**OpenHack – Security, Compliance, and Identity**

Overview

**This OpenHack enables participants to** establish and defend baseline security and compliance configurations for organizations using Microsoft cloud services. This will be done with Microsoft Security and Compliance tools and recommended security best-practices by working through challenges inspired from real-world scenarios.

**During the “hacking” participants will focus on** analyzing and remediating security configurations in a pre-configured Microsoft online organization. Additionally, participants will implement security and compliance policies to enforce regulations required by the company and mitigate any threats discovered during the assessment.

**By the end of the OpenHack**, participants will have gained the knowledge on how to better protect an organization that uses hybrid cloud organizations leveraging SaaS, IaaS and PaaS solutions. Participants will also gain experience creating policies and procedures to meet the compliance needs of an organization. …(to what level/degree?)

Technologies

[Microsoft Defender for Office 365](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide), [Compliance Manager](https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide), [Microsoft 365 Defender](https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-threat-protection?view=o365-worldwide), [Microsoft Secure Score](https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-secure-score?view=o365-worldwide), [Secure score in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls), [Azure Regulator compliance](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/regulatory-compliance), [Azure Defender](https://docs.microsoft.com/en-us/azure/security-center/azure-defender), [Azure policy](https://docs.microsoft.com/en-us/azure/governance/policy/overview), [Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/policy-reference), [Azure Identity protection](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/), [Microsoft Cloud App Security](https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security), [Microsoft Defender for Identity](https://docs.microsoft.com/en-us/defender-for-identity/), [Data loss prevention](https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide), [Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/overview)

Prerequisites

**Knowledge Prerequisites**

To be successful and get the most out of this OpenHack, it is highly recommended that participants have previous experience with:

* Azure Active Directory
* Microsoft 365 Security and Compliance
* Azure Security Center

Required knowledge of [Azure fundamentals](https://docs.microsoft.com/en-us/learn/paths/az-900-describe-cloud-concepts/).

**Tooling Prerequisites**

To avoid any delays with downloading or installing tooling, have the following ready to go ahead of the OpenHack:

* A modern laptop running Windows 10 (1703 or higher), Mac OS X (10.13 or higher), or one of [these Ubuntu versions](https://github.com/Azure/azure-functions-core-tools#linux)

**Links & Resources**

Review the following links and resources:

* [How to organize your security team: The evolution of cybersecurity roles and responsibilities](https://www.microsoft.com/security/blog/2020/08/06/organize-security-team-evolution-cybersecurity-roles-responsibilities/)
* [Threat Modeling](https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling)
* [Microsoft security blog](https://www.microsoft.com/security/blog/2021/03/02/4-ways-microsoft-is-delivering-security-for-all-in-a-zero-trust-world/)
* [Security, Compliance & Identity](https://www.microsoft.com/en-us/security/content-library/)

**Post Learning Recommendations**

* [Security Engineer](https://docs.microsoft.com/en-us/learn/certifications/roles/security-engineer)
* [Microsoft Certified: Security, Compliance, and Identity Fundamentals](https://docs.microsoft.com/en-us/learn/certifications/security-compliance-and-identity-fundamentals/)
* [Demonstrate fundamental knowledge of Microsoft 365 security and compliance capabilities](https://docs.microsoft.com/en-us/learn/paths/m365-security-compliance-capabilities/)

Challenges

**Overview:**

Contoso Mortgage is a mortgage company that has grown organically and through the acquisition of other lenders and loan-servicing organizations. Recently, Contoso Mortgage completed their migration from their on-premises datacenter to Microsoft Azure and has fully embraced the cloud with their messaging, identity, communications, and collaboration in Microsoft 365 leaving a minimal on-premises infrastructure.

Public cloud computing is still a new concept to Contoso Mortgage's security teams. The new CIO has determined that the company’s growth and recent move to the cloud requires a retune to modernize its security and compliance foundation. The CIO has tasked the chief information security officer (CISO) with assembling their teams and ensuring they are ready to protect the organization’s online systems and processes. It has been decided that, unless otherwise recommended by the security teams, the organization will use tools native to the services they currently subscribe to.

To begin the process of making the cloud environment more secure, a security audit will be performed that will identify vulnerabilities and make recommendations on way to minimize those vulnerabilities. The team needs to assess the impact of high priority items found and remediate the findings. [Challenge 1] The CISO’s teams have been tasked with identifying the tools they have in their service offering to report and implement security and compliance policies as well as their identity management. [Challenge 2,3]

Along with the security and compliance improvements, the company needs to leverage policies for both their SaaS applications and IaaS infrastructure to protect data from loss and to ensure resources are deployed to the right place in the correct configuration. Additionally, the company wants to ensure remote access to resources is controlled. [Challenge 4,5,6]

The teams are expected to be able to use threat protection tools to defend, if necessary, the organization from current and potential threats. Using these tools and reports as well as configuring a security information and event management is essential to the company. [Challenge 7,8,9]

**Business drivers for this effort include:**

* Increasing cloud security across the organization.
* Limiting user impact.
* Ensure the application of changes is understood and communicated.
* Consider if changes will impact the company’s employees and what additional awareness or training may be needed.
* Increasing security and compliance posture. Regulatory compliance is important to ensure the company and customers are protected.

**IT leadership's goals for this effort include:**

* Ensuring the teams work with modern tools and know where to focus security and compliance efforts to be efficient. [Challenge 1]
* Remediate all identified security and compliance vulnerabilities. [Challenge 2,3]
* Safeguard the organization’s intellectual property and assets. [Challenge 4]
* Deploy and enforce identity access management. [Challenge 5]
* Assure cloud policies align with corporate security requirements. [Challenge 6]
* Establish monitoring and alerting and implement protection of newly identified threats. [Challenge 7,8]

**Challenge 1 – What’s in the toolbox**

In this challenge your team will collect a list of resources found in Microsoft Azure and Microsoft 365 that your team can use to assist in the discovery of security and compliance risks. In addition to resources that identify risk, you must also collect a list of methods that are used to implement and affect policy implementation.

Your team will present a list of resources and methods to the CISO and be able to describe how each can be used to protect or manage the organization’s security and compliance requirements.

Learning objectives:

* Identify and describe built-in Microsoft tools for analyzing the organizations security and compliance posture.
* Identify tools or locations used to implement security and compliance improvements.

**Challenge 2 – Make it better**

Now that your team has identified many of the different tools you have for reporting security improvements and places where you can go to implement those improvements, your CISO has work the team need to get done.

In this challenge your team will identify the first 10-15 improvement actions found in your company’s Microsoft 365 secure score and work together to address them.

The CIO has directed that user accounts will not be required to use any additional authentication mechanisms, but they are planned. Also, no additional risk policies will be enabled either because they are also planned for later project.

Learning objectives:

* Use native Microsoft 365 and Azure tools to report on the current security posture.
* Complete 10-12 improvement actions identified in the report.
* Implement business requirements related to SaaS that will enhance security.

**Challenge 3 – Regulators, mount-up**

In the first challenge, your team identified tools the organization can use to support the improvement and implementation of its regulatory and compliance goals in addition to security and identity protections.

During this challenge, your team will work with Compliance Manager assessments, create assessments using available assessment templates and use identified improvement actions to help align the company with regulatory requirements.

Learning objectives:

* Use the Microsoft 365 compliance manager and identify compliance risk.
* Use regulatory compliance templates to identify recommended remediations and apply controls.

**Challenge 4: Treat our data right**

So far, you’re team has been able to address some of the security and compliance concerns and implemented improvements to increase Contoso Mortgage’s protective posture.

The CIO is concerned about customer data not being properly handled and being exfiltrated from the organization, both intentionally and unintentionally. This data is composed of PII, bank account information, and credit card information.

Your team must implement measures designed to protect the company's data and mark it in accordance with company policy.

Learning objectives:

* Implement data loss prevention policies.
* Automatically protect sensitive items using labels.
* Create notifications about risky behavior.

**Challenge 5: It’s me, I can prove it**

Contoso Mortgage has already taken steps to protect privileged access by adding multi-factor authentication (MFA) to administrator accounts. The CISO needs that additional level of security extended to all Contoso Mortgage user accounts. The intent is to have all accounts MFA enabled, but each user will be treated differently during authentication based on their function or permission level in the business.

Your team has been directed to enhance the protection of your users' identities and limit the use of privileged accounts.

Learning objectives:

* Configure Azure conditional access.
* Using Azure identity protection.
* Enable multi-factor authentication for all users.
* Deploy Azure Privileged Identity Management (PIM)

**Challenge 6: We need policies**

As the organization continues to secure the environment, they need to ensure that new resources deployed follow the best practices and security requirements that are set. These policies should restrict the ability to deploy new resources that would be deemed out of compliance and identify any existing resources that must be remediated.

Learning objectives:

* Create Azure to restrict the region and sizes allowed by the company.
* Protect data in transit.
* Be able to audit activity.

**Challenge 7: This has been a test**

The team must run a simulated attack against a test device in the Microsoft Defender Security Center. Once complete, the team should be able to identify different elements of the attack. Additionally, the team must create one advanced hunting rule that identifies antivirus reports from a specific target device. As part of the larger security effort, the team will create an Azure Playbook to alert team members if an incident occurs in the Azure Security Center. A new analytics rule also needs to be created in Azure Sentinel that will monitor Cloud App Security for any medium or high severity alerts.

Learning objectives:

* Run an attack simulation against one of the provisioned lab virtual machines.
* Identify aspects of the attack.
* Create an advanced hunting query.
* Create an Azure Playbook.
* Create an Azure Sentinel Analytics rule.x

**Challenge 8: Trip the wire**

Contoso Mortgage is ready to get their company devices onboarded into Microsoft Endpoint Manager. They need to test out automatic enrollment and ensure the devices are enrolled in Microsoft Defender for Endpoint. Using one of the newly onboarded test devices, the security team will run a simulated attack against it and analyze the reported incidents. Employees and their efforts to help protect the organization will not be overlooked. The team will take employee training to the next level and test the available phishing attack simulations found in Office 365 Security & Compliance.

Learning objectives:

* Enable automatic enrollment of Windows devices.
* Create a configuration profile to enroll devices in Microsoft Defender for Endpoint.
* Create compliance and access control policies.
* Run an attack simulation against a test device and analyze the incident.
* Test phishing attack simulations and their training benefit for end users.

**Challenge 9: What we do in the shadows**

Your team has already accomplished a tremendous amount of work and now it is time to make sure there are no surprise shadowy IT apps lurking around your company’s devices. With the move to the cloud and most of the work being performed remotely, the CIO knows the company must have a good handle on the apps that may be getting used without infrastructure's knowledge.

Learning objectives:

* Enable and configure Microsoft Cloud App Security features to integrate with Azure Sentinel, Microsoft Defender for Endpoint, and SaaS apps.
* Create policies to notify administrators when unsanctioned apps are discovered.
* Analyze a point-in-time snapshot of the company’s firewall logs prior to the remote worker paradigm shift.

Value Proposition

* Microsoft Security and Compliance solutions provide differentiated value for customers. The key elements are:
  + Built-in experiences across platforms that provide a friction-free experience so everyone can work securely from anywhere, on any platform.
  + Leverage AI and automation to help improve security. Specifically, this automation empowers your team against emergent cyberthreats with machine learning and automation.
  + Best in class and integrated. Our comprehensive suite of leading solutions is unified across people, devices, apps, and data.

Technical Scenarios

* Identify Azure and Microsoft 365 tools for reporting and improving security and compliance.
* Apply Azure and Microsoft 365 security and compliance policies, including classification labels and tags.
* Enforce MFA and managing risks associated with user identities.
* Protect resources using Azure policies.
* Leverage monitoring in Microsoft 365 Defender, Azure Defender, and Azure Sentinel.
* Work with a threat summary report and identify security functions responsible for mitigation actions.
* React to simulated intrusions.

Audience

* Target Audience:
  + Security Practitioners active in Security Operations roles
  + IT professionals tasked with protecting their companies
  + Security decision makers evaluating solutions
* Target verticals: Cross-Industry
* Customer profile:
  + Medium to large business and enterprise.

Registration Questions

|  |  |  |
| --- | --- | --- |
| **Required** | **Field** | **Response Options** |
| Yes | What is your level of understanding using Azure today? | None Some understanding  I have some pilot work on Azure  I rely on Azure today for cloud |
| Yes | How much time have you spent with Azure Security Center? | [Dropdown or Radio Buttons]  < 3 months  3-6 months  6 months - 1 year  > 1 year |
| Yes | How much time have you spent with Microsoft 365 Security and Compliance? | [Dropdown or Radio Buttons]  < 3 months  3-6 months  6 months - 1 year  > 1 year |

Competitive Landscape (optional)

The security space is fragmented and most frequently we compete with point solution providers including:

* Okta competes primarily in the Identity and Access Management space with Azure Active Directory. They often drive a story that Microsoft identity solutions are only for Microsoft workloads. Azure AD is a complete cloud IAM solution that supports thousands of non-Microsoft apps.
* Crowdstrike is a leader in the endpoint security space. They are often seen as a thought leader and leverage their managed services as a lever for sales. Microsoft Defender for Endpoint is a leader in the Gartner Magic quadrant and protects 10’s of millions of devices across platform
* Proofpoint is our primary competitor in email protection. They position themselves to Office 365 customers as additional protection.

Microsoft solutions are best of breed across their categories. They are also built to work together simplifying security, saving customers money, and providing better security outcomes.

FAQs

Q: Is there a suggested flow of OpenHacks which participant should attend first, before going to yours?

A: No, but you will need to understand the different offers and implementations of natively available in Microsoft 365 and Azure when supported by an Enhanced Mobility and Security E5 license and Microsoft Defender for Endpoint.

Q: What tools will I need?

A: This OpenHack does not require additional software to be installed, however, team members may find having the PowerShell module for Azure Active Directory and Az module or Azure PowerShell module installed if using PowerShell is a preferred method to retrieve information from the subscriptions.