EDAO

Identity Exposure

Secure Active Directory and Disrupt Attack Paths

Behind every breach headline is an insecure Active Directory (AD) deployment. 80% of attacks use AD to perform lateral movement and privilege escalation; 60% of new malware includes codes to target AD misconfigurations. AD has become the favored target for attackers to elevate privileges and facilitate lateral movement through leveraging known flaws and misconfigurations. Unfortunately, most organizations struggle with Active Directory security due to misconfigurations piling up as domains increase in complexity, leaving security teams unable to find and fix flaws before they become business-impacting issues. EDAO enables you to see every change in your Active Directory, predict which anomalies or weaknesses carry the greatest risk, and act to disrupt critical attack paths before attackers exploit them.

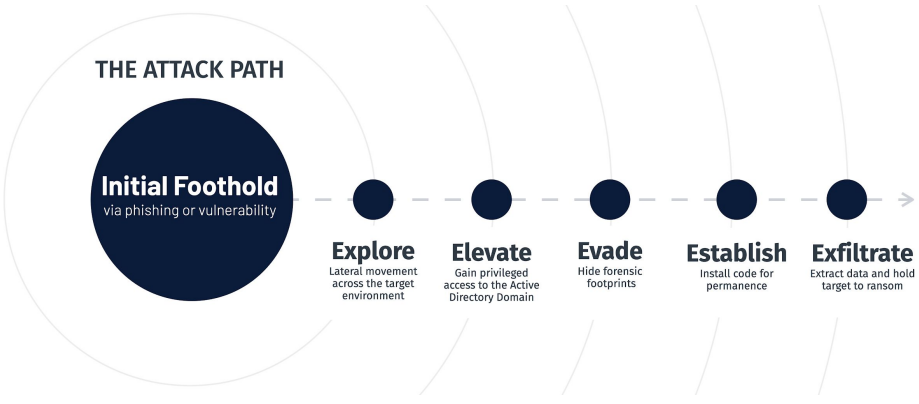
Challenges with Securing Active Directory

The constant changes in Active Directory (AD) in every company limits visibility to the AD attack surface and frequently introduces new attack pathways. Few security teams have enough visibility and context to find and remediate AD misconfigurations and vulnerabilities.

Trying harder doesn't help. The size and complexity of most AD implementations make manual monitoring impractical and real-time detection of attacks impossible. Incident response and threat hunting is hampered because teams can't see all the hidden misconfigurations and interconnected relationships.

Consequences of Weak Active Directory Security

Successful breaches are usually followed by attacks on Active Directory to escalate privileges, move laterally, install malware and exfiltrate data. Attackers can successfully hide these advances from logs and other monitoring tools since their movements through Active Directory appear compliant within existing security policies. The high cost of weak AD security hits when attackers successfully deliver payloads that result in data loss, ransom demands, environment reconstruction or brand impact.



CONTINUOUSLY DETECT AND PREVENT ACTIVE DIRECTORY ATTACKS WITH EDAO

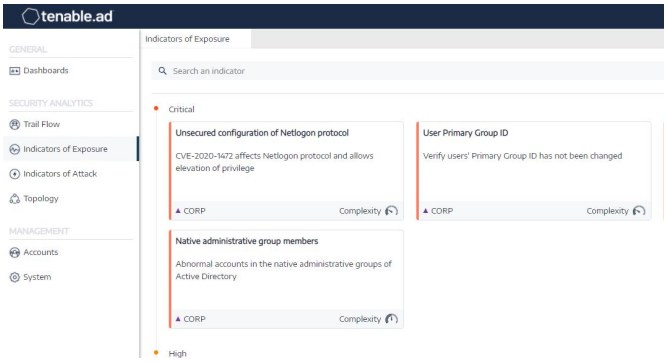
- Uncover any hidden weaknesses within your Active Directory configurations
- Discover the underlying issues threatening your AD security
- Dissect each misconfiguration – in simple terms
- Get recommended fixes for each issue
- Create custom dashboards to manage your AD security to drive risk reduction
- Discover dangerous trust relationships
- Catch every change in your AD
- Uncover attacks occurring in your AD
- Visualize every threat from an accurate attack timeline
- Consolidate attack data in a single view
- Make the link between AD changes and malicious actions
- Analyze in-depth details of an AD attack
- Explore MITRE ATT&CK ® descriptions directly from the incident

EDAO Secures Active Directory and Disrupts Attack Paths

EDAO's proactive, risk-based approach to AD security enables you to see all of your vulnerabilities, predict which pathways attackers may target, and act to detect, shut down and prevent attacks.

Find and Fix Active Directory Weaknesses Before Attacks Happen

Proactively discover and prioritize weaknesses within your existing Active Directory domains and reduce your exposure by following EDAO's step-by-step remediation guidance. By hardening your Active Directory, you can stop attackers in their tracks, eliminate their potential movements and ensure that fewer breaches result in escalated privileges, lateral movement or malware execution.

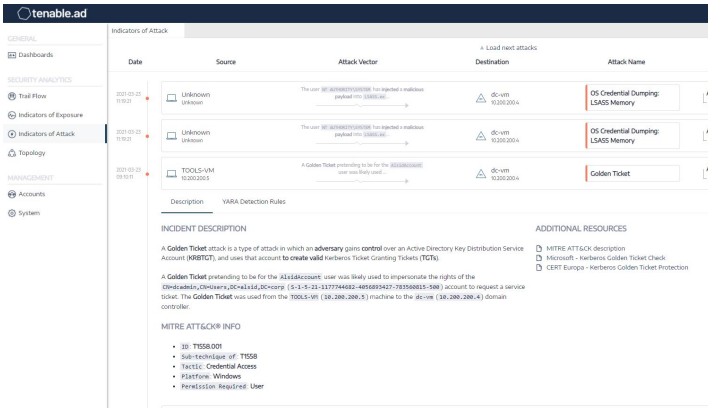


Detect and Respond to Active Directory Attacks in Real Time

Continuously monitor and detect Active Directory attacks like Golden Ticket, DCShadow, brute force, password spraying, DCSync and more. EDAO enriches your SIEM, SOC or SOAR with attack insights so you can quickly respond and stop attacks. Automated AD attack detection alleviates the monitoring burden on security teams and frees up their time for other priorities.

Flexible, lightweight deployment secures your Active Directory wherever it extends — from on-prem to the cloud.

- **No Agents. No Privileges. No Delays.**
  Prevents and detects sophisticated Active Directory attacks without agents and privileges.
- **Clouds Covered**
  Check the security of Azure Active Directory Domain Services, AWS Directory Service, or Google Managed Service for Active Directory in real time.
- **Deployed Anywhere**
  EDAO provides the flexibility of two architectural designs. On-prem to keep your data on-site and under your control. SaaS, so you can leverage the cloud.



Contact Us: Please email us at info@edaogroup.io or visit https://edaogroup.io

EDAO