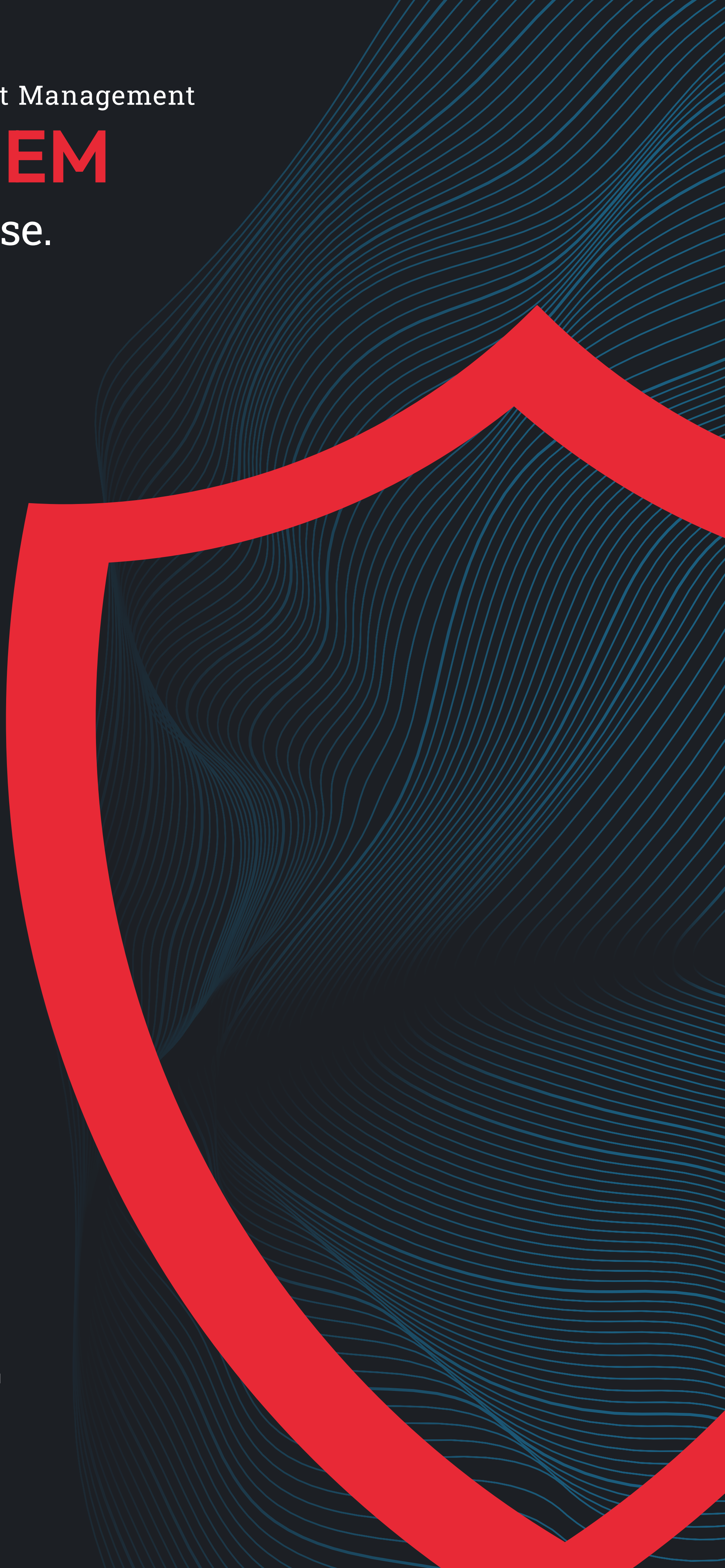
Security Information & Event Management

CyberSift SIEM

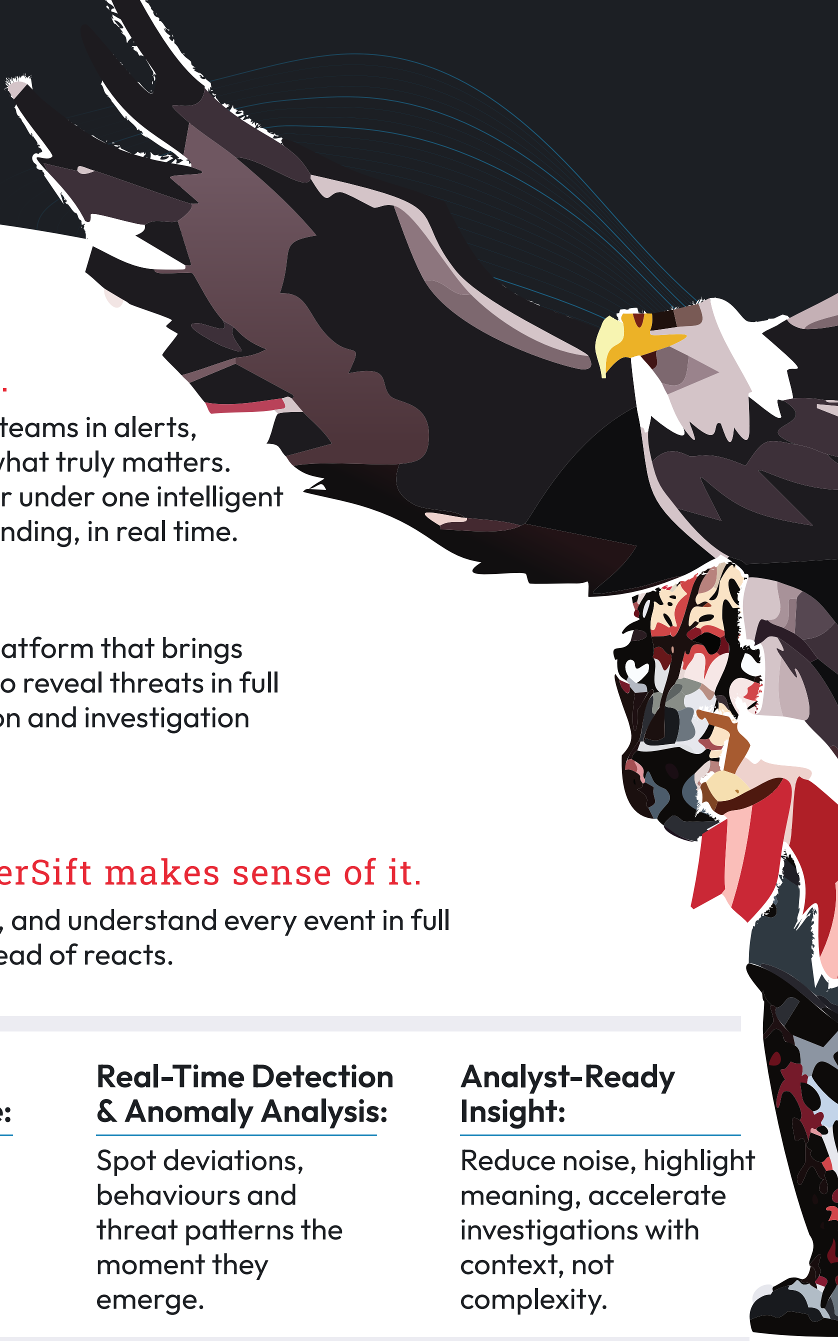
Cut through the noise.
See the unseen.



cybersift
SIEM

cybersift

SIEM SOLUTION



Where signals find meaning.

The SIEM built for clarity, not noise.

While traditional SIEM platforms drown security teams in alerts, CyberSift SIEM cuts through the noise to reveal what truly matters. By unifying logs, events, anomalies and behaviour under one intelligent engine, it transforms raw data into real understanding, in real time.

What is CyberSift SIEM

CyberSift SIEM is a unified security intelligence platform that brings together logs, events, behaviour and anomalies to reveal threats in full context. It delivers real-time detection, correlation and investigation capabilities and unified security intelligence.

Why CyberSift SIEM

Traditional SIEM collects data. CyberSift makes sense of it.

See threats as they form, detect anomalies early, and understand every event in full context, all through one platform that thinks instead of reacts.

Key characteristics

Unified Signal Visibility:

Bring every log, event and behaviour together into one clear, normalised view.

Intelligent Correlation Engine:

Connect signals automatically to reveal the full story behind every threat.

Real-Time Detection & Anomaly Analysis:

Spot deviations, behaviours and threat patterns the moment they emerge.

Analyst-Ready Insight:

Reduce noise, highlight meaning, accelerate investigations with context, not complexity.

CyberSift SIEM	vs	Traditional SIEM
Cuts alert noise with correlation, behaviour and context-aware analysis.		Generates high alert volumes with limited context.
Combines rules + anomalies + UEBA-style patterns for deeper detection.		Relies mostly on rule-based detection.
Unified visibility across logs, network activity, authentication, cloud and endpoints.		Fragmented visibility across logs, tools and data sources.
Clear investigations with linked events and narrative-style timelines.		Complex investigation workflows with slow triage.
Dramatically reduced false positives through intelligent enrichment.		Difficult tuning, frequent false positives.
Designed for analyst clarity including AI-first line analyst reducing complexity.		Requires heavy manual analysis from security teams.

How CyberSift SIEM works

1. **Log Collection & Normalisation**

   CyberSift ingests logs from servers, endpoints, firewalls, cloud services & applications, turning them into a consistent, readable dataset.

2. **Correlation & Behaviour Analysis**

   Signals are connected across systems to uncover relationships, suspicious chains and anomalies that rules alone cannot see.

3. **Real-Time Detection Engine**

   Threats are identified the moment patterns change — from brute force attempts to lateral movement indicators.

4. **Investigation & Alert Context**

   Each alert becomes a full narrative: linked events, indicators, timestamps, actors and impact — all visible in seconds.

5. **Continuous Visibility & SOC Alignment**

   24/7 awareness with optional SOC escalation for deeper analysis and response support.

Deliverables

Real-Time Alerts & Notifications

Instant insight into suspicious behaviour, anomalies and security events.

Unified Dashboards

Visibility across authentication, network activity, endpoint behaviour and cloud logs.

Advanced Data Processing Pipeline

Transforms and enriches high-volume security data in real time.

Compliance Reporting

Exportable reports for PCI, ISO, CIS and internal audits.

Forensics Timeline

Structured view of all relevant activity from first timestamp to final action.

Log Storage & Retrieval

Long-term log retention with fast, intuitive search.

Talk to Our Team

www.cybersift.com
info@cybersift.io
+356 7949 8471 (MT)
+44 20 8638 0550 (UK)

Book a demo

www.cybersift.com/demo

Core capabilities

Clarity reveals threats. Understanding stops them.

Real-Time Threat Detection

Identify attacks, anomalies and suspicious patterns instantly.

Behaviour Analytics

Spot lateral movement, compromised accounts and out-of-pattern activity.

Log Management & Normalisation

Centralised visibility across all systems and applications.

Correlation & Context Enrichment

Turn scattered events into complete threat narratives.

Network & Endpoint Visibility

Monitor traffic, user behaviour, access attempts and system actions.

Cloud & Hybrid Monitoring

Unified insight across on-premise, cloud workloads and SaaS services.

Forensics & Investigation Tools

Understand the "how, where and why" behind every security event.

Protection Through Collective Intelligence

At Cybersift, we believe cybersecurity should be intelligent, accessible, and built to empower everyone.

Born from a fusion of research and real-world expertise, we transform advanced AI into clear, strategic protection – enabling every organization to stay secure and resilient.

Guided by our vision to make cybersecurity accessible to everyone and to serve as a protector for the unprepared, we stand as a trusted partner in a world where digital threats evolve faster than awareness.

We don't just protect systems - we protect confidence, continuity, and growth.

Protection, at its core, is not about standing alone – it's about standing together. Like in nature, where every instinct contributes to survival, our technology learns, adapts, and protects as one.