TRAINING

SPECTEROPS

AZURE: SECURITY FUNDAMENTALS

Organizations are increasingly adopting cloud-based infrastructure for some or all of its corporate production network. Microsoft's Azure provides organizations with the ability to deploy cloud hosts and services to augment or replace existing functionality.

More cloud resources implemented means more cloud resources needing protecting, through defensive or offensive security, but understanding how these new technologies work and the nuances of securing them can quickly become complicated.

Azure Security Fundamentals aims to provide participants without previous Azure experience a solid foundational understanding of Microsoft Azure, its common architectures, its authentication mechanisms, and how adversaries 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

- OAuth
- Authentication Mechanisms
- Credential and Identity Syncing Mechanisms

DAY 4

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

TRAINING

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

SpecterOps researches and understands how Azure and Entra ID are being used in organizations today. We often see our clients configure permissions to enable the business, without fully understanding the risk behind those configurations. This course will dive into how each configuration and a combination of configurations can create Attack Paths that can be leveraged by adversaries to compromise your organization and its data. We will even demonstrate how access can be pivoted from cloud to on-premise resources.

Why isn't this material taught in other places?

SpecterOps combines an adversary's view of Azure and Entra ID with the technical depth of system administrators job is to enable the organization.

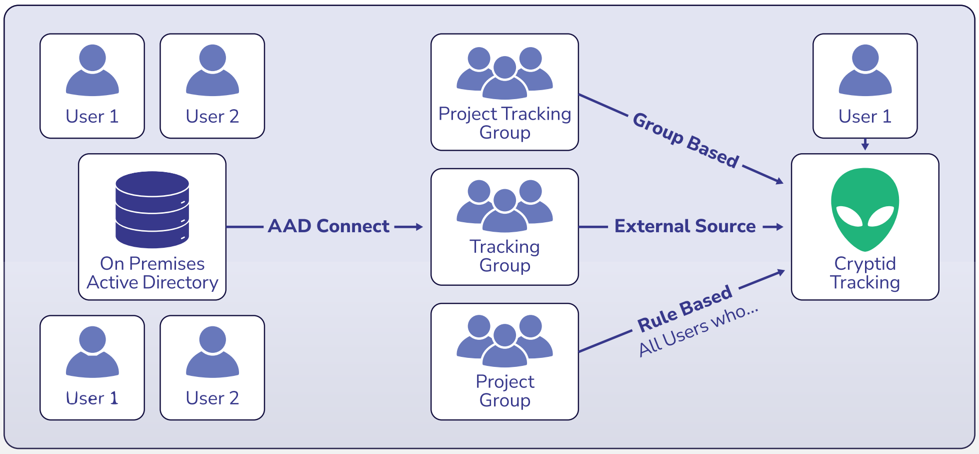
Who should take your courses?

- Offensive operators who are looking to validate security controls and configurations.
- Administrators who want to understand how an adversary sees Azure and Entra ID.
- Identity and Access Management team members who need require a foundational understanding of security implications.

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? Azure: Security Fundamentals 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 Azure: Security Fundamentals 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 Azure fundamentals written from the perspective 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**