Active Directory Security Checklist

As they turn their attention to identity-focused attack surfaces, threat actors are identifying on-premise and cloud-hosted Active Directory (AD) environments as primary targets. But because AD administrators must balance operational requirements with restrictive security measures, protecting these environments is daunting.

While many solutions can secure on-premise and Azure AD infrastructures, security professionals struggle to identify the right solution for a particular organization's risk profile.

Enterprise security teams can use the following checklist to evaluate risks and gaps in their Active Directory security procedures.

Questions to Ask When Looking to Secure Active Directory

On-Premise and Cloud-Based Active Directory Cyber Hygiene Benchmarks

- Is there an inventory of all user or device accounts?
- Is there an inventory of all privileges & entitlements for every account?
- Is there an implemented least privilege policy for all accounts?
- Are AD security settings regularly reviewed and reassessed?
- Are Kerberos vulnerabilities regularly assessed in AD?
- Are AD servers hardened against the latest CVEs and other vulnerabilities?
- Are trust relationships across forests regularly audited?

Benchmarks to Identify Attack Indicators

- Are attempts to harvest AD data detected or stopped?
- Are audit policies enabled?
- Are audit logs periodically analyzed?
- Is there visibility into Domain directory replication?
- Is there visibility into attempts to discover user and group permissions?
- Is there real-time visibility into mass changes to AD?
- Is there real-time detection for attacks like Kerberoasting and DCShadow?

How to Secure Enterprise Active Directory and Azure AD Accounts

- Are account privileges regularly audited and reassessed for each account?
- Are service or privileged accounts regularly audited and reassessed?
- Is there a limit to the scope and number of privileged accounts?
- Are delegations regularly audited & reassessed?
- Are password policies sufficient and regularly reassessed?
- Is there real-time detection for built-in AD "Administrator" account usage?

Benchmarks to Detect Endpoint Attacks

- Is there detection for intelligence-gathering and discovery attempts from the endpoints targeting AD?
- Are there security controls to misdirect AD discovery queries originating from endpoints?
- Are AD credentials stored on endpoints? If so, should they be removed?
- Is there visibility to privileged or high-risk AD credentials stored at the endpoints that attackers can leverage for lateral movement?
- Is there visibility into attempts to discover delegated accounts with special privileges?

Definitions

On-Premise and Cloud-Based Active Directory Cyber Hygiene Benchmarks

The items in this checklist category can help identify exposures within Active Directory that attackers can leverage to compromise the environment. Identifying and remediating vulnerabilities that attackers can target is vital to maintaining a hardened and secure AD infrastructure.

How to Secure Enterprise Active Directory and Azure AD Accounts

Account policies and settings can determine the extent to which attackers can exploit a particular Active Directory identity, whether on-premises or based in Azure. Organizations should audit and assess each account to ensure they have only the necessary permission to accomplish their functions, especially for privileged accounts and accounts with delegated administrative privileges (shadow admin accounts).

Benchmarks to Identify Indicators of Attack

Many organizations lack controls to detect attack activities targeting AD data, such as data harvesting and privilege escalation attacks like Kerberoasting. Organizations should establish mechanisms to identify when attackers target AD, such as auditing and reviewing AD changes for activities indicating an attack.

About SentinelOne

SentinelOne is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity XDR platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733