CHECKLIST

Checklist: Detect Lateral Movement with Network Traffic Analysis

A practical, vendor-neutral checklist for detecting lateral movement using internal network traffic analysis, from prerequisites and baselining to validation and follow-up.

Checklist: Detect Lateral Movement with Network Traffic Analysis

Use this checklist to build a repeatable, operationally useful workflow for spotting lateral movement in internal network traffic.

---

1) Confirm you have enough telemetry

- [ ] Internal east-west visibility is available from at least one source:
- [ ] span port
- [ ] network tap
- [ ] flow records
- [ ] firewall logs
- [ ] NDR sensor
- [ ] Timestamps are synchronized across network, host, and identity data
- [ ] Asset inventory includes hostnames, IP ranges, roles, and critical segments

- [ ] You can map source and destination pairs over time
- [ ] You have a ticketing or case workflow for triage and follow-up

Stop-here-if checks

- [ ] You only collect north-south perimeter traffic
- [ ] Timestamps are unreliable across sources
- [ ] NAT prevents you from identifying the true source host
- [ ] Encryption leaves you with no useful metadata or flow records
- [ ] You cannot distinguish workstations, servers, and admin hosts

> If any stop-here-if condition is true, fix collection or enrichment first.

---

2) Validate basic visibility on a small segment

For a small internal segment, confirm you can answer these questions:

- [ ] Which host initiated the connection?
- [ ] Which internal host received it?
- [ ] What port, protocol, and session timing were used?
- [ ] Is the source a workstation, server, or admin host?
- [ ] Has this source-destination pair been seen before?
- [ ] You can answer at least 4 of 5 reliably
- [ ] If not, you have a plan to improve collection or enrichment

---

3) Build a baseline of normal internal traffic

Baseline collection

- [ ] Capture a representative period of internal traffic
- [ ] Include business hours
- [ ] Include maintenance windows
- [ ] Include at least one change cycle
- [ ] Group events by:
- [ ] source asset
- [ ] destination asset
- [ ] destination port
- [ ] protocol
- [ ] connection frequency

Baseline questions

- [ ] Which systems regularly talk to domain controllers?
- [ ] Which systems regularly talk to file servers?
- [ ] Which systems regularly talk to database servers?
- [ ] Which systems regularly talk to management tools?
- [ ] Which subnets initiate the most east-west connections?
- [ ] Which ports are common between specific roles?
- [ ] Which hosts communicate with only a small set of peers?

Baseline table

Source role	Common destinations	Common ports	Normal frequency

User endpoints	File server, DC, proxy	53, 88, 135, 445	Burst-based, office hours
Admin hosts	Servers, hypervisors	22, 3389, 5985	Low volume, predictable
App servers	DB, API, queue	1433, 3306, etc.	Stable, scheduled
Workstations	Peer workstations	Rare or none	Usually suspicious

Baseline validation

- [ ] Test random known-benign events against the baseline
- [ ] Confirm routine admin activity is not flagged as anomalous
- [ ] If benign activity looks suspicious, adjust the baseline window or asset labels
- [ ] Verify the baseline covered backups, patching, and maintenance

---

4) Identify likely lateral movement patterns

Look for behaviors that are unusual in your environment and plausible for internal pivoting.

- [ ] One source host touches many internal destinations in a short period
- [ ] A workstation connects to server-only ports on multiple hosts
- [ ] Rare remote management traffic comes from non-admin endpoints
- [ ] Authentication-heavy bursts occur to several systems after a compromise-like event
- [ ] Short-lived connections hit many ports on the same host
- [ ] Unusual access to file shares, admin shares, or remote shell services
- [ ] New source-destination pairs appear in segments that normally do not interact

Hypothesis checks

- [ ] Each pattern is role-aware, not just ?internal traffic = suspicious?
- [ ] Each pattern can be explained or disproven with benign testing
- [ ] Each pattern is likely to correlate with endpoint, auth, or identity context

Benign comparisons

Test your hypotheses against:

- [ ] patch-management jobs
- [ ] software deployment activity
- [ ] normal administrator sessions
- [ ] scheduled backup or inventory tasks
- [ ] Suspicious patterns are flagged
- [ ] Routine automation remains explainable
- [ ] False positives are manageable

---

5) Enrich traffic with context

For each suspicious flow or session, add:

- [ ] asset role
- [ ] asset ownership
- [ ] user logon activity near the event time
- [ ] administrative group membership
- [ ] known management jump hosts
- [ ] business function of the destination
- [ ] vulnerability exposure or recent changes

Context checks

- [ ] The source is clearly identified as workstation, server, or admin host
- [ ] The destination role is known
- [ ] Authorized exceptions are documented
- [ ] You can explain whether the source is permitted to access the destination in that way

Common enrichment issues

- [ ] hosts are only represented as IP addresses
- [ ] role labels are missing
- [ ] jump hosts are not identified
- [ ] directory or inventory integration is incomplete

> If enrichment is weak, fix labels before tightening detections.

---

6) Write practical detection rules or hunt queries

Start simple and explainable.

- [ ] Detect a non-admin host connecting to multiple internal systems in a short period
- [ ] Detect workstation access to server-only ports across several hosts
- [ ] Detect rare remote management from non-admin systems
- [ ] Detect unusual authentication bursts to multiple internal assets
- [ ] Detect internal port sweeps or scan-like connection patterns
- [ ] Detect first-time source-destination pairs in sensitive segments

Rule-writing checks

- [ ] Each rule has a clear purpose
- [ ] Each rule uses observable conditions

- [ ] Each rule includes a known-good exception path
- [ ] Each rule can be tuned without losing the original intent

Suggested fields to include

- [ ] source IP / host
- [ ] destination IP / host
- [ ] source role
- [ ] destination role
- [ ] port and protocol
- [ ] connection count
- [ ] time window
- [ ] first-seen indicator
- [ ] authentication or logon context
- [ ] management host exception list

---

7) Validate detections before production use

Validation workflow

- [ ] Compare the detection against benign admin activity
- [ ] Compare the detection against patching and backup traffic
- [ ] Compare the detection against software deployment events
- [ ] Compare the detection against known suspicious test cases, if allowed
- [ ] Confirm the rule explains why the event is unusual

Evidence to collect

- [ ] source and destination details
- [ ] timestamps and duration
- [ ] port and protocol
- [ ] role context
- [ ] authentication context
- [ ] first-seen / rarity information
- [ ] related endpoint or identity alerts

Validation outcome

- [ ] True positives are understandable
- [ ] False positives are documented
- [ ] Exceptions are justified
- [ ] Tuning changes are recorded

---

8) Triage alerts consistently

When a candidate event fires, confirm:

- [ ] Is the source authorized to access the destination?
- [ ] Is the source a workstation, server, or admin host?
- [ ] Is this a known jump host or management system?
- [ ] Is the timing consistent with normal operations?
- [ ] Do endpoint or identity logs show related suspicious activity?
- [ ] Is the pattern isolated or repeated across several hosts?

Triage decision guide

- [ ] benign and explainable
- [ ] suspicious but unconfirmed
- [ ] likely lateral movement
- [ ] confirmed incident requiring response

---

9) Tune and operationalize

- [ ] Review false positives regularly
- [ ] Adjust baselines after major environment changes
- [ ] Maintain a list of approved admin hosts and jump systems
- [ ] Update role labels when systems change function
- [ ] Track which detections produce the most useful findings
- [ ] Document tuning decisions and exception rationale

Operational readiness checks

- [ ] Analysts know how to interpret the alert
- [ ] Analysts know what evidence to request next
- [ ] Analysts know when to escalate to incident response
- [ ] Results are reportable to stakeholders

---

10) Final readiness checklist

Before using this workflow in production, confirm:

- [ ] east-west traffic visibility is sufficient
- [ ] timestamps are trustworthy
- [ ] asset roles are labeled well enough to support exceptions
- [ ] baseline coverage includes normal maintenance activity
- [ ] detection logic is explainable and testable
- [ ] enrichment reduces ambiguity
- [ ] validation demonstrates useful signal
- [ ] triage and follow-up are documented

Quick-use summary

If you only have time for the essentials, do these four things first:

- [ ] build a baseline of normal internal traffic
- [ ] look for role-mismatched pivots and rare management use
- [ ] enrich flows with asset and identity context
- [ ] validate against benign admin and maintenance activity

Goal: surface suspicious east-west traffic that deserves investigation without overwhelming analysts with noise.