

Seceon DFIR

Digital Forensics and Incident Response

Live host evidence and offline disk-image investigation in the same case as detection with timeline, NSRL filtering, chain of custody, and audit-ready reports on Seceon OTM.



Product Overview

Seceon DFIR puts digital forensics and incident response on the same Open Threat Management platform that already detects and responds. Analysts do not leave the console to collect host artifacts, ingest a disk image, reconstruct a timeline, or produce a defensible report.

Telemetry from endpoints, network, identity, email, cloud, and OT is collected and correlated by the Collection and Correlation Engine (CCE), analyzed by the Analytics and Policy Engine (APE), and retained in Long-Term Storage (LTS). The Digital Forensics investigation layer is where that evidence becomes a case: live collections, offline images, search, timeline, custody, and reporting.

The practical outcome is faster scoping, coordinated containment, and evidence that survives audit, regulatory, and legal scrutiny.



What Analysts See in Digital Forensics

Grounded in the live Digital Forensics module (Cases and Host evidence).



Highlights



One investigation case from alert to evidence to report not a second forensic tool beside SIEM/XD



Live host evidence from Linux and Windows agents (hashed artifacts, in-page preview, attach to case)



Offline disk-image investigation (E01, DD, RAW, ZIP; L01 when ZIP-compatible)



Content search (simple, Boolean, phrase, fuzzy, proximity) with NSRL known-good filtering



Timeline, relationship graph, custody manifest, playbook, PDF/CSV reports



Evidence retained with SHA-256 hashing and an auditable chain of custody



Platform correlation through CCE, APE, and LTS for look-back, hunting, and response

Area	What it does
Cases	Create and manage open/closed cases; search by name or ID; short case IDs
Host evidence	Collect hashed artifacts from live Linux/Windows agents; preview in-page; attach to a case
Acquire from agent	Pull evidence from a selected agent into the case
Offline images	Add E01 / DD / RAW / ZIP images; ingest; browse the file tree
Upload from workstation	Upload an image from the analyst workstation into the case
Browse files	Walk ingested trees; preview, download, bookmark, extract into custody
Search content	Indexed text and paths: simple, Boolean (AND / OR / NOT / phrase), fuzzy, proximity; optional hide NSRL-known
NSRL	Import SHA-256 known-good sets; chip files as NSRL; filter them from search noise
Timeline	Ordered events (time, source, kind, path); export CSV
Graph / relationships	Node-edge view of extracted relationships, with a table fallback
Findings & notes	Case findings and analyst notes
Custody	Evidence handling record; download JSON custody manifest
Playbook	Investigation playbook plus queued PDF report and CSV report
Jobs	Track collect, ingest, extract, and report jobs

Typical case workflow in the console

- Create a case
- Add an image (or acquire / collect host evidence)
- Browse and extract
- Record custody and generate the report



DFIR Lifecycle (NIST-aligned)

Phase	Objective	Seceon support
Preparation	Visibility, retention, playbooks, roles	Continuous collection; LTS retention; playbook library

Phase	Objective	Seceon support
Detection and analysis	Validate the incident and determine scope	APE AI/ML and UEBA; Digital Forensics search, timeline, graph
Containment	Stop spread without destroying the audit trail	Orchestrated response; actions recorded against the case
Eradication	Remove malware, persistence, and access	IOC/IOA hunting; host and image artifact review
Recovery	Restore and confirm normal operation	Post-recovery monitoring and re-detection
Post-incident	Learn, report, improve	PDF/CSV case reports, custody manifest, detection tuning



Evidence Sources and Forensic Value

Domain	Example evidence	Forensic value
Endpoints and servers	Process, file, registry, logon, script, USB; live hashed collections	Execution chain, malware behaviour, persistence, attribution
Disk and media	E01, DD, RAW, ZIP (and ZIP-compatible L01) images	Deep file-system investigation when live telemetry is not enough
Network and perimeter	Firewall, IDS/IPS, proxy, DNS, VPN, WAF, NetFlow	Entry, C2, lateral movement, exfiltration
Identity and email	AD / Entra ID, MFA, mailbox and gateway events	Credential theft, phishing delivery, privilege abuse
Cloud and SaaS	CloudTrail, Azure/GCP audit, SaaS trails	Control-plane abuse spanning on-prem and cloud
OT / ICS	Protocol telemetry, historian/HMI, jump-host access	IT-to-OT crossing and affected control systems
Known-good filtering	NSRL SHA-256 imports	Reduce noise so unknown files stand out

Key Capabilities

Digital Forensics casework (core product surface)

- Live host evidence collection with hashes and in-page preview
- Offline image ingest, tree browse, extract-to-custody
- Content search with Boolean / fuzzy / proximity and NSRL hide-known
- Timeline and relationship graph
- Chain of custody with downloadable JSON manifest
- Playbook-driven PDF and CSV investigation reports

Platform DFIR (OTM)

- Unified evidence model via CCE (parse, normalize, correlate)
- Prioritized threats and ATT&CK-mapped analytics via APE
- Look-back and preservation via LTS (raw and normalized retention)
- Cross-domain pivot: host, network, identity, email, cloud, OT



Primary Use Cases

Use case	How Seceon DFIR helps
Ransomware outbreak	Host process/file evidence + image review + timeline; isolate via playbooks; report for recovery and insurance
Phishing to credential theft	Correlate mailbox/identity events with host execution; collect artifacts; document affected accounts
Insider data movement	USB/file/cloud evidence plus hashed host collections and custody records
Disk-image investigation	Ingest E01/DD/RAW, search content, extract exhibits, emit custody manifest
Known-good noise reduction	NSRL import so analysts hunt unknowns, not operating-system files
MSSP / multi-tenant IR	Tenant-isolated agents, jobs, inventory, cases, and reports



Why Seceon DFIR

Differentiator	Benefit
Same platform as detection	Alert, host, image, timeline, IOCs, response, and report stay in one case
Live + offline in one module	Agent collect and disk-image ingest without swapping tools

Differentiator	Benefit
Search that matches how investigators work	Boolean, phrase, fuzzy, proximity – not keyword-only
NSRL in the same search path	Known-good hashes filtered at investigation time
Defensible output	SHA-256, custody manifest, PDF/CSV reports
OTM-native	CCE / APE / LTS correlation and retention behind the case



Technical Highlights (SE / RFP)

- Case API family under /api/v1/forensics/cases (images, ingest, files, search, timeline, findings, notes, playbook, report, custody, acquire)
- NSRL import/status APIs for SHA-256 known-good sets
- Image formats: E01, DD, RAW, ZIP; L01 when ZIP-compatible
- Timeline export CSV; case report PDF and CSV
- Custody manifest JSON for chain-of-custody packages
- Live collections run as jobs against Linux/Windows agents
- Multi-tenant isolation of agents, jobs, inventory, and cases



Ideal Buyers

- Enterprises that already run Seceon aiSIEM / aiXDR / OTM and need DFIR without a sidecar forensic stack
- SOC teams that must produce audit-ready evidence packages
- MSSPs delivering investigation as a service with tenant isolation
- Regulated sectors (financial, healthcare, government, critical infrastructure) that need look-back retention and host/image forensics



Related Public Documents

Document	URL
Digital Forensics (Ver-2.0-2026)	https://seceon.com/wp-content/Seceon OTM Digital Forensics.pdf
Digital Forensics and Incident Response (Ver-2.0-2026)	https://seceon.com/wp-content/Seceon OTM DFIR.pdf

Document	URL
Cloud and Private Cloud Forensics (Ver-2.0-2026)	https://seceon.com/wp-content/Seceon OTM Cloud Forensics.pdf
Seceon datasheets hub	https://seceon.com/datasheets/

One-Line Pitch

Seceon DFIR lets SOC and forensic teams investigate live hosts and offline disk images in the same case as detection and response with search, timeline, NSRL filtering, chain of custody, and audit-ready reports on the Seceon OTM platform.

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon



Schedule a Demo

www.seceon.com/contact-us/

