

Learn how to put next-generation Microsoft security tools to work for you.

## Description

Like most businesses, you're probably under constant attack by cyber-criminals. And if terms like SIEM, MDR, SOC, or XDR leave you in a bit of a head spin and you don't know where to begin or how to how to best prioritise your efforts, then this workshop will help set you on the right path.

In a world with ever-growing volume of data and alerts, shrinking IT budgets, and the need to protect vulnerable legacy systems, Fusion5 can help you to achieve your broader security objectives—and identify current and real threats—with the Defend Against Threats with SIEM Plus XDR Workshop:

- Review your security goals and objectives
- Identify real threats in your cloud environment with Threat Check
- Map identified threats to specific solution recommendations
- Showcase security scenarios with interactive product demos
- Develop joint plans and next steps

During this workshop, we'll work with you on strengthening your organisation's approach to cyber security. We'll help you better understand how to prioritise and mitigate potential attacks, with:

- Deep analysis of cyber-attack threats that are targeting your organisation
- Actionable recommendations to help immediately mitigate the identified threats
- A detailed assessment of your IT and security priorities and initiatives, direct from cyber security professionals
- An inside look at Microsoft's holistic approach to security, and how it relates to your organisation
- Demonstrations of integrated security, including the latest tools and methods
- Long-term recommendations from Microsoft experts about your security strategy, with key initiatives and tactical next steps

The products that we'll be working with you on include:

- Microsoft Sentinel
- Microsoft 365 Defender
- Azure Active Directory Identity Protection
- Microsoft Defender for Office 365
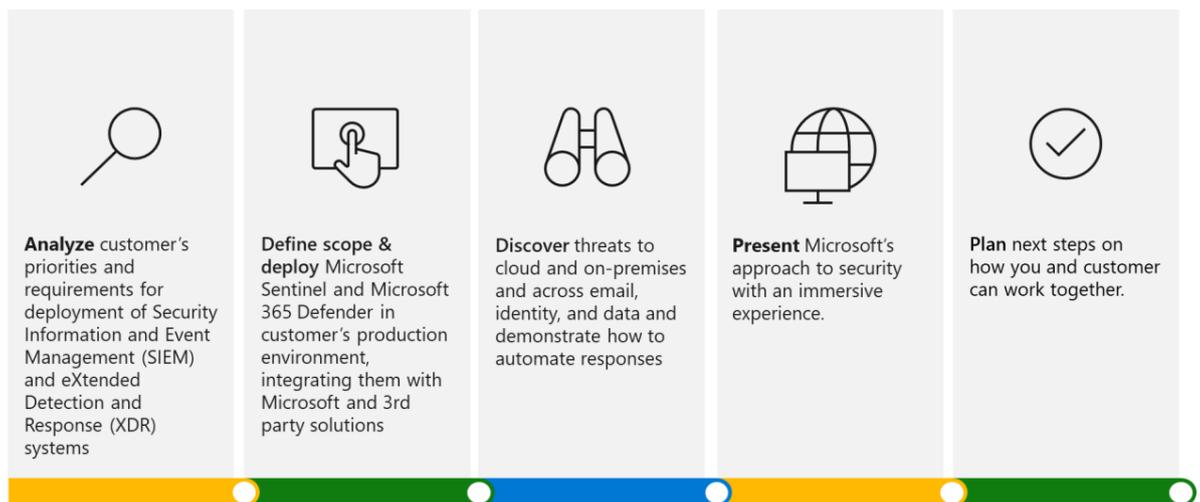- Microsoft Defender for Cloud Apps

Trial licenses and trial Azure credit may be available from Microsoft for organisations not yet licensed.

# Duration

The workshop is delivered over 5-weeks. The workshop is performed over this period of time to allow for data to be collected in the environment. At a high-level, the activities for the workshop can be grouped into the following phases:

- Week 1 – Pre-engagement
- Weeks 1-2 – Readiness
- Week 2 – Engagement Setup
- Weeks 2-4 – Data Collection
- Weeks 5 – Exploration and Report Generation, Workshop Day, and Engagement Decommissioning

## What is expected during workshop delivery

**Analyze** customer's priorities and requirements for deployment of Security Information and Event Management (SIEM) and eXtended Detection and Response (XDR) systems

**Define scope & deploy** Microsoft Sentinel and Microsoft 365 Defender in customer's production environment, integrating them with Microsoft and 3rd party solutions

**Discover** threats to cloud and on-premises and across email, identity, and data and demonstrate how to automate responses

**Present** Microsoft's approach to security with an immersive experience.

**Plan** next steps on how you and customer can work together.

## Approach

### Analyze
- Business and IT requirements
- Existing SIEM/SOC tools
- Data sources to be connected
- Security Operations automation requirements

### Define scope & deploy
- Define the scope of the Microsoft Sentinel deployment
- Deploy and configure Microsoft Sentinel
- Connect Microsoft Sentinel to ingest data from:
  - Office 365 & Azure
  - Azure AD Identity Protection
  - Microsoft 365 Defender
    - Microsoft Defender for Office 365
    - Microsoft Defender for Identity
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender for Endpoint
  - Agreed 3rd party Syslog integration (firewalls, proxy servers)
  - Limited number of servers

### Discover
- Use Microsoft Sentinel to analyze and discover threats to customer's organization
- **Optional -** Use Microsoft Sentinel to proactively hunt for security threats across all ingested data

### Recommend
- Map found threats to Microsoft 365 security products
- Provide a Microsoft Sentinel deployment roadmap