Professional Services

Scale Together

SOCFortress Professional Services provide a next generation security stack perfect for MSSPs, or those interested in building an in-house security team. When you deploy the SOCFortress stack, you align forces with the fastest growing Security company providing SIEM capabilities and SOC management for every enterprise—all delivered through Open-Source tools.

Why Professional Services?

Our experienced engineers understand the components of a precise and intelligent security stack. Stop spending a fortune on a commercial security stack and allocate that budget to greater profit generating expenditures. The provided security stack is built with Open-Source tools meaning no licensing costs! Once the stack is deployed, your only costs are running / maintaining the infrastructure. Together, we ensure MSSPs attract more cliental by providing stronger security offerings.

What is SOCFortress?

SOCFortress is a SaaS company that unifies Observability, Security Monitoring, Threat Intelligence and Security Orchestration, Automation, and Response (SOAR). SOCFortress helps organizations align strategic and operational goals by exposing the risks and threats that matter most.

Unfortunately, many security providers' high barrier to entry costs prohibit businesses with smaller budgets from obtaining next-level security monitoring. SOCFortress believes security is a right, not a privilege.

Why the SOCFortress Stack?

Let's face it, security is hard. However, it does not have to be. Our stack consolidates security logs from all types of sources (endpoint, network, 3rd parties, etc.) and details alerts within our single pane of glass approach. From alert notifications, case management, threat intel, to responsive actions, your SOC team will have the tools for success. Best of all, the tools are free and can dynamically scale as your coverage grows!

Shared Vision

SOCFortress's success equates to your success. Designed to be integrated into any environment, the SOCFortress stack is built to your unique wants / needs. Implement a single tenant or multi-tenant stack within days. We make it easy to scale your business with us.

- We have a Team ready to work for you
- Training capacity
- 24/7 Support
- Level 3 Support

Pricing

The professional services program was designed to ensure clients have what they need to provide security monitoring services, leading to more predictable profits and a business-centric relationship.

	SIEM in the Making	SOC Ready	MSSP Ready
NextGen SIEM for EDR	Included	Included	Included
Endpoint Agent	Included	Included	Included
Security Dashboards	Included	Included	Included
AntiVirus Agent #	$3.95/per endpoint	$3.95/per endpoint	$3.95/per endpoint
Network Logs Collection	Included	Included	Included
3rd Party Integrations #	$250/per integration	$250/per integration	$250/per integration
Threat Intel (Via SOCFortress) #	$99/per month	$99/per month	$99/per month
Alerts and Notifications	Included	Included	Included
Advanced Detection Rules	X	Included	Included
Infrastructure Monitoring/Alerting	X	Included	Included
Security Homepage	X	Included	Included
High Risk Vulnerability Reporting	X	Included	Included
Key Performance Indicators	X	Included	Included
Case Management	X	Included	Included
Incident Response	X	Included	Included
SOAR Automation	X	Included	Included
Single sign-on	X	X	Included
Custom Branding	X	X	Included
End User Documentation #	$500	$1,000	$1,200
Service Credit #	$60/per credit	$60/per credit	$60/per credit

* price subject to change depending on log volume and deployment type (single tenant vs multi tenant)

Total Bundle does not include services with a per month cost such as the threat intel, cloud backup (if using SOCFortress cloud), antivirus agent, and OSINT

NextGen SIEM for EDR
The endpoint agent provides full telemetry into the endpoint such as network connections, user logons, running processes, dns queries and much more! File integrity monitoring, vulnerability assessment, and CIS benchmark checks are just a few of the many included modules.

Security Dashboards
Quickly drilldown into individual host's processes, view activity on all of your endpoints, or spot high severity alerts with our detailed dashboards.

AntiVirus Agent
For those interested in an antivirus solution other than Windows Defender, SOCFortress has partnered with WithSecure who offers an proactive antivirus agent that seamlessly integrates with the SOCFortress stack to block malware in real time.

Network Logs Collection
Endpoint monitoring is only half the battle. Ingesting logs outputted from your firewalls, switches, access points, etc. provides full visibility into data flowing in and out of the network. Collecting IDS/IPS events enables quick triage to conclude the full impact of an event.

3rd Party Integrations
With so many products and services out there, maintaining visibility can become a challenge. The SOCFortress stack seamlessly integrates with 3rd party services such as O365, AWS, CrowdStrike, Sophos, Google Cloud, and so much more!

Threat Intel
SOCFortress provides threat intel as a service for $99 per month. Quickly spot IoCs such as malicious IPs, command and control domains, malicious file hashes and much more! The SOCFortress stack integrates with our threat intel service to automate IoC enrichment, saving your SOC team time and energy.

Alerts and Notifications
Receive security alerts into your favorite communication channel such as Email, Teams, Slack, Pager Duty, and much more! Enable your SOC team with the ability to provide quick response times.

Cloud Backup
Store your security logs to meet your data retention requirements. The SOCFortress team can work with you to implement daily backups within your own environment, or SOCFortress offers a managed cloud storage enabling you to restore backups within minutes (subject to monthly invoicing).

Advanced Detection Rules
Backed by sigma rules, our advanced ruleset queries your security logs to detect malicious activity such as suspicious PowerShell commands, executions, malicious insiders, and much more!

Infrastructure Monitoring / Alerting
Collect all endpoint metrics and built-in alerting for when thresholds are met or critical processes (such as a webserver) are not running. This allows your team to proactively respond to potential issues before they escalate to a serious impact.

Security Homepage
Keep your team organized with a security homepage that links to your security stack and provides widgets detailing attacks spotted by security researchers.

High Risk Vulnerability Reporting
Quickly spot critical vulnerabilities currently being exploited in the wild that your endpoints are exposed to.

Key Performance Indicators
Give your management team oversight into the current coverage of deployed agents and detect any endpoints in breach of full coverage.

Case Management
Provide a platform that enables your SOC team to collaborate, enrich, and respond to high severity alerts all in real time. Consolidate alerts so nothing goes missed!

Security Playbooks
Detailed procedures and tasks for your SOC analysts will help guide them through alerts detected and allow them to focus on CRITICAL alerts.

Incident Response
Enable your SOC analysts with the ability to thoroughly investigate alerts by interacting with the monitored endpoints in a manner that is scalable and fast.

- Listing running processes
- Enumerating logged in users
- Detect listening ports
- View downloaded files
- Quarantining a device
- And much more!

SOAR Automation
Integrate your security stack with advanced and fully automated workflows such as:

- Quick Client Onboarding
- Phishing analysis
- Routine jobs
- Report generation
- Literally anything :)

OSINT
Provide insight into possible data leaks, vulnerabilities or other sensitive information that can be leveraged during a penetration test, red team exercise or for threat intelligence against any organization.

Single Sign On
Conveniently offer your end users seamless access to any tools within the security stack dependent on their supported roles.

Admin Portal
Host an admin portal to enable your clients to get high level insight into their current security footprint, current services, and more!

User Training and Documentation
The SOCFortress team will train your team on all tools used within the stack. Individuals will learn how to build their own modules, enable their own integrations, and MASTER the security stack, saving you time and money as you begin to incorporate your own use cases without requiring SOCFortress support. Your success is our success!

Service Credits
The SOCFortress team offers service credits where your team can engage SOCFortress for any troubleshooting, feature requests, level 3 support, or any other needs. Subject to $60/credit pricing.

What If I Don't Want All Bundled Services?
No problem! The beauty of the SOCFortress stack is that we can plug in any of the offered services that you seem fit. And if you change your mind, we can deploy ad hoc services whenever you'd like.

What Is Required from Me?
You will be responsible for deploying the servers, firewall configurations, and remote access to your environment during the engagement. The SOCFortress team ensures secure remote access with our 2 Factor VPN and ask clients to whitelist our external VPN IP.

What Deployment Options Are Available?
We can deploy our security solutions in a private cloud or public cloud (Azure, AWS, Google Cloud, and others).

Fully Managed Model
We can deliver our security solutions in a VPC using SOCFortress Cloud Services with all the required security settings: perimeter security, network segmentation, and secure access. Perfect for those not wanting to host the infrastructure themselves but wanting full access into the environment. Subject to additional pricing.

What's Our Delivery Time?
That depends on the desired setup (security services to implement) and the deployment model (private vs public cloud, etc).

In most cases, we can get your security solution up and running, ready to ingest metrics, log data and security events in a matter of days.

How Do We Deploy Agents?
As part of our deployment, we include one-line bash or powershell scripts that can be used to install all the required software on the end-point.

The script can be used for an automated install using standard tools or RMM solutions.

Infrastructure Required
SOCFortress provides guidelines to VM sizing and resources needed to ensure smooth operations of the security stack. See next page.

	Number Of	CPU	Memory	OS Disk	Data Disk	OS
NextGen SIEM for EDR (BackendStorage)	1	8	32GB	75GB	2TB	Debian 11
NextGen SIEM for EDR (Log Analyzer)	1	4	8GB	75GB	150GB	Debian 11
NextGen SIEM for EDR (Log Ingestion)	1	8	16GB	75GB	150GB	Debian 11
NextGen SIEM for EDR (Visualizations)	1	4	4GB	75GB	150GB	Debian 11
Load Balancer / Reverse Proxy	1	4	6GB	75 GB	150GB	Debian 11
Case Management	1	6	6GB	75GB	500GB	Debian 11
Incident Response	1	4	6GB	75GB	500GB	Debian 11
SOAR Automation	1	8	8GB	75GB	500GB	Debian 11
Admin Portal Security Homepage Single Sign On	1	4	4GB	75GB	150GB	Debian 11

*Built in support of up to 1,000 endpoint agents, 10 network devices and 3 months of hot data. Subject to change depending on client's needs.

SOCFortress Professional Services

SOCFortress Professional Services provide a next generation security stack perfect for MSSPs, or those interested in building an in-house security team. When you deploy the SOCFortress stack, you align forces with the fastest growing Security company providing SIEM capabilities and SOC management for every enterprise—all delivered through Open-Source tools.

SOCFortress is a SaaS company that unifies Observability, Security Monitoring, Threat Intelligence and Security Orchestration, Automation, and Response (SOAR). SOCFortress helps organizations align strategic and operational goals by exposing the risks and threats that matter most. Unfortunately, many security provider's high barrier to entry costs prohibit businesses with smaller budgets from obtaining next-level security monitoring. SOCFortress believes security is a right, not a privilege.

Questions?
Contact us with questions or to request additional information at info@socfortress.co.

www.socfortress.co