SPECTEROPS
Creators of BloodHound

TRAINING

ADVERSARY PERSPECTIVES

Azure

Real Results

- **Security-focused insights written from the viewpoint of security testers and researchers**
- **View Entra ID through the lens of an adversary**
- **Hands-on training with security tools where students get experience identifying and exploiting security misconfigurations in multiple ways**
- **Deep dive into identity and authentication methods**
- **An overview of Azure Resource Manager covering many of the common resources**

Adversary Perspectives: Azure provides participants who have limited previous Azure Resource Manager and Entra ID experience with an understanding of how attackers look at Microsoft cloud technologies. Students will learn in depth about the components of Azure and Entra ID, covering topics such as identity, authentication, resources, and security configurations.

Participants will learn nuances of these systems, which will help to identify misconfigurations and weak security settings. Hands-on labs will help take the theory from lectures to actionable approaches for exploiting and securing cloud assets.

Labs allow students to gain experience with current offensive tooling while also exploring and practicing with approaches used by administrators. **This will teach students not only how to attack Azure and Entra but also provide them with the perspective administrators often work from with the goal of informing students on how misconfigurations occur.**

What will you teach that students can't get elsewhere?

Adversary Perspectives: Azure is the first installment in the SpecterOps Adversary Perspectives series. This Adversary Perspectives class looks to teach security professionals from the viewpoint of an attacker. Heavily rooted in theory, the course covers security considerations in depth while providing an attacker perspective. Throughout the course, participants will reinforce what they learn through hands-on labs and instruction given by SpecterOps practitioners.

DAY 1

Class Introduction
Entra ID
Application Registration
- Entra Roles

Azure Resource Manager
Azure Roles

DAY 2

Microsoft 365
- App Services

Virtual Machines
Microsoft Graph
- Microsoft Intune

OAuth

DAY 3

Hybrid Identities
Authentication
Device Authentication
Passwordless Authentication
- OIDC

Multi-Factor Authentication

DAY 4

Conditional Access Policies
External Information Gathering
Credentials
- PIM

Tooling

The Adversary Perspectives course differs from Adversary Tactics in two main ways. First, students will not execute a full kill chain for compromising an Entra ID tenant. Students start from an assume breach perspective to complete stand-alone attacks on specific resources.

Second, students will not gain complete identity dominance as part of the course. While escalation methods are discussed and practiced in the lab, full tenant compromise is not a part of the course. Labs are derived directly from real-world scenarios SpecterOps has encountered and exploited.

Who should take your courses?

Adversary Perspectives: Azure is intended for security professionals looking to learn more about Azure and Entra ID security and common attacks from an adversary perspective.

What is the benefit of taking this course over other available training courses?

Adversary Perspectives: Azure does not aim to provide students with easy, quick-win skills and knowledge. **This course dives deep into topics so students gain a thorough understanding of theory, practice, and security implications.** Since Microsoft's cloud offerings make frequent changes, specific attacks and exploits often become irrelevant within a matter of months. Understanding the underlying concepts and theory will increase the longevity of the knowledge gained in this course. Learning this theory will put students in a better position to:

- Conduct security assessments in a variety of environments and set ups
- Develop, customize, and update tooling
- Dive deeper into security research
- Advise clients and administrators more effectively

Have you found yourself in a job role needing to attack or defend Azure or Azure Active Directory architecture? Has your fast-paced organization moved to the cloud while leaving security to catch up? **Adversary Perspectives: Azure cuts through the fog of the cloud by building participants' understanding of Azure's infrastructure components, common architecture designs, and security controls in the context of the attacker lifecycle.**

Through hands-on labs, this course also teaches participants how to identify misconfigurations in Azure that are commonly leveraged by attackers. Participants should expect to walk away from Adversary Perspectives: Azure with a strong foundation of Azure security knowledge while taking their first step on the journey of attacking or defending corporate Azure environments.

Email info@specterops.io ›

Learn more at specterops.io ›

Why SpecterOps

SpecterOps is at the forefront of researching and educating the industry on the risks associated with Azure and Entra ID. Anchored by our publicly available research and tooling, SpecterOps educates clients and our community about the configuration risk and complexities of adversaries who attack Azure, Entra ID, Active Directory, or hybrid environments. Our experts not only conduct the research, they also have a passion for teaching those concepts to our clients and ensuring they understand which combinations of configurations can lead to compromise.