SPECTEROPS

ACTIVE DIRECTORY:
SECURITY FUNDAMENTALS

Dig into Active Directory! This course will help you roll up your sleeves and get hands-on with Active Directory, enabling participants to gather answers directly when questions surrounding their organization's AD architecture arise in the future.

Learn Active Directory components and not only how they work together but also how they can work against your organization's security posture. Countless organizations leverage Active Directory (AD) to provide the foundation or entirety of their production environment's identity and access management. But widespread usage doesn't mean AD is simple; beyond its architecture and design considerations lie security implications that can directly impact your organization.

Active Directory: Security Fundamentals details key components of AD technology and architectures, focusing on the security implications of each.

We'll cover physical & logical components, forests & domains, Kerberos, and various tooling like ADUC – all from a security perspective. Course participants will get hands-on experience enumerating the architectures and security controls of a live Active Directory environment and will then analyze the data extracted.

DAY 1
- Active Directory Topology
  – Physical Components
  – Logical Components
- Active Directory Users and Computers
  – Nested Group Membership
  – Abuse of Trusts
  – Fundamentals of Relationships
- Searching for and Identifying Misconfigurations
  – How to Query and Find Data in Active Directory
  – Hands-On with Industry Standard Toolsets

DAY 2
- Kerberos
  – Common Abuses and Protocol Extensions
- Identifying Attack Paths
- Tiered Administration
- Degradation of Active Directory

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

Active Directory: Security Fundamentals is designed to provide students with a foundational understanding of Active Directory and how to secure it effectively. Students will be exposed to practical examples to gain understanding in common mistakes that organizations will make that introduce misconfigurations in an Active Directory environment. This course focuses on how a series of misconfigurations can turn into an Attack Path that an adversary can leverage to compromise your most critical assets. Once the student understands the attack paths, we provide the foundation to eliminate those issues with Attack Path Management.

Why isn't this material taught in other places?

Active Directory: Security Fundamentals focuses on avoiding the issues that create Attack Paths in the first place. SpecterOps has the technical depth to fully understand how these attack paths work in order to deliver specific guidance on how to avoid them all-together.
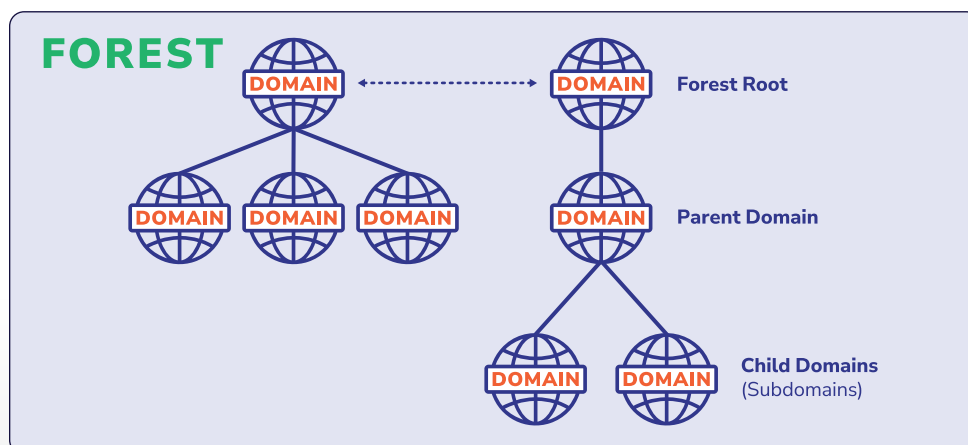
Who should take your courses?

Offensive and defensive security professionals that are interested in or need a fundamental introduction into Active Directory its basic security principals. Identity and Access Management team members who have administrative responsibilities over an Active Directory environment.

Why SpecterOps?

SpecterOps is at the forefront of researching and educating the industry on the risks associated with Active Directory. ADCS, SCCM, and ACE Attack Path research all originated from the SpecterOps team. We also release a series of tools, freely available to the community to help educate folks on adversary tradecraft and empower people to reduce risk in their environments.

RECAP: Forests and Domains

FOREST

DOMAIN ◁------------▷ DOMAIN   **Forest Root**

DOMAIN   DOMAIN   DOMAIN   DOMAIN   **Parent Domain**

DOMAIN   DOMAIN   **Child Domains** (Subdomains)

Stop being passive with your Active Directory! Kerberos, ADUC, Golden Tickets, Security Principals – have you come across these or similar words in penetration test reports or security bulletins and felt a little… lost? Active Directory comprises many components that fulfill complex architectural requirements but can also open cracks through which attackers may slip. Active Directory: Security Fundamentals demystifies the various Active Directory components and illustrates how these components can potentially introduce risks to your organization. This course empowers network defenders to directly look under the hood of their Active Directory architecture and understand their environment better than attackers. Instructors share their knowledge and personal experiences testing Active Directory in hundreds of environments to reveal not only common pitfalls in securing their environment but also how they commonly occur.

SPECTEROPS

Learn more at **specterops.io**
Email **info@specterops.io**