SOCFORTRESS

MDR · FOR MSPs & MSSPs

socfortress.co

MANAGED DETECTION & RESPONSE

# A SOC that works for you, without building one.

Our engineers triage your alerts, cut the noise, write new detections every day and stand with you through every incident, on an open-source platform with no vendor lock-in.

**Suspicious PowerShell on FIN-LAPTOP-07**

Illustrative example · ESCALATED

| 01 · TRIAGED | 02 · INVESTIGATED | 03 · REPORTED |
|---|---|---|
| Encoded command spawned by Outlook. Not on the client's known-good list. | Velociraptor pulls the process tree and the downloaded payload from the host. | Stakeholders get the findings and next steps. We stay with them until it's closed. |

**3,000+**
endpoints monitored

**5,000+**
detection rules in our library

**Daily**
new detections for emerging threats

Talk to our team

info@socfortress.co

THE PROBLEM

# Collecting alerts is easy. Acting on them isn't.

Most organisations already have the logs. What they lack is the people and the hours to turn them into decisions.

### Alert fatigue

Thousands of events a day, most of them noise. Real threats get buried, and analysts stop looking.

### No team to run a SOC

Hiring, training and keeping security analysts is slow and expensive, especially for smaller teams.

### Threats move daily

New techniques appear every week. Detection content that isn't updated constantly falls behind.

THE SOCFORTRESS ANSWER

## We become your security operations team.

YOU KEEP

Your tools, your data in its own isolated tenant, and full visibility into how every detection works.

→

WE HANDLE

Triage, tuning, detection engineering, incident response and the daily health of your SIEM stack.

→

YOU GET

Fewer, better alerts, clear reports, and a team on your side when something real happens.

CORE SERVICES

# What we do for you, every working day.

Six services sit at the heart of every engagement. They run continuously, not as one-off projects.

## Alert triage 01

Every alert is reviewed by an analyst who decides what is a real threat and what is benign, so your team only hears about what matters.

## Noise & alert exclusion 02

We tune exclusions continuously around your environment, removing the false positives that drown out real signal.

## Daily detection engineering 03

New detection rules are written every day for the latest threats and events, so your coverage keeps pace with attackers.

## Incident response 04

When something is real, we report it to your stakeholders and help you through the whole response, from first alert to closure.

## Daily SIEM health checks 05

Agents, log flow and indices across the stack are checked every day, so a gap in visibility is caught before it matters.

## A real SOC partnership 06

New detections, integrations, dashboards or tuning: we walk through every SOC request with you, engineer to engineer.

ALWAYS ON, NOT ONE-OFF

These services run every working day from the moment you go live, and keep adapting as your environment changes.

EXTENDED CAPABILITIES

# Deeper visibility, faster answers.

Beyond the core service, the platform gives our analysts the tools to dig in when an alert needs more than a first look.

## Threat hunting & DFIR 07

With Velociraptor we hunt across every endpoint at once and collect forensic evidence, including memory, straight from affected hosts.

## Microsoft 365 & cloud 08

Sign-ins, mailbox rules, data-loss activity and admin changes in your Microsoft 365 tenant are monitored alongside your endpoints.

## Threat intelligence 09

Alerts are enriched against threat intelligence feeds, so known-bad IPs, domains and hashes are flagged with context.

## Automated response 10

Shuffle SOAR playbooks let us act quickly and consistently on confirmed threats, with the actions agreed with you in advance.

## Endpoint visibility 11

We alert you when something looks off on a host: a suspicious package installed, an unexpected open port, or an unusual process running.

## Dashboards & reporting 12

Custom dashboards for your environment, weekly reports on activity and trends, and a full report for every incident.

THE PLATFORM BEHIND IT

Wazuh · Graylog · OpenSearch · Velociraptor · Grafana · Shuffle · SOCFortress CoPilot

WHY SOCFORTRESS

# Built differently, on purpose.

## Coverage on your hours

Our analysts work when your business is running. You get focused coverage for your operating hours without paying for capacity you don't need.

## Open source, no lock-in

The platform is built on proven open-source tools: Wazuh, Graylog, OpenSearch, Velociraptor and Grafana. Full transparency, and lower cost than proprietary stacks.

## Your data, isolated

Every client runs in its own tenant. Data, agents and alert settings are separated, and one client can never see another's results.

## Direct access to engineers

You talk to the people who build your detections and run your SOC, not a ticket queue that passes you along.

WORKS WITH WHAT YOU ALREADY RUN · NO RIP AND REPLACE

Firewalls · EDR / AV · Microsoft 365 · Cloud platforms · Backup platforms · Windows · Linux · Network devices

FOR MSPs

### Add security to your services

Offer your clients managed detection and response without hiring a security team of your own.

FOR MSSPs

### Scale your SOC

Extend your analysts with our engineering, detection content and multi-tenant platform.

HOW ONBOARDING WORKS

# From first call to full coverage.

01

SCOPE

### Discovery call

We learn your environment, your log sources and what you need protected.

02

DEPLOY

### Agents & tenant

Your isolated tenant is provisioned and agents are rolled out to your endpoints.

03

TUNE

### Integrations & tuning

Existing tools are connected and detections tuned to cut noise from day one.

04

GO LIVE

### Monitoring & reporting

Triage, daily detections, health checks and reporting begin.

## Your alerts handled. Your team back.

Every environment is different, so pricing is tailored to yours. Get in touch and we'll scope what you need, whether you're protecting your own business or your clients'.

Contact us for pricing

info@socfortress.co
socfortress.co