■ INCIDENT RESPONSE & FORENSICS

Full-scope IR, on a single *platform.*

Collect, preserve and analyze evidence at scale — across endpoints, cloud, identity, network and email — in one console. No stitching together a dozen DFIR tools, no per-seat forensic licenses. Stand up an investigation in minutes and pay only for the data you ingest.

FIG. 01 — ONE CORRELATED CASE FILE ACROSS ENDPOINT, CLOUD, IDENTITY AND EMAIL.

01 / Collect

Get the data.

Forensic triage and live-response collection across endpoint, cloud, identity and email — sensors deploy in minutes.

02 / Analyze

Find the story.

Timeline reconstruction, behavioral analytics and threat hunting over billions of events in one correlated case file.

03 / Contain

End it fast.

Isolate hosts, revoke access and run SOAR playbooks to contain intrusions — with chain of custody intact.

IR & FORENSICS CAPABILITIES

12 MODULES · ONE CASE FILE

01
Rapid Triage Collection
Volatile + persistent artifacts in minutes, no pre-staged agents.

02
Live Response
Run commands, pull files and acquire memory on remote hosts.

03
Timeline Analysis
Reconstruct the full attack sequence on one correlated timeline.

04
Disk & Memory Forensics
Examine images and memory for malware and credential theft.

05
Threat Hunting
Behavioral analytics and IOC / IOA matching at cloud scale.

06
Host Containment
Isolate endpoints and workloads while preserving evidence.

07
Identity Investigation
Trace account takeover and lateral movement across SaaS.

08
Cloud Forensics
AWS, Azure and GCP control-plane logs, configs and snapshots.

09
Email Compromise
Trace phishing and BEC: message paths and mailbox rules.

10
Malware Analysis
Detonate and triage files; extract IOCs for the SOC.

11
Chain of Custody
Tamper-evident audit trails built for legal review.

12
SOAR & Playbooks
Codify response into repeatable, owner-assigned playbooks.

PLATFORM SPECIFICATIONS

CLOUD-NATIVE · MULTI-TENANT

ARCHITECTURE	Cloud-native SaaS · multi-tenant · zero on-premise infrastructure.
DEPLOYMENT	Investigation live in minutes across endpoint, cloud, identity and email.
ANALYSIS	Correlated timelines and threat hunting tuned for billion-event cases.
PRICING	Ingest-based · unlimited investigators and cases · no per-seat fees.
INTEGRATIONS	Hundreds of on-prem and cloud data sources, connected in clicks.
SOC SUPPORT	Dedicated DFIR team for expert-led response and threat hunting.

"We recommend Cylerian to clients early in the security maturity curve, and to established teams looking to improve their posture with a more holistic solution."

DAVID ARMSTRONG · APHTHORIA

WEB cylerian.com
SALES sales@cylerian.com
PHONE +1 (833) 295-7426