SOCFortress

YOUR AI LEVEL 1 SOC ANALYST, BUILT INTO SOCFORTRESS COPILOT

Level 1 is where SOC hours disappear. Reclaim them.

Your AI Level 1 SOC analyst, built into SOCFortress CoPilot, gathers context and writes evidence-cited reports. Analysts decide.

Level 1 triage is repetitive and never stops. It gathers context across your security information and event management (SIEM) stack and writes structured, evidence-cited reports, so Security Operations Centre (SOC) analysts can focus on decisions.

Built for MSPs MSSPs Enterprises

THE CHALLENGE

What stands in the way

01

Triage that never stops

Every alert means the same routine: open the event, check the host, look up the hash, search for related activity, write it up and decide whether to escalate. Then the next one.

02

Evidence scattered across consoles

Evidence sits across SIEM, endpoint detection and response (EDR) and threat intel tools, so analysts spend more time hunting for data than making decisions.

03

Queues outpace analysts

Alert queues grow faster than analysts can triage them. Manual context collection is slow and inconsistent, and context is lost between shifts, analysts and customers.

THE SOLUTION

The repetitive groundwork, handled

Your AI Level 1 SOC analyst, built into SOCFortress CoPilot takes on the repetitive triage groundwork. It searches the Wazuh Indexer, queries Velociraptor, enriches indicators with threat intel and correlates related activity, then delivers a structured report: summary, raw event details, indicator of compromise (IOC) analysis, SIEM correlation, severity, confidence and recommended actions. Analysts make the call.

WHY IT'S DIFFERENT

01

Investigates, not just enriches

Multi-step investigations pivot across several data sources and build timelines, rather than relying on a single large language model (LLM) enrichment call.

02

Guardrails enforced in code

Required investigation steps always run, every IOC must appear in the evidence, claims link back to tool calls, and a suspected pentest never lowers severity.

03

Built for multi-tenant SOCs

Every tool, memory and chat thread is bound to one customer, and the customer is set by the job, never by the model. Each customer's memory of lessons and false positives stays separate.

KEY CAPABILITIES

What Your AI Level 1 SOC analyst, built into SOCFortress CoPilot delivers

Host context in every report

Agent status and last check-in, operating system, running processes, open ports, installed packages and the host's critical vulnerabilities, sourced from Wazuh and Velociraptor.

Templates that guide investigations

Built-in templates for Sysmon, Windows Defender, Autoruns and Sigcheck alerts steer what is examined. Add your own as simple text files.

Escalation on your strongest model

Critical, High and low-confidence findings are automatically re-investigated on your strongest model, while smaller models can handle simpler jobs such as summaries.

Reports routed where you work

Route reports per customer by severity to Slack, Microsoft Teams, email or ServiceNow.

Chat and a learning loop

Chat about an alert, host or customer in customer-scoped threads. Grade reports, correct IOC verdicts and teach lessons used in later investigations.

Model cost visibility and budgets

Usage and per-investigation model cost are visible in CoPilot, with daily and monthly budgets per customer and user that warn at 80% and stop runs when reached.

HOW IT WORKS

Talon runs as a lightweight, self-hosted container on a separate virtual machine (VM) next to CoPilot, with no re-architecture or migration. It connects to Wazuh, Graylog and Velociraptor through their application programming interfaces (APIs) using Model Context Protocol (MCP).

1 → 2 → 3 → 4

Alert reaches CoPilot
With automatic triggers enabled for that customer, the investigation can be complete before an analyst opens the alert.

Evidence gathered
Talon searches the Wazuh Indexer, queries Velociraptor, enriches indicators and correlates related activity, guided by a template.

Sensitive data tokenised
Usernames, hostnames, emails and internal IP addresses are tokenised before reaching the model and restored only in that customer's report.

Cited report delivered
A cited report with severity, confidence and recommended actions is routed by severity. Analysts decide and approve any action.

USE CASES

Reports ready at shift start

With automatic triggers enabled per customer, the investigation report can already be waiting when an analyst opens CoPilot, so analysts start from evidence rather than raw alerts.

Approved containment

When a host looks compromised, Talon can propose quarantining it through Velociraptor. An authorised analyst approves the action in CoPilot under their own login before anything runs.

Multi-tenant service delivery

Managed security service providers (MSSPs) keep each customer's tools, memory and chat threads separate, with provider allowlists and per-customer budgets controlling where data goes and what is spent.

WHO IT'S FOR

Value for every kind of team

MSPs

Add SOC depth without re-architecting. A lightweight container beside CoPilot handles repetitive context collection and report writing, and SOCFortress professional services can help you deploy.

MSSPs

Serve many customers from one SOC: tools, memory and chat threads are bound to one customer, with per-customer routing, provider allowlists and budgets, and each new customer starting in shadow mode.

Enterprises

Keep control of your data and spend: identifiers are tokenised before reaching the model, every run is auditable with full transcripts, and analysts approve any containment action.

WHY SOCFORTRESS

- **Humans approve every action**
  The model can only propose. Quarantine, alert changes and endpoint commands run only after an authorised analyst approves them in CoPilot.
- **Fully auditable runs**
  Every run records full transcripts, tool calls and costs. Memory is searchable, and lesson removals are audited.
- **Open source and sandboxed**
  Talon is open source on GitHub and runs in an isolated Docker container, with all tool interactions inside that sandbox.
- **Built by SIEM practitioners**
  Built by Taylor Walton, with over a decade of experience building SIEM stacks with Wazuh, Graylog, Velociraptor and Grafana.

Give your Level 1 hours back to your analysts

See how Your AI Level 1 SOC analyst, built into SOCFortress CoPilot can take on repetitive triage in your SOC. For more information, visit the SOCFortress Product Page.

For more information, visit SOCFortress Product Page → www.socfortress.co

Scan with your phone

Product information current as of 2026-10-26. Features and availability may change.