ONE PLATFORM. COMPLETE VISIBILITY. SMARTER SECURITY.

The unified, AI-driven security operations platform

Baseel Kestrel brings security monitoring, threat detection, vulnerability management, software supply-chain security, threat intelligence, compliance monitoring and automated incident response into a single console — across cloud, on-premises, endpoints, applications and containers.

The problem

Security tools that work in silos leave risk in the dark. Teams face rising threats, software supply-chain attacks, unknown vulnerable dependencies, alert fatigue and manual response that slows everything down. Many also lack complete asset visibility and struggle to correlate events across environments, while compliance grows more complex.

The solution

Baseel Kestrel continuously collects telemetry from infrastructure, endpoints, applications, cloud services and software components. AI analyses it to surface suspicious activity, prioritise risk and speed up investigations, so analysts respond quickly with complete visibility across the organisation.

How it works

01 Collect
Agents, syslog, APIs and cloud connectors bring all telemetry into one place.

02 Detect
Built-in and custom rules correlate events into one prioritised alert stream.

03 Triage
Alerts are scored, enriched with threat intelligence and auto-triaged.

04 Investigate
Pivot to forensics, intel and dependencies without switching tools.

05 Respond
Open a case, assign an owner and run playbooks through to containment.

06 Recover and report
Restore systems, close with a full audit trail and feed post-incident reviews.

Key features and benefits

24×7 security monitoring
Continuous monitoring across cloud, on-premises, endpoints and applications.

AI-powered threat detection
Detects anomalies, insider threats, malware, ransomware and suspicious behaviour.

Software bill of materials
Generates and analyses SBOMs to find vulnerable libraries across apps and containers.

Vulnerability management
Correlates CVEs with OSV, NVD, EPSS and CISA KEV and prioritises remediation.

Asset inventory
Discovers hardware, software, cloud resources, containers and applications.

Threat intelligence
Correlates global threat feeds with organisational telemetry.

Incident management
Centralised triage, investigation, tracking and response workflows.

Security automation (SOAR)
Automates repetitive response actions to cut analyst workload.

Compliance monitoring
ISO/IEC 27001, SOC 2, PCI DSS, HIPAA, GDPR, NIST CSF and CIS Controls.

Behaviour analytics (UEBA)
Detects unusual user and entity behaviour to uncover insider threats.

Container and Kubernetes security
Monitors container workloads and Kubernetes clusters continuously.

Dashboards and reporting
Real-time dashboards, executive and compliance reports, and security KPIs.

Custom detection rules
Write and tune your own rules alongside the built-in detection library.

Configurable log retention
Hot, searchable data and long-term archives on a schedule you set.

Flexible log collection
Agents, syslog, APIs and cloud connectors, with parsers for custom formats.

Customer-built automation
Build your own response playbooks and actions to fit your processes.

Baseel Kestrel

PRODUCT DATASHEET

Platform modules

SIEM
TIER-1 SIEM

Cloud-native SIEM and EDR telemetry: log correlation, endpoint and cloud security.

Case Management
RESPONSE & INTEL

Case orchestration, automated response actions and security incident response.

Hunt Management
THREAT HUNTING

Endpoint DFIR and live response: monitoring, digital forensics and event collection.

UBA
THREAT DETECTION

User behaviour analytics, anomaly and insider-threat detection, and risk scoring.

Baseel Osprey
SUPPLY CHAIN

SBOM and dependency risk scanning for private repos and uploads, CVE and licence risk.

Baseel Owl
PAID ADD-ON

Threat intelligence and deep web search, data-leak detection and domain monitoring.

Use cases

- Continuous monitoring across cloud, on-premises and hybrid
- Centralised incident tracking, assignment and case management
- AI-assisted threat hunting and anomaly detection
- Software supply-chain security through component inventory
- Continuous vulnerability assessment and risk prioritisation
- Compliance monitoring and automated audit reporting

Differentiators

- Integrated AI-powered SOC platform
- Built-in SBOM and software supply-chain security
- Native case management with enhanced reporting and analytics
- AI risk scoring, false-positive scoring and AI-suggested remediation
- Guided playbooks and runbooks for analysts
- Scalable architecture for organisations of every size

Integrations and compatibility

TICKETING AND ITSM
Jira

CLOUD PLATFORMS
Microsoft Azure, AWS, Google Cloud Platform

IDENTITY
Microsoft Entra ID, Active Directory, LDAP, Okta

ENDPOINT SECURITY
Microsoft Defender, CrowdStrike, SentinelOne

DEVSECOPS
GitHub, GitLab

CONTAINER PLATFORMS
Docker, Kubernetes, OpenShift

THREAT INTELLIGENCE
STIX/TAXII, MISP, commercial threat feeds

LOG SOURCES
Syslog, Windows Event Logs, Linux logs, firewalls, VPNs, IDS/IPS, network devices

Deployment and licensing

- **Cloud:** fully managed SaaS
- **On-premises:** inside your own infrastructure
- **Hybrid:** one view across cloud and on-premises
- **Private cloud:** a dedicated environment
- **Licensing:** commercial subscription, licensed per asset

Why organisations trust Baseel

ISO/IEC 27001
Certified (Baseel Partners LLP)

CREST
Member company

SOC 2
Controls aligned with Trust Services Criteria

Secure development
Reviewed, tested, SBOM-tracked

SecOps expertise
Experienced security team

Customer-centric
Dedicated support

Secure your business with Baseel Kestrel

Request a personalised demo to see how Baseel Kestrel helps you detect threats faster, reduce risk and simplify compliance.

Web baseel.com/products/security-products/baseel-kestrel
Email contactus@baseel.com
Phone +44 (0) 20 4540 0111