CHECKLIST

Active Directory Password Spray Detection and Prevention Checklist

A practical, vendor-neutral checklist to help detect, validate, and reduce the risk of Active Directory password spray attacks before production use.

Active Directory Password Spray Detection and Prevention Checklist

Use this checklist to assess whether your environment can detect password spray activity, confirm where you are exposed, and verify that practical controls are in place before production use.

---

1) Scope and assumptions

- [ ] Identify all authentication paths that ultimately reach Active Directory
- [ ] Domain controllers
- [ ] VPN and remote access portals
- [ ] Federation or SSO services
- [ ] Legacy applications using AD credentials
- [ ] RDP gateways / bastions
- [ ] Any external-facing sign-in endpoints
- [ ] Document which accounts are in scope

- [ ] Human user accounts
- [ ] Privileged/admin accounts
- [ ] Service accounts
- [ ] Former or dormant accounts
- [ ] Break-glass accounts
- [ ] Note any known exceptions that may create legitimate centralized authentication bursts
- [ ] VPN concentrators
- [ ] IdP or federation proxies
- [ ] Automation and scheduled jobs
- [ ] Shared service paths

---

2) Logging readiness

- [ ] Confirm authentication logs are being collected from all relevant systems
- [ ] Verify timestamps are normalized to a common time source
- [ ] Ensure logs include at least:
- [ ] Username or account identifier
- [ ] Source IP or source host
- [ ] Timestamp
- [ ] Authentication result
- [ ] Failure reason or code
- [ ] Logon type / protocol when available
- [ ] Confirm log retention is long enough to spot low-and-slow activity
- [ ] Validate that SIEM or log tooling can query across users, sources, and time windows
- [ ] Confirm that failed logons are not being dropped, deduplicated away, or sampled too aggressively

---

3) Detection logic checks

- [ ] Alert on many failed logons across many users in a bounded time window
- [ ] Alert when one source targets multiple accounts with similar failure patterns
- [ ] Alert on repeated failures that remain below account lockout thresholds
- [ ] Alert on abnormal timing such as:
- [ ] Outside business hours
- [ ] During low-activity periods
- [ ] After password reset campaigns
- [ ] During onboarding or offboarding windows
- [ ] Alert on failed attempts against accounts that should not normally authenticate interactively
- [ ] Consider grouping by campaign traits rather than per-account thresholds only
- [ ] Tune to exclude known-good sources and expected automation

---

4) Validation queries and review questions

- [ ] Can you identify the top source IPs by unique users affected?
- [ ] Can you identify one password candidate or failure pattern spanning many users?
- [ ] Can you distinguish legitimate centralized auth traffic from suspicious spray activity?
- [ ] Can you see whether a source is probing accounts across a long time window?
- [ ] Can you correlate failure spikes with VPN, SSO, or remote access logs?
- [ ] Can you identify dormant, disabled, or former employee accounts that are still reachable?
- [ ] Can you show whether MFA was present on the targeted auth path?

---

5) Exposure checks

- [ ] Review whether external authentication surfaces are minimized
- [ ] Identify legacy protocols or weak auth paths that are still enabled
- [ ] Confirm stale, orphaned, and inactive accounts are removed or disabled
- [ ] Review privileged accounts for additional protections
- [ ] Verify that password policy includes banned-password or weak-password protections where possible
- [ ] Confirm MFA is enforced for interactive and remote access where feasible
- [ ] Check whether lockout settings are balanced to avoid easy denial-of-service

---

6) Response and containment checks

- [ ] Define when a spray pattern becomes an incident
- [ ] Assign an owner for triage and escalation
- [ ] Create a review step for source reputation and geolocation context
- [ ] Confirm you can quickly identify affected accounts
- [ ] Confirm you can check whether any account succeeded after repeated failures
- [ ] Prepare a playbook for:
- [ ] Resetting credentials
- [ ] Forcing sign-out / token invalidation where supported
- [ ] Blocking or rate-limiting suspicious sources
- [ ] Reviewing privilege escalation paths
- [ ] Document when to disable exposed accounts or require MFA re-enrollment

---

7) Prevention controls to verify

- [ ] Strong password policy is enforced
- [ ] Known-bad or banned passwords are blocked
- [ ] MFA is enabled where feasible for user-facing auth
- [ ] Conditional access or equivalent risk-based controls are in place
- [ ] Legacy auth paths are reduced or removed
- [ ] Externally reachable sign-in surfaces are minimized
- [ ] Dormant accounts are cleaned up regularly
- [ ] Privileged accounts have stronger authentication requirements
- [ ] DNS and network telemetry can be correlated with identity activity

---

8) Quick decision guide

Use this simple decision rule during review:

- [ ] Low confidence: You only alert per account, cannot group by source, and cannot see timing patterns.
- [ ] Moderate confidence: You can correlate source and time, but exclusions are immature or incomplete.
- [ ] High confidence: You can detect broad failure patterns, distinguish expected automation, and confirm MFA or access controls reduce exposure.

---

9) Minimum operational standard

Before relying on your controls in production, confirm all of the following:

- [ ] Failed authentication logs are collected from relevant paths
- [ ] Detection can aggregate by source, account, and time window
- [ ] Known-good sources are documented and excluded carefully
- [ ] MFA coverage is enforced where possible
- [ ] Stale and inactive accounts are regularly removed
- [ ] Legacy auth exposure is reviewed and reduced
- [ ] Incident response steps are documented and tested

---

10) Notes and follow-up actions

Gaps discovered

- [ ] _____
- [ ] _____
- [ ] _____
- [ ] _____

Owners

- [ ] Detection engineering: _____
- [ ] Directory services: _____
- [ ] Identity / IAM: _____
- [ ] SOC / incident response: _____
- [ ] Network / perimeter: _____

Next review date

- [ ] _____

Final check

If you can answer yes to the following, you are in a stronger position against password spray attacks:

- [ ] Do we see broad failed authentication patterns across users, not just per-account failures?
- [ ] Do we know which sources are normal and which are suspicious?
- [ ] Can we confirm MFA or other controls reduce the impact of a guessed password?
- [ ] Can we remove or contain exposed accounts quickly enough to matter?
- [ ] Can we validate these controls before an attacker does?