ITSentinel™ Managed SIEM Solution

SECURITY INFORMATION AND EVENT MANAGEMENT PRODUCT OVERVIEW

FLAGSHIP NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.358.0800

FlagshipNetworks.com

Flagship ITSentinel™ Security Information and Event Management (SIEM) solution powered by ConnectWise® SIEM (formerly Perch Security) is a threat detection and response platform that detects cybersecurity threats. It works in collaboration with the ConnectWise Security Operations Center (SOC), which responds to those threats. You have full access to view your alert data and can even have your team analyze alongside us. The SIEM is available as a Flagship ITSentinel managed or co-managed service, as well as a SaaS solution.

Threat detection requires visibility and understanding of the massive sets of log data that your IT environment generates. What's normal? What's anomalous and in need of investigation?

Providing preventive security measures is a must-have in today's cybersecurity landscape. Security information and event management (SIEM) solutions offer an additional layer of security, however, most SIEM solutions are routinely difficult to manage, expensive to deploy, and require a significant amount of in-house cybersecurity expertise.

Flagship ITSentinel SIEM offers a powerful alternative to expand your security perspective to both prevention and detection. The solution includes comprehensive, flexible SIEM software that streamlines safety and security across your network without additional full-time employee costs or complicated implementations.

Top 3 Reasons to Leverage SIEM Services

Compliance and regulatory requirements

From HIPAA to FINRA and PCI-DSS to CMMC, organizations can have a wide range of compliance and regulatory needs. Our SIEM enables you to meet them with flexible log capture, retention, and review features.

Too many data sources and alerts

Many organizations have data coming in from multiple data sources and get flooded by alerts. A SIEM helps you aggregate the data and filter out the noise.

You need added protection

Relying on prevention alone is insufficient and can't stop all threats. Our SIEM solution adds an extra layer of defense to catch the threats that could crush your clients. You'll get complete visibility and multi-source data analytics to detect events when prevention fails.

SIEM PLATFORM FEATURES & BENEFITS

Threat Hunting. We offer fully managed threat intel, at your fingertips. With our Security Operations Center, you take advantage of our included tier-1 alert support, reducing noise and alerting you of only real threats. While the SOC works through alerts, you can also investigate alerts, analyze network traffic and logs, and drill down into data details. The SOC triages all your alerts and only escalates threats that you care about. Your own team or third party SOCs can connect and work alongside our SOC.

Log Ingestion. You can ingest logs from syslog and Windows Event Logs, and retain them to meet compliance requirements. Flagship ITSentinel SIEM also generates alerts to highlight notable log events based on log data, and enhance reporting and visualizations; and it gives our SOC extra insight into your endpoints and network traffic data. Unlimited number of events, unlimited GB storage (30-day, 90-day & 365-day retention options available), and unlimited access to log integrations including Office 365, G-Suite, ConnectWise, and Cisco AMP for Endpoints and Umbrella. Flagship's SIEM generates alerts to highlight notable log events and enhance reporting and visualizations.

Intel Agnosticism. The SIEM connects to and consumes the best sources of threat intel for your business, free and paid. Best-in-class threat intel included on day one. Share reported threats with others in your community. When someone sees a threat, you see it too, giving you the "bird's eye view" of how threats are moving, and what attacks you should be prepared for.

Threat Management. The SIEM interface lets you enter and manage your own threat indicators, sharing them with your community if you wish. You can even build your own threat intelligence repository, at a fraction of the traditional Threat Intelligence Platform price tag. However, you use it, this feature gives you even more control of your threat data, and lets you give back to your community.

Reporting. Easily access the big-picture information you need when you need it. Build your own visualizations and add them to custom dashboards, or use pre-built reports such as PCI DSS or HIPAA compliance, Windows logs, or Office 365 to name a few

Collect

Bring all your logs into a single pane of glass, right next to the network data you're already sending us.

- **Windows event logs**. Insight into services activity and changes, including Active Directory
- **Syslog data.** Insight into device activity, including firewall logs, change management tracking and error logs
- **Event parsing.** Supports strong search and reporting
- **Collected alongside network data.** View log data next to the critical network data you're already collecting to further enrich the picture around potential incidents
- **Flexible retention**. Keep your data for as long as you want – meet your regulatory retention requirements easily
- **Easy deployment.** If a ConnectWise or SIEM sensor is already in your environment, just point your logs our way for collection and retention

Detect

Add log metadata to reveal behavior patterns, and identify potential brute force and other attacks.

- **Activity detection.** Detection rules for dozens of vendors ensure the broadest out-of-the-box overage possible
- **Event correlation.** The ConnectWise SOC includes collected log data in their analysis to correlate events and further identify potentially malicious activities
- **Alerting.** Alerts on bad network activity escalate to you after the SOC has investigated the incident. SOC uses log data to enrich the context of the network activity to provide even more fidelity when investigating a potential incident.

For more information on our Security Operations Center (SOC) from ConnectWise and other security offerings, visit www.flagshipnetworks.com/security.

Respond

- **Dashboards.** Understand log (and network) activity in a glance with a fully customizable view
- **Reports.** Gain insight into the data you are looking at and ensure organizational and regulatory compliance by generating reports around interesting data patterns
- **Searching and hunting.** Conduct forensic investigations – access network data and log history in a single pane of glass.

Microsoft 365 Support

Include your Microsoft 365 logs

Empower ConnectWise SOC to defend your business from account takeovers and business email compromise (BEC) and satisfy compliance requirements. With Microsoft 365 integration, alerts are generated through the SIEM platform based on your Microsoft 365 logs. From your SIEM console, you can customize which alerts you receive and how you receive them. Then investigate any impact in real time; or let the SOC do it for you.

Investigate reported threat activity

With Microsoft 365 integration, ITSentinel SIEM provides everything you need to respond to and investigate alerts from Microsoft 365 logs. Logs are searchable, parsed, cleaner, and reportable. Increase log retention without the extra price tag to satisfy compliance requirements. Take advantage of a comprehensive list of pre-configured alerts to defend yourself from malicious activity, including:

- The number of failed logins for your users
- Suspicious logins
- File integrity monitoring
- File access and changes
- SIEM gives you the tools to decipher the magnitude of an incident and pinpoint what exactly is affected

BENEFITS AT A GLANCE

- Aggregate Microsoft 365 logs, add them to your network metadata for deeper understanding of your universe
- Get alerts for signs of Microsoft 365 account takeovers and business email compromise
- Investigate Microsoft 365 alerts with the SIEM's online investigation tools

Google G Suite® Support

Both stand-alone log aggregation & cloud monitoring are included with our SIEM offering.

Include your G Suite logs in your threat analysis:

Empower ConnectWise Security Operations Center (SOC) to defend your business from account takeovers and business email compromise and satisfy compliance requirements. With G Suite integration, alerts are generated through the platform based on your G Suite logs. From your console, you can customize which alerts you receive and how you receive them. Then investigate any impact in real time; or let the SOC do it for you. Investigate reported threat activity With G Suite integration, the SOC provides everything you need to respond to and investigate alerts from G Suite logs. Logs are searchable, parsed, cleaner, and reportable. And you can increase log retention without the extra price tag to satisfy compliance requirements. Take advantage of a comprehensive list of pre-configured alerts to defend yourself from malicious activity, including:

- The number of failed logins for your users
- Suspicious logins
- File integrity monitoring
- File access and changes tools decipher the magnitude of an incident and pinpoint exactly what is affected

BENEFITS AT A GLANCE

- Aggregate G Suite logs, add them to your network metadata for deeper understanding of your universe
- Get alerts for signs of G Suite account takeovers and business email compromise (BEC)
- Investigate G Suite alerts with ITSentinel SIEM online investigation tools

Cybersecurity Maturity Model Certification (CMMC) Compliance

Flagship ITSentinel SIEM helps your organization achieve various CMMC compliance requirements.

- Monitor and control remote access sessions (AC.2.013)
- Capture the execution of privileged functions in audit logs (AC.3.018)

Audit & Accountability

- Ensure that the actions of users can be uniquely traced so that the proper users can be held accountable (AU.2.041)
- Create and retain system audit logs to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity (AU.2.042)
- Collect audit information into one or more central repositories (AU.3.048)
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion (AU.3.049)
- Provide audit record reduction and report generation to support on-demand analysis and reporting (AU.3.052)
- Automate analysis of audit logs to identify and act on critical indicators and/or organizationally defined suspicious activity (AU.4.053)

FLAGSHIP
NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.538.0800

FlagshipNetworks.com