NETWITNESS

Network Threat Hunting: A Six-Stage Funnel

A practical guide to investigating suspicious activity and building evidence-backed findings



Core Hunting Principles

Treat unusual activity as a lead, not proof of a threat

Assess suspicious patterns against asset roles, expected workflows, and supporting evidence before concluding that they are malicious.

Let new evidence reshape the hunt

A connection, domain, host, or account may reveal a new investigative path. Revisit earlier stages and expand the scope when warranted.

Stage 1

Define the Investigation Scope

Establish what you are investigating and what you can observe

- **Scope:** Hosts, identities, apps, and network segments.
- **Time:** Set fixed start and end points.
- **Telemetry:** Map available network, DNS, proxy, firewall, endpoint, and authentication data.
- **Gaps:** Record missing data and retention limits.

Practical check: Can the available evidence answer the hunt question? Missing telemetry is a limitation, not evidence that suspicious activity did not occur.

Stage 2

Establish Direction and Context

Determine who is communicating with whom

- **Inbound ↓:** Unexpected paths or administrative services?
- **Outbound ↑:** Unfamiliar external destinations?
- **Lateral ↔:** Access outside the system's expected role?

Practical check: Validate DMZ, cloud, VPN, and partner network boundaries before interpreting traffic direction.

Stage 3

Focus on Relevant Protocols

Use the hypothesis to decide which communications to examine

- **DNS:** Volume, failures, record types, and subdomain patterns.
- **HTTP:** Methods, destinations, paths, and uploads.
- **SMB:** Peer connections, share access, and transfers.

Practical check: Does the communication make sense for the host, application, and user involved?

Stage 4

Identify Behavioral Anomalies

Look for deviations from expected communication

- **Cadence:** Spikes or machine-like intervals.
- **Services:** Unexpected ports or protocols.
- **Destinations:** Rare or first-seen connections.
- **Flow:** Shifts in volume, timing, or direction.
- **Privilege:** Administrative activity from unusual systems.

Practical check: Could an approved application, scheduled task, maintenance window, or security test explain the behavior?

Stage 5

Correlate Specific Indicators

Connect suspicious behavior to concrete evidence

- **Artifacts:** Pivot on domains, IPs, files, paths, and hashes.
- **Intelligence:** Check relevant threat matches.
- **Correlation:** Link traffic to sign-ins and endpoint processes.
- **Expansion:** Find related destinations, identities, and artifacts.

Practical check: Do independent sources support the same explanation? A reputation match or an unfamiliar filename alone does not establish compromise.

Stage 6

Validate Evidence and Reconstruct the Activity

Establish what happened and what remains uncertain

- **Origin:** Identify the host, account, or process.
- **Connections:** Link related communications and actions.
- **Timeline:** Establish sequence and scope.
- **Alternatives:** Test legitimate explanations.
- **Confidence:** Separate facts from assumptions.

Practical check: Does the evidence support a malicious finding, a benign explanation, or further investigation? Document the supporting timeline, affected assets, confidence level, and unresolved gaps.

Measuring SOC Hunting Impact

The infographic identifies six metrics for measuring threat-hunting effectiveness.

Metric	Measurement focus
Hypothesis-to-validation time	Measure how quickly analysts can prove or disprove a hunt lead.
Evidence coverage	Measure how much critical attack evidence is evaluated, including network, endpoint, identity, and cloud telemetry.
Evidence coverage (environment focus)	Evaluate whether critical attack paths are visible across network, endpoint, identity, and cloud telemetry.
Time to scope	Track the speed of identifying all affected users, hosts, services, and data during an incident.
Detection conversion rate	Track how many hunt findings are converted into durable detection rules and playbooks.
Repeat exposure rate	Track whether identified attack paths, misconfigurations, or techniques recur.

Move from a scoped question to a supported decision, not from an unusual pattern to an assumed compromise.