Microsoft training guide

For SIEM and XDR

Microsoft captured

8x

more threat signals in 2023 than in 2021.[1]

As the digital landscape grows larger and more complex, the corresponding threat landscape becomes increasingly sophisticated and more diverse.

Microsoft solutions synthesize **65 trillion signals a day** across all types of devices, apps, platforms, and endpoints.[1]

This guide points to curated training and documentation resources on Microsoft Defender and Microsoft Sentinel to help your organization meet the evolving threat landscape head on.

Get training and information on key Microsoft solutions for security operations so you can:

Protect endpoints from ransomware

Microsoft Defender for Endpoint

Secure collaboration and prevent phishing

Microsoft 365 Defender
Microsoft Defender for Office

Optimize the Security Operations Center

Microsoft Sentinel

Microsoft Security

[1] Microsoft Security Blog. Microsoft Security reaches another milestone—Comprehensive, customer-centric solutions drive results. January 2023.

Protect endpoints from ransomware

Don’t just react to threats; understand how to get ahead of them. Ransomware evolves quickly and is constantly growing more sophisticated, from out-of-the-box malware deployments to elaborate attacks executed by skilled cybercriminals.

As endpoints within an organization become more diverse, securing them is more critical. Adopt a unified security approach and reduce the need for various 3rd-party point solutions with a single, cloud-powered solution, Microsoft Defender for Endpoint.

Explore these key training resources and ensure your endpoints are protected.

Onboard and enable customer devices into Microsoft Defender for Endpoint.

Start training

Mature threat and vulnerability management with a focus on inventory and assessment usage.

Start training

Improve protection and response time when detecting threats to endpoint devices.

Start training

Microsoft Security

Secure collaboration and prevent phishing

Stopping attacks before they happen is the easiest way to stay secure. Detect malicious and suspicious content and correlate attack patterns to identify campaigns designed to evade protection.

Defender for Office 365 protects across the kill chain, providing prevention and detection capabilities backed by detailed reporting and automated investigation and response—a complete solution across your collaboration tools.

Combined with Microsoft 365 Defender, the deep integration between each solution will help stop cross-domain attacks spanning email, collaboration tools, endpoints, identities, and cloud apps.

Explore these key training resources and ensure your endpoints are protected.

Improve protection and reduce response times when detecting threats in customer collaboration workloads (Exchange Online, Microsoft Teams, Office).

Start training

Prevent threats from occurring with configuration management improvements.

Start training

Protect the digital estate with attack simulation training.

Start training

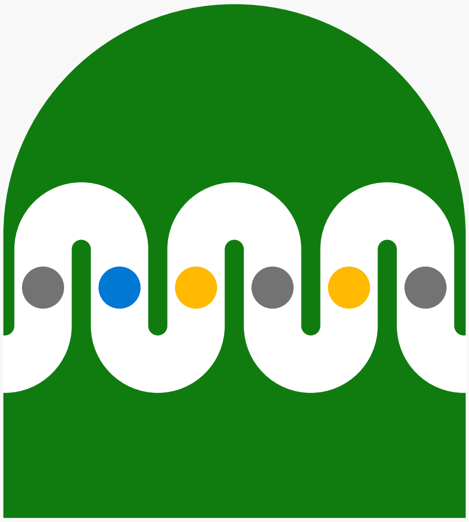
Address malicious emails delivered in Office 365 or identify and respond to compromised email accounts.

Start training

Microsoft Security

Optimize the Security Operations Center

The need to stay ahead of attackers is never-ending and requires operational efficiencies to scale and detect the evolving threats. Find and stop sophisticated cross-domain attacks within your organization and protect your workloads with intelligent security analytics.



Microsoft Sentinel is your cloud-native SIEM solution that brings together data, analytics, and workflows to unify and accelerate threat detection and response across your entire digital estate.

Explore these key training resources and ensure your organization is effectively defending against threats.

- Monitor Microsoft Sentinel health with queries and visualize security data using Microsoft Sentinel workbooks.

  Start training

- Investigate and manage security incidents with case management in Microsoft Sentinel.

  Start training

- Orchestrate Microsoft 365 Defender integration and 3rd-party logs into Microsoft Sentinel.

  Start training

- Utilize notebooks to perform analytics, create data visualizations, and integrate data sources outside of Microsoft Sentinel.

  Start training

- Parse and filter security threats across organizational data to advance threat hunting.

  Start training

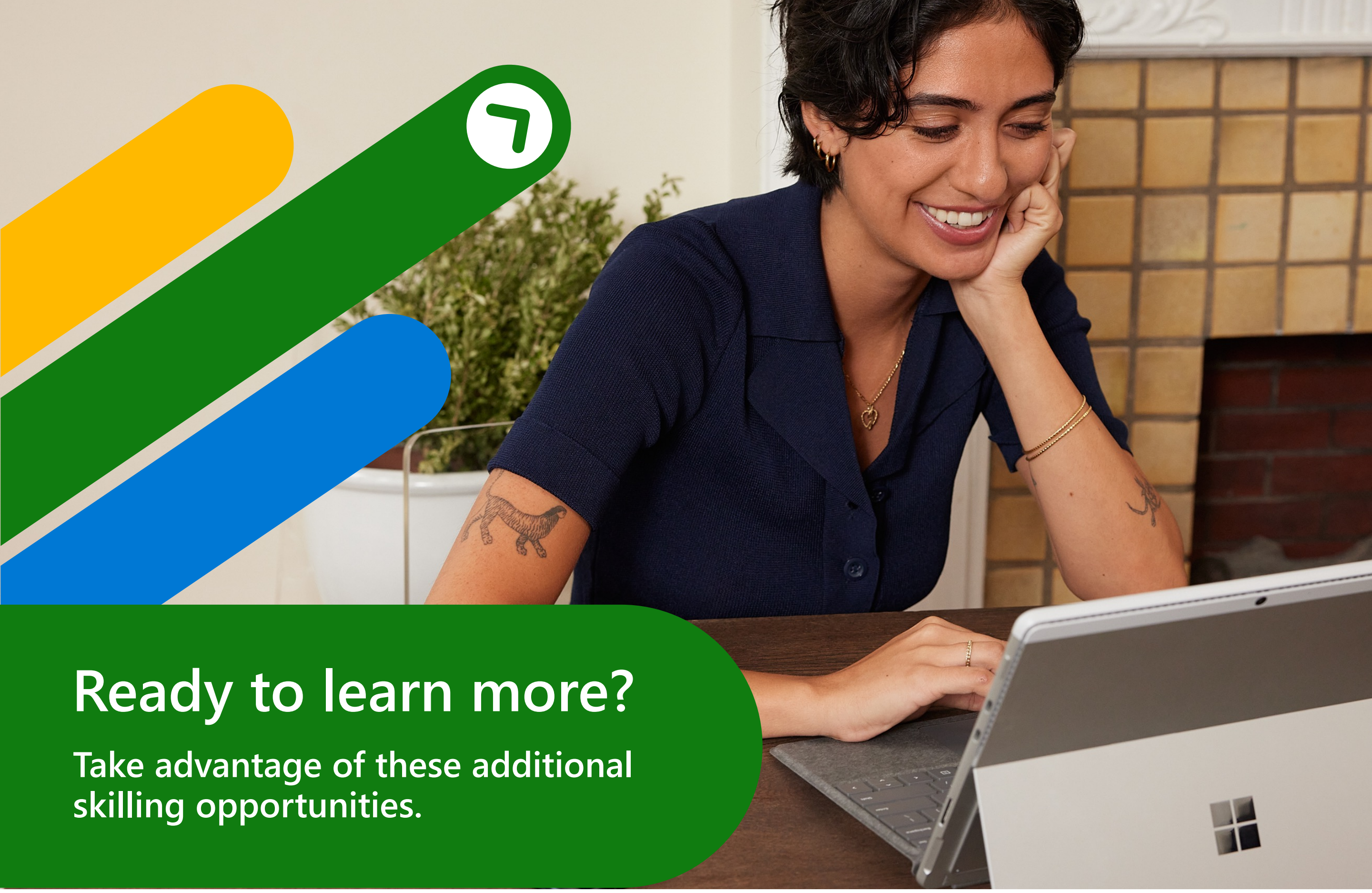
- Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft Sentinel.

  Start training

- Install a content hub and connect a GitHub repository in Microsoft Sentinel.

  Start training

Microsoft Security



Ready to learn more?

Take advantage of these additional skilling opportunities.

Microsoft Security Certification

Grow in your role

[Microsoft Certified: Security Operations Analyst Associate]

Ideally suited for security operations professionals who design their threat protection and response systems.

Self-guided training

Grow your knowledge and advance at your own pace

Microsoft Security: Beginner

Microsoft Security: Intermediate

Microsoft Security: Advanced

Microsoft Security

Maximize the capabilities of Microsoft Defender for Endpoint and Microsoft Defender for Office 365. Explore our solution feature guides and realize the potential of your investment.

Microsoft Defender for Endpoint solution feature guide

Microsoft Defender for Office 365 solution feature guide

Microsoft Documentation

Microsoft Defender for Office 365 Documentation

Microsoft Defender for Endpoint Documentation

Microsoft Sentinel Documentation

Join other security professionals in the online Microsoft Tech community.

Participate in discussions, explore additional trainings, and continue your skilling journey.