Evalian Limited

Managed SIEM & SOC (SOC-as-a-Service) Service Description

28 January 2026

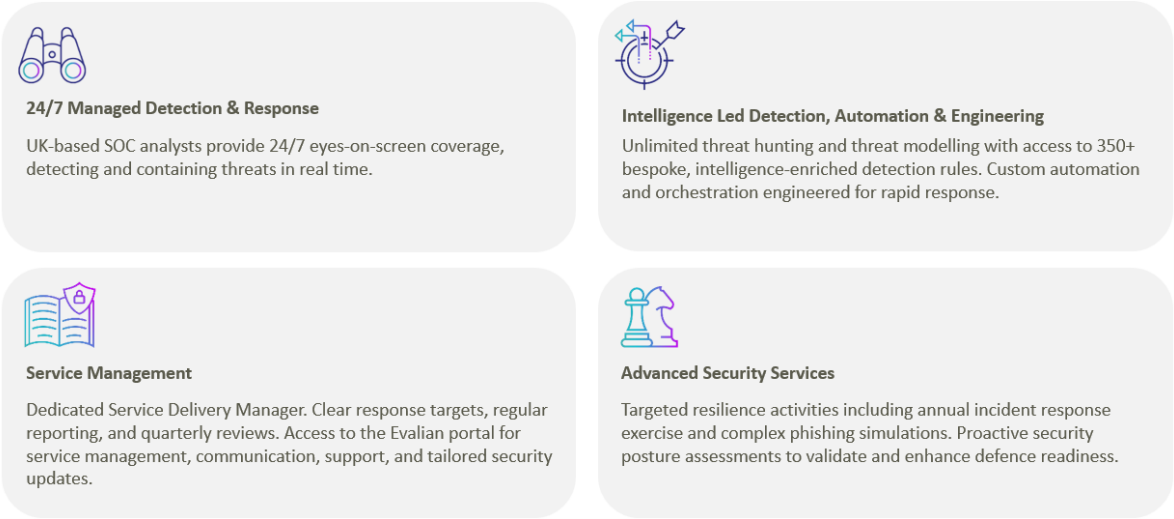
1. Service Summary

Evalian's Managed SIEM & SOC Service (the "Service") delivers 24x7x365 monitoring, threat detection, and incident response to help our customers stay ahead of cyber threats. Fully managed and modular, the Service enhances existing security capability, supports compliance, and maximises return on investment in existing security tools without the capital expenditure required to build and staff an in-house SOC.

Delivered from our UK-based Security Operations Centre, the Service is operated by experienced security analysts, engineers, and consultants with deep expertise in security operations, threat intelligence, and incident detection and response. The SOC is built on Microsoft Sentinel and is compatible with both Microsoft and third-party security technologies.

Evalian is an award-winning cybersecurity provider, certified to ISO 27001, ISO 9001, ISO 22301 and Cyber Essentials Plus. We are an NCSC Assured Service Provider for Cyber Incident Response and Cyber Incident Exercising and hold additional accreditations from the NCSC and CREST across advisory, penetration testing, and incident response services.

1.1. Key Features



The Service is delivered through three tiers: **Essentials**, **Standard**, and **Enterprise**. Each tier builds on a foundation of 24x7x365 monitoring, incident containment and response. Higher tiers introduce additional capabilities such as domain monitoring, custom log integration, threat-led detection engineering, proactive threat hunting, extended detection and response, and advanced security services.

1.2. How the Service Works

Service Setup: During onboarding, our engineers work with you to configure your environment, cloud services, licenses, and permissions. We integrate standard log sources, build custom connectors where required, conduct threat modelling, and develop tailored detection rules. Log optimisation helps manage data volume and cost without reducing visibility.

Service Operations: Starting from the service activation date, our SOC provides monitoring, triage, investigation, and response. Alerts are communicated clearly and tracked against service levels. Security tools and detection rules are tuned to your environment and aligned to the MITRE ATT&CK framework.

2. Service Tiers

Evalian recognises that organisations have varying security and business objectives, risk profiles, and maturity levels. To provide the right level of support and value, the Service is offered in clearly defined tiers. Each tier is designed to deliver core protection while allowing you to scale capabilities as your requirements evolve.

The Service is provided at the following three tiers:

Service Feature	Essentials	Standard	Enterprise
24x7x365 Continuous Security Monitoring	☑	☑	☑
Incident Containment & Response	☑	☑	☑
Out of Hours Response & Escalation	☑	☑	☑
Standard and Custom Detection Rules	☑	☑	☑
Security Orchestration & Automation	☑	☑	☑
Engineering & Customisation	☑	☑	☑
Threat Enriched Monitoring	☑	☑	☑
Service Targets and Reporting	☑	☑	☑
Endpoint Detection & Response	☑	☑	☑
Custom Log Connectors	☒	☑	☑
Custom Detection Rules	☒	☑	☑
Threat Hunting	☒	☑	☑
Extended Detection & Response	☒	☑	☑
Domain Monitoring	Optional	☑	☑
Annual Incident Response Exercising	Optional	☑	☑
Annual Phishing Exercise	Optional	☑	☑
Advanced Security Services	Optional	Optional	☑

While our service tiers aim to provide organisations with a clear structure, we remain flexible by design and can adapt or extend the Service to meet the specific requirements of each customer's environment, risk profile, business priorities and budget.

2.1. Essentials – Core Threat Protection

Intended for smaller organisations or those early in their security journey. The Essentials tier provides comprehensive 24x7x365 monitoring, threat detection and response across business endpoints (laptops, desktops, and servers) and your chosen identity management platform. It is best suited to environments built on commonly used technologies that can be integrated with Microsoft Sentinel out of the box.

2.2. Standard – Enhanced Detection & Resilience

Ideal for growing organisations, those operating in regulated or high-risk sectors, or environments with more complex or diverse infrastructure requiring custom log integration. The Standard tier builds on all Essentials features, adding proactive threat hunting, custom log connectors, threat modelling, and the development of tailored detection rules. It also includes Extended Detection and Response (XDR), which expands visibility beyond endpoints to include telemetry from native and 3rd party cloud applications and services, networks, and other third-party tools and infrastructure.

Additionally, the Standard tier includes:

- **Domain Monitoring** using Evalian's proprietary vTrace solution to identify suspicious, malicious, or spoofed domains associated with your organisation.
- **Annual incident response exercise**, delivered as an NCSC Assured Service Provider, to validate preparedness and improve response capability.
- **Annual phishing campaign**, delivered by experienced penetration testers using real-world attacker techniques to strengthen user awareness and organisational resilience.

2.3. Enterprise – Cyber Security Managed Service

Suited to organisations seeking end-to-end cybersecurity support, the Enterprise tier builds on the Standard service and incorporates Evalian's Cyber Security Managed Service (CSMS). It links day-to-day SOC operations with governance, risk management, and business priorities to drive measurable improvements in security maturity.

Alongside advanced monitoring and response, the service provides ongoing security leadership, including strategy and planning, risk and supplier assurance, policy and compliance management, incident response planning and exercising, and board-level reporting. Ensuring cybersecurity is aligned to business resilience, regulatory requirements, and long-term improvement.

3. Service Setup

To ensure a smooth and coordinated start to the Service, Evalian follows a structured onboarding Setup Methodology delivered across five phases as follows:

- Phase 1: Scoping & Project Planning
- Phase 2: Technical Setup & Onboarding
- Phase 3: Configure Detection & Alerting
- Phase 4: Operational Readiness
- Phase 5: Service Activation

4. Service Operations

Following service activation Evalian delivers security event monitoring, threat detection and response for customer assets in scope consisting of:

- Security Monitoring
- Threat Detection

- Incident Triage
- Incident Response

Clear communication is maintained throughout, with timely notification to nominated contacts and structured incident reporting following resolution.

All operational activity relating to the Service is managed through Evalian's customer SecOps Portal. This platform acts as the central point for incident tracking, communication, and service requests between the customer and our SOC.

In addition to the portal, Evalian provides a dedicated SharePoint for storing and accessing service-related documents, and a Teams channel for day-to-day communication between customer staff and Evalian analysts.

To ensure the Service is being delivered effectively and in accordance with the service targets set out below, Evalian will designate a named Service Delivery Manager ("SDM"). The SDM is the customer's primary non-technical point of contact.

Evalian provides a monthly insights report providing details of threats detected, security incidents managed, security event trends and supporting information for the month in review.

Customers also benefit from quarterly service reviews led by their SDM. These also include security deep dive reporting, which provides actionable security recommendations based on the last quarter of monitoring and current threat intelligence.

5. Service Targets

Delivery performance for the Service is measured against the following service targets:

Incident Severity	Mean Time to Respond Target
P1 (Critical)	15 mins
P2 (High)	30 mins
P3 (Medium)	240 mins
P4 (Low)	1 Business Day
P5 (Informational)	2 Business Days