TRAINING

SPECTEROPS

ADVERSARY PERSPECTIVES: AZURE

Organizations have their heads in the clouds, or at least their infrastructure. Gone are the days of on-prem domain controllers and Exchange servers. Microsoft's Azure provides organizations with the ability to deploy cloud hosts and services to augment, or in some cases, replace existing functionality completely. All of these new cloud assets need protection, both through traditional defensive security measures, and offensive security assessments. For new and veteran security professionals alike, understanding how these new technologies work and the nuances of securing them can quickly become complicated.

Adversary Perspectives: Azure aims to provide participants without previous Azure experience with a solid understanding of how attackers look at Microsoft Azure, its authentication mechanisms, and how they commonly attack Azure-based environments.

DAY 1

- Class Introduction
- Azure Basics
- Accounts and Identities
- Roles
- Groups

DAY 2

- Function Apps
- Microsoft 365
- Virtual Machines
- MS Graph

DAY 3

- Hybrid Authentication
- Azure Authentication Flows
- OAuth
- Passwordless Authentication
- Multi-Factor Authentication
- Authentication Methods in Azure
- Credential and Identity Sync Mechanisms

DAY 4

- Conditional Access Policies
- External Information Gathering
- Credential Collection
- Attack Lifecycle

TRAINING

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

Adversary Perspectives: Azure is the first installment in the SpecterOps Adversary Perspectives series. Known for our Adversary Tactics courses, we realized that there is often a gap of understanding that needs to be bridged before a practitioner is ready to start taking offensive or defensive actions in a particular environment. While other courses aim to simply build basic knowledge from a general user standpoint, this Adversary Perspectives class looks to teach security professionals from the viewpoint of an attacker. Don't just look at your security posture in Azure, actually understand the abuse mechanisms and holistic security of your deployment.

Participants will build on this knowledge through an understanding of how Azure architectures, like solely cloud-based environments or hybridized on-premises and Azure environments, can affect the overall security of an environment. Throughout the course, participants will reinforce what they learn through hands-on labs and instruction given by SpecterOps practitioners.

Why isn't this material taught in other places?

SpecterOps combines an adversary's perspective on Azure and Entra ID with the technical expertise of system administrators to empower organizations.

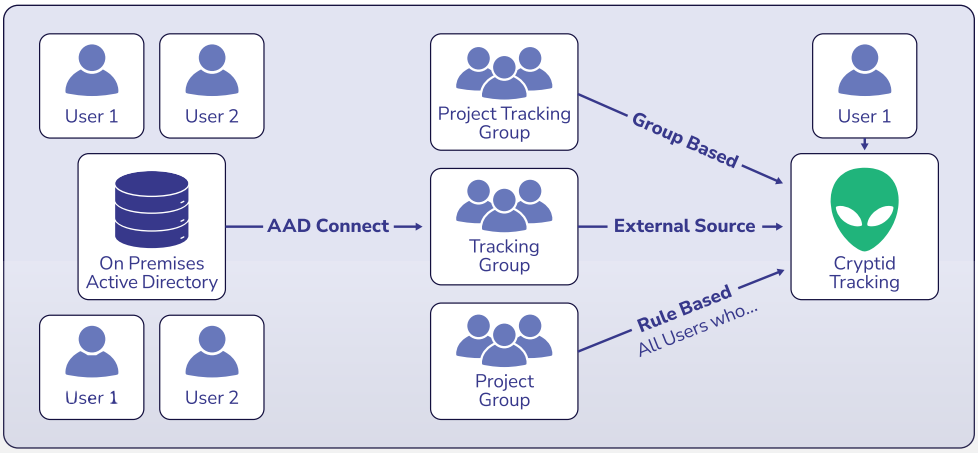
Who should take your courses?

Adversary Perspectives: Azure is intended for security professionals of any experience level looking to learn more about Azure security and common attacks from an adversary's perspective.

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, but have a passion for teaching those concepts to our clients and ensuring they have an understanding of which combinations of configurations can lead to a compromise.

Access Rights Management



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 and first step on their journey of attacking or defending corporate Azure environments.

REAL RESULTS

Security-focused insights in Adversary Perspectives: Azure, written from the viewpoint of security testers and researchers.

Entra ID through the lens of an adversary.

Hands on training with security tools where students can get experience identifying security misconfigurations in multiple ways.

A deep dive into authentication methods.

An overview of Azure Resource Manager covering many of the common resources.

SPECTEROPS

Learn more at **specterops.io**

Email **info@specterops.io**