

Seceon Digital Forensics

Evidence-driven investigation on Seceon OTM

Live host evidence, offline disk images, local mail parsing, timeline, chain of custody, and audit-ready reports in the same case as detection.



Product Overview

Seceon Digital Forensics extends the Open Threat Management platform from detection and response into evidence-driven investigation. An analyst moves from an alert to endpoint triage, evidence acquisition, forensic analysis, timeline reconstruction, IOC extraction, and a defensible report without opening a second tool.

Digital Forensics sits alongside SIEM/log analytics, XDR correlation, and EDR telemetry, drawing on the same host and incident context. Original evidence is protected; analysis runs against working copies; cryptographic hashes and custody records travel with the case.



Investigation Lifecycle

Alert → Investigate → Acquire → Analyze → Contain → Remediate → Report. Collection can start from an existing incident so host context, identity attribution, and the case record stay attached.



Highlights



Start from a detection and stay in one case through triage, acquisition, analysis, and report



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



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



Local mail parsing: Microsoft .PST / .OST and Thunderbird .mbox, including attachments



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



Timeline, relationship graph, SHA-256 hashing, chain of custody, PDF/CSV reports



What Analysts See in the Console

Area	What it does
Cases	Open/closed case management; search by name or ID
Host evidence	Live Linux/Windows collection; hash, preview, and attach to case
Acquire / upload	Acquire from agent or upload an image from the workstation
Offline images	Ingest E01/DD/RAW/ZIP; browse tree; extract into custody
Local mail parsing	Parse PST/OST/mbox; extract messages and attachments
Search content	Indexed text and paths; Boolean, fuzzy, and proximity search; hide NSRL
NSRL	Import SHA-256 known-good sets; filter OS noise
Timeline / Graph	Ordered events and relationship nodes/edges
Custody	Handling record and JSON custody manifest
Playbook / Report	Investigation playbook; PDF and CSV case reports

Typical workflow: create a case → add an image or collect host evidence → browse and extract → custody and report.



Capability Groups

Group	Capabilities
Core	Forensic triage, artifact collection, IOC extraction, timeline, and case management
Advanced	Memory acquisition and analysis; logical and full disk imaging; enhanced chain of custody
Strategic	Automated analytics, cross-endpoint hunting, mobile/removable media, virtual/container workloads, and multi-tenant operation
Local mail	Microsoft Mail PST/OST deep scan (contents and attachments); standalone Outlook PST indexing; Thunderbird mbox ingest and parse



Endpoint and Artifact Coverage

- Running processes, command lines, hashes, network connections, logged-in users
- Windows Event Logs, PowerShell, registry persistence, services, scheduled tasks
- Prefetch, Amcache, Shimcache; USB and removable-media history
- Linux auditd, syslog, shell history, cron/systemd; macOS unified logs and LaunchAgents
- File-system metadata (including NTFS MFT where collected)
- Local mail stores (.PST / .OST / .mbox) and extracted attachments



Evidence Handling

- Policy-controlled, auditable acquisition
- Originals protected; analysis on hashed working copies
- SHA-256 (and MD5/SHA-1 where generated) at acquisition
- Chain-of-custody events: who acquired, accessed, exported, or analyzed each item
- Reports distinguish collected evidence, automated findings, and analyst conclusions



Why Seceon Digital Forensics

Differentiator	Benefit
Same platform as detection	Alert, host, image, mail, timeline, response, and report stay in one case
Live + offline together	Agent collection and disk-image ingest without switching tools
Mail in the same case	PST/OST/mbox parsed as nested exhibits, not a separate mailbox tool
Investigator-grade search	Boolean, phrase, fuzzy, and proximity search plus NSRL known-good filtering
Defensible output	Hashes, custody manifest, and PDF/CSV reports

One-Line Pitch

Seceon Digital Forensics lets analysts start from a detection, collect live and offline evidence including disk images and local mail stores reconstruct the timeline, preserve chain of custody, and issue an audit-ready report 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/

