
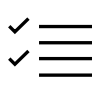



# Defend Against Threats with SIEM Plus XDR Workshop


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


## Workshop highlights

 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 product demos

 Develop joint plans and next steps

Do you know how many phishing attacks your organization has received? If employees are using the right password protocol? Whether personal data is being exposed? In short, is your organization's cloud environment as secure as you think it is?

## Improve your security posture with a Defend Against Threats with SIEM Plus XDR Workshop

Organizations today are managing a growing volume of data and alerts while dealing with tight budgets and vulnerable legacy systems. Get help achieving your broader security objectives—and identify current and real threats—by scheduling a Defend Against Threats with SIEM Plus XDR Workshop.

We can help you develop a strategic plan customized for your organization and based on the recommendations of Microsoft experts in security. You'll gain visibility into immediate threats across email, identity, and data, plus clarity and support on how to upgrade your security posture for the long term.



## Why you should attend

Given the volume and complexity of identities, data, applications, devices, and infrastructure, it's essential to learn how secure your organization is right now, and how to mitigate and protect against threats moving forward. By attending this workshop, you can:

Identify current, ongoing security threats in your cloud environment

Walk away with actionable next steps based on your specific needs and objectives

Document your security strategy for the benefit of key stakeholders

Better understand how to accelerate your security journey using the latest tools

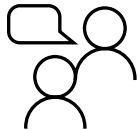
## What to expect:

During this-workshop, we'll partner with you to strengthen your organization's approach to cybersecurity. We'll help you better understand how to prioritize and mitigate potential attacks, with:

- Deep analysis of cyberattack threats that are found targeting your organization
- Actionable recommendations to help immediately mitigate the identified threats
- A detailed assessment of your IT and security priorities and initiatives, direct from cybersecurity pros
- An inside look at Microsoft's holistic approach to security, and how it relates to your organization
- 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



Pre-Engagement  
Call



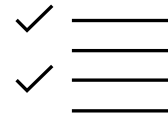
Kick-off  
Meeting



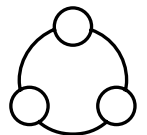
Cloud  
Discovery Log  
Collection



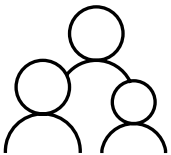
Threat  
Exploration



Threat Results  
Presentation



Engagement  
Decommissioning



## Who should attend

The workshop is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Data Protection Officer
- Data Governance Officer
- IT Security, IT Compliance, and/or IT Operations
- Data Governance

## Why Red Canary?

Red Canary MXDR provides 24x7 security expertise across your critical Microsoft workloads. Our [Microsoft Verified MXDR solution](#) helps you detect and respond to more threats, faster. We start by taking raw telemetry and alerts from your Microsoft security tools--Microsoft 365 Defender and its component products, Microsoft Sentinel, Microsoft Defender for Cloud, and more. When we detect a threat, we help you respond, recover, and improve so that you can get back to business as usual.



Contact us today to get started!

Red Canary | [microsoft@redcanary.com](mailto:microsoft@redcanary.com) | 1601 19th St Suite 900, Denver, CO 80202 | [redcanary.com](http://redcanary.com)