



TECHNICAL CAPABILITY DOCUMENT

Digital Forensics

Architecture, investigation workflow and feature set for evidence-driven investigation across endpoints, servers, virtual workloads, mobile and removable media.

Seceon OTM · SIEM, XDR, EDR, Digital Forensics

Ver-2.0-2026

Seceon OTM Digital Forensics extends the platform from security detection and response into evidence-driven investigation. This document describes the architecture, the investigation workflow and the feature set: what the platform collects from an endpoint, how evidence integrity is maintained, what an analyst sees at each stage, and how the resulting case produces a defensible investigation report.

Document title	Seceon OTM Digital Forensics: Capabilities, Architecture and Investigation Workflow
Document type	Technical / RFP-RFI response reference
Platform	Seceon OTM (SIEM, XDR, EDR, Digital Forensics)
Coverage	Windows, Linux and macOS endpoints and servers; memory, disk and logical acquisition; operating-system artifacts; mail and application databases; offline forensic images; mobile and removable media; virtual and container workloads; multi-tenant operation
Version	Ver-2.0-2026
Classification	Confidential

CONTENTS

1. Executive summary.....	3
2. Investigation lifecycle.....	3
3. Platform architecture.....	3
4. Endpoint forensic triage.....	4

5. Memory forensics.....	5
6. Disk and logical evidence acquisition.....	5
7. Evidence timeline.....	5
8. IOC extraction and correlation.....	5
9. Case management.....	6
10. Chain of custody.....	6
11. Automated forensic investigation workflow.....	6
12. Worked example: process hollowing.....	6
13. Investigation workflow in the OTM console.....	7
14. Product positioning.....	7
15. Capability set.....	7
16. Outcome.....	8
17. Detailed capability coverage.....	8
17.1 Evidence integrity, endpoint acquisition and file-system forensics.....	8
17.2 Windows registry and user-activity artifact forensics.....	9
17.3 Linux, macOS and server artifact forensics.....	9
17.4 Local mail and database parsing.....	9
17.5 Offline forensic image and media analysis.....	10
17.6 Mobile, removable media and peripheral evidence.....	10
17.7 Virtual workload and container forensics.....	11
17.8 Multi-tenant and service-provider operation.....	11
18. Capability-to-workflow mapping.....	11
19. Product differentiation.....	12
20. Evidence-handling practice.....	12

DOCUMENT HISTORY

VERSION	DATE	SUMMARY
1.0	May 2025	Initial release
2.0	October 2026	Cross-platform, mobile, virtual workload and multi-tenant coverage added

1. Executive summary

Seceon OTM Digital Forensics extends the platform from security detection and response into evidence-driven investigation. An analyst moves, without leaving the platform, from an alert to endpoint triage, evidence acquisition, forensic analysis, timeline reconstruction, IOC extraction, containment, remediation and a final investigation report.

The organising idea is that a forensic investigation is not a separate activity from incident response. In most environments an analyst who needs evidence leaves the detection platform, works in a dedicated forensic tool, and then reconciles the two by hand. Seceon OTM keeps the alert, the endpoint, the evidence, the timeline, the indicators, the response actions and the final report inside one investigation case.

Forensic collection is initiated from an existing incident or detection. The analyst does not open a second tool, re-establish scope, or maintain a separate evidence trail alongside the one the incident already has.

2. Investigation lifecycle

The investigation lifecycle runs through seven stages.

ALERT	INVESTIGATE	ACQUIRE	ANALYZE	CONTAIN	REMEDiate	REPORT
Detection raised	Triage the endpoint	Collect evidence	Artifacts and timeline	Limit the damage	Remove access	Document findings

The capability integrates with Seceon EDR and XDR, so that forensic collection starts from an incident or detection that already exists in the platform, carrying its host context, its asset and identity attribution and its case record with it.

3. Platform architecture

Digital Forensics sits alongside the SIEM and log analytics, XDR and correlation, and EDR endpoint telemetry layers of Seceon OTM, drawing on the same host and incident context rather than collecting independently.

OTM LAYER	COMPONENTS
SIEM / log analytics	Log collection, normalisation and retention
XDR / correlation	Cross-source correlation and threat prioritisation
EDR endpoint telemetry	Process, file, registry and network host telemetry
Digital Forensics	Automated forensic triage; evidence acquisition (files and artifacts, memory images, disk and logical images); evidence repository; timeline and IOC analysis; case management; chain of custody; investigation reports

Seceon OTM Digital Forensics

End-to-end evidence acquisition and analysis workflow, from detection to investigation report

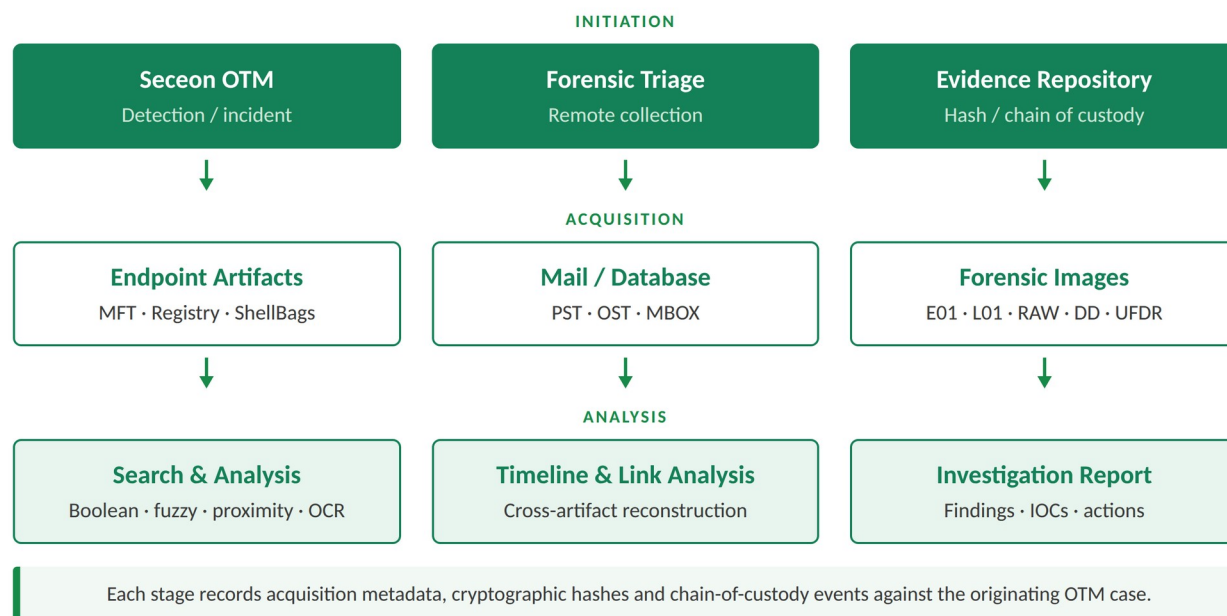


Figure 1 · Seceon OTM Digital Forensics architecture and investigation workflow

4. Endpoint forensic triage

First response collects high-value evidence without imaging the entire endpoint. Full imaging is slow, intrusive and often unnecessary to answer the question actually in front of the analyst. Triage runs against Windows, Linux and macOS hosts, physical or virtual, and covers:

- Running processes, the process tree, command lines and parent/child relationships
- Executable metadata, file paths and cryptographic hashes
- Active network connections, DNS cache and related network artifacts
- Logged-in users, sessions and account information
- Windows Event Logs, PowerShell and security telemetry
- Registry persistence, services and scheduled tasks
- Startup folders and other persistence locations
- Prefetch, Amcache and Shimcache artifacts
- Browser history, downloads and extensions, where authorized
- USB and removable-media activity
- WMI activity and persistence artifacts
- Linux auditd, syslog, shell history, cron and systemd unit definitions
- macOS unified logs, LaunchAgents, LaunchDaemons and quarantine metadata
- Container runtime and orchestration records where the host carries workloads

5. Memory forensics

Memory acquisition is available for high-severity incidents where disk artifacts are insufficient on their own. It matters most for fileless malware, process injection, credential theft and other evidence that exists only in volatile memory. The analysis surfaces processes and loaded modules, injected or otherwise suspicious memory regions, handles and execution artifacts, network connections, in-memory malware indicators, and potential credential-access artifacts.

6. Disk and logical evidence acquisition

For major investigations the platform supports logical collection and full forensic imaging. Original evidence is protected from modification, and analysis is performed against a working copy. Supported image formats are RAW/DD, E01 and AFF4.

Each evidence item carries a cryptographic hash, an acquisition timestamp, the source endpoint, the identity of the collector, and its evidence status.

7. Evidence timeline

OTM correlates EDR telemetry, SIEM events and forensic artifacts into a single chronological investigation timeline. The extract below shows the shape of a reconstructed intrusion sequence.

TIME	ACTIVITY	EVIDENCE
09:41:12	User downloaded invoice.zip	Browser / file artifact
09:41:19	Archive extracted	File-system artifact
09:41:22	PowerShell started	Process / Event Log
09:41:24	Encoded command executed	PowerShell telemetry
09:41:26	Process injection observed	EDR / memory evidence
09:41:29	External connection established	Network telemetry

Seventeen seconds separate the download from the outbound connection. That compression is the argument for automated triage: by the time an analyst has opened a second console, the activity worth capturing has already finished.

8. IOC extraction and correlation

Indicators are extracted automatically from collected evidence and made searchable across the OTM environment, so that one endpoint's findings drive cross-endpoint investigation and hunting. The extraction covers:

- File hashes, including SHA-256 and other supported algorithms

- File names, paths and metadata
- Domains, URLs and IP addresses
- Process names, command lines and execution paths
- Registry keys, services and scheduled tasks
- Certificates and digital-signature information
- Mutexes, named pipes and other host-level execution markers
- Email addresses, message IDs and sender infrastructure drawn from mail stores
- Container image digests and registry references

9. Case management

The case is the container for everything an investigation produces: its status as active, closed or archived; the evidence inventory; investigation notes and findings; the timeline; the IOC repository; analyst actions; the evidence access history; and the final investigation report.

10. Chain of custody

For evidence intended for formal investigation, OTM maintains an auditable chain of custody. The record for each item includes its evidence ID, source endpoint, evidence type, acquisition date and time, collector or analyst, SHA-256 hash, whether it is the original or a working copy, and its access and handling history.

11. Automated forensic investigation workflow

The automated path through an investigation runs as follows.

1. A high-severity detection triggers forensic triage.
2. OTM collects the selected volatile and persistent artifacts.
3. The forensic engine extracts indicators and reconstructs the timeline.
4. The analyst reviews the findings and determines whether deeper acquisition is required.
5. Memory or disk acquisition is initiated for deeper investigation.
6. Evidence is hashed and recorded in the case.
7. Containment and remediation actions are linked to the investigation.
8. A final report is generated with evidence, findings, IOCs and actions.

12. Worked example: process hollowing

Take a process-hollowing detection involving ScreenConnect.ClientService. The investigation workflow collects the affected process metadata, the parent and child process relationships, executable and DLL information, hashes, network connections and persistence artifacts, and, where the severity justifies it, memory evidence. The resulting case correlates those artifacts with the original detection and produces an investigation timeline, without the analyst assembling the sequence by hand from three separate tools.

13. Investigation workflow in the OTM console

The capability is exposed as a coherent path through the product rather than a set of disconnected screens.

STEP	SCREEN	PURPOSE
1	Incident / alert → Investigate	Entry point from an existing detection
2	Forensic triage	Initiate and review first-response collection
3	Acquire evidence	Select and run deeper acquisition
4	Evidence explorer	Browse what has been collected
5	Memory analysis	Examine volatile evidence
6	Disk / file analysis	Examine persistent evidence
7	Timeline	Reconstruct the sequence of events
8	IOC explorer	Review and pivot on extracted indicators
9	Chain of custody	Inspect the evidence handling record
10	Case report	Produce the investigation output
11	Cross-endpoint hunt	Pivot an indicator across the estate from inside the case

14. Product positioning

Seceon OTM Digital Forensics provides an integrated DFIR workflow that connects security detection with endpoint evidence collection and investigation. Rather than treating a forensic investigation as a separate activity performed in a separate tool, OTM connects the alert, the endpoint, the evidence, the timeline, the indicators, the response actions and the final report inside one investigation case.

15. Capability set

The capability is delivered in five groups. The table below summarises what each contains and how it is classified for packaging and discovery.

GROUP	CAPABILITY	CLASSIFICATION
Group 1	Forensic triage, artifact collection, IOC extraction, timeline and case management	Core
Group 2	Memory acquisition and analysis, and advanced Windows artifacts	Advanced
Group 3	Logical and full disk imaging, evidence repository and enhanced chain of custody	Advanced

GROUP	CAPABILITY	CLASSIFICATION
Group 4	Automated forensic analytics, cross-endpoint hunting and investigation automation	Strategic
Group 5	Mobile and removable media evidence, virtual and container workload forensics, and multi-tenant operation for service providers	Strategic

16. Outcome

The result is a unified Seceon investigation workflow in which an analyst starts from a detection, collects the evidence required, reconstructs what happened, identifies the affected systems and indicators, preserves evidence integrity, performs response actions, and generates a defensible investigation report — all within one case and one platform.

17. Detailed capability coverage

The capabilities below are delivered in Seceon OTM Digital Forensics. They span endpoint evidence acquisition across Windows, Linux and macOS, operating-system artifact parsing, local mail and database analysis, offline forensic image analysis, advanced search and OCR, visual relationship analysis, mobile and removable media, virtual and container workloads, and multi-tenant operation.

17.1 Evidence integrity, endpoint acquisition and file-system forensics

CAPABILITY	DETAIL
Cryptographic hashing	Generates MD5, SHA-1 and SHA-256 hashes of raw files on disk to establish and verify forensic chain of custody.
File-system structure extraction	Extracts raw directory structures and low-level, file-system-specific timestamps, including Master File Table (MFT) records on NTFS and equivalent metadata on other file systems.
Remote file-system browsing	Provides an interactive visual exploration tool to browse a remote endpoint's local file-directory structure before committing to a collection.
Targeted content extraction	Selectively extracts or pulls raw physical file contents from endpoints using keyword, filename or regular-expression filters.
Deleted and slack-space recovery	Recovers deleted file records and examines unallocated and slack space within collected volumes and images.
Volatile user-context capture	Captures, pulls and stores volatile user clipboard text logs, subject to endpoint collection policy and authorization.

17.2 Windows registry and user-activity artifact forensics

CAPABILITY	DETAIL
Offline registry hive analysis	Remotely extracts and opens offline Windows Registry hives (SOFTWARE, SYSTEM, SECURITY, NTUSER) and presents their structures for analysis.
User-activity artifacts	Parses local host-user activity configurations and artifacts such as ShellBags, UserAssist shortcuts and TypedPaths.
Document and shortcut history	Extracts and parses RecentDocs and related .LNK files to reconstruct activity across applications that were not directly monitored.
Shell folder analysis	Analyzes local ShellFolders for default folder paths, shortcut relationships and associated artifacts.
Resource usage history	Extracts and parses Windows System Resource Usage Monitor data (srudb.dat) for per-application network and resource history.
Execution artifacts	Parses Prefetch, Amcache and Shimcache for evidence of execution, including binaries no longer present on disk.
Event log analysis	Parses Windows Event Logs, PowerShell operational and script-block logs, and security telemetry.

17.3 Linux, macOS and server artifact forensics

CAPABILITY	DETAIL
Linux host artifacts	Collects and parses auditd and syslog records, shell history, cron and systemd unit definitions, SSH authorized_keys and known_hosts, and package-manager history.
macOS host artifacts	Collects and parses unified logs, LaunchAgents and LaunchDaemons, plist configurations, quarantine metadata and keychain access records.
Server and application logs	Ingests web server, application server, database and middleware logs from the affected host for correlation with host-level activity.
Persistence across platforms	Identifies persistence mechanisms specific to each platform and maps them to the corresponding MITRE ATT&CK techniques.

17.4 Local mail and database parsing

CAPABILITY	DETAIL
Microsoft mail stores	Parses and deep-scans local Microsoft Mail data files (.PST and .OST), including message contents, headers and attachments.

CAPABILITY	DETAIL
Standalone Outlook databases	Opens, indexes and audits standalone Microsoft Outlook database files (.PST) recovered from an endpoint or an image.
Open-format mail stores	Ingests, opens and parses Mozilla Thunderbird mail stores and related .mbox data.
Local application databases	Parses local SQLite and comparable application databases, including browser history, messaging clients and cached application state.

17.5 Offline forensic image and media analysis

CAPABILITY	DETAIL
Image format support	Ingests and views standard raw and wrapped forensic image formats, including .E01, .L01, .DD, .RAW, .AFF4 and .UFDR.
Advanced content search	Performs Boolean, fuzzy, phrase and proximity searches inside static offline forensic disk images and collected evidence sets.
Nested structures and OCR	Extracts metadata from nested archive and image structures and processes image content using Optical Character Recognition.
Visual link analysis	Generates document-to-document visual link analysis from extracted file parameters and relationships.
Keyword and entity lists	Applies analyst-supplied keyword, entity and regular-expression lists across an entire image in a single pass.

17.6 Mobile, removable media and peripheral evidence

CAPABILITY	DETAIL
Removable media history	Reconstructs USB and removable-media connection history, including device identifiers, mount points and first and last connection times.
Mobile extraction ingestion	Ingests mobile extraction packages in .UFDR and comparable formats into the same case, timeline and search workflow as endpoint evidence.
Peripheral and print activity	Collects evidence of peripheral use and print activity where the operating system records it and collection policy permits.
Cross-device correlation	Correlates removable-media and mobile evidence with endpoint file access and network egress to support data-movement investigation.

17.7 Virtual workload and container forensics

CAPABILITY	DETAIL
Virtual machine evidence	Ingests virtual disk and memory artifacts captured through hypervisor snapshot facilities, and records the acquisition metadata in the case.
Container and orchestration evidence	Collects container runtime events, image and registry metadata, and orchestration audit records for the affected workload.
Ephemeral workload handling	Preserves evidence from short-lived workloads by retaining collected telemetry independently of the workload lifecycle.
Workload-to-identity attribution	Links a workload to the identity and the control-plane action that created it, so an investigation reaches the operator and not only the host.

17.8 Multi-tenant and service-provider operation

CAPABILITY	DETAIL
Tenant isolation	Keeps evidence, cases and reports segregated per tenant, so a service provider can investigate for several customers from one deployment.
Role-based evidence access	Restricts acquisition and evidence access by role, and records every access against the case audit trail.
Per-tenant retention	Applies retention and evidence-handling policy per tenant, matching the obligations of each customer rather than a single shared setting.
Consolidated and per-tenant reporting	Produces investigation reports scoped to one tenant, and operational reporting across the estate for the provider.

18. Capability-to-workflow mapping

These functions are exposed as one investigation workflow, so an analyst starts from a Seceon alert and moves progressively from remote triage through artifact extraction and offline analysis to evidence reporting.

9. Identify the affected endpoint and open the associated OTM investigation case.
10. Perform remote forensic triage and interactively browse the endpoint's file structure.
11. Collect selected files or raw contents using filename, keyword or regex criteria.
12. Calculate and record cryptographic hashes for the collected evidence.
13. Extract Windows file-system artifacts such as MFT records and low-level timestamps.
14. Collect and analyze Registry hives, ShellBags, UserAssist, TypedPaths, RecentDocs, ShellFolders and SRU data on Windows, or the equivalent auditd, unified-log and persistence artifacts on Linux and macOS.
15. Parse local mail stores and attachments where the investigation requires mailbox evidence.
16. Ingest forensic images such as E01, L01, DD, RAW or UFDR into the offline analysis workflow.
17. Run advanced content searches and OCR across the forensic image or collected evidence.

18. Generate timelines, relationships and document-to-document visual link analysis.
19. Pivot any extracted indicator across the rest of the estate to establish the true scope of compromise.
20. Preserve evidence metadata and chain-of-custody records, and generate the final investigation report.

19. Product differentiation

The combination of live endpoint telemetry, remote forensic acquisition, cross-platform artifact parsing, mail-store analysis, forensic image processing, mobile and removable-media evidence, and visual investigation provides a continuous path from detection to evidence-based investigation. The SOC analyst and the forensic investigator work from the same incident context instead of exchanging exports, and evidence integrity and traceability are preserved throughout.

20. Evidence-handling practice

Six constraints govern how evidence is handled. They are as much a part of the capability as the feature list, because a forensic tool that cannot demonstrate its own handling discipline has limited value in the proceedings its output is meant to support.

Policy-controlled acquisition. Evidence acquisition is policy-controlled and auditable.

Original integrity. Original evidence is protected from modification, and analysis is performed against a verified working copy.

Hashing at acquisition. Cryptographic hashes are calculated at the point of acquisition and retained with the case record.

Authorization and privacy. Access to clipboard, mail, registry and user-activity artifacts follows applicable organizational authorization and privacy requirements.

Custody events. Chain-of-custody events record who acquired, accessed, exported or analyzed each evidence item.

Separation in reporting. Reports distinguish collected evidence, automated findings and analyst conclusions.

See it against a case you have already worked

The fastest way to judge a forensic capability is against an investigation your team has already been through by hand. Ask for a walkthrough using your own endpoint estate and artifact types, and compare the evidence trail and the time to a defensible report against what that investigation actually cost you.

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