

# AWN Active Directory Audit Service

## Ensure Privileged Users and Business-Critical Systems Are Protected



**When was the last time you verified your Active Directory and had your DNS/DHCP policies reviewed by a security professional?**

### **Get started in under two days!**

- Assess Active Directory and DNS/DHCP configurations
- Recommend changes to password policies, AD and DNS/DHCP configurations, and share permissions
- Validate logging to support optimal compliance reporting

Companies today operate under constant threat of cyberattacks from both outside attackers and inside bad actors. In many threat scenarios, attackers attempt to gain control of accounts with administrative privileges, allowing them to reallocate data or resources, subvert security controls and policies, and cover their tracks by destroying evidence of compromise.

Attackers also frequently alter Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) services to direct traffic to illegitimate and malicious locations. However, many organizations do not monitor their active directory and DNS/DHCP servers, which leaves them with no opportunity to identify or remediate vulnerabilities.

The Active Directory (AD) audit service from Arctic Wolf Network (AWN) provides total visibility into your AD and DNS/DHCP servers, gives expert security guidance on best practices and risk avoidance, and offers ongoing insight into privileged user activity and asset mapping.



### **Tailored Active Directory Auditing**

Every organization employs different AD configurations and policies, and tailors them to their technology resources and business needs. AWN's cybersecurity experts work with your team and perform a comprehensive, thorough, and tailored review of your servers. Our CSEs define actionable steps to improve your security posture, including deactivation of dead accounts, identifying and blocking malicious IP addresses making repeated login attempts, and more.

## Directory Auditing Workflow

The AWN Concierge Security Engineer performs the following tasks.

### 1. Onboard

- Collects customer's AD design/architecture and replication policies
- Reviews DHCP/DNS configurations, share permissions

### 2. Conducts monthly reporting to:

- Validate logging for optimal reporting and forensics capabilities
- Track the following:
  - AD, DHCP/DNS changes
  - Changes to GPOs, admin groups
  - Users added/deleted
  - Computers added/removed
  - DHCP/DNS changes
  - Failed logins for users/admins

### 3. Performs semi-annual strategic review that includes:

- AD configuration
- Password policies
- DNS/DHCP configuration
- Replication review
- Share permissions review
- Stale account review
- Windows Firewall configuration review for data centers

## AWN Advisory Services Ensure Your Assets Are Always Secure

Arctic Wolf Networks provides customized advisory services that leverage our experience running the industry's leading cloud-based SOC-as-a-Service platform. AWN CyberSOC™ continuously monitors the network infrastructure of hundreds of customers and enables them to rapidly detect and respond to security incidents with actionable intelligence. The unique value proposition of our Active Directory Audit Service includes:

- **Security Expertise:** Our experienced Concierge Security Engineers hunt down and triage the most challenging security threats. We leverage AD best practices for the top attack vectors we see across multiple customers.
- **Customized to Your Specific Needs:** Once we monitor your IT infrastructure, we gain comprehensive knowledge of your business risks and compliance requirements, and can customize AD configurations to meet your exact needs.
- **Ongoing Support:** Our offering provides ongoing monitoring and regular review, delivering not just point-in-time protection, but also continuous improvement of your security posture.



#### Contact us

arcticwolf.com  
1.888.272.8429  
ask@arcticwolf.com