



A SNARE SOLUTIONS RESOURCE

The Security Evidence Coverage Map

Know what evidence exists, where it exists, how long it exists and whether an investigator can use it, across endpoint, identity, SaaS, cloud, third parties and AI agents.

A practical worksheet for SOC leads, security architects and CISOs.

BEFORE YOU START

Map the evidence, not the tools

Attackers now operate wherever a trusted identity can reach: SaaS applications, cloud control planes, supplier platforms and AI agents, as well as endpoints and servers. This map shows whether your evidence has kept up.

The objective isn't to get every box into the SIEM. It is to answer four questions for every evidence source an investigation might need:

What exists?	Where?	How long?	Usable?
Is the source collected at all, at the depth an investigation needs?	Which platform holds it, and who can reach it during an incident?	What is its retention, and is that the default or a decision?	Can it be searched quickly and joined to the rest of the chain?

How to use this map

Allow 60 to 90 minutes for a first pass. Bring the owners of your SOC, identity, cloud, IT operations and supplier relationships.

- 1 Fill in the map (page 3).** One row per evidence plane. Use the prompts on pages 4 to 6 to list the actual sources behind each row.
- 2 Run the chain test (page 7).** Take one investigation chain and mark which plane holds evidence for each link. This is where gaps between planes show up.
- 3 Test one supplier (page 8).** Request 30 days of your audit logs from your most critical SaaS or identity provider, and record what you got and how quickly.
- 4 Score and prioritise (page 9).** Count your gaps, find your shortest retention horizon, and turn each gap into a decision with an owner.

Rating key

Use the same four marks in every cell of the map and the chain test.

Covered Collected, retained long enough, searchable and joinable.	Partial Exists, but incomplete, short-lived, slow to retrieve or hard to join.	Gap Not collected, already expired, or not accessible to investigators.	? Unknown Nobody in the room can say. Count it as a gap.
---	--	---	---

The investigation chain used throughout this map

identity → device → access → privilege → action → destination → outcome

In an identity-led attack each link can sit in a different evidence plane, and the investigation stops at the first link you can't reach or join.

STEP 1

The Security Evidence Coverage Map

Mark each cell ● ◐ ○ ? · Organisation: _____ Date: _____

Evidence source	Collected? At investigation depth, not just alerts	Retention Days kept · default or decided?	Searchable? Time to retrieve 60-day-old events	SIEM? Ingested, routed on demand, or not	Investigation owner Who retrieves it during an incident	Gap What's missing, in one line
Endpoint Workstations, laptops, VDI						
Server Domain controllers, file, application, database and hypervisor hosts						
Identity Identity provider, Active Directory, MFA, PAM						
SaaS Productivity, CRM, collaboration and ITSM platforms						
Cloud Control plane and data plane, every account and subscription						
Network Firewall, VPN, proxy, DNS, NAT and DHCP						
Security platforms EDR, email security, backup and RMM consoles, the SIEM itself						
Third parties Critical SaaS providers, MSPs and MSSPs, software suppliers						
AI / agent activity AI agents, automation, service accounts, OAuth apps						

STEP 1 · PROMPTS

What to look for in each evidence plane

For each plane: the sources to list, the evidence to check for, the join keys that connect it to the rest of the chain, and the gap most often found during an investigation.

Endpoint		HOST EVIDENCE
INCLUDE Workstations, laptops and VDI pools, including devices that are only sometimes on the corporate network.	CHECK FOR Logons 4624 / 4625 , explicit credentials 4648 , process creation with command line 4688 , services 7045 , scheduled tasks 4698 , audit policy change 4719 , log cleared 1102 .	
JOIN KEYS SID, logon ID, hostname, source IP, device ID shared with the identity provider.	COMMON GAP Command-line auditing not enabled. Local logs overwritten before collection on devices that are often offline.	

Server		HOST EVIDENCE
INCLUDE Domain controllers, file, application and database servers, hypervisor hosts, Linux and Unix systems.	CHECK FOR Kerberos 4768 / 4769 , special privileges 4672 , account and group changes 4720 / 4728 / 4732 , share access 5140 / 5145 ; Linux auth and auditd.	
JOIN KEYS SID, hostname, service account names, the IP-to-host mapping for each server.	COMMON GAP Busy domain controllers rolling the Security log over within hours. Linux and appliance logs not collected at all.	

Identity		WHO AUTHENTICATED, AND HOW
INCLUDE Every identity provider (for example Entra ID or Okta), on-premises Active Directory, MFA services, privileged access management.	CHECK FOR Interactive, non-interactive and service principal sign-ins; authentication protocol (including device code); MFA registration changes; Conditional Access results; consent grants; role changes.	
JOIN KEYS Object ID, UPN, the onPremisesSecurityIdentifier that maps cloud identities to AD SIDs, session and correlation IDs.	COMMON GAP Non-interactive and service principal sign-ins not exported. Default retention of 7 or 30 days. Upgrading the licence doesn't recover expired data.	

STEP 1 · PROMPTS

SaaS		WHAT HAPPENED INSIDE THE APPLICATION	
INCLUDE	Microsoft 365 or Google Workspace, CRM, collaboration, file sharing, ITSM and HR platforms. List every application that holds sensitive data.	CHECK FOR	Admin actions, permission and sharing changes, new OAuth app connections, mailbox and file access, bulk download or export, API activity.
JOIN KEYS	Application user ID mapped to the identity provider, session ID, client IP, OAuth app ID.	COMMON GAP	Audit depth tied to licence tier. A different schema in every application. Applications not federated to the identity provider.

Cloud		CONTROL PLANE AND DATA PLANE	
INCLUDE	Every AWS account, Azure subscription and Google Cloud project, including development and acquired environments.	CHECK FOR	Control plane: role assignments, key and secret creation, policy changes. Data plane: object reads, secret retrieval, storage access. Workload and serverless identities.
JOIN KEYS	Principal ARN or object ID, request ID, caller IP, the session issuer and source identity on assumed roles.	COMMON GAP	Data-plane logging off by default (for example S3 data events, Azure resource logs). Accounts that sit outside the organisation-wide trail.

Network		PATHS AND TRANSLATIONS	
INCLUDE	Firewalls, VPN concentrators, web proxies, DNS resolvers, NAT gateways, DHCP servers, network detection tools.	CHECK FOR	VPN authentication, outbound volume by destination, DNS queries, east-west flows, NAT translations, DHCP leases.
JOIN KEYS	Source IP plus time, NAT translation, DHCP lease to device, VPN or proxy user mapping.	COMMON GAP	NAT and DHCP records not kept, so an IP address can't be tied back to a device or user weeks later.

STEP 1 · PROMPTS

Security platforms		THE TOOLS' OWN RECORDS	
INCLUDE EDR, email security, CASB, identity protection, backup and hypervisor consoles, RMM tools, the SIEM itself.		CHECK FOR Alerts and their context, tamper and status changes, admin console logins, policy and exclusion changes.	
JOIN KEYS Device ID, user, alert ID, console account.		COMMON GAP Console audit logs kept only inside each vendor platform, so they're reachable only through that one platform during an incident.	

Third parties		EVIDENCE YOU DON'T HOLD	
INCLUDE Critical SaaS providers, identity platforms, MSPs and MSSPs, payment and CRM providers, software suppliers with access.		CHECK FOR Which logs are exposed to you and which stay with the provider; retention; export API and format; incident evidence clauses in the contract.	
JOIN KEYS Provider tenant and user IDs, mapped to your own identities; timestamps in UTC.		COMMON GAP No contractual right to provider-side logs, and no tested way to get them quickly. Step 3 on page 8 tests this.	

AI / agent activity		NON-HUMAN IDENTITIES	
INCLUDE AI agents and assistants with tool access, automation, service accounts, OAuth applications, integrations.		CHECK FOR The agent's own sign-ins, tool and API calls, permission changes, approvals, and the user or process it acted for.	
JOIN KEYS Agent or workload identity ID, on-behalf-of user, shared correlation ID across steps.		COMMON GAP Agents acting under a borrowed human credential, so their actions can't be separated from the person's.	

Tip: If a row has more than one source (for example two identity providers or three cloud providers), mark the row with the worst result and note the weakest source in the Gap column.

STEP 2

The chain test: where would the investigation break?

Pick one scenario, for example *a privileged account was phished 60 days ago and used to reach a SaaS application and a cloud subscription*. For each link, mark every plane that holds evidence for it (● ○ ?). Then circle the first link where no plane is marked ●. That is where this investigation would stop.

Link in the chain	Endpoint / server	Identity	SaaS	Cloud	Network	Third party	AI / agent	Can you join this link to the previous one?
Identity Which identity, under every name it has	☐	☐	☐	☐	☐	☐	☐	Start of chain
Device Which device or client	☐	☐	☐	☐	☐	☐	☐	
Access How it authenticated, from where	☐	☐	☐	☐	☐	☐	☐	
Privilege What it could do, and changes to that	☐	☐	☐	☐	☐	☐	☐	
Action What it did	☐	☐	☐	☐	☐	☐	☐	
Destination Which system or data it reached	☐	☐	☐	☐	☐	☐	☐	
Outcome What changed or left	☐	☐	☐	☐	☐	☐	☐	

Scenario tested: _____ First link with no ●: _____

STEP 3

Test one supplier evidence request

Choose the provider an attacker would most want to reach. Ask for 30 days of administrative and authentication activity for one privileged account, the way you would during an incident, and record what happens. Add a second and third provider if time allows.

Question	Provider 1	Provider 2	Provider 3
Provider and service			
Audit logs available to you Which events, at which licence tier			
Default retention And the cost of extending it			
Export method and format Console, API, streaming; JSON, CSV			
Time to first record			
Time to all 30 days			
Does it join to your evidence? UTC timestamps, user IDs, source IPs			
Provider-side logs you can't export And how you would obtain them			
Contract covers incident evidence? Access, timeframe, retention			
Overall mark ● ● ○ ?			

Anything you couldn't get, couldn't get quickly or couldn't join is part of your evidence gap, now outside your own boundary. Carry the result into the **Third parties** row of the map.

STEP 4

Score it, then decide

Count the marks on the map (page 3)

● Covered

◐ Partial

○ Gap

? Unknown
 Add to Gap

Your shortest retention horizon: _____ days, in _____

A correlated investigation can only go back as far as the shortest retention among the planes it depends on.

Fix in this order

1. **Gaps that break the identity join.** If you can't prove two records belong to the same identity, nothing after that point holds together.
2. **The shortest retention horizon** on a high-value chain, especially identity evidence that expires before the cloud or SaaS evidence it explains.
3. **Data-plane logging that is switched off**, where the control plane shows access was granted but nothing shows what was read.
4. **Third-party evidence with no tested or contractual route** to obtain it.
5. **Evidence reachable only through one platform**, so an investigation depends on a single console or a single SIEM.

Turn each gap into a decision

Gap	Link it breaks	Decision	Owner	Due
		Collect · retain · route · join · contract		

REFERENCE

Default retention to check first

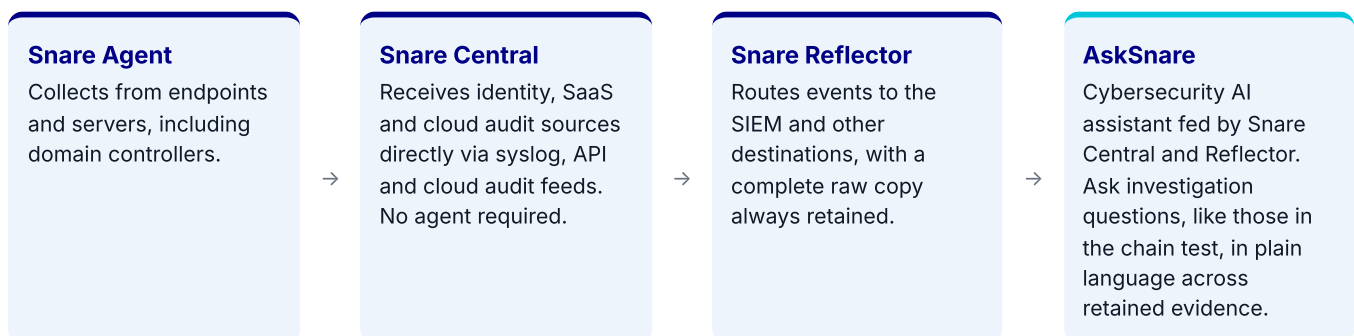
Defaults at the time of writing (October 2026). Confirm them against your own tenants and licences.

Source	Default retention	Worth knowing
Microsoft Entra ID sign-in and audit logs	7 days (Free) · 30 days (P1/P2)	Upgrading the licence isn't retroactive.
Microsoft Purview Audit	180 days (Standard) · 1 year for Entra ID, Exchange, SharePoint, OneDrive (Premium)	Records from non-user entities, such as service principal actions, are kept for a fixed year.
Okta System Log	90 days	Export to storage you control for longer history.
AWS CloudTrail Event history	90 days, management events	Data events and longer retention need a configured trail.

For comparison: joint guidance from ASD's ACSC, CISA and partners on implementing SIEM and SOAR platforms recommends keeping administrative and security event logs for at least a year. PCI DSS v4.0.1 requirement 10.5.1 requires 12 months, with the latest three months immediately available.

Where Snare fits

The map shows where your evidence is. Snare helps keep it collected, retained and joinable as it moves, while you decide where it is analysed, and AskSnare helps your team ask questions of it.



Keep going. Book a demo at snaresolutions.com to see how Snare and AskSnare keep your evidence collected and ready to investigate across every plane on this map.

References

1. NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, CSWP 29, February 2024, DE.AE-03: information is correlated from multiple sources.
2. ASD's ACSC, CISA, FBI, NSA et al., *Best Practices for Event Logging and Threat Detection*, August 2024.
3. ASD's ACSC, CISA et al., *Implementing SIEM and SOAR Platforms: Practitioner Guidance*, May 2025.
4. NSA and CISA, *Top Ten Cloud Security Mitigation Strategies*, March 2024.
5. Microsoft Learn, *Microsoft Entra data retention; Learn about auditing solutions in Microsoft Purview*.
6. PCI Security Standards Council, *PCI DSS v4.0.1*, Requirement 10.5.1.