



TECHNICAL CAPABILITY DOCUMENT

Digital Forensics and Incident Response

Detection, investigation, containment and recovery across endpoints, network, identity, cloud, OT and mobile, on one AI/XDR platform.

Seceon OTM • AI/XDR, CCE, APE, LTS

Ver-2.0-2026

Modern intrusions move across endpoints, identities, networks and cloud services faster than most teams can assemble the evidence to understand them. This document sets out how Seceon OTM supports the full DFIR cycle: what evidence it collects, how the platform correlates it, what an investigation looks like in practice, and what the customer must have in place for the evidence to exist when it is needed.

Document title	Seceon OTM DFIR: Capabilities, Architecture and Incident Response Workflow
Document type	Technical / RFP-RFI response reference
Platform	Seceon OTM (AI/XDR, CCE, APE, LTS)
Coverage	Endpoints and servers, network and perimeter, identity and email, cloud and applications, OT/ICS, container and virtual workloads, mobile and removable media; single-tenant and multi-tenant operation
Version	Ver-2.0-2026
Classification	Confidential

CONTENTS

1. Executive overview.....	3
2. What is DFIR.....	3
2.1 Incident response lifecycle and Seceon OTM support.....	3

2.2 Core principles applied by Seceon OTM.....	4
3. Seceon OTM DFIR architecture.....	4
3.1 Architecture overview.....	4
3.2 Endpoints and servers.....	6
3.3 Network and perimeter.....	6
3.4 Identity, directory and email.....	6
3.5 Cloud and applications.....	6
3.6 Evidence sources and forensic value.....	6
3.7 CCE, APE and LTS.....	7
3.8 AI/XDR analytics and the DFIR workflow.....	7
3.9 Response orchestration.....	8
4. Detailed DFIR capability matrix.....	9
5. Sample investigation scenarios.....	12
6. Capability summary.....	13
6.1 Assumptions and dependencies.....	14

DOCUMENT HISTORY

VERSION	DATE	SUMMARY
1.0	September 2025	Initial release
2.0	October 2026	OT, container, mobile, multi-tenant and sovereign coverage added

1. Executive overview

Modern attacks move quickly across endpoints, identities, networks and cloud services. A security team has to detect the intrusion, establish what happened, contain it, remove the attacker and restore operations, and it has to do all of that while preserving evidence that will stand up to audit, regulatory and legal scrutiny. Those are two different disciplines. Incident response limits damage and restores service; digital forensics establishes the facts through rigorous evidence handling. DFIR is the practice of doing both at once.

Seceon OTM brings the two onto one AI/XDR platform. Telemetry from endpoints, servers, network devices, identity systems, email and cloud services is collected through the Collection and Correlation Engine (CCE). The Analytics and Policy Engine (APE) applies AI/ML, behavioural and threat-intelligence analytics. Long-Term Storage (LTS) retains raw and normalised evidence under the customer's retention policy. On top of these, an investigation layer gives analysts search, timeline reconstruction, IOC and IOA hunting, MITRE ATT&CK mapping, case management, response orchestration and reporting.

The practical difference this makes to the customer falls into five areas.

Faster detection and triage. Correlated, risk-scored threats rather than thousands of isolated alerts competing for the same analyst.

Accurate scoping and root cause. One view of initial access, lateral movement, persistence and impact, rather than a reconstruction assembled by hand from several consoles.

Coordinated containment. Playbook-driven response actions that shorten dwell time, with each action recorded against the case.

Defensible evidence. Retention, integrity hashing and chain-of-custody records that survive later scrutiny.

Continuous improvement. Post-incident reporting and hunting that feed back into detection policies.

2. What is DFIR

DFIR is the combined practice of responding to a security incident and investigating it forensically. The response side follows a lifecycle such as the one described in NIST SP 800-61. The forensic side follows the identification, preservation, collection, examination, analysis and reporting stages used in established digital forensic practice. The two run concurrently, and the tension between them is real: containment that is too aggressive can destroy the evidence an investigation depends on.

2.1 Incident response lifecycle and Seceon OTM support

LIFECYCLE PHASE	OBJECTIVE	SECEON OTM SUPPORT
Preparation	Have visibility, retention, playbooks and roles in place before an incident	Broad telemetry onboarding, retention policies in LTS, detection policies, playbook library
Detection and analysis	Identify the incident, validate it and determine scope	AI/ML and UEBA detection, correlation, threat-intelligence matching, timeline and search
Containment	Stop spread and limit damage	Orchestrated response actions and playbooks with endpoint, network and identity controls

LIFECYCLE PHASE	OBJECTIVE	SECEON OTM SUPPORT
Eradication	Remove attacker access, malware and persistence	Persistence and IOC hunting; verification that indicators no longer appear
Recovery	Restore systems and confirm normal operation	Post-recovery monitoring and re-detection of related activity
Post-incident activity	Learn, report and improve	Case reports, ATT&CK mapping, evidence archive, detection tuning

2.2 Core principles applied by Seceon OTM

Visibility first. Evidence has to exist before the incident, so telemetry is collected and retained continuously rather than switched on in response to an alert.

Correlate across domains. Endpoint, network, identity, email and cloud events are linked to the same actor, host or session.

Balance speed and evidence. Response actions are recorded in the case, so containment does not destroy the audit trail it was meant to protect.

Maintain integrity. Evidence carries its source, acquisition metadata and cryptographic hashes.

Report defensibly. Findings are time-stamped, reproducible and mapped to MITRE ATT&CK.

3. Seceon OTM DFIR architecture

3.1 Architecture overview

Seceon OTM collects evidence from endpoints and servers, network and perimeter devices, identity and email systems, cloud and application platforms, and OT, IoT and mobile sources, using agents, syslog and flow collectors, and API connectors. The CCE normalises and correlates those events, the APE analyses them, LTS retains them, and the investigation layer exposes them to analysts.

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

Seceon OTM DFIR Architecture

Evidence and telemetry flow from endpoints, network, identity, cloud, OT and mobile into Seceon OTM detection, investigation and response

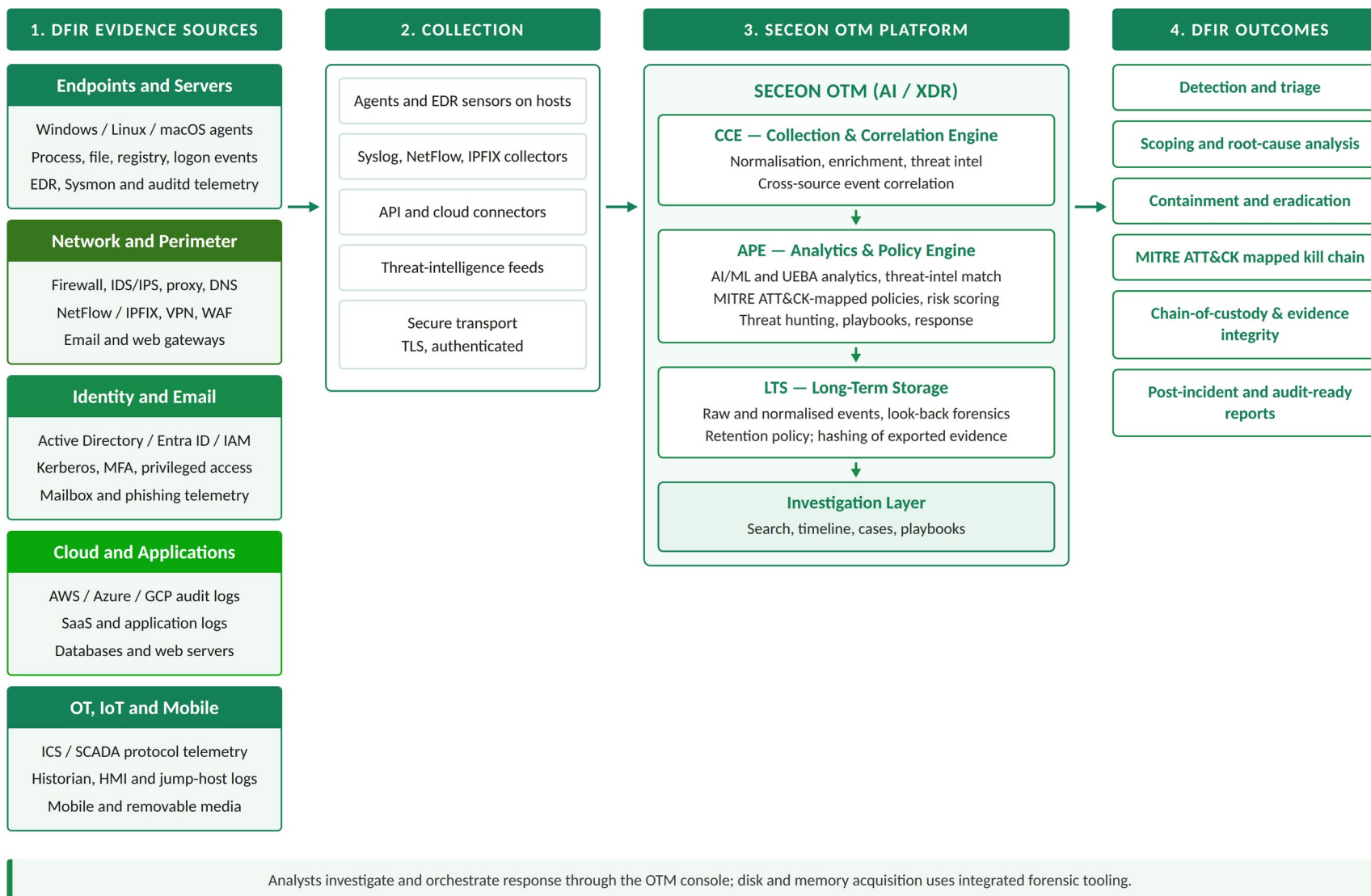


Figure 1 · Seceon OTM DFIR architecture and evidence flow

3.2 Endpoints and servers

Endpoint and server telemetry is the core of host forensics. Seceon OTM ingests process creation and command lines, file and registry changes, service and scheduled-task creation, logon and privilege events, PowerShell and script activity, USB and removable-media events, and Linux auditd and syslog records, drawn from agents, EDR sensors, Sysmon and native operating-system logs. This is what lets an analyst reconstruct an execution chain, identify malware and ransomware behaviour, find persistence, and trace the user session behind each action.

Where a full memory image, disk image or triage package is required, acquisition and deep artefact analysis are performed with integrated forensic tooling. Seceon OTM records the acquisition metadata in the case and correlates the findings with the surrounding telemetry.

3.3 Network and perimeter

Firewall, IDS/IPS, proxy, DNS, VPN, WAF and NetFlow/IPFIX data show how an attacker entered, how they communicated and where they moved. Correlating these with host and identity events reconstructs command-and-control traffic, lateral movement, scanning, tunnelling and data transfers, and matches external destinations against threat intelligence.

3.4 Identity, directory and email

Identity abuse features in most modern intrusions. Seceon OTM analyses Active Directory and Entra ID events, Kerberos and NTLM authentication, MFA outcomes, privileged group changes, service-account use, and email gateway and mailbox events. UEBA baselines surface credential theft, pass-the-hash and pass-the-ticket behaviour, impossible travel, mailbox rule abuse and phishing delivery, and tie each of them back to the hosts and sessions involved.

3.5 Cloud and applications

Cloud audit logs (AWS CloudTrail, Azure Activity Log and Entra ID logs, Google Cloud Audit Logs), SaaS audit trails, and database and web-server logs extend an investigation to workloads and data outside the data centre. These are correlated with on-premises evidence so that an incident crossing both environments is investigated as one case rather than two.

3.6 Evidence sources and forensic value

DOMAIN	EXAMPLE EVIDENCE	FORENSIC VALUE
Endpoints and servers	Process, file, registry, service, logon, script and USB events; EDR alerts	Execution chain, malware behaviour, persistence, user attribution
Network and perimeter	Firewall, IDS/IPS, proxy, DNS, VPN, WAF, NetFlow	Entry point, C2, lateral movement, exfiltration paths
Identity and directory	AD / Entra ID authentication, group and policy changes, MFA	Credential theft, privilege escalation, account abuse
Email	Gateway, mailbox and attachment/URL telemetry	Phishing delivery, mailbox compromise, initial access

DOMAIN	EXAMPLE EVIDENCE	FORENSIC VALUE
Cloud and SaaS	Audit logs, storage and application access events	Cloud control-plane abuse, data access, cross-environment movement
OT and ICS	Protocol telemetry from OT networks, historian and HMI logs, engineering workstation and jump-host access records	Crossing from IT into the process environment, and unauthorised control-system interaction
Mobile and removable media	Removable-media connection history, mobile extraction packages, peripheral activity	Data movement off the estate by physical means rather than over the network
Threat intelligence	IP, domain, URL and hash feeds	IOC matching and enrichment

3.7 CCE, APE and LTS

COMPONENT	ROLE IN DFIR	FORENSIC AND RESPONSE VALUE
CCE — Collection and Correlation Engine	Collects, parses, normalises and enriches events from agents, collectors and APIs, then correlates across sources	A unified evidence model linking host, network, identity and cloud events
APE — Analytics and Policy Engine	AI/ML, UEBA, threat-intelligence matching and MITRE ATT&CK-mapped policies; drives alerting and response	Prioritised threats, investigation leads and response triggers
LTS — Long-Term Storage	Retains raw and normalised events under the configured retention policy	Look-back investigation, evidence preservation and audit support

3.8 AI/XDR analytics and the DFIR workflow

Seceon OTM analytics combine related low-level events into a small number of prioritised threats. From there the DFIR workflow runs in seven stages.

STAGE	ACTIVITY	HOW SECEON OTM SUPPORTS IT
1	Detect and triage	AI/ML and policy detection raises threats with risk scoring and MITRE ATT&CK context
2	Scope and preserve	Identify affected hosts, users and data; retain evidence in LTS; register evidence in the case
3	Investigate and correlate	Pivot across endpoint, network, identity, email and cloud events for the same actor, host or indicator
4	Reconstruct timeline	Build the sequence from initial access through movement, persistence and impact
5	Contain and eradicate	Run response playbooks; hunt for remaining persistence and indicators

STAGE	ACTIVITY	HOW SECEON OTM SUPPORTS IT
6	Recover and verify	Monitor recovered assets for re-infection and related activity
7	Report and improve	Generate case reports with evidence references and integrity records; tune detections

3.9 Response orchestration

Playbooks can trigger containment actions such as isolating a host, blocking an IP address, domain or URL, disabling or resetting an account, or opening a ticket. Every action is recorded against the case so that responders and auditors can see what was done, when, and by whom. Which actions are available depends on the customer's endpoint, firewall, identity and ticketing products and on the deployed Seceon OTM release.

4. Detailed DFIR capability matrix

The matrix below lists each DFIR capability, the evidence it relies on, the corresponding Seceon OTM capability, and the investigation outcome it produces.

#	CAPABILITY	DESCRIPTION	EVIDENCE / DATA SOURCE	SECEON OTM CAPABILITY	INVESTIGATION OUTCOME
1	Evidence collection and preservation	Continuous collection and retention of telemetry so evidence exists before an incident is declared.	Endpoint, network, identity, email, cloud and application logs	Agents, collectors and connectors in CCE; retention and archival in LTS	Preserved, time-stamped evidence base for look-back investigation
2	DFIR incident response workflow	Guided path from detection through scoping, containment, recovery and reporting.	Alerts, correlated events, asset and identity context	AI/XDR threat prioritisation, search, drill-down, cases and playbooks	Repeatable, documented response from alert to closure
3	Endpoint and host forensics	Investigation of process, file, registry, service and logon activity on hosts.	Process, file, registry, service, script and logon events; EDR / Sysmon / auditd	EDR/XDR telemetry ingestion and host-level correlation	Execution chain and user attribution on affected hosts
4	Memory and disk forensics integration	Acquisition and deep analysis of memory, disk images and triage packages with integrated tooling.	Memory images, disk images, triage collections	Case workflow, evidence metadata and correlation with telemetry	Deep artefact findings linked to the incident case
5	Malware and ransomware investigation	Identification of malicious files and behaviour, encryption activity and spread.	File hashes, process trees, file-rename bursts, shadow-copy and backup tampering	Behavioural and threat-intelligence detection; correlation	Patient zero, spread path and impacted systems
6	Timeline reconstruction	Ordered view of events across hosts, network, identity and cloud.	Events from multiple sources and time zones	Cross-source correlation and time-ordered event views	Incident timeline from initial access to impact
7	Network forensics	Reconstruction of communications and data movement.	Firewall, IDS/IPS, proxy, DNS, VPN, NetFlow / IPFIX	Network analytics and threat-intelligence matching	C2 and lateral-movement paths; external destinations
8	Identity and Active Directory forensics	Investigation of authentication, privilege and service-account activity.	AD / Entra ID logons, Kerberos events, group and policy changes, MFA	UEBA and XDR analytics on identity activity	Credential abuse and privilege-escalation findings
9	Lateral movement investigation	Detection of remote execution, remote services and internal pivoting.	Logon type events, SMB/RDP/WinRM/SSH activity, internal flows	Correlation of host, identity and network events	Movement path and compromised systems
10	Email and phishing investigation	Tracing delivery, user interaction and follow-on activity of malicious email.	Gateway and mailbox events, URL and attachment telemetry, endpoint execution	Correlation of email, endpoint and identity events	Initial-access vector and affected recipients

#	CAPABILITY	DESCRIPTION	EVIDENCE / DATA SOURCE	SECEON OTM CAPABILITY	INVESTIGATION OUTCOME
11	Data exfiltration and insider threat	Detection of unusual data access and transfer by external or internal actors.	File-access, USB, cloud-storage, proxy and network egress events	Behavioural analytics and correlation	Data accessed, volume, destination and responsible identity
12	Persistence investigation	Identification of mechanisms that let an attacker retain access.	Services, scheduled tasks, run keys, startup items, new accounts, cron jobs	Correlation and analytics mapped to ATT&CK persistence techniques	Persistence mechanisms identified for eradication
13	Cloud and SaaS incident evidence	Investigation of incidents that extend into cloud and SaaS platforms.	AWS / Azure / GCP audit logs, SaaS audit trails	Cloud log ingestion and cross-domain correlation	Unified case spanning on-premises and cloud
14	IOC / IOA investigation and threat hunting	Search and hunting for indicators of compromise and of attack.	IPs, domains, hashes, URLs, behavioural patterns	XDR analytics, threat-intelligence integration, search	Scope of compromise and previously unseen activity
15	MITRE ATT&CK mapping	Mapping of detections and evidence to tactics and techniques.	Correlated detections across domains	ATT&CK-mapped policies and analytics	Kill-chain view and detection-gap identification
16	Containment and response orchestration	Automated or analyst-approved actions to stop spread.	Alert context, asset and identity data, integrated control points	Playbooks and orchestration with integrated controls	Faster containment with recorded actions
17	Eradication and recovery validation	Confirmation that attacker access is removed and systems are clean.	Post-remediation telemetry, IOC and persistence searches	Hunting, re-detection and monitoring policies	Verified eradication and early warning of re-compromise
18	Cryptographic hashing and evidence integrity	Generation and verification of hashes for collected and exported evidence.	Collected artefacts and exported evidence sets	Hash generation and verification (for example SHA-256)	Evidence integrity validation
19	Chain of custody	Recording who acquired, accessed and transferred evidence, and when.	Evidence metadata and acquisition records	Case, audit-trail and reporting workflow	Traceable forensic evidence
20	Incident case management and reporting	Case tracking, evidence attachment, analyst notes and reporting.	Correlated evidence, notes, response actions	Case management and reporting	Investigation-ready incident report
21	Post-incident review and lessons learned	Structured review of root cause, response effectiveness and control gaps.	Case timeline, response actions, ATT&CK mapping	Reporting, detection tuning and policy updates	Improved detections and response playbooks
22	Compliance and audit evidence	Retention and reporting of evidence for regulatory and audit needs.	Retained logs, access records, incident reports	LTS retention, compliance-oriented reports and dashboards	Audit-ready evidence packages
23	OT and ICS incident evidence	Investigation of incidents that reach the process environment from the enterprise network.	OT protocol telemetry, historian and HMI logs, engineering workstation and jump-host access	Correlation of OT network telemetry with IT identity and endpoint events	The IT-to-OT crossing point and the control systems affected

#	CAPABILITY	DESCRIPTION	EVIDENCE / DATA SOURCE	SECEON OTM CAPABILITY	INVESTIGATION OUTCOME
24	Container and virtual workload forensics	Investigation of containerised and virtualised workloads and the identities that created them.	Kubernetes audit logs, container runtime and registry events, hypervisor management records	Audit log ingestion and workload-to-identity correlation	Compromised workload, image provenance and lateral movement between namespaces
25	Mobile and removable media evidence	Investigation of data movement by physical means rather than over the network.	Removable-media connection history, mobile extraction packages, peripheral and print activity	Ingestion into the same case, timeline and search workflow as endpoint evidence	Devices connected, data copied and the user responsible
26	Multi-tenant and service-provider operation	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
27	Sovereign and air-gapped operation	Full DFIR 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
28	Regulatory and sectoral reporting	Production of incident evidence in the form a regulator or sector body requires.	Case timeline, evidence inventory, response actions, integrity records	Case reporting with configurable scope, retention aligned to the applicable obligation	Reporting packages suited to financial, healthcare, critical-infrastructure and data-protection regimes

5. Sample investigation scenarios

The scenarios below show how the capabilities in Section 4 combine during incidents that security teams encounter regularly.

5.1 Ransomware outbreak

Trigger	Alerts on mass file renaming, shadow-copy deletion and a suspicious process on a file server.
Evidence used	Endpoint process and file events; logon events; SMB and internal flow data; email and proxy logs; threat-intelligence matches.
Seceon OTM analysis	Trace the encrypting process to its parent and initial execution, identify the account and source host, map lateral movement, and trigger isolation playbooks.
Forensic outcome	Patient zero, entry vector, spread path, impacted systems, and a verified containment and recovery record.

5.2 Phishing leading to credential theft

Trigger	A user reports a suspicious email; later, sign-ins occur from an unfamiliar location.
Evidence used	Email gateway and mailbox events; proxy and DNS logs; identity sign-in and MFA events; endpoint execution.
Seceon OTM analysis	Identify all recipients and those who clicked, link the credential harvest to the subsequent sign-in, and detect mailbox rule creation and follow-on access.
Forensic outcome	Affected users, compromised accounts, actions the attacker took, and the accounts requiring reset.

5.3 Active Directory compromise and lateral movement

Trigger	Detection of unusual Kerberos activity and new privileged group membership.
Evidence used	Domain-controller and member-server logon events; group and policy changes; remote-execution and network flow data.
Seceon OTM analysis	Correlate authentication anomalies with host activity, map the movement path and privilege gain, and hunt for persistence.
Forensic outcome	Compromised accounts and hosts, the escalation path, persistence to remove, and controls to harden.

5.4 Insider data theft

Trigger	Unusual bulk file access followed by USB and cloud-storage activity by a single user.
----------------	---

Evidence used	File-access, USB, proxy and cloud-storage events; VPN and logon history; HR-provided context.
Seceon OTM analysis	Baseline the user's normal behaviour, correlate access, copy and upload events, and quantify the data involved.
Forensic outcome	Timeline of user actions, data affected, destination of transfers, and an evidence package with integrity records.

5.5 Web server compromise

Trigger	WAF and IDS alerts followed by an unexpected outbound connection from a web server.
Evidence used	WAF, web-server and application logs; host process and file events; firewall and DNS logs.
Seceon OTM analysis	Identify the exploited request, the web shell or dropped files, the process tree, and any pivot into the internal network.
Forensic outcome	Exploit vector, attacker commands, affected systems, and remediation steps including patching and rebuilding.

6. Capability summary

AREA	SUMMARY
Coverage	Endpoints and servers, network and perimeter, identity and directory, email, cloud and applications, OT and ICS, container and virtual workloads, mobile and removable media
Evidence types	Host process, file, registry and logon events; network flow and gateway logs; authentication events; email telemetry; cloud and SaaS audit logs
Platform components	CCE for collection and correlation, APE for AI/ML and policy analytics, LTS for retention, investigation layer for search, timelines, cases and playbooks
Investigation functions	Host, network, identity, email, exfiltration, persistence and malware investigation; timeline reconstruction; IOC/IOA hunting
Response functions	Playbook-driven containment, eradication verification and recovery monitoring
Evidence handling	Retention, hashing (for example SHA-256) and chain-of-custody records for collected and exported evidence
Frameworks and reporting	NIST-aligned lifecycle, MITRE ATT&CK mapping, case management, incident and compliance reporting

AREA	SUMMARY
Deployment	On-premises, hybrid, sovereign and air-gapped; single-tenant and multi-tenant operation for service providers
Outcome	Faster detection, accurate scoping, coordinated response, defensible evidence and audit-ready reporting

6.1 Assumptions and dependencies

The capability described in this document rests on four conditions. Each is worth confirming during solution design rather than during an incident.

Evidence scope. Evidence is available only for sources onboarded to Seceon OTM before or during the incident, and only for the retention period configured in LTS.

Acquisition tooling. Memory, disk-image and triage acquisition use integrated or customer-provided forensic tooling. Seceon OTM supports the case, metadata and chain-of-custody workflow around it.

Response integrations. Response actions depend on integrations with the customer's endpoint, firewall, identity and ticketing products.

Release and licensing. Agent, connector and log-source support, and specific feature behaviour, depend on the deployed Seceon OTM version and licensing.

Preparation determines what an investigation can establish. The sources onboarded and the retention configured before an incident set the ceiling on what any DFIR process can reconstruct afterwards.

Review this against your environment

The value of a DFIR capability depends on which of your sources are onboarded, how long evidence is retained, and which response integrations are in place. Ask for a working session against your current log sources, retention policy and control points, and we will map this document onto what your environment can actually support today.

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