



— SNARE · PLAYBOOK

The modern security logging & investigation playbook

From forensic-grade log collection to AI-assisted investigation: a practical guide to building a security evidence architecture that improves visibility, right-sizes SIEM costs and keeps critical evidence available when it matters.

From more telemetry to evidence you can trust

Security teams have access to more telemetry than ever, from endpoints, servers, identity systems, cloud platforms, applications, network infrastructure and security controls. The opportunity is to turn that telemetry into usable evidence: collected deliberately, protected from tampering and available the moment an investigation needs it.

That means deciding what evidence must be collected, how it is protected, what deserves premium analytics processing, what must be retained independently, and how analysts can interrogate it quickly during an incident.

Gartner describes log management as an important but undervalued tool for threat detection, investigation and response. Forrester has separately highlighted SIEM ingestion cost as a persistent challenge, and argues for data-pipeline approaches that reduce, route and manage telemetry before it reaches high-cost analytics platforms.

This playbook treats logging as a security evidence discipline, not a transport mechanism. It shows how a resilient collection, retention, routing and investigation layer can support the SIEM investments you already have, right-size ingestion, preserve historical evidence and give AI-assisted investigation a stronger foundation.

The question is no longer “How do we collect more logs?” It is “How do we build a security evidence architecture we can trust?”

INSIDE THIS PLAYBOOK

03 Foundations

Evidence, the data problem, the Security Evidence Chain and five decisions

08 Use cases

Ten security scenarios, from compromised credentials to missing telemetry

15 Economics and maturity

Data tiers, the maturity model and an architecture checklist

06 Architecture

Four deployment pathways and where Snare fits

14 AI-assisted investigation

AskSnare, and why AI still depends on evidence

17 Next steps

Industry guidance, bringing it together and assessing your architecture

Reference: [Gartner, Adopt Log Management for Security Operations Use Cases](#) (27 October 2025)

Reference: [Forrester, If You're Not Using Data Pipeline Management for Security and IT, You Need To](#) (12 November 2024)

Investigations are only as complete as the evidence behind them

When an incident occurs, security teams reconstruct what happened from evidence spread across operating systems, identity platforms, infrastructure, applications and security controls.

- ✓ Authentication and logon events
- ✓ Privilege and group membership changes
- ✓ Configuration and policy changes
- ✓ Application and cloud control-plane events
- ✓ Endpoint and process activity
- ✓ Network connections and remote services
- ✓ Administrative activity
- ✓ Security-control events and alerts

NIST defines a log as a record of events occurring within computing assets, and log management as generating, transmitting, storing, accessing and disposing of log data. It links log management directly to investigating cybersecurity incidents and keeping records for the required period.

Logs are not simply machine data. In an investigation, they are evidence.

Reference: [NIST SP 800-92 Rev. 1 \(initial public draft\)](#), Cybersecurity Log Management Planning Guide

02 · THE MODERN SECURITY DATA PROBLEM

More sources, more volume, more choices to make

Cloud adoption, SaaS, hybrid work, distributed infrastructure and expanding security tooling have increased both the number of sources and the volume of events security teams manage.

Endpoint & identity

Windows, Linux and macOS; authentication, directory and privilege events

Cloud & applications

Control-plane operations, SaaS, APIs, databases and business systems

Network & security

Firewalls, DNS, proxies, EDR/XDR, vulnerability and other security controls

The challenge has moved beyond collection

It is now about balancing visibility, cost, retention, performance and portability. The Australian Signals Directorate's event-logging guidance recommends filtering logs before they reach SIEM or XDR platforms, where that helps those platforms receive the most valuable data while minimising cost and capacity pressure.

Reference: [ASD ACSC, Best practices for event logging and threat detection](#) (August 2024)

Eight links from event to action

Every investigation relies on an unbroken chain. Each link is a design decision, and each one maps to a specific part of the Snare architecture.

1 Collect

Capture the security-relevant activity needed to detect, investigate and reconstruct events.

Snare: Snare Agent: Windows, Linux, macOS, plus syslog, NetFlow and cloud sources

2 Protect

Reduce the risk that an attacker can erase, alter or suppress the only copy of critical evidence.

Snare: TLS/mTLS transport, off-host retention and a hash-verified archive

3 Normalise

Represent events consistently for downstream search, correlation and analytics.

Snare: Snare Central normalises sources into one pipeline

4 Optimise

Filter, aggregate, de-duplicate or transform telemetry by security and economic value.

Snare: Agent filtering at source; Central aggregation and de-duplication

5 Route

Send the right data to the right SIEM, archive, MSSP or analytics destination.

Snare: Snare Reflector, with per-destination filtering and formatting

6 Retain

Keep historical evidence for as long as risk, regulation and policy require.

Snare: Snare Central multi-year archive, with object-storage archive tiers

7 Investigate

Make evidence searchable for incident response, threat hunting and forensics.

Snare: Central forensic search, 800+ reports, Event Replay and AskSnare

8 Act

Contain, remediate, escalate, tune controls or strengthen future detections.

Snare: Your SIEM, SOC and response tooling, fed with the evidence they need

A chain is only as strong as its weakest link

Detection depends on collection; investigation depends on retention; response depends on both. Designing the chain end to end means a gap at one stage does not quietly undermine every stage after it.

Decide what the evidence must do, then design for it

Settling these five decisions first keeps every technology choice that follows anchored to security outcomes.

1

What must we collect?

Start with the threats, assets and investigations that matter, then map those outcomes to the telemetry required to observe them.

With Snare: Agent policies and filtering set what is captured at each source.

2

What must enter the SIEM?

Separate evidence that must be collected from evidence that needs continuous premium analytics processing.

With Snare: Reflector sends each destination only the events its detections use.

3

What must we retain?

Define retention by investigation window, regulation, business risk and forensic need, not only by SIEM storage cost.

With Snare: Central retains the full record, independently of the SIEM.

4

Where can the data reside?

Account for on-premises, cloud, hybrid, sovereign, isolated and restricted environments.

With Snare: Four deployment pathways, including fully on-premises and separated zones.

5

How will we investigate?

Decide how SIEM search, retained logs, threat hunting and AI-assisted investigation work together.

With Snare: Central search, Event Replay and AskSnare complement the SIEM.

Design collection around detection and investigation goals

MITRE ATT&CK v18 introduced detection strategies that connect observable telemetry and data components to adversary techniques. They are a practical starting point for answering the first decision: which evidence each technique needs.

Reference: [MITRE ATT&CK, Detection Strategies](#)

Choice is part of the architecture

There is no single correct deployment model. Some teams need complete on-premises control; others run hybrid estates or want to add AI-assisted investigation. Every Snare pathway is built from the same Snare Agents, Snare Central and Snare Reflector, so you can start where you are and evolve.

PATHWAY 1

Fully on-premises

For environments that need local collection, management and retention with no dependency on cloud or AI.

- Snare Agents, syslog and NetFlow into Snare Central
- Archive retained inside your network
- Reflector routes to on-premises or cloud SIEMs

PATHWAY 2

On-premises + AskSnare

For teams that want to keep collection and retention on-premises and add AI-assisted investigation.

- Everything in pathway 1
- Reflector feeds selected security data to AskSnare
- Natural-language questions over retained evidence

PATHWAY 3

Unified on-prem + cloud

For mixed estates that need one collection and retention layer across on-premises and cloud.

- Adds Microsoft 365, Azure, AWS and Oracle Cloud sources
- Retrieves selected events from Splunk and Secureworks Taegis
- The widest context for AskSnare

PATHWAY 4

Hybrid / separated

For organisations that must keep protected zones isolated while modernising elsewhere.

- Separate Snare Central instances per zone
- Protected logs never leave their zone
- Connected zone can add cloud, SIEM retrieval and AskSnare

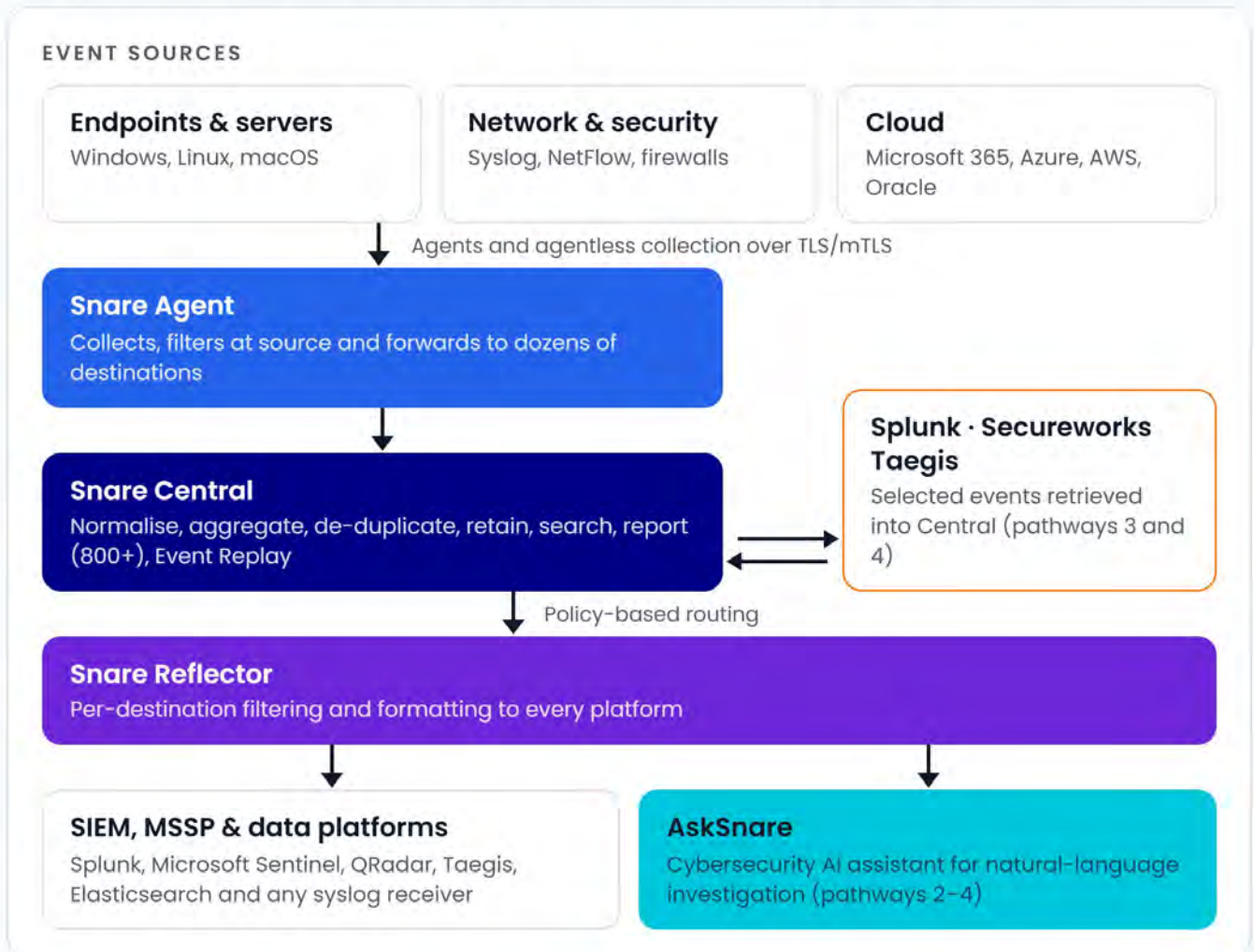
Keep data where it needs to live, and add capabilities where they create value.

The on-premises pathway remains a complete security architecture

Cloud and AI are additional options, not prerequisites for continuing to strengthen logging and evidence management. Existing customers can move between pathways as requirements change, without replacing collection.

An evidence layer between your sources and your analytics

Snare sits between event sources and downstream platforms, separating the collection and evidence layer from whichever analytics destination you use today.



Snare Agent

Collects security telemetry at the source.

Snare Central

Management, policy, retention and investigation.

Snare Reflector

Routes the right data to each destination.

AskSnare

AI-assisted investigation over security evidence.

Snare complements the SIEM. It makes the security data feeding it more controllable, portable and investigation-ready.

Ten use cases, mapped to the evidence lifecycle

Each use case that follows covers the security challenge, the evidence required, how the Snare architecture supports it, example investigation questions and the resulting operational value.

Use case	Collect	Retain	Optimise	Route	Investigate	AI assist	Page
01 Compromised credentials	✓	✓	✓	—	✓	✓	p. 09
02 Insider threat	✓	✓	✓	—	✓	✓	p. 09
03 Privilege escalation	✓	✓	✓	—	✓	✓	p. 10
04 Lateral movement	✓	✓	✓	—	✓	✓	p. 10
05 Ransomware investigation	✓	✓	✓	✓	✓	✓	p. 11
06 Threat hunting	✓	✓	—	—	✓	✓	p. 11
07 Compliance & forensics	✓	✓	—	✓	✓	—	p. 12
08 SIEM cost optimisation	✓	✓	✓	✓	—	—	p. 12
09 SIEM migration & portability	✓	✓	✓	✓	✓	—	p. 13
10 Missing telemetry	✓	✓	✓	—	✓	✓	p. 13

Collect: Snare Agent and agentless sources

Retain: Snare Central archive

Optimise: Agent filtering, Central aggregation

Route: Snare Reflector

Investigate: Central search, reports, Event Replay

AI assist: AskSnare (pathways 2–4)

Read the use cases as a set

Most investigations touch several stages at once. A credential compromise becomes lateral movement, which becomes a ransomware investigation. The same evidence layer supports all of them, which is why it pays to design it once and well.

Compromised credentials and abnormal authentication

Valid credentials make malicious activity look legitimate. The challenge is recognising authentication that is unusual for the account, system, location or surrounding activity, and linking it to what happened next.

EVIDENCE REQUIRED

- Authentication successes and failures
- Account and group changes
- Privileged logon events
- Process creation and commands
- Endpoint and server security events

HOW SNARE SUPPORTS IT

Snare Agent captures Windows, Linux and macOS security events and filters at source. Snare Central retains them off-host and makes them searchable; Snare Reflector routes the detections-relevant subset to the SIEM and feeds AskSnare, so analysts can interrogate the evidence without starting every investigation with a complex query.

ASK THE EVIDENCE

"Show failed logins followed by a successful privileged login for the same account in the last 24 hours."

"Which accounts accessed systems they have not used before?"

"Build a timeline for this account across the affected systems."

- ✓ Faster validation of suspected compromise
- ✓ Authentication correlated with endpoint behaviour
- ✓ Clearer reconstruction after access is gained

Reference: [MITRE ATT&CK, Logon Session Creation \(DC0067\)](#)

Insider threat and unusual user behaviour

Insiders already have authorised access, so a single event is rarely suspicious on its own. Investigations depend on changes in behaviour and on activity that differs from a user's role or history.

EVIDENCE REQUIRED

- Authentication and sessions
- Privileged or administrative actions
- File and application access
- Removable-media events where available
- Process and command execution

HOW SNARE SUPPORTS IT

By retaining detailed endpoint and system activity in Snare Central, Snare preserves the history needed to compare current behaviour with past behaviour. AskSnare helps analysts pose exploratory questions and narrow the investigation step by step.

ASK THE EVIDENCE

"Show unusual administrative activity for this user in the last seven days."

"Has this account accessed resources it has not used before?"

"Show privilege changes followed by unusual file access or commands."

- ✓ More context around legitimate-but-risky activity
- ✓ Faster prioritisation for human review
- ✓ Historical evidence for internal investigations

Privilege escalation and privileged account abuse

Attackers seek elevated privileges soon after initial access. Detecting it needs visibility of account changes, elevated sessions, service creation, admin tools and follow-on execution, often across several hosts.

EVIDENCE REQUIRED

- Group membership and role changes
- Privilege assignment and privileged logons
- Service and scheduled-task creation
- Process creation
- Security-policy changes

HOW SNARE SUPPORTS IT

Snare provides the operating-system evidence that links initial access to elevated execution. Snare Central retains it off-host in a hash-verified archive, so the investigation does not depend on the compromised machine. AskSnare helps correlate privilege changes with the sessions and processes that followed.

ASK THE EVIDENCE

"Show accounts added to privileged groups in the last 48 hours."

"Which privilege changes were followed by remote access or process execution?"

"Show services or scheduled tasks created by newly privileged accounts."

✓ Earlier visibility of attacker progression

✓ Better evidence for containment decisions

✓ Complete privilege-abuse timelines

Lateral movement across the environment

Once attackers have a foothold, lateral movement exposes more systems, credentials and data. Living-off-the-land techniques can look like normal administration, so defenders need detailed histories correlated across hosts.

EVIDENCE REQUIRED

- Authentication events
- RDP, SMB and remote-service activity
- PowerShell and command execution
- Process creation
- Remote-administration events

HOW SNARE SUPPORTS IT

Snare preserves host-level evidence across the estate, so analysts are not limited to a single endpoint view. Retained logs in Snare Central can be searched alongside SIEM detections, and AskSnare helps trace a user or host across many systems.

ASK THE EVIDENCE

"Show systems accessed by this account after the suspected compromise."

"Identify remote administrative activity originating from this endpoint."

"Build a timeline of authentication and process activity across these systems."

✓ Faster incident scoping

✓ Better identification of affected systems

✓ Stronger evidence for containment and eradication

Reference: [ASD ACSC, Best practices for event logging and threat detection](#) (living-off-the-land and lateral movement detection)

05

USE CASE 05

Ransomware and post-compromise investigation

Ransomware is an outcome, not the start of the incident. Investigators must reconstruct what came before encryption: initial access, execution, privilege escalation, discovery, lateral movement, persistence and possible exfiltration.

EVIDENCE REQUIRED

- Authentication and identity events
- Process and command execution
- Privilege changes
- Remote-service activity
- File, system and policy events

HOW SNARE SUPPORTS IT

Snare Central retains historical evidence outside the compromised endpoints, often beyond the SIEM's retention window, so the full sequence can be reconstructed. Event Replay can return that history to Splunk or Sentinel, and AskSnare helps build a cross-system timeline.

ASK THE EVIDENCE

"What happened on this endpoint before the encryption event?"
"Which other systems show the same sequence of behaviour?"
"Summarise the timeline from initial access to encryption."

- ✓ Faster incident reconstruction
- ✓ More accurate scope assessment
- ✓ Evidence that pre-dates the SIEM window

Reference: [Mandiant M-Trends 2026](#) (global median dwell time rose to 14 days in 2025 investigations)

06

USE CASE 06

Proactive threat hunting across historical logs

Monitoring asks whether a rule has fired. Threat hunting asks what may be happening that no rule has recognised yet, which needs accessible historical telemetry and the ability to search for behaviour, not just known indicators.

EVIDENCE REQUIRED

- Historical endpoint and server events
- Authentication activity
- Process and command execution
- Administrative activity
- Network-relevant OS events

HOW SNARE SUPPORTS IT

Retained evidence in Snare Central supports hypothesis-driven hunting whether or not an alert fired at the time. Event Replay can send a historical slice back into Splunk or Sentinel for analysis with existing content, and AskSnare lets analysts start with a question and refine it.

ASK THE EVIDENCE

"Show PowerShell activity that is unusual for each endpoint."
"Find sequences of failed logons, privilege change and remote execution."
"Which hosts exhibit similar suspicious behaviours?"

- ✓ Find activity that never raised an alert
- ✓ Faster hunting iterations
- ✓ Better use of retained history

Compliance, audit and forensic evidence

Security logging must do more than real-time detection. Organisations may need historical records for compliance, audits, internal investigations, incident response, legal processes and cyber-insurance requirements.

EVIDENCE REQUIRED

- User and system activity for each control
- Administrative and privileged actions
- Configuration and policy changes
- Authentication and access records
- Logs retained for the required period

HOW SNARE SUPPORTS IT

Snare's forensic logging heritage supports collection and multi-year retention independent of the analytics platform, with hash verification on archive. More than 800 pre-built reports cover frameworks such as PCI DSS, ISO 27001 and HIPAA, so an expired SIEM retention window does not become an evidence gap.

ASK THE EVIDENCE

"Show all privileged changes on these systems during the audit period."

"Retrieve the security events for this incident date range."

"Show the sequence of administrative actions for this account."

- ✓ Evidence ready for audits and investigations
- ✓ Retention decoupled from SIEM economics
- ✓ Less reliance on evidence left on endpoints

Reference: [NIST SP 800-92 Rev. 1 \(initial public draft\)](#)

Right-sizing SIEM ingestion and storage costs

Ingest-based pricing makes "send everything to the SIEM" hard to sustain, yet discarding data at the source can leave investigation gaps. The architectural answer is to separate collection from destination.

EVIDENCE REQUIRED

- Full-fidelity record of collected events
- Detection requirements per platform
- Event volumes by source and type
- Retention requirements by data class
- Format needs of each destination

HOW SNARE SUPPORTS IT

Snare acts as the control layer before the SIEM. Snare Agent filters at source; Snare Central aggregates and de-duplicates while keeping the full record; Snare Reflector applies per-destination filtering and formats events for each platform. You keep the evidence and pay premium rates only for what detections use.

ASK THE EVIDENCE

"Which sources contribute the most SIEM volume?"

"Which event types are never used by a detection?"

"What would retention cost outside the SIEM?"

- ✓ Lower premium ingestion
- ✓ Evidence preserved, not discarded
- ✓ Predictable growth as sources increase

Reference: [Forrester, data pipeline management for security and IT](#) and ASD ACSC guidance on filtering before SIEM/XDR.

Changing SIEM without rebuilding log collection

Organisations consolidate vendors, adopt cloud SIEM, change MSSPs, merge environments or run several analytics platforms at once. The logging layer should not turn every analytics decision into a collection project.

EVIDENCE REQUIRED

- Consistent collection across all sources
- Destination-specific formats
- Parallel delivery during transition
- Historical data for the new platform
- Per-tenant routing for MSSPs

HOW SNARE SUPPORTS IT

Snare Agent can send to dozens of destinations, and Snare Reflector routes each event set to the right platform, so old and new SIEMs can run in parallel during migration. Event Replay can seed the new platform with history, and Central retains everything regardless of destination.

ASK THE EVIDENCE

"Today: Snare → existing SIEM"

"Transition: Snare → existing SIEM + new SIEM"

"Future: Snare → new SIEM, or customer + MSSP platforms"

- ✓ Change the destination, not the collection
- ✓ Lower-risk parallel running
- ✓ Freedom to choose analytics on merit

Finding gaps in visibility and missing telemetry

An often-overlooked risk is missing telemetry. An agent can stop reporting, logging can be disabled, configuration can drift, a new system can appear outside policy, or a source can suddenly send far fewer events.

EVIDENCE REQUIRED

- Expected host and source inventory
- Event-flow and volume history
- Logging-service and config events
- Agent and collector health
- Log-clearing attempts (ATT&CK T1070)

HOW SNARE SUPPORTS IT

Snare monitors the evidence pipeline itself. Snare Agent Manager flags agents that go offline, and Snare Central can alert when a source's event volume deviates from its normal pattern, with tunable sensitivity. Activity around logging changes is preserved, and AskSnare can answer which sources stopped reporting.

ASK THE EVIDENCE

"Which systems stopped sending security logs in the last six hours?"

"Which sources are sending materially less telemetry than normal?"

"Show activity around the time logging stopped on this host."

- ✓ Faster detection of blind spots
- ✓ Less risk of silent logging failure
- ✓ Assurance that analytics see expected data

Reference: MITRE ATT&CK, Indicator Removal (T1070)

AskSnare: from a security question to the evidence that answers it

The value of AI in investigation is reducing friction between an analyst's question and the evidence that answers it, so they can move from a broad question to specific steps without starting over.

AN INVESTIGATION AS A CONVERSATION

- 1 Show failed logins followed by successful privileged authentication in the last 24 hours.
- 2 Which of those accounts have never logged into those systems before?
- 3 Show process activity from those sessions.
- 4 Which behaviour is unusual compared with prior activity?
- 5 Summarise the evidence and the investigation timeline.

Fed by Snare Reflector

Reflector sends AskSnare the security data you choose in pathways 2–4. AskSnare can also take in Kafka and Kinesis streams.

More collection, more context

In pathways 3 and 4, Central retrieves selected Splunk and Taegis events, the first of many SIEMs, giving AskSnare more to interrogate.

Analysts stay in control

AskSnare is a cybersecurity AI assistant. It helps analysts ask, refine and summarise; judgement stays with your team.

The goal is not to replace analyst judgement. It is to make evidence easier to interrogate, correlate and explain.

WHY AI STILL DEPENDS ON EVIDENCE

Good security AI starts with good security telemetry

AI makes the quality and availability of telemetry more important, not less. Assistants can only reason over what has been captured, retained and made available to them.

MIT Lincoln Laboratory research published in March 2026 examined automated analysis of large-scale host-based logs, reducing hundreds of raw fields into informative dimensions to surface coordinated deviations not obvious in individual log streams. Scalable analytics depend on rich, well-structured telemetry.

Reference: [Schofield, Jananthan and Kepner, AI for Scalable Defensive Cyber Log Analysis, MIT Lincoln Laboratory \(20 March 2026\)](#)

Separate analytics needs from retention needs

A sustainable strategy treats security data by how urgently it must be queried, how often it is used and how long it must remain available.

Tier	Primary purpose	Typical destination	With Snare	Retention
HOT	Immediate detection and active investigation	SIEM or high-performance analytics	Reflector sends each SIEM the events its detections need	Hours to weeks
WARM	Investigation context not queried continuously	Searchable lower-cost repository	Snare Central archive on local or SAN storage, searchable and reportable	Weeks to months
HISTORICAL	Forensic, audit or long-range evidence	Economical retained storage	Central archive tiers on Amazon S3, Oracle Object Storage or Azure Blob; Event Replay when needed	Months to years

ASD ACSC guidance similarly distinguishes readily searchable “hot” data from more economical “cold” storage, weighing capacity against forensic value. Object storage suits archive tiers; local or SAN storage is recommended for active, frequently searched data.

Reference: [ASD ACSC, Best practices for event logging and threat detection](#)

10 · SECURITY LOGGING MATURITY MODEL

Five levels, from collecting to intelligent investigation

1 · Collect

Security events are captured from key systems.

Outcome: A baseline, often with evidence gaps and source-by-source administration.

2 · Control

Policies, collection and retention are centrally managed.

Outcome: Greater reliability, governance and integrity.

3 · Optimise

Telemetry is filtered, de-duplicated, remapped and routed intentionally.

Outcome: Lower downstream cost and better signal quality.

4 · Investigate

Historical evidence supports hunting, search and attack reconstruction.

Outcome: Faster incident response and stronger forensics.

5 · Intelligent

AI helps analysts ask, refine and summarise investigations.

Outcome: Less investigation friction and wider access to evidence.

The questions to ask in your next working session

Work through it with security operations, infrastructure, architecture and risk teams. Unticked boxes are not a failure: each one points to a specific link in the Security Evidence Chain, and most can be closed without replacing the tools you already rely on.

Collection

- ☐ Do we know which security events are collected?
- ☐ Have we mapped key threat techniques to the telemetry needed to investigate them?
- ☐ Are endpoint, identity, server, infrastructure and cloud sources covered?
- ☐ Do we know which critical systems are not logging?

Integrity

- ☐ Are logs protected from unauthorised modification or deletion?
- ☐ Could an attacker erase the only copy of evidence by compromising an endpoint?
- ☐ Are access and admin actions on the logging environment auditable?

Retention

- ☐ Are retention periods set by investigation and regulatory needs?
- ☐ Can investigators retrieve evidence from the likely dwell-time window?
- ☐ Can evidence be retained independently of premium SIEM storage?

SIEM optimisation

- ☐ Does every collected event need to enter the SIEM?
- ☐ Can unnecessary or duplicate events be reduced before ingestion?
- ☐ Can different event sets go to different destinations?
- ☐ Can events be reformatted for each downstream platform?

Portability

- ☐ Can we change SIEM without replacing endpoint collection?
- ☐ Can we send telemetry to several platforms during migration?
- ☐ Can we support on-premises, hybrid and cloud destinations?

Investigation

- ☐ Can analysts search historical logs?
- ☐ Can they reconstruct a cross-system attack timeline?
- ☐ Can they hunt proactively rather than wait for alerts?
- ☐ Can AI help analysts interrogate evidence in natural language?

Independent guidance points in the same direction

These sources are cited as independent evidence of the industry challenge. They are not endorsements of Snare.

Gartner

Log management is important but often undervalued when planning threat detection, investigation and response operations.

[Adopt Log Management for Security Operations Use Cases \(27 Oct 2025\)](#)

Forrester

SIEM ingestion is expensive, and security data-pipeline management can help control what reaches high-cost analytics platforms.

[If You're Not Using Data Pipeline Management for Security and IT, You Need To \(12 Nov 2024\)](#)

NIST

Log management spans generation, transmission, storage, access and disposal, and supports both investigation and required retention.

[SP 800-92 Rev. 1 \(initial public draft\), Cybersecurity Log Management Planning Guide](#)

MIT Lincoln Laboratory

Large-scale host telemetry can support automated, interpretable analysis when it is structured and reduced into informative dimensions.

[AI for Scalable Defensive Cyber Log Analysis \(20 Mar 2026\)](#)

MITRE ATT&CK

Detection strategies map adversary techniques to observable telemetry, reinforcing the need to design collection around detection and investigation goals.

[ATT&CK Detection Strategies](#)

ASD ACSC and international partners

Effective logging centralises access, protects integrity, supports relevant detections and considers filtering before SIEM/XDR to manage cost and capacity.

[Best practices for event logging and threat detection \(22 Aug 2024\)](#)

Mandiant / Google Cloud

M-Trends 2026 reported a 14-day global median dwell time in 2025 investigations, up from 11 days, highlighting why historical evidence still matters after initial compromise.

[M-Trends 2026 \(March 2026\)](#)

One requirement stays constant: reliable evidence

SIEM platforms will evolve, organisations will change vendors and operating models, AI will become part of everyday investigation, and threat actors will keep adapting. Through all of it, security teams need evidence they can rely on.

Collect once

Protect the evidence

Control what goes where

Retain what matters

Route to any platform

Investigate when needed

Use AI to find insight faster

Modern logging should not simply “send logs to the SIEM”. It should maintain a security evidence architecture that stays useful when the SIEM changes, the investigation starts late, a system has been compromised, or analysts need to ask questions nobody anticipated when the data was first collected.

14 · ASSESS YOUR SECURITY EVIDENCE ARCHITECTURE

Six steps to a clear picture

Establish where evidence is generated, how it is protected and routed, what it costs to analyse, how long it is kept and how quickly analysts can interrogate it.

1 Map your current logging architecture

Sources, collectors, destinations and owners.

2 Identify evidence gaps and high-risk sources

Where collection, integrity or retention fall short.

3 Review what enters the SIEM and why

Volume by source against detection use.

4 Model retention and ingestion economics

Hot, warm and historical tiers.

5 Assess portability across SIEM and MSSP

How hard it would be to change destination.

6 Find where AskSnare can accelerate investigations

The questions analysts ask most.

Start with your logging architecture, not another security tool. Our team can run the assessment with you.

Sources cited in this playbook

Independent research and guidance referenced throughout. These sources describe the industry challenge and are not endorsements of Snare.

Gartner	Adopt Log Management for Security Operations Use Cases 27 October 2025 https://www.gartner.com/en/documents/7114630
Forrester	If You're Not Using Data Pipeline Management for Security and IT, You Need To 12 November 2024 https://www.forrester.com/blogs/if-youre-not-using-data-pipeline-management-dpm-for-security-and-it-you-need-to/
NIST	SP 800-92 Rev. 1 (initial public draft): Cybersecurity Log Management Planning Guide 11 October 2023 https://csrc.nist.gov/pubs/sp/800/92/r1/ipd
MIT Lincoln Laboratory	Schofield, Jananthan and Kepner, AI for Scalable Defensive Cyber Log Analysis 20 March 2026 https://dspace.mit.edu/entities/publication/3d929315-2e73-4929-9a48-6ec1ddb2ddc7
MITRE ATT&CK	Detection Strategies; Logon Session Creation (DC0067); Indicator Removal (TI070) Current framework https://attack.mitre.org/detectionstrategies/
ASD Australian Cyber Security Centre	Best practices for event logging and threat detection 22 August 2024 https://www.cyber.gov.au/business-government/detecting-responding-to-threats/event-logging/best-practices-for-event-logging-and-threat-detection
Mandiant / Google Cloud	M-Trends 2026: Data, Insights, and Strategies From the Frontlines March 2026 https://cloud.google.com/security/resources/m-trends-executive-edition

About the Snare figures in this playbook

Capabilities described here reflect the current Snare release. Deployment pathway availability, supported platforms and destinations vary by configuration; please check the Snare support matrix or speak with our team for your environment.

Start with the evidence. Build from there.

Snare gives security teams a collection, retention and routing layer that stays useful when the SIEM changes, an investigation starts late or analysts need to ask questions nobody anticipated.

- ✓ **Collect once**
Snare Agents for Windows, Linux and macOS, plus syslog, NetFlow and cloud sources.
- ✓ **Protect the evidence**
TLS/mTLS transport and a hash-verified archive, retained off-host.
- ✓ **Route to any platform**
Dozens of destinations, so the SIEM can change without re-collecting.
- ✓ **Investigate faster**
Forensic search, 800+ reports, Event Replay and AskSnare.

NEXT STEPS

Assess your security evidence architecture

Book a technical session with our team to map your sources, retention requirements, SIEM destinations and the deployment pathway that fits your environment.

snareolutions.com