Continuous Threat Exposure Management (CTEM) Service

Service Definition Document

Supplier: **Sailotech UK Limited Document**

Version: **V1.1**

Date: 27th January, 2026

Table of Contents

1. Service Overview

Our CTEM service continuously monitors multi-cloud and on-premises environments to identify, prioritise, and remediate threats. It combines real-time dashboards, automated alerts, and advanced reporting to help organisations maintain a strong security posture and reduce risk exposure.

Deployment model: Hybrid cloud
Multi-cloud support: Yes

2. Features and Benefits

2.1. Features

2.1.1. Discover – "What do we own?"

- Asset discovery (cloud, on-prem, SaaS, OT, IoT, shadow IT)
- External Attack Surface Management (EASM)
- IP / domain / certificate / exposed service discovery
- Cloud misconfiguration detection (AWS, Azure, GCP)
- Business context tagging (system owner, criticality, data type)

2.1.2. Prioritise – "What matters most?"

- Risk scoring using:
  - CVSS + exploitability
  - Threat intelligence (KEV, ransomware gangs)
  - Business impact weighting (NHS, council, school)
- Crown Jewel Mapping
- Attack Path Simulation
- MITRE ATT&CK mapping
- Compliance risk scoring (ISO, NCSC CAF, NHS DSP Toolkit, GDPR)

2.1.3. Validate – "Can this actually be exploited?"

- Continuous vulnerability scanning
- Automated breach & attack simulation (BAS)
- Red Team / Purple Team orchestration
- AI-based exploit likelihood modelling
- Safe proof-of-exploit engine

2.1.4. Mobilise – "Who fixes what?"

- Auto-ticketing (Jira, ServiceNow, Freshservice)
- Ownership & SLA mapping
- Risk-based remediation plans
- Executive dashboards
- Business unit accountability

Compliance & Governance Engine Especially for UK public sector:

- ISO 27001 control mapping
- NCSC CAF maturity heatmap
- NHS DSP Toolkit mapping
- PSN compliance
- GDPR Article 32 risk view
- G-Cloud readiness dashboard
- Audit-ready evidence vault

Threat & Exposure Fusion

- Integrates:
  - EDR, SIEM, SOAR
  - Cloud Security Posture Mgmt (CSPM)
  - Identity & PAM (CyberArk)
  - Threat intel feeds (MISP, NCSC, CISA KEV)
- Real-time attack surface + threat fusion

2.2.Benefits

2.2.1. Prevent Breaches Before They Happen

CTEM continuously identifies and validates real attack paths so you fix what can actually be exploited, not just what looks risky on paper.

Outcome: Reduced likelihood of ransomware, data theft, and service outages.

2.2.2. Reduce Cyber Risk by 40–70% in 6–12 Months

By prioritising based on business impact + threat activity, CTEM focuses resources on the exposures that matter most.

Outcome: Measurable risk reduction and faster security maturity.

2.2.3. Cut Remediation Time by 50%+

Automated prioritisation, ticketing, and ownership mapping remove guesswork and delays.

Outcome: Faster closure, fewer backlogs, less firefighting.

2.2.4. Improve Compliance & Audit Readiness

CTEM maps technical risks directly to:

- ISO 27001
- NCSC CAF
- NHS DSP Toolkit
- GDPR Article 32

Outcome: Fewer audit findings, easier reporting, stronger governance.

2.2.5. Executive Visibility & Board Confidence

Real-time dashboards translate cyber risk into financial and operational impact, not just technical metrics.

Outcome: Better funding decisions and leadership trust.

2.2.6. Optimise Security Spend (15–30% savings)

Eliminates tool overlap, reduces wasted scanning, and directs spend to where it reduces risk most.

Outcome: Lower cost, higher security ROI.

2.2.7. Continuous Risk Management

CTEM replaces static audits with live exposure monitoring across cloud, identity, networks, and endpoints.

Outcome: Always-on security posture.

2.2.8. Faster Incident Containment

Validated attack paths show how a breach would spread, so teams can block lateral movement before damage occurs.

Outcome: Shorter dwell time and reduced blast radius.

2.2.9. Supports Digital Transformation Securely

Cloud, remote work, SaaS, and OT environments are continuously mapped and assessed.

Outcome: Security keeps pace with business change.

2.2.10. Builds Trust with Citizens, Patients & Customers

Demonstrates proactive protection of sensitive data and essential services.

Outcome: Stronger reputation and regulatory confidence

"Our CTEM platform gives you a real-time view of your true cyber exposure, prioritises what attackers can exploit, and drives measurable risk reduction across your organisation."

3. Security and Compliance

- **Data protection:** TLS 1.2+, IPsec/VPN for in-transit; encryption, sharding, and physical access control for data at rest
- **Audit and logging:** Real-time dashboards, regular reports; logs retained ≥12 months
- **Vulnerability management:** Continuous monitoring, threat intelligence, patching; compliant with CSA CCM v4.0
- **Incident management:** ISO/IEC 27035 aligned; predefined workflows, rapid response, post-incident reporting
- **Staff security:** BS7858:2019 screening; role-based access; MFA and PKI authentication
- **Datacentre:** Managed by third-party, compliant with CSA CCM v4.0, ISO/IEC 27001
- **Resilience & availability:** Multi-region redundancy, failover, load balancing; SLA 99.9% uptime

4. User Access and Authentication

- Multi-factor authentication and identity federation
- Role-based access controls for management interfaces and support channels
- Audit visibility for buyers' users (real-time and periodic)
- Management access via MFA, PKI, and dedicated links

5. Data Management

- **Export/Import formats:** CSV, ODF, PDF
- **Retention:** Audit and logs ≥12 months
- **End-of-contract:** Secure export via web or API; cryptographic erasure, secure overwrite, hardware destruction
- **Customisation:** Dashboards, alerts, reports, integrations; API-driven configuration
- **Mobile access:** Full dashboard and alert functionality; desktop for full operational control

6. Support

- **Levels:** Standard (24/5), Premium (24/7), Enterprise (dedicated TAM/engineer)
- **Web chat, email, and phone support**
- **SLA-backed response times**
- **Third-party access:** Authorised buyers' third parties can access support

7. Onboarding and Training

- Online, webinar, and optional onsite training
- Comprehensive user documentation in HTML, PDF, and ODF
- API and integration guides provided
- Free trial available for 30 days

8. Pricing and Discounts

- Special pricing available for educational organisations
- Free trial includes core dashboards, alerts, and reporting; excludes integrations and dedicated support