SOCFortress

SOCFORTRESS SIGNALS

More signals. Less noise. Clearer action.

SOCFortress Signals pulls security advisories into one view, matches them to the technology you run and tells you what to do next.

Stop chasing advisories across vendors, feeds and mailing lists. SOCFortress Signals brings advisories, vulnerability data and exploitation evidence together, then explains why each one matters and what to do first.

Built for MSPs MSSPs SMBs

THE CHALLENGE

What stands in the way

01

Advisories scattered everywhere

Security advisories are spread across vendors, feeds and mailing lists, so keeping track of them means checking many places at once.

02

Severity scores don't tell the full story

A severity score alone won't show whether a vulnerability affects your environment, is being exploited or should be fixed first, and new Common Vulnerabilities and Exposures (CVEs) arrive every week.

03

Leadership expects Patch Tuesday clarity

Leadership expects a clear summary every Patch Tuesday, while the team is still working through the latest stream of advisories, CVEs and patches.

THE SOLUTION

One view, matched to what you run

SOCFortress Signals brings security advisories, vulnerability data and exploitation evidence together in one place and links related records. Declare the vendors, products and versions you depend on, and SOCFortress Signals matches advisories to them, explains with supporting evidence why each one matters and how urgent it is, and recommends what to do next.

WHY IT'S DIFFERENT

01

Relevance, not just severity

Advisories are matched to your declared products and versions, with an explanation of why each matters, how urgent it is and the next step, backed by evidence.

02

Evidence you can verify

SOCFortress Signals links to original sources and shows the evidence behind its prioritisation, so your team can check the intelligence rather than take it on trust.

03

Intelligence for people, beside your SIEM

SOCFortress Signals is intelligence for people, designed to sit alongside machine-oriented intelligence for your security information and event management (SIEM) platform.

KEY CAPABILITIES

What SOCFortress Signals delivers

One searchable view

Search advisories, vulnerabilities, threat actors, malware and indicators of compromise (IOCs) in one place, follow original sources and explore related intelligence.

Patch Tuesday and KEV views

Dedicated Microsoft Patch Tuesday views and Known Exploited Vulnerabilities (KEV) views from the Cybersecurity and Infrastructure Security Agency (CISA), plus a timeline.

Exploitation context at a glance

An advisory view can show exploitation status, an Exploit Prediction Scoring System (EPSS) score, patch availability, a profile match and a recommended next step.

Technology profile matching

Declare the vendors, products and versions you depend on to build a technology profile and asset inventory, then see advisories matched to what you run.

Near-real-time alerts and digests

Email alerts on relevant intelligence arrive in near real time, with configurable urgency thresholds, quiet hours and notification preferences, plus weekly digests.

Scheduled PDF reports

A weekly intelligence and advisory PDF and a monthly Patch Tuesday PDF in Flash and Full editions, emailed only to recipients on verified domains, with archive and delivery history.

HOW IT WORKS

SOCFortress Signals draws on intelligence sources such as the Microsoft Security Update Guide, CISA Known Exploited Vulnerabilities, the National Vulnerability Database (NVD), FIRST EPSS and MITRE ATT&CK.

1 → 2 → 3 → 4

Collect and link
Advisories, vulnerability data and exploitation evidence are gathered in one place, with related records linked together.

Declare your technology
Your team declares the vendors, products and versions you depend on, building a technology profile and asset inventory.

Match and explain
Advisories are matched to your declared products, with evidence showing why each matters, how urgent it is and what to do next.

Alert and report
Near-real-time email alerts, weekly digests and scheduled PDF reports keep the team and leadership informed.

USE CASES

Patch Tuesday briefings for leadership

Use the monthly Patch Tuesday PDF and Patch Tuesday views to give leadership the clear summary they expect, and bring the wider team up to speed.

Weekly vulnerability triage

Work through the week's advisories, CVEs and patches by relevance: focus on what matches your profile, check exploitation evidence and act on the recommended next step.

Investigating a threat

Search a threat actor, malware family or indicator, follow the original sources and explore related intelligence to understand the context before deciding what to do.

WHO IT'S FOR

Value for every kind of team

MSPs

Track advisories in one view instead of across vendors, feeds and mailing lists, and use scheduled PDF reports to bring your team up to speed and brief leadership on Patch Tuesday.

MSSPs

Give analysts searchable intelligence on advisories, vulnerabilities, threat actors, malware and IOCs, with evidence and original sources they can verify, alongside your SIEM.

SMBs

See which threats deserve attention and what to do next. Declare the technology you run, get advisories matched to it, and explore the global intelligence with a free account.

WHY SOCFORTRESS

Verifiable by design

SOCFortress Signals shows the evidence behind its prioritisation and links to original sources, so your team can verify the intelligence.

Global intelligence on the free plan

The free plan includes all of the global intelligence available in SOCFortress Signals, subject to source licensing and enablement.

Part of the SOCFortress stack

SOCFortress Signals sits within the SOCFortress stack, where detection and response are handled, including Managed Detection and Response for your SIEM and team.

See which threats deserve your attention

Create a free account to explore the global intelligence in SOCFortress Signals today, then match advisories and exploitation evidence to the technology you run.

Create a free account → signals.socfortress.co

Scan to create a free account

Product information current as of 2026-10-25. Features and availability may change.