Microsoft

Who Hacked?
Preparation guide for attendees

Microsoft Learn Cloud Games

Join Microsoft Learn Cloud Games, and collaborate with other technical professionals to role-play your way through real-world tech problems. Implement solutions with Microsoft technologies in this hands-on, multiplayer learning game that offers a fun, risk-free, simulated environment where you can apply what you know and add to your technical skills, knowledge, and experience.

Who Hacked?

Who Hacked? is a game in which you are a detective, gathering clues and evidence to investigate, remediate, and protect against cybersecurity incidents at Best for You Organics (BFYO), one of the largest organic produce e-retailers in the nation.

For a preview, **watch this short video**.

To play the game, you select one of three IT specialist roles at BFYO—cybersecurity, compliance, or identity.

The game has related episodes with multiple challenges that can be played in any order, including:

- **"Keeping up Appearances,"** which tackles a ransomware attack.
- **"In the Cross Hairs,"** which brings suspicious web shell activity.

To make the most of the experience, you:

- Currently work in any or all of the following fields: security, compliance, or identity.
- Have foundational knowledge and experience with cybersecurity basics (**Course SC-900T00: Microsoft Security, Compliance, and Identity Fundamentals**).
- Are familiar with Microsoft Sentinel and Microsoft Defender.
- Have knowledge of identity and access in Microsoft Azure.

"Keeping up Appearances"

The Chief Privacy Officer (CPO) receives a ransom email on the morning that Best for You Organics (BFYO) plans to roll out its new European Union website.

The Chief Executive Officer (CEO) has locked down the C-suite in the boardroom to try to contain news of the breach until BFYO's security team can mitigate the situation. Given just a file name and an account, your job is to follow the forensics clues using Microsoft security, compliance, and identity solutions to find the culprit. Then you need to protect BFYO from future attacks while continuing to build incident response plans.

In the episode, you and your colleagues learn to use Microsoft Sentinel and Microsoft 365 Defender to investigate a breach. And you learn to use Azure Active Directory (Azure AD) to perform identity forensics and protection. Plus, you discover that compliance is not just for data loss prevention (DLP)—you also use the compliance tools to analyze documents and Microsoft Teams communications.

Prerequisites

- Experience working with Azure Cloud Services, like Azure AD Identity Protection
- Experience with Microsoft Sentinel investigation and remediation techniques
- Experience with the Microsoft 365 compliance center
- Knowledge of Microsoft Endpoint Manager

Learning outcomes

In this episode, you practice the following skills. To refresh your knowledge before or after the event, check out the recommended learning paths.

Area	Skills practiced	Recommended learning paths
Security	Build KQL queries	SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

Area	Skills practiced	Recommended learning paths
	Investigate devices with Microsoft Defender for Endpoint	Perform device investigations in Microsoft Defender for Endpoint
	Perform remote access on a device to collect forensics information, and investigate devices with Microsoft Defender for Endpoint	Perform actions on a device using Microsoft Defender for Endpoint
	Protect devices by configuring attack surface reduction rules	Microsoft Endpoint Manager fundamentals
Compliance	Use the Microsoft 365 compliance center Content search tool to investigate a file	Search for content in the Microsoft 365 compliance center
	Configure insider risk policies	Manage insider risk in Microsoft 365
	Configure data loss prevention (DLP) policies	Prevent data loss in Microsoft 365
	Search Teams chat messages	Search for content in the Microsoft 365 compliance center
Identity	Investigate identities in Azure AD Identity Protection, and configure Azure AD Identity Protection policies	Protect your identities with Azure AD Identity Protection
	Review Azure AD sign-in logs	Find activity reports in the Azure portal

"In the Cross Hairs"

After successfully expanding into the European Union, Best for You Organics (BFYO) is approached by a journalist who is writing a piece on the company. Chief Executive Officer (CEO) Abigail Jackson invites her to come to headquarters, get to know the team, and interview Chief Information Officer (CIO) Andrea Divkovic. But the morning of the interview, BFYO receives a high-priority cybersecurity alert. You and the team must work quickly but circumspectly to resolve the issue without drawing the attention of the inquisitive and ever-present reporter.

In this episode, with the alert from Microsoft Defender for App Service in Microsoft Defender for Cloud, you and your colleagues follow the trail to uncover whose data has been compromised, to what extent, and how it happened. You learn to identify, investigate, and protect against identity-based attacks on Azure services. And you use Microsoft Sentinel to enable identity attack detections. Plus, you work with the Microsoft 365 compliance center Content search tool to investigate user activity and you implement Microsoft Defender for Cloud Apps, as you discover the source of the cybersecurity alert and determine how to remediate the situation.

Prerequisites

- Experience working with Microsoft Defender for Identity and Azure Active Directory (Azure AD) Identity Protection
- Experience with Microsoft Sentinel investigation and remediation techniques
- Knowledge of Microsoft Defender for Cloud Apps
- Knowledge of Microsoft 365 content search capabilities

Learning outcomes

In this episode, you practice the following skills. To refresh your knowledge before or after the event, check out the recommended learning paths.

Area	Skills practiced	Recommended learning paths
Security	Manage alerts in Microsoft Defender for Cloud	Remediate security alerts using Microsoft Defender for Cloud
	Enable detection rules in Microsoft Sentinel	Threat detection with Microsoft Sentinel analytics
	Manage organization settings	Configure how users consent to applications
	Search with Azure Monitor	Azure Monitor overview
Compliance	Implement access controls for cloud apps	Secure your cloud apps and services with Microsoft Defender for Cloud Apps
	Search Teams chat messages	Search for content in the Microsoft 365 compliance center
Identity	Search with Azure Monitor	Azure Monitor overview
	Understand Azure role permissions	Azure RBAC documentation

Area	Skills practiced	Recommended learning paths
	Build KQL queries	SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
	Assign Azure roles	Implement app registration
	Implement Conditional Access	Plan, implement, and administer Conditional Access

