



TECHNICAL CAPABILITY DOCUMENT

Cloud and Private Cloud Forensics

Incident investigation across public cloud, private cloud and hybrid estates, with one evidence model and one investigation workflow.

Seceon OTM · AI/XDR, CCE, APE, LTS

Ver-2.0-2026

When an incident happens in a cloud tenant there is no disk to seize and no server to carry away. The evidence is scattered across control-plane audit logs, identity events, flow records, workload telemetry, storage access logs and SaaS activity, and much of it is short-lived or retained only briefly by default. A private cloud changes the constraints without removing the problem: the organisation controls the hypervisor and the logs, but workloads are just as ephemeral and the evidence is just as scattered. This document sets out how Seceon OTM turns both into a single correlated investigation, and what the customer must enable for the evidence to exist at all.

Document title	Seceon OTM Cloud and Private Cloud Forensics: Capabilities, Architecture and Investigation Workflow
Document type	Technical / RFP-RFI response reference
Platform	Seceon OTM (AI/XDR, CCE, APE, LTS)
Cloud coverage	Public cloud (AWS, Microsoft Azure, Google Cloud, Oracle Cloud Infrastructure, IBM Cloud); private cloud (VMware, Nutanix, OpenStack, Hyper-V); container platforms; identity providers; SaaS; hybrid and air-gapped estates
Version	Ver-2.0-2026
Classification	Confidential

CONTENTS

1. Executive overview.....	3
2. What is cloud forensics.....	3

- 2.1 How cloud forensics differs from traditional digital forensics..... 3
 - 2.2 Private cloud: a different evidence problem..... 4
 - 2.3 Core principles applied by Seceon OTM..... 4
- 3. Seceon OTM Cloud Forensics architecture..... 5
 - 3.1 Architecture overview..... 5
 - 3.2 Cloud accounts, subscriptions and projects..... 7
 - 3.3 Public cloud telemetry..... 7
 - 3.4 Private cloud and virtualisation telemetry..... 8
 - 3.5 Control-plane audit logs..... 9
 - 3.6 Cloud workloads, VMs and containers..... 9
 - 3.7 Identity and access events..... 9
 - 3.8 Cloud storage and SaaS evidence..... 9
 - 3.9 Hybrid and air-gapped operation..... 9
 - 3.10 CCE, APE and LTS..... 10
 - 3.11 AI/XDR analytics and the investigation workflow..... 10
- 4. Detailed cloud forensics capability matrix..... 11
- 5. Sample investigation scenarios..... 14
- 6. Capability summary..... 16
 - 6.1 Assumptions and dependencies..... 16

DOCUMENT HISTORY

VERSION	DATE	SUMMARY
1.0	September 2025	Initial release
2.0	October 2026	Private cloud, hybrid and sovereign coverage added

1. Executive overview

Cloud adoption has moved critical workloads, identities and data outside the traditional perimeter. When an incident occurs in AWS, Microsoft Azure or Google Cloud, an investigator cannot seize a disk or a server. The evidence lives in control-plane audit logs, identity events, network flow records, workload telemetry, storage access logs and SaaS activity, and a good deal of it is ephemeral or retained for only a short period by default.

Seceon OTM Cloud Forensics turns that fragmented evidence into a single, searchable and correlated investigation record. Cloud audit, identity, network, workload and storage telemetry is ingested through the Collection and Correlation Engine (CCE). The Analytics and Policy Engine (APE) applies AI/ML and threat-intelligence analytics. Long-Term Storage (LTS) retains raw and normalised evidence. An investigation workflow then covers timeline reconstruction, IOC and IOA hunting, MITRE ATT&CK mapping, case management and reporting.

Five outcomes matter most to the customer.

Faster scoping. One correlated view of who did what, from where, to which cloud resource, and when.

Defensible evidence. Retention, integrity hashing and chain-of-custody records that support internal investigations, regulators and legal review.

One model across public and private. The same investigation workflow and data model across AWS, Azure, GCP, VMware, Nutanix, OpenStack, Hyper-V, identity providers and SaaS, rather than a separate investigative habit per platform.

Hybrid incidents as one case. An intrusion that starts on a private-cloud workload and ends in a public cloud tenant is investigated as a single timeline rather than two disconnected efforts.

Retrospective capability. Long-term retention supports look-back investigation when detection comes late, which in cloud incidents it often does.

Audit readiness. Evidence and reports that map to compliance and audit obligations.

2. What is cloud forensics

Cloud forensics applies the established digital forensic stages — identification, preservation, collection, examination, analysis and reporting — to cloud environments. The goal is unchanged: establish what happened during an incident, how it happened, what was affected and who or what was responsible, using the evidence the provider and the customer's own tenant expose. What changes is almost everything about how that evidence is obtained.

2.1 How cloud forensics differs from traditional digital forensics

ASPECT	TRADITIONAL	PUBLIC CLOUD	PRIVATE CLOUD
Evidence location	Local disks, memory, endpoints and on-premises servers	Provider audit logs, identity platforms, flow logs, snapshots, object stores and SaaS APIs	Hypervisor and management-plane logs, VM snapshots, virtual switch flows, private object stores

ASPECT	TRADITIONAL	PUBLIC CLOUD	PRIVATE CLOUD
Physical access	Direct access to devices	None; evidence comes through provider APIs and log exports	Available in principle, but workloads are virtual and rarely tied to one physical host
Volatility	Memory and disk state	Short-lived instances, containers and serverless functions; default retention can be brief	Short-lived VMs and containers; retention is set by the organisation rather than a provider default
Scope	Single host or network	Multi-account, multi-region, multi-cloud and identity-centric	Multi-cluster and multi-tenant across datacentres, often spanning into public cloud
Responsibility	Owned entirely by the organisation	Shared: the provider secures infrastructure; the customer enables, collects and retains logs	Owned entirely by the organisation, including the hypervisor and management plane
Primary attack surface	Endpoints and network	Identities, access keys, APIs, misconfigurations and workloads	Management-plane credentials, hypervisor access, orchestration APIs and inter-VM traffic

2.2 Private cloud: a different evidence problem

Private cloud is often assumed to be the easy case, on the grounds that the organisation owns everything. In practice it trades one set of constraints for another. There is no provider to ask for logs and no shared-responsibility boundary to argue about, and the hypervisor offers acquisition options a public cloud does not: a VM can be snapshotted with its memory intact, and the virtual disk can be examined offline without touching the running workload.

What does not improve is the fragmentation. Evidence is spread across the management plane (vCenter, Prism, Horizon, the OpenStack services), the hypervisor hosts, the virtual network layer, the guest operating systems, the orchestration platform, and whatever identity directory the estate authenticates against. Each has its own log format, its own default retention and often its own administrator. An investigation that stops at the guest OS misses the management-plane action that created the workload, and an investigation that stops at the management plane misses what then ran inside it.

Seceon OTM treats private cloud as a first-class evidence domain rather than as on-premises infrastructure that happens to be virtual. Management-plane, hypervisor, virtual-network and guest telemetry are normalised into the same schema used for public cloud, so a hybrid incident is one case with one timeline.

2.3 Core principles applied by Seceon OTM

Preserve early. Cloud telemetry is ingested and retained continuously, so evidence exists before an incident is declared rather than after someone thinks to look.

Correlate across sources. Identity, control-plane, network, workload and data-access events are linked into one timeline.

Maintain integrity. Source, acquisition metadata and cryptographic hashes are recorded for evidence sets.

Investigate with context. Events are enriched with threat intelligence, asset and identity context, and MITRE ATT&CK mapping.

Report defensibly. Findings are reproducible and time-stamped, and suitable for management, audit and legal audiences.

3. Seceon OTM Cloud Forensics architecture

3.1 Architecture overview

Seceon OTM collects evidence from public cloud accounts, subscriptions and projects, and from private cloud management planes, hypervisor hosts and virtual networks, using API connectors, log-streaming pipelines, object-store log buckets, and agent or syslog forwarders. Collected events are normalised and correlated by the CCE, analysed by the APE, retained in LTS, and exposed to analysts through the investigation layer.

Figure 1 overleaf shows the end-to-end evidence flow, from the five source domains through collection and the platform layers to the forensic outcomes an investigation produces.

Seceon OTM Cloud and Private Cloud Forensics Architecture

Evidence flow from public cloud, private cloud, container platforms, identity and storage into the Seceon OTM collection, analytics, storage and investigation layers

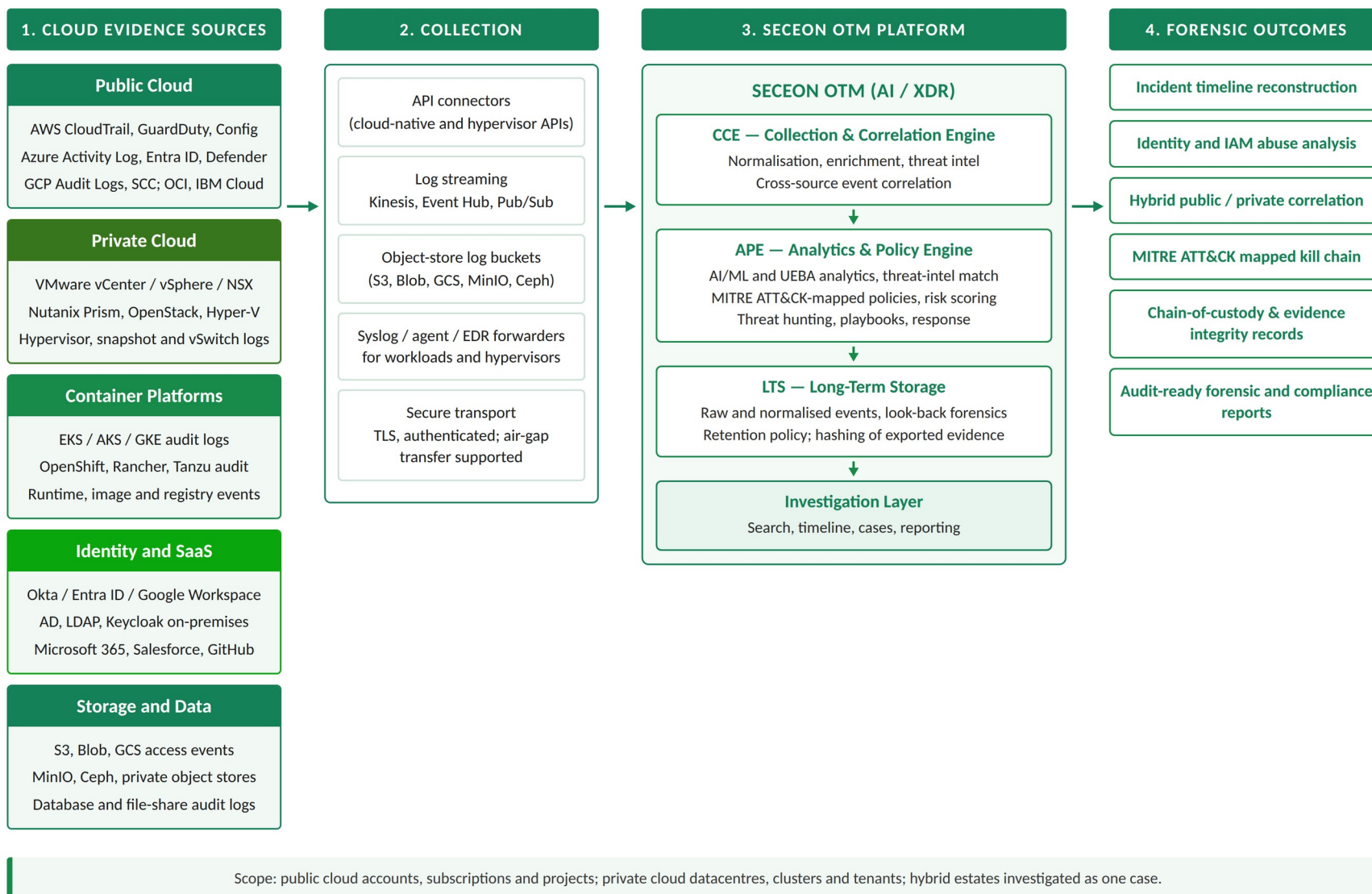


Figure 1 · Seceon OTM cloud and private cloud forensics architecture and evidence flow

3.2 Cloud accounts, subscriptions and projects

Evidence collection is organised around the customer's cloud hierarchy so that every event carries its tenant context.

PROVIDER	SCOPE OBJECTS	FORENSIC RELEVANCE
AWS	Organizations, management and member accounts, regions	Cross-account role assumption and regional activity can be traced to a single actor
Microsoft Azure	Tenant, management groups, subscriptions, resource groups	Links subscription-level actions to Entra ID identities
Google Cloud	Organization, folders, projects	Attributes API calls to users and service accounts by project
VMware	vCenter instances, datacentres, clusters, resource pools, folders	Ties a VM action to the vCenter role and session that performed it
Nutanix	Prism Central, clusters, projects, categories	Attributes workload changes to a Prism user or service account
OpenStack	Domains, projects, regions, availability zones	Scopes Keystone identity and Nova/Neutron actions to a project
Microsoft Hyper-V	SCVMM management groups, host clusters, VM networks	Links VM operations to the SCVMM or host administrator account

Collection at the top of each hierarchy is recommended — an AWS organization trail, Azure tenant-wide diagnostic settings, a GCP organization log sink, a vCenter-level syslog target or a Prism Central export — so that newly created accounts, projects, clusters and tenants are covered automatically rather than discovered as gaps during an incident.

3.3 Public cloud telemetry

TELEMETRY CLASS	AWS	MICROSOFT AZURE	GOOGLE CLOUD
Control-plane audit	CloudTrail management and data events	Azure Activity Log	Cloud Audit Logs (Admin Activity, Data Access, System Event, Policy Denied)
Identity	IAM, STS and console sign-in events via CloudTrail	Entra ID sign-in and audit logs	Cloud IAM and service-account activity; Workspace login events
Network	VPC Flow Logs, Route 53 Resolver query logs, load balancer logs	VNet / NSG flow logs, Azure Firewall and DNS logs	VPC Flow Logs, Cloud DNS logs, Cloud Firewall logs

TELEMETRY CLASS	AWS	MICROSOFT AZURE	GOOGLE CLOUD
Threat and posture	GuardDuty, Security Hub, AWS Config	Microsoft Defender for Cloud, Azure Policy	Security Command Center
Workloads	EC2 OS logs, EKS audit logs, Lambda / CloudWatch Logs	VM diagnostics, AKS audit logs, Function logs	GCE OS logs, GKE audit logs, Cloud Run / Functions logs
Storage	S3 server access logs and CloudTrail data events	Storage resource logs (Blob)	Cloud Storage Data Access audit logs

Oracle Cloud Infrastructure and IBM Cloud are covered on the same pattern: control-plane audit events, identity and key usage, flow logs and object-storage access are normalised into the same schema as the three providers above, so a tenant on any of them is investigated the same way.

Exact source availability depends on the log types enabled in the customer tenant and on the connector catalogue of the deployed Seceon OTM release.

3.4 Private cloud and virtualisation telemetry

Private cloud evidence comes from four layers, and an investigation usually needs all four. Seceon OTM collects them through the same mechanisms it uses elsewhere: API connectors against the management plane, syslog from hypervisor hosts and virtual network devices, agents inside guest workloads, and flow collectors for east-west traffic.

LAYER	EXAMPLE EVIDENCE	FORENSIC VALUE
Management plane	vCenter events and tasks, Nutanix Prism audit, OpenStack Keystone and Nova records, SCVMM job history	Who created, moved, cloned, snapshotted or deleted a workload, and from which session
Hypervisor hosts	ESXi host logs, AHV host records, KVM and Hyper-V host events, host authentication and shell access	Direct access to the virtualisation layer, which bypasses every guest-level control
Virtual network	NSX and distributed firewall logs, virtual switch flow records, overlay and segmentation events	East-west movement between workloads that never crosses a physical firewall
Guest workloads	Guest OS process, file, registry and authentication telemetry via agents or EDR	What actually executed inside the workload after it was created

The management plane deserves particular attention. A credential there can clone a running database server, mount its disk elsewhere and read the contents without generating a single authentication event inside the guest. Correlating management-plane actions with guest telemetry is what makes that pattern visible, and it is the reason private cloud evidence cannot be treated as an extension of endpoint logging.

Connector availability and supported log types for each virtualisation platform depend on the deployed Seceon OTM release.

3.5 Control-plane audit logs

Control-plane logs are the primary forensic record in the cloud, because they capture every administrative and API action. Seceon OTM ingests AWS CloudTrail, Azure Activity Logs and Google Cloud Audit Logs and normalises them into a common schema of actor, action, resource, source IP, user agent, region, result and time. That normalisation is what lets an investigator ask the same four questions on any provider:

- Who created, modified or deleted a resource, role, key or policy?
- From which IP address, geography, device or user agent was the action performed?
- Was logging itself disabled, or was a trail, diagnostic setting or sink modified?
- Which API calls followed an unusual authentication?

3.6 Cloud workloads, VMs and containers

Workload telemetry adds host-level and container-level depth to control-plane evidence. Seceon OTM ingests operating-system authentication logs, process and command activity, security agent or EDR telemetry, Kubernetes audit logs and container runtime events, from managed services (EKS, AKS, GKE) and from self-managed distributions running in private cloud (OpenShift, Rancher, Tanzu, upstream Kubernetes). Correlating these with cloud API events lets an analyst link a newly created instance or pod to the identity that launched it, and then to the processes and outbound connections that followed.

Where a full disk or memory image is required, acquisition uses the provider's native snapshot facilities: EBS snapshots, managed-disk snapshots, persistent-disk snapshots. Seceon OTM records the acquisition metadata and supports the surrounding case and chain-of-custody workflow.

3.7 Identity and access events

Identity is the most common initial access vector in the cloud. Seceon OTM analyses sign-in events, MFA outcomes, token and access-key usage, role assumptions, privilege changes, service-account activity and federation events from cloud IAM services, on-premises directories such as Active Directory, LDAP and Keycloak, and third-party identity providers. UEBA models establish per-identity baselines, so impossible travel, anomalous API usage, privilege escalation and dormant-account activation are surfaced and tied to the resource activity that followed.

3.8 Cloud storage and SaaS evidence

Object storage (Amazon S3, Azure Blob Storage, Google Cloud Storage, and private stores such as MinIO, Ceph and vSAN file services) and SaaS platforms such as Microsoft 365, Google Workspace, Salesforce and GitHub hold the data attackers are usually after. Seceon OTM ingests storage access and SaaS audit events to show who listed, read, downloaded, shared or deleted data, when permissions or public-access settings changed, and how much data moved. Combined with network telemetry, this is what supports an exfiltration investigation.

3.9 Hybrid and air-gapped operation

Most estates are hybrid, and most incidents that matter cross the boundary: a credential phished on a corporate endpoint is used against a public cloud tenant, or a compromised private-cloud workload reaches an object store

running in a provider datacentre. Because public cloud, private cloud and on-premises evidence are normalised into one schema and retained in one store, that crossing is a pivot inside a single case rather than a handoff between two investigations.

For estates with restricted or no egress, Seceon OTM runs entirely within the customer boundary. Collection, analytics, retention and investigation all operate without an outbound path to a vendor service, and evidence sets move between instances as signed bundles, which suits sovereign deployments, segregated enclaves and genuinely air-gapped environments.

3.10 CCE, APE and LTS

COMPONENT	ROLE IN CLOUD FORENSICS	FORENSIC VALUE
CCE — Collection and Correlation Engine	Collects, parses, normalises and enriches events from cloud APIs, streams, log buckets and agents; performs cross-source correlation	A consistent multi-cloud schema; linked identity, control-plane, network and workload events
APE — Analytics and Policy Engine	Applies AI/ML, behavioural (UEBA) and rule-based analytics, threat-intelligence matching and MITRE ATT&CK-mapped policies	Prioritised, explainable detections and investigation leads
LTS — Long-Term Storage	Retains raw and normalised events under the configured retention policy	Look-back investigation, evidence preservation and audit support

3.11 AI/XDR analytics and the investigation workflow

Analytics run across every collected source so that related low-level events are combined into a small number of prioritised threats rather than thousands of individual alerts. The investigation workflow then follows six stages.

STAGE	ACTIVITY	HOW SECEON OTM SUPPORTS IT
1	Detect and triage	AI/ML and policy-based detection raises threats with risk scoring and MITRE ATT&CK context
2	Scope and preserve	Identify affected accounts, identities and resources; retain raw evidence in LTS; export evidence sets with metadata
3	Collect and correlate	Pivot across audit, identity, network, workload and storage events for the same actor, resource or IP
4	Reconstruct timeline	Order correlated events chronologically to establish initial access, escalation, persistence, impact and exfiltration
5	Contain and respond	Trigger orchestrated response actions and playbooks in coordination with cloud, identity and network controls
6	Report and close	Generate case reports with evidence references, integrity records and ATT&CK mapping; retain the case for audit

4. Detailed cloud forensics capability matrix

The matrix below lists each capability, the evidence it relies on, the corresponding Seceon OTM capability, and the forensic outcome it produces, across public cloud, private cloud and hybrid estates.

#	CAPABILITY	DESCRIPTION	EVIDENCE / DATA SOURCE	SECEON OTM CAPABILITY	FORENSIC OUTCOME
1	Evidence collection and preservation	Continuous collection and retention of cloud telemetry so evidence exists before an incident is declared.	CloudTrail, Azure Activity and Entra ID logs, GCP Audit Logs, flow logs, workload and SaaS logs	API connectors, streaming and agent collection in CCE; retention and archival in LTS	Preserved, time-stamped evidence base available for look-back investigation
2	Cloud audit log collection	Centralised ingestion of provider audit logs across all accounts, subscriptions and projects.	AWS CloudTrail, Azure Activity Log, GCP Cloud Audit Logs	Centralised ingestion, normalisation and analytics	Reconstruction of administrative activity
3	Cloud incident investigation workflow	Guided path from detection to scoping, correlation, response and reporting.	Alerts, correlated events, asset and identity context	AI/XDR threat prioritisation, search, drill-down and playbooks	Repeatable, documented investigation from alert to closure
4	Timeline reconstruction	Ordered view of events across services, accounts and clouds for an actor, resource or incident.	Events from multiple cloud services and identity providers	Cross-source correlation and time-ordered event views	Incident timeline showing initial access through to impact
5	Identity and IAM forensics	Investigation of user, role, service-account and access-key behaviour.	Sign-in, MFA, STS/role-assumption, IAM change and token events	UEBA and XDR analytics on identity activity	Identification of suspicious identity behaviour and privilege escalation
6	Cloud API activity analysis	Analysis of control-plane API calls for unauthorised or anomalous changes.	Cloud control-plane API calls and error patterns	Correlation and behavioural analytics	Detection of unauthorised changes and reconnaissance
7	Cloud network forensics	Reconstruction of communication paths and traffic volumes between cloud resources and the internet.	VPC / VNet flow logs, firewall, DNS and load balancer logs	Network analytics and threat-intelligence matching	Communication-path reconstruction and identification of malicious endpoints
8	Compute, VM and container forensics	Host-level and container-level investigation tied to the launching identity.	OS, process, authentication and security logs; Kubernetes audit and runtime events	EDR/XDR telemetry and workload log correlation	Host-level investigation and workload-to-identity attribution
9	Storage and object forensics	Investigation of access, sharing and deletion of objects and buckets.	S3, Blob and GCS access events; permission and public-access changes	Cloud log correlation with network telemetry	Identification of suspicious access, exposure and exfiltration

#	CAPABILITY	DESCRIPTION	EVIDENCE / DATA SOURCE	SECEON OTM CAPABILITY	FORENSIC OUTCOME
10	Data exfiltration investigation	Detection and scoping of possible data theft from storage, databases and SaaS.	Storage access events plus network egress telemetry	Correlation and behavioural detection	Investigation of possible data theft with volume and destination
11	Cloud configuration and control-plane forensics	Detection of security-control changes and misconfigurations.	Configuration, policy, logging and security-setting change events	Analytics and alerting on control-plane changes	Identification of disabled logging, weakened controls and exposure
12	Persistence investigation	Identification of mechanisms that let an attacker retain access.	IAM users, keys and roles; scheduled jobs, functions, startup mechanisms	Correlation and analytics against ATT&CK persistence techniques	Detection of persistence mechanisms for eradication
13	Cryptomining investigation	Detection of resource abuse for cryptocurrency mining.	Process, network and cloud-resource activity, compute spikes	Behavioural detection and threat-intelligence matching	Identification of resource abuse and the initiating identity
14	Cryptographic hashing and evidence integrity	Generation and verification of hashes for collected and exported evidence.	Collected forensic artefacts and exported evidence sets	Hash generation and verification (for example SHA-256)	Evidence integrity validation
15	Chain of custody	Recording of who acquired, accessed and transferred evidence, and when.	Evidence metadata and acquisition records	Investigation, audit-trail and reporting workflow	Traceable forensic evidence
16	IOC / IOA investigation	Search and hunting for indicators of compromise and of attack.	IP addresses, domains, file hashes, URLs, behavioural patterns	XDR analytics and threat-intelligence integration	IOC- and behaviour-based scoping of affected assets
17	MITRE ATT&CK mapping	Mapping of detections and evidence to ATT&CK tactics and techniques.	Correlated detections across cloud sources	ATT&CK-mapped policies and analytics	Kill-chain view and gap identification
18	Incident case management and reporting	Case tracking, evidence attachment and production of investigation reports.	Correlated investigation evidence, analyst notes, actions taken	Case management and reporting	Investigation-ready forensic report
19	Compliance and audit evidence	Retention and reporting of evidence to support regulatory and audit requirements.	Retained logs, access records, investigation reports	LTS retention, compliance-oriented reports and dashboards	Audit-ready evidence packages
20	Private cloud management-plane forensics	Investigation of workload creation, cloning, migration and deletion through the virtualisation management plane.	vCenter events and tasks, Nutanix Prism audit, OpenStack Keystone and Nova records, SCVMM job history	API and syslog collection from the management plane, correlated with guest telemetry	Attribution of workload changes to an administrator session and role
21	Hypervisor host forensics	Investigation of access to and activity on the virtualisation hosts themselves.	ESXi, AHV, KVM and Hyper-V host logs; host authentication and shell access	Host log ingestion correlated with management-plane and identity events	Detection of hypervisor-level access that bypasses guest controls

#	CAPABILITY	DESCRIPTION	EVIDENCE / DATA SOURCE	SECEON OTM CAPABILITY	FORENSIC OUTCOME
22	Virtual network forensics	Reconstruction of east-west traffic between workloads that never crosses a physical boundary.	NSX and distributed firewall logs, virtual switch flow records, overlay and segmentation events	Flow and firewall analytics across the virtual network layer	Lateral movement paths inside the virtual estate
23	VM snapshot and image acquisition	Acquisition of virtual disk and memory state for offline forensic analysis.	Hypervisor snapshot and checkpoint facilities; virtual disk and memory files	Case workflow, acquisition metadata, hashing and chain of custody around the captured image	Deep artefact findings, including guest memory, linked to the case
24	Private container platform forensics	Investigation of self-managed Kubernetes distributions running in private cloud.	OpenShift, Rancher, Tanzu and upstream Kubernetes audit logs; runtime, image and registry events	Audit log ingestion and workload-to-identity correlation	Compromised workload, image provenance and lateral movement between namespaces
25	Hybrid incident correlation	Investigation of incidents that cross between on-premises, private cloud and public cloud.	Normalised evidence from all three environments in one store	Single schema, single retention store and cross-domain correlation	One case and one timeline spanning the whole estate
26	Sovereign and air-gapped operation	Full investigation capability with no outbound path to a vendor service.	Locally collected and retained evidence; signed evidence bundles for transfer	On-premises deployment, local analytics and retention, offline enrichment data	Investigation capability preserved in segregated and air-gapped estates
27	Multi-tenant investigation	Segregated investigation for several tenants or business units from one deployment.	Tenant-scoped evidence, cases and access records	Tenant isolation, role-based evidence access and per-tenant retention policy	Per-tenant cases and reporting without cross-tenant evidence exposure

5. Sample investigation scenarios

The scenarios below illustrate how the capabilities in Section 4 combine during cloud incidents that occur regularly in practice.

5.1 Compromised access key and cryptomining

Trigger	Alert on unusual instance launches and a spike in compute spend.
Evidence used	CloudTrail RunInstances and CreateAccessKey events; VPC Flow Logs to mining pool endpoints; instance process telemetry; IAM key history.
Seceon OTM analysis	Correlate the launching identity with its prior behaviour, geo-IP and user agent; match destination IPs to threat intelligence; map to ATT&CK Resource Hijacking.
Forensic outcome	Compromised key, time of first misuse, affected regions and instances, and the persistence created, with a timeline and report for closure.

5.2 Object storage data exfiltration

Trigger	Anomalous volume of object downloads from a sensitive bucket.
Evidence used	S3 / Blob / GCS access events; permission and public-access changes; network egress telemetry; identity sign-in events.
Seceon OTM analysis	Baseline normal access, identify the actor and source IP, link the access to a recent privilege change, and quantify the data moved and its destination.
Forensic outcome	Actor, objects accessed, volume and destination of transfer, and the control that failed, as evidence for breach assessment.

5.3 Privilege escalation and persistence in a cloud tenant

Trigger	Detection of a new privileged role assignment outside change windows.
Evidence used	Entra ID audit and sign-in logs; Azure Activity Log role assignments; service-principal credential changes; scheduled automation.
Seceon OTM analysis	Chain the sign-in, MFA event, role assignment and new credentials into a single timeline, and check for logging or policy changes.
Forensic outcome	Initial access method, escalation path, persistence mechanisms to remove, and the scope of resources touched.

5.4 Kubernetes container compromise

Trigger	Alert on a suspicious process and outbound connection from a pod.
----------------	---

Evidence used	Kubernetes audit logs; container runtime and process events; flow logs; image and deployment API activity.
Seceon OTM analysis	Trace the pod to the deployment and the identity that created it; correlate connections with threat intelligence; identify lateral movement to other workloads.
Forensic outcome	Compromised workload and image, entry point, lateral movement path and affected namespaces.

5.5 Private cloud management-plane compromise

Trigger	A virtual machine is cloned outside a change window, and the clone is powered on in an unmonitored network segment.
Evidence used	vCenter or Prism task and event records; hypervisor host authentication; virtual switch flow logs; guest telemetry from both the source and the clone; directory sign-in events.
Seceon OTM analysis	Attribute the clone operation to a management-plane session and role, trace how that credential was obtained, and follow the clone's network activity and any data read from its mounted disk.
Forensic outcome	The administrator account used, the data exposed through the cloned disk, the segment the clone reached, and the management-plane controls that failed.

5.6 Hybrid incident crossing private and public cloud

Trigger	A workload in the private cloud begins authenticating to a public cloud tenant with a service credential never used from that network before.
Evidence used	Guest process and network telemetry; virtual switch and egress flow logs; public cloud control-plane audit events; IAM and key-usage records; object storage access events.
Seceon OTM analysis	Join the private-cloud workload, the credential and the subsequent public cloud API activity into one timeline, and establish whether the credential was stored on the workload or harvested from elsewhere.
Forensic outcome	The full path from the private-cloud foothold to the public cloud resources touched, with the credential exposure window and the data accessed in each environment.

5.7 Service-account abuse in Google Cloud

Trigger	A service-account key used from an unfamiliar location.
Evidence used	GCP Cloud Audit Logs; IAM policy change events; VPC Flow Logs; Cloud Storage Data Access logs.

Seceon OTM analysis	Baseline service-account behaviour, detect anomalous API calls and source, and follow the resulting resource and storage activity.
Forensic outcome	Key exposure window, actions performed with the key, data accessed, and the required key rotation and least-privilege remediation.

6. Capability summary

AREA	SUMMARY
Public cloud coverage	AWS, Microsoft Azure, Google Cloud, Oracle Cloud Infrastructure and IBM Cloud
Private cloud coverage	VMware vSphere and NSX, Nutanix, OpenStack, Microsoft Hyper-V and SCVMM; self-managed Kubernetes (OpenShift, Rancher, Tanzu); private object storage
Identity and SaaS coverage	Cloud IAM, Entra ID, Okta, on-premises Active Directory, LDAP and Keycloak; Microsoft 365, Google Workspace, Salesforce, GitHub
Evidence types	Control-plane and management-plane audit logs, hypervisor host logs, identity events, physical and virtual network flow and DNS logs, workload and container telemetry, storage and SaaS access events, VM snapshots and images
Platform components	CCE for collection and correlation, APE for AI/ML and policy analytics, LTS for retention, investigation layer for search, timelines and cases
Investigation functions	Timeline reconstruction, IAM and management-plane forensics, physical and virtual network forensics, workload and container forensics, storage and exfiltration investigation, persistence and cryptomining detection, hybrid correlation, IOC/IOA hunting
Evidence handling	Retention, hashing (for example SHA-256) and chain-of-custody records for collected and exported evidence
Frameworks and reporting	MITRE ATT&CK mapping, case management, forensic and compliance reporting
Deployment	On-premises, hybrid, sovereign and air-gapped; multi-tenant operation for service providers
Outcome	Faster scoping, defensible evidence, consistent investigation across public and private estates, and audit-ready reporting

6.1 Assumptions and dependencies

Four conditions govern what this capability can deliver. Each belongs in the solution design conversation rather than the incident.

Log enablement. Forensic evidence is available only if the relevant logs are enabled in the customer's cloud tenant and forwarded to Seceon OTM before or during the incident.

Retention. Log retention in the source cloud is limited by the customer's configuration; LTS retention is governed by the customer's retention policy and storage sizing.

Acquisition tooling. Disk, memory and snapshot acquisition uses cloud-provider or hypervisor native tooling. Seceon OTM supports the case, metadata and chain-of-custody workflow around it.

Virtualisation coverage. Supported management platforms, hypervisor log types and virtual network sources depend on the deployed Seceon OTM release and should be confirmed against the customer's virtualisation estate during solution design.

Release and licensing. Connector availability, supported log types and specific feature behaviour depend on the deployed Seceon OTM version and licensing.

In the cloud, the investigation is bounded by what was logged at the time. Organisation-level log collection and a retention period matched to realistic detection delay are the two decisions that most determine whether a later investigation can answer anything at all.

Test this against your own tenant

Cloud forensic readiness is specific to a tenant: which trails and sinks are enabled, at which scope, and for how long the evidence survives. Ask for a readiness review of your AWS, Azure and GCP logging configuration, and we will show where an investigation would succeed today and where it would run out of evidence.

ABOUT SECEON

Seceon's Open Threat Management (OTM) platform consolidates detection, investigation and response into a single data pipeline, delivered to enterprises and to the managed service providers that serve them. The platform is used by more than 10,000 customers and 850 partners worldwide, across financial services, government, healthcare, manufacturing and critical infrastructure.



Seceon, Inc. · 238 Littleton Rd, Suite #200, Westford, MA 01886 · +1-978-923-0040 · www.seceon.com