Baseel Kestrel



PLATFORM BROCHURE · 2026

BASEEL KESTREL PLATFORM

AI-Powered Security Operations Center
& Continuous Risk Intelligence

One Platform.
Complete Visibility. Smarter Security.

Baseel
Security - Technology - Transformation

EXECUTIVE

SUMMARY

Baseel Kestrel is a comprehensive Security Operations Center (SOC) solution that unifies security monitoring, threat detection, vulnerability management, Software Bill of Materials (SBOM) analysis, AI-driven threat intelligence, compliance monitoring, and automated incident response into a single platform.

Designed for modern enterprises, it provides continuous visibility across cloud, on-premises, endpoints, applications, containers, and software supply chains — helping security teams detect threats faster, reduce risk, and simplify compliance.

ONE PLATFORM.
COMPLETE VISIBILITY.
SMARTER SECURITY.

THE PROBLEM

SECURITY TOOLS IN SILOS, RISK IN THE DARK

Modern organizations struggle with security tools operating in silos, increasing cyber threats, and software supply chain attacks. Unknown vulnerable dependencies, alert fatigue among SOC analysts, and manual incident response processes further slow detection and response.

Compounding these challenges, many organizations lack complete asset visibility, face growing compliance complexity, and struggle to correlate security events across disparate environments.

Without centralized visibility, organizations face increased security risks, slower response times, and higher operational costs.

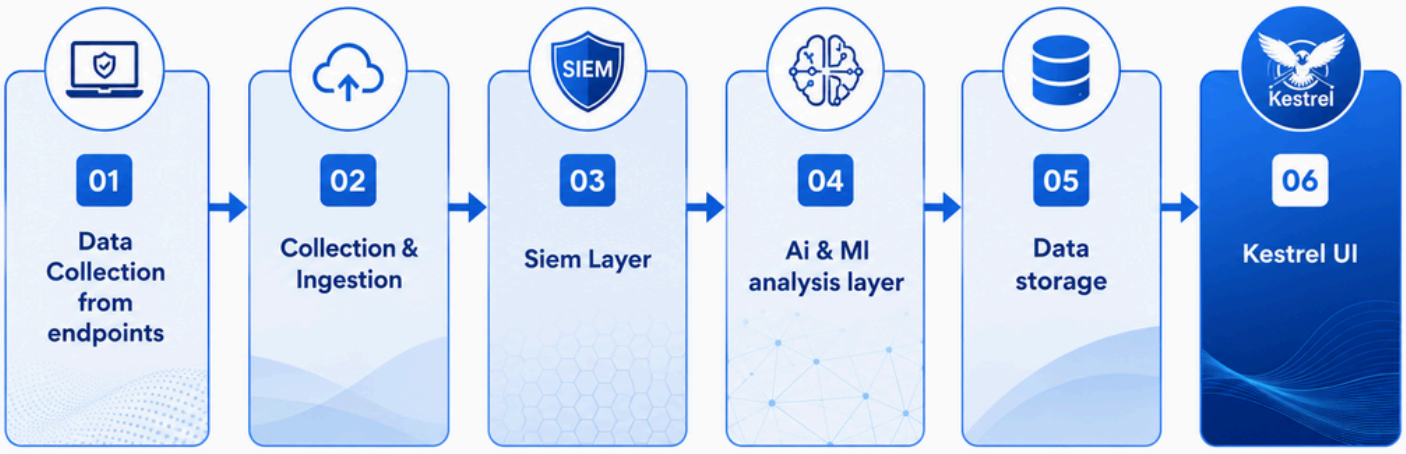
THE SOLUTION

ONE UNIFIED, AI-DRIVEN SOC

Baseel Kestrel brings together security monitoring, AI-powered analytics, vulnerability management, SBOM analysis, threat intelligence, and automated response into a unified solution.

The platform continuously collects telemetry from infrastructure, endpoints, applications, cloud services, and software artifacts. AI analyzes this data to identify suspicious activity, prioritize risks, and automate investigations, enabling security teams to respond quickly while maintaining complete visibility across the enterprise.

ARCHITECTURE



Baseel
Security - Technology - Transformation

KEY FEATURES & BENEFITS

Twelve capabilities, one console — from continuous monitoring to compliance reporting.

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 behavior using machine learning.

SOFTWARE BILL OF MATERIALS

Generates and analyzes SBOMs to identify components, dependencies, and vulnerable libraries across apps and containers.

VULNERABILITY MANAGEMENT

Correlates CVEs with OSV, NVD, EPSS, and CISA KEV intelligence and prioritizes remediation with AI-generated guidance.

ASSET INVENTORY

Automatically discovers hardware, software, cloud resources, containers, and applications.

THREAT INTELLIGENCE

Correlates global threat feeds with organizational telemetry to identify known threats.

INCIDENT MANAGEMENT

Centralized investigation, tracking, and response workflows.

SECURITY AUTOMATION (SOAR)

Automates repetitive response actions, reducing analyst workload.

COMPLIANCE MONITORING

Supports ISO 27001, SOC 2, PCI DSS, HIPAA, CIS, NIST, and other frameworks.

BEHAVIOR ANALYTICS (UEBA)

Detects unusual user and entity behavior to uncover insider threats.

CONTAINER & KUBERNETES SECURITY

Continuously monitors container workloads and Kubernetes clusters.

DASHBOARD & REPORTING

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

USE CASES

- Continuous security monitoring across cloud, on-prem, and hybrid
- Centralized 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 prioritization
- User and entity behavior analytics for insider threats
- Standardized runbooks for faster incident resolution
- Asset discovery and continuous inventory management
- Security dashboarding and executive risk reporting
- Cloud workload, container, and Kubernetes security
- Reduced MTTD and MTTR across the security lifecycle
- Real-time threat detection and incident investigation
- Automated threat containment and response workflows
- Endpoint visibility, forensic investigation, and remote response
- Identification and prioritization of vulnerable components
- Compliance monitoring and automated audit reporting
- Security orchestration with automated playbooks
- Threat intelligence correlation with internal events
- Ransomware, malware, and unauthorized access detection
- Root cause analysis and digital forensic investigations

DIFFERENTIATORS

- ✓ Integrated AI-powered SOC platform
- ✓ Built-in SBOM and software supply chain security
- ✓ Native case management with enhanced reports analytics
- ✓ Automated threat detection and response
- ✓ Comprehensive asset inventory
- ✓ Compliance-ready reporting
- ✓ Scalable architecture for enterprises of all sizes
- ✓ Extensible integrations with existing security ecosystems
- ✓ AI risk scoring, AI false positive score, AI remedies
- ✓ Guided playbooks and runbooks for analysts
- ✓ Unified visibility across cloud, on-prem, endpoints, and applications

INTEGRATIONS & COMPATIBILITY

CLOUD PLATFORMS

Microsoft Azure , AWS , Google Cloud Platform

IDENTITY

Microsoft Entra ID , Active Directory , LDAP ,Okta

ENDPOINT SECURITY

Microsoft Defender , CrowdStrike , SentinelOne , Enterprise endpoints

DEVSECOPS

GitHub ,GitLab

CONTAINER PLATFORMS

Docker ,Kubernetes , OpenShift

THREAT INTELLIGENCE

STIX/TAXII ,MISP , Commercial threat feeds

SIEM & LOG SOURCES

Syslog ,Windows Event Logs , Linux logs , Firewalls , VPNs , IDS/IPS , Network devices

DEPLOYMENT & PACKAGING

CLOUD
Fully managed SaaS deployment

ON-PREMISES
Deployed within customer infrastructure

HYBRID
Unified visibility across cloud and on-premises

PRIVATE CLOUD
Dedicated enterprise environment

Every organization has unique security, compliance, and deployment requirements. Contact our sales team for a personalized solution and pricing proposal.

WHY ORGANIZATIONS TRUST BASEEL

ISO 27001 Certified	**CREST Certified**
SOC 2 Compliant	**Quality Assured**
Enterprise Security Expertise	**Experienced SecOps Team**
Secure Development Practices	**Customer-Centric Support**

CALL TO ACTION

SECURE YOUR BUSINESS WITH BASEEL KESTREL

Gain complete visibility, strengthen your cyber resilience, and protect your software supply chain with an AI-powered security operations center. Request a personalized demo to see how Kestrel helps your organization detect threats faster, reduce risk, and simplify compliance.

EMAIL
contactus@baseel.com

WEB
www.baseel.com

PHONE
+44 20 4540 0111