BONUS · MITRE ATT&CK REMEDIATION CHECKLIST

Track every technique. Close every gap.

> An auditor-ready remediation worksheet covering every Active-Directory technique ADscan reasons about. Sign it. File it. Re-baseline against it.

$297 value

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

included free with ADscan

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

Initial Access

2 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1133	**External Remote Services**	HIGH	Require MFA on every external service; disable legacy auth and basic protocols.	OPEN
☐	T1190	**Exploit Public-Facing Application**	HIGH	Patch internet-facing systems with a 7-day SLA; deploy a WAF with virtual patching.	OPEN

Persistence

2 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1098	**Account Manipulation**	HIGH	Alert on AdminSDHolder DACL changes and on new ACEs on privileged objects.	OPEN
☐	T1136	**Create Account**	HIGH	Restrict Create Account rights; alert on new admin or service account births.	OPEN

Privilege Escalation

3 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1078	Valid Accounts	CRITICAL	Tier accounts; require MFA and PAW for every privileged credential.	OPEN
☐	T1078.002	Domain Accounts	CRITICAL	Disable inactive domain accounts after 30 days; rotate service-account secrets.	OPEN
☐	T1068	Exploitation for Privilege Escalation	HIGH	Patch monthly with a 14-day SLA on critical CVEs; track exploitation telemetry.	OPEN

Defense Evasion

3 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1556.007	**Hybrid Identity**	HIGH	Audit hybrid identity sync agents; require MFA on Entra Connect service accounts.	OPEN
☐	T1027	**Obfuscated Files or Information**	MEDIUM	Enable AMSI + Sysmon process-create logging; block unsigned PowerShell.	OPEN
☐	T1070	**Indicator Removal**	MEDIUM	Forward security logs to an out-of-domain SIEM; alarm on log-clear events.	OPEN

TACTIC 05 · CREDENTIAL ACCESS

Credential Access

14 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1003	OS Credential Dumping	CRITICAL	Enforce Credential Guard and RunAsPPL; restrict admin tooling to PAW.	OPEN
☐	T1003.001	LSASS Memory	CRITICAL	Enable LSASS protected process light; deploy Credential Guard fleet-wide.	OPEN
☐	T1003.006	DCSync	CRITICAL	Restrict Replicate Directory Changes to a named, audited set of accounts.	OPEN
☐	T1558	Steal or Forge Kerberos Tickets	CRITICAL	Enforce AES-only encryption on every privileged Kerberos principal.	OPEN
☐	T1558.003	Kerberoasting	CRITICAL	Reset SPN passwords to 30+ char random; enforce AES-only; rotate quarterly.	OPEN
☐	T1558.004	AS-REP Roasting	CRITICAL	Enable Kerberos pre-auth on every human account; alert on disablement.	OPEN
☐	T1110.003	Password Spraying	HIGH	Forbid weak passwords via banned-password list; alert on spray fingerprints.	OPEN
☐	T1187	Forced Authentication	HIGH	Disable LLMNR / NBT-NS via GPO; require SMB signing on every host.	OPEN
☐	T1552.006	Group Policy Preferences	HIGH	Remove cpassword from SYSVOL; rotate every account it ever referenced.	OPEN
☐	T1557.001	LLMNR/NBT-NS Poisoning + SMB Relay	HIGH	Disable LLMNR + NBT-NS + mDNS; enforce SMB signing required domain-wide.	OPEN
☐	T1649	Steal or Forge Authentication Certificates	HIGH	Audit ADCS templates for ESC1-ESC11; disable EDITF_ATTRIBUTESUBJECTALTNAME.	OPEN
☐	T1110.001	Password Guessing	MEDIUM	Enforce smart-lockout: 10 attempts / 15 min; alert on brute-force patterns.	OPEN

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1552.001	**Credentials in Files**	MEDIUM	Scan SYSVOL and shares for cleartext secrets; rotate any exposed credential.	OPEN
☐	T1555	**Credentials from Password Stores**	MEDIUM	Block userland access to DPAPI master keys; require MFA on password vaults.	OPEN

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

Discovery

5 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1018	**Remote System Discovery**	MEDIUM	Restrict anonymous SMB / RPC enumeration; alert on bulk DC discovery scans.	OPEN
☐	T1069	**Permission Groups Discovery**	MEDIUM	Tier privileged groups; deny enumeration to standard users via GPO.	OPEN
☐	T1087	**Account Discovery**	MEDIUM	Disable anonymous LDAP binds; require authenticated enumeration only.	OPEN
☐	T1087.002	**Account Discovery: Domain Account**	MEDIUM	Block LDAP queries from unmanaged hosts; require LDAP signing on every DC.	OPEN
☐	T1482	**Domain Trust Discovery**	MEDIUM	Audit and prune unused trusts; enforce SID filtering on every external trust.	OPEN

Lateral Movement

5 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1550.002	**Pass the Hash**	CRITICAL	Add Tier 0 admins to Protected Users; deny network logon to local admins.	OPEN
☐	T1550.003	**Pass the Ticket**	CRITICAL	Add Tier 0 admins to Protected Users; rotate krbtgt twice after compromise.	OPEN
☐	T1021.001	**Remote Services: RDP**	HIGH	Enforce Restricted Admin and Remote Credential Guard for RDP to servers.	OPEN
☐	T1021.002	**Remote Services: SMB/Windows Admin Shares**	HIGH	Disable admin shares on workstations; enforce SMB signing on every server.	OPEN
☐	T1570	**Lateral Tool Transfer**	MEDIUM	Block lateral file copy via SMB / WinRM from unmanaged hosts; alert on PsExec.	OPEN

Impact

1 TECHNIQUES TRACKED · STATUS SET TO **OPEN** BY DEFAULT — UPDATE DURING THE REMEDIATION REVIEW.

	ATT&CK ID	TECHNIQUE	SEVERITY	MITIGATION	STATUS
☐	T1486	**Data Encrypted for Impact**	CRITICAL	Maintain offline immutable backups; rehearse restore quarterly with a tabletop.	OPEN

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

STATUS LEGEND · SIGN-OFF

A checklist isn't finished until someone signs it.

OPEN

No mitigation applied; the technique remains exploitable in this environment.

MITIGATED

Mitigation deployed and validated by re-scan; carry forward to next baseline.

ACCEPTED

Risk explicitly accepted by leadership; document compensating control + expiry.

Sign-off

CISO NAME

DATE

AUDIT REFERENCE

ADSCAN WORKSPACE