

OSM

SOC AI

Your AI Security Operations Center — running with your team, not instead of it

L1 SOC Analyst

Security Operations Specialist

CISO Assistant

Three agents cover the SOC shift end to end: the L1 SOC Analyst triages every alert, the Security Operations Specialist investigates and coordinates the response, and the CISO Assistant turns the night into decisions and board-ready reporting. Every material action still passes a human.

The three-tier SOC AI model

01

Tier 1

L1 SOC Analyst — Watch and Triage

Monitors every alert around the clock, correlates it against asset context and threat intelligence, kills the false positives and escalates only what is real — with the evidence already attached.

Alert noise cut
93%

Coverage
24/7/365

Escalation

02

Tier 2

Security Operations Specialist — Investigate and Respond

Picks up escalations, reconstructs the incident across tools and layers, builds the containment and remediation plan, and drives it through your existing ITSM, EDR and firewall stack to closure.

Repetitive work
80-94% automated

MTTR
Hours, not weeks

Action

03

Tier 3

CISO Assistant — Decide and Report

Rolls the shift up into business language: what was hit, what it would have cost, what changed, what needs a decision — as an executive brief, a board pack or an audit trail, generated on demand.

Faster reporting
84%

Communication
+91%

Decision

HUMAN IN THE LOOP

What changes on day one

93%

Less alert noise
Only verified incidents

24/7

Shift coverage
No handover gaps

4h

Mean time to detect
Down from days

84%

Faster reporting
Exec and audit ready

OSM

Offensive
Security
Manager

<https://www.ofsecman.io>

01

Agent

L1 SOC Analyst

Detection and triage

Runs 24/7

Runs autonomously

- Watches every alert from SIEM, EDR, scanners and CI/CD.
- Correlates each signal against asset context and live threat intel.
- Deduplicates and closes the noise – 93% never reaches a person.
- Escalates real incidents with evidence and blast radius attached.

Escalates to humans

- Anything that looks like an active intrusion.
- Ambiguous signals where business context is missing.
- Containment that would touch production.

Triage

Continuous

Noise removed

93%

Escalations

Evidence-first

02

Agent

Security Operations Specialist

Investigation and response

Runs 24/7

Runs autonomously

- Reconstructs the incident across network, web, container and code.
- Builds containment and permanent remediation together.
- Drives the work through your ITSM, EDR, firewall and DevOps tools.
- Tracks SLA, ownership and progress to closure.

Escalates to humans

- The decision to isolate, block or take a service down.
- Remediation that changes architecture or business process.
- Anything crossing a legal, privacy or disclosure threshold.

Coordination

Cross-tool

Repetitive work

80–94% automated

MTTR

Hours

03

Agent

CISO Assistant

Decision support and reporting

Runs 24/7

Runs autonomously

- Aggregates the shift into risk in business terms, not alert counts.
- Answers what the board asks: what happened, what it cost, what changed.
- Generates executive briefs, audit evidence and compliance packs.
- Flags where posture is drifting and where budget is the constraint.

Escalates to humans

- Risk acceptance and residual risk sign-off.
- Budget, headcount and roadmap decisions.
- External communication – regulators, customers, press.

Reporting

84% faster

Communication

+91%

Audit

Zero-touch evidence

One shift, three agents, one team



The shift board – who is on, and when

	00:00	06:00	12:00	18:00	24:00
LI SOC Analyst	Continuous watch				
Sec Ops Specialist	On every escalation				
CISO Assistant	Rolling brief + on demand				
Your team	Business hours / on call				

A single night, step by step

03:14

LI SOC Analyst

22,890 signals overnight. One cluster on a payment service correlates with a live exploit and an asset holding cardholder data. Three alerts survive triage, one is escalated with full evidence.

03:19

Sec Ops Specialist

Reconstructs the path, confirms the blast radius, drafts containment (WAF rule now, patch tonight) and opens the change with the plan attached.

03:22

Your on-call engineer

Wakes to one page – not a backlog. Reviews the prepared plan, approves the WAF rule, defers the restart to the maintenance window. Total human time: 6 minutes.

03:24

Sec Ops Specialist

Executes the approved action across the stack, verifies containment and tracks the permanent fix against SLA until it closes.

08:00

CISO Assistant

The morning brief is already written: what happened, what it would have cost, what changed, and the audit evidence filed against PCI DSS – no one assembled it by hand.

What your team still owns

Risk acceptance

Production change approval

Isolate, block or take down

Legal, privacy and disclosure

Budget and headcount

External communication

The outcome of that night

6 min

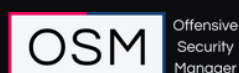
Total human time
One page, not a backlog

10 min

Signal to containment
Approved, then executed

08:00

Brief already written
Evidence filed, zero effort



<https://www.ofsecman.io>



OSM

SOC AI

Your AI Security Operations Center

01

L1 SOC Analyst

02

Security Operations Specialist

03

CISO Assistant

Agents run the shift. People make the calls.



www.ofsecman.io
contact@ofsecman.io

2026