CHECKLIST

Checklist: Detecting Active Directory Privilege Escalation Paths with BloodHound

A practical checklist for reviewing BloodHound findings, validating escalation paths, and prioritizing the risks that matter most in production Active Directory environments.

Checklist: Detecting Active Directory Privilege Escalation Paths with BloodHound

Use this checklist to review BloodHound findings in a way that is practical, current, and focused on real production risk.

---

1) Confirm the scope of the analysis

- [ ] Define which domain, forest, or business unit is in scope.
- [ ] Identify the collection window and when data was last refreshed.
- [ ] Confirm whether host session data, ACLs, group membership, and local admin relationships were included.
- [ ] Note any systems excluded from collection.
- [ ] Record the asset owners responsible for any affected users, groups, or hosts.

2) Focus on high-value targets first

- [ ] List Tier 0 or equivalent high-value assets.
- [ ] Identify domain admin, enterprise admin, privileged operator, and service account targets.
- [ ] Prioritize paths that end at systems or accounts with broad administrative reach.
- [ ] Separate business-critical paths from low-impact hardening issues.

3) Review the path type, not just the path length

- [ ] Determine whether the path uses group membership, local admin rights, ACL changes, delegation, or session access.
- [ ] Mark any path that depends on a privileged session on a server or workstation.
- [ ] Mark any path that includes rights to modify users, groups, computers, or service accounts.
- [ ] Flag direct control over privileged groups as higher risk than indirect or theoretical reach.

4) Validate each hop in the chain

For every edge in the path:

- [ ] Is the source account enabled and active?
- [ ] Is the destination object or host still in service?
- [ ] Is the relationship direct, inherited, or conditional?
- [ ] Is the permission actually usable from the source context?
- [ ] Is the edge based on current data or a potentially stale collection?

If any hop fails validation, note why and lower the confidence of the finding.

5) Check whether the path is operationally reachable

- [ ] Confirm whether network segmentation could block the chain.

- [ ] Check whether endpoint protections, access controls, or policy restrictions limit abuse.
- [ ] Determine whether the path requires interactive access, elevated credentials, or a one-time session.
- [ ] Assess whether the starting account could realistically reach the first host or object.
- [ ] Separate technically possible paths from probable attack paths.

6) Assess business impact

- [ ] Identify the final privilege boundary reached by the path.
- [ ] Determine whether the path leads to domain-wide control, local administrative control, or a narrower privilege.
- [ ] Estimate the blast radius if the path were used successfully.
- [ ] Map the affected systems to business functions.
- [ ] Rank the path based on exposure, criticality, and ease of use.

7) Look for common escalation ingredients

- [ ] Nested group membership crossing team boundaries.
- [ ] Local administrator rights on shared workstations or servers.
- [ ] Delegated rights to reset passwords or modify privileged objects.
- [ ] Permissions over service accounts or management groups.
- [ ] Misconfigured ACLs allowing write, ownership, or account control changes.
- [ ] Privileged sessions on systems that are accessible from lower-trust accounts.

8) Decide whether the path is real enough to act on

- [ ] Does the path rely on current, confirmed relationships?

- [ ] Is the chain short enough to be operationally meaningful?
- [ ] Does breaking one edge materially reduce attacker movement?
- [ ] Would the path be usable without unlikely assumptions?
- [ ] Is the risk high enough to justify change, not just documentation?

9) Assign remediation ownership

- [ ] Identify the owner for each object in the path.
- [ ] Separate directory administration issues from server administration issues.
- [ ] Route local admin problems to endpoint or infrastructure owners.
- [ ] Route group and ACL issues to directory service owners.
- [ ] Assign a due date based on risk and change complexity.

10) Choose the most effective remediation

- [ ] Remove unnecessary local administrator rights.
- [ ] Tighten delegation boundaries.
- [ ] Reduce or eliminate privileged sessions on shared hosts.
- [ ] Rework ACLs that allow privilege-bearing changes.
- [ ] Review service account permissions and ownership.
- [ ] Remove stale users, groups, and hosts from sensitive paths.

11) Re-test after changes

- [ ] Refresh BloodHound data after remediation.
- [ ] Confirm the path no longer exists or is no longer reachable.
- [ ] Verify that the fix did not create a new alternate path.
- [ ] Document the before-and-after state.

- [ ] Record any residual risk that remains.

12) Keep the analysis production-ready

- [ ] Use current data for every review cycle.
- [ ] Maintain a clean record of findings and owners.
- [ ] Separate confirmed paths from suspected paths.
- [ ] Track remediation progress over time.
- [ ] Reassess paths after major directory, host, or privilege changes.

Quick triage guide

Treat as urgent if the path:

- [ ] Reaches Tier 0 or domain-wide administrative control.
- [ ] Uses an active privileged session.
- [ ] Depends on direct control of a sensitive group or account.
- [ ] Can be used from a commonly reachable host.
- [ ] Has a clear, validated chain with little reliance on edge-case conditions.

Treat as medium priority if the path:

- [ ] Is valid but requires additional conditions to succeed.
- [ ] Reaches a limited administrative boundary.
- [ ] Depends on infrequently used or partially scoped access.
- [ ] Has business impact but not broad domain impact.

Treat as lower priority if the path:

- [ ] Relies on stale data or unconfirmed relationships.
- [ ] Ends at a low-impact system.
- [ ] Is blocked by current segmentation or policy controls.
- [ ] Requires assumptions that are unlikely in production.

One-page review record

Finding name: _____

Source account or object: _____

Path type: _____

Destination asset or privilege: _____

Collection date: _____

Validation status: ? Confirmed ? Partially confirmed ? Unconfirmed

Business impact: ? High ? Medium ? Low

Remediation owner: _____

Target fix date: _____

Notes:

- _____
- _____
- _____

Final review questions

- [ ] Does this path represent a real and current attack opportunity?
- [ ] Would an attacker be able to reach the first step from a realistic foothold?
- [ ] Does the path end at a meaningful privilege boundary?
- [ ] Is the remediation clear and owned?
- [ ] Have you re-tested after the fix?

Use this checklist to turn BloodHound output into operational decisions, not just graph observations. The goal is to identify the few paths that matter most, prove whether they are real, and remove the ones that create the greatest production risk.