DEFENSE.COM™

Service overview

Managed SIEM

Defend against cyber attacks with 24/7 proactive threat detection and log monitoring.

Defense.com Managed SIEM alleviates the pressure on your IT team by monitoring your environment 24/7 for cyber threats. Our in-house Service Operations Centre (SOC) analysts will become an extension of your team, proactively looking for malicious activity in your network on your behalf and raising security alerts to your attention.

Defense.com ingests and correlates log data from any system, device or application to ensure that every area of your environment is being monitored for suspicious activity. When there is a genuine security event, our expert SOC analysts will notify you and provide clear remediation advice, so you can fix issues fast and get back to other tasks.

Fully managed threat detection

Complete coverage

Ingest logs from all sources including applications, endpoints, servers, network devices and cloud environments.

Identify threats

Never miss a genuine security threat with our team of SOC analysts monitoring your network 24/7 on your behalf.

Prevent breaches

Quickly respond to threats and protect your business with clear, step-by-step remediation actions.

Stay compliant

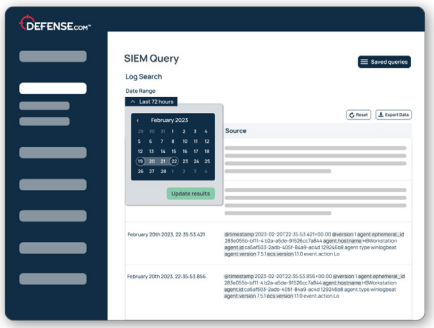
Meet the requirements of PCI DSS, GDPR and other regulatory standards with proactive monitoring and reporting.

Key service highlights

- 24/7/365 protection and monitoring of systems, networks, applications and users
- Ingest security logs from any device, system or vendor
- Simple and automated deployment for on-premises devices
- Support for cloud services including Azure, AWS, GCP and Salesforce
- Real-time threat intelligence data from multiple sources such as CareCERT, MITRE CVEs, etc.
- Scalable and predictable pricing based on log sources, not volume

> "This service is really useful for small to medium enterprises who don't have the dedicated internal tech or services that provide the capability.
>
> *Alexandra Vujcich, Infrastructure Team Lead, St Andrew's Healthcare*

St Andrew's HEALTHCARE

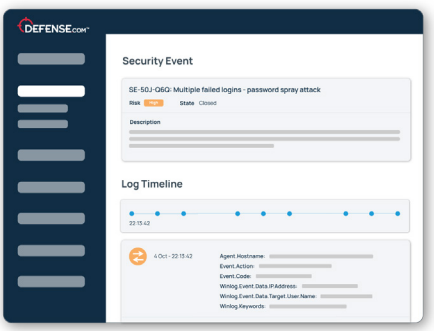


Complete log collection

Send security logs from any device or system to maintain complete visibility over your environment. We use machine learning and human expertise to analyse your logs and detect any threats on your behalf.

Tailored security alerts

Our SOC team will eliminate alert fatigue by proactively monitoring your network for suspicious activity and only bringing genuine security concerns to your attention.



Actionable advice

Spend less time investigating each alert with detailed remediation advice. When a security event is triggered you'll get a list of step-by-step actions to take to quickly remediate the threat.

Key features

- 24/7/365 monitoring
- SaaS delivery model
- Collect log data from any vendor or system
- Support from experienced SOC analysts
- Proactive threat hunting
- Real-time threat intelligence
- MITRE ATT&CK mapping
- Integrated machine learning
- 90 days of immediate log searching
- 1 year of archived logs included
- Service aligned to the cyber kill chain and SANS incident response

Why choose Defense.com?

Defense.com transforms the way businesses manage cyber security by allowing them to easily identify, prioritise and remediate threats from a single platform.

We help to solve security complexity for IT and SecOps teams, helping them to protect their brand and assets against today's evolving threat landscape. Businesses of all sizes rely on Defense.com to strengthen their cyber security posture, detect and respond to threats and significantly reduce the risk of cyber attacks.

To learn more about our Managed SIEM service, get in touch today.

+44 (0)1438 500 209 contact@defense.com www.defense.com

DEFENSE.COM™