BASEEL

Kestrel

UNIFIED SECURITY OPERATIONS PLATFORM

AI-powered security operations and continuous risk intelligence

One platform. Complete visibility. Smarter security.

SIEM | Case Management | Hunt Management | UBA | Baseel Osprey | Baseel Owl · paid add-on

BASEEL PARTNERS LLP (BASEEL GROUP)

THE CHALLENGE AND OUR ANSWER

Security teams are drowning in silos and noise

Fragmented tooling

No shared context, so analysts stitch the picture together by hand.

Alert fatigue

Thousands of alerts a day with little prioritisation.

Supply-chain blind spots

Vulnerable dependencies hidden in apps and containers.

Slow, manual response

Inconsistent investigation and containment.

Incomplete asset visibility

No reliable answer to "what do we have, and where?"

Compliance complexity

Audit-ready evidence is hard to sustain continuously.

THE BASEEL KESTREL ANSWER

Telemetry in. AI analysis. Automated response. One console across cloud, on-premises, endpoints, applications, containers and the software supply chain.

6
integrated modules

24×7
continuous monitoring

16
SOC capabilities

HOW IT WORKS

From telemetry to closed case, in one console

A single workflow aligned with the NIST SP 800-61 incident response lifecycle.

01
Collect
Agents, syslog, APIs and cloud connectors bring endpoint, network, cloud and user telemetry together.

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

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

04
Investigate
Pivot from an alert 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.

PLATFORM MODULES

Six modules. One console. Full-spectrum coverage.

TIER-1 SIEM

SIEM

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

RESPONSE & INTEL

Case Management

AI-assisted triage, tiered cases, playbooks, runbooks and SOC reporting.

THREAT HUNTING

Hunt Management

Endpoint DFIR and live response: fleet-wide hunts, forensics and evidence collection.

THREAT DETECTION

UBA

User and entity behaviour analytics: baselines, anomalies, attack chains and risk scoring.

SUPPLY CHAIN

Baseel Osprey

SBOM generation, vulnerability and licence risk, and cross-project correlation.

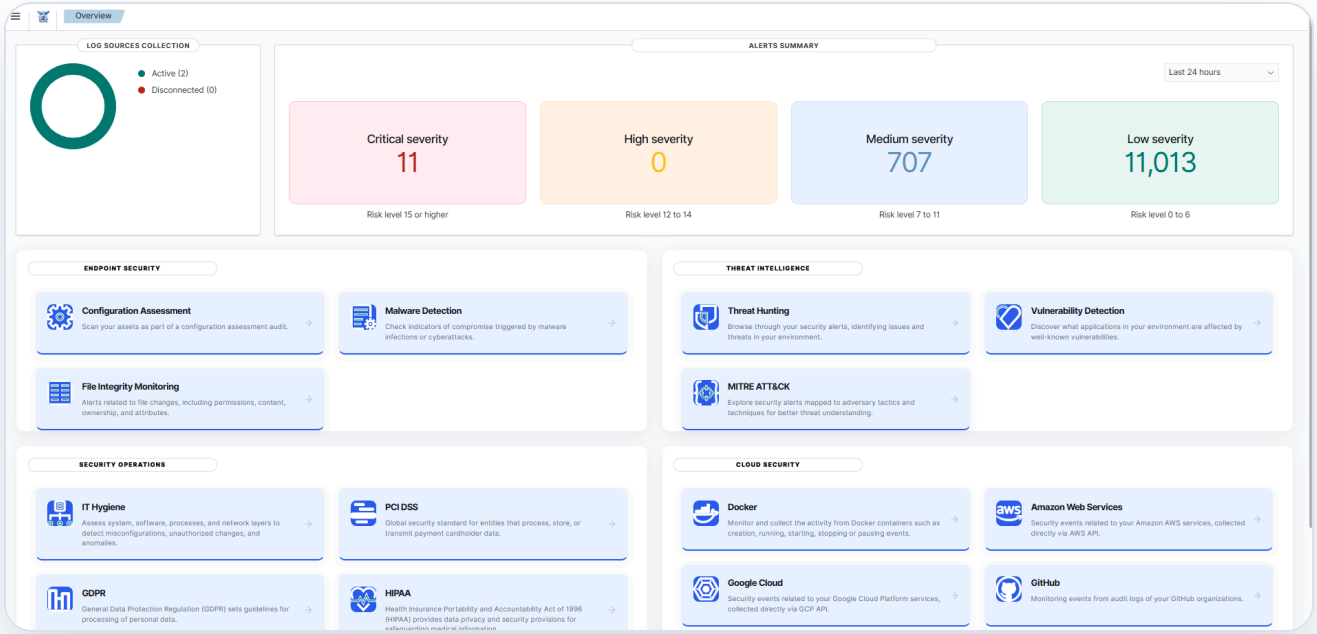
PAID ADD-ON

Baseel Owl

Threat intelligence and deep web monitoring that enriches every investigation.

MODULE · SIEM

Unified detection across endpoint, cloud and compliance



Critical
Immediate response

High
Persistence, privilege abuse

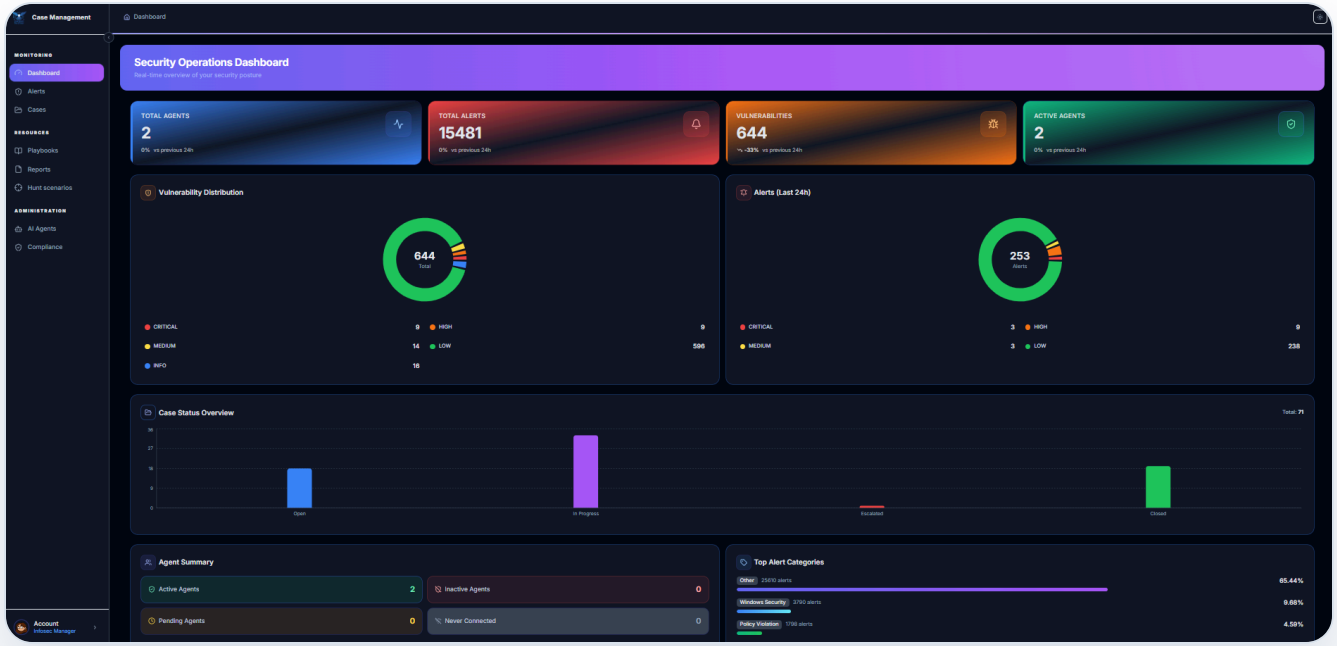
Medium
Investigate and correlate

Low
Context and audit

- **Endpoint security:** configuration assessment, malware detection and file integrity monitoring
- **Threat detection:** vulnerability detection and MITRE ATT&CK mapping
- **Custom rules:** write and tune your own detections
- **Compliance:** ISO/IEC 27001, SOC 2, PCI DSS, HIPAA, GDPR, NIST CSF and CIS Controls
- **Cloud security:** AWS, Microsoft Azure, Google Cloud, Docker and GitHub

MODULE · CASE MANAGEMENT

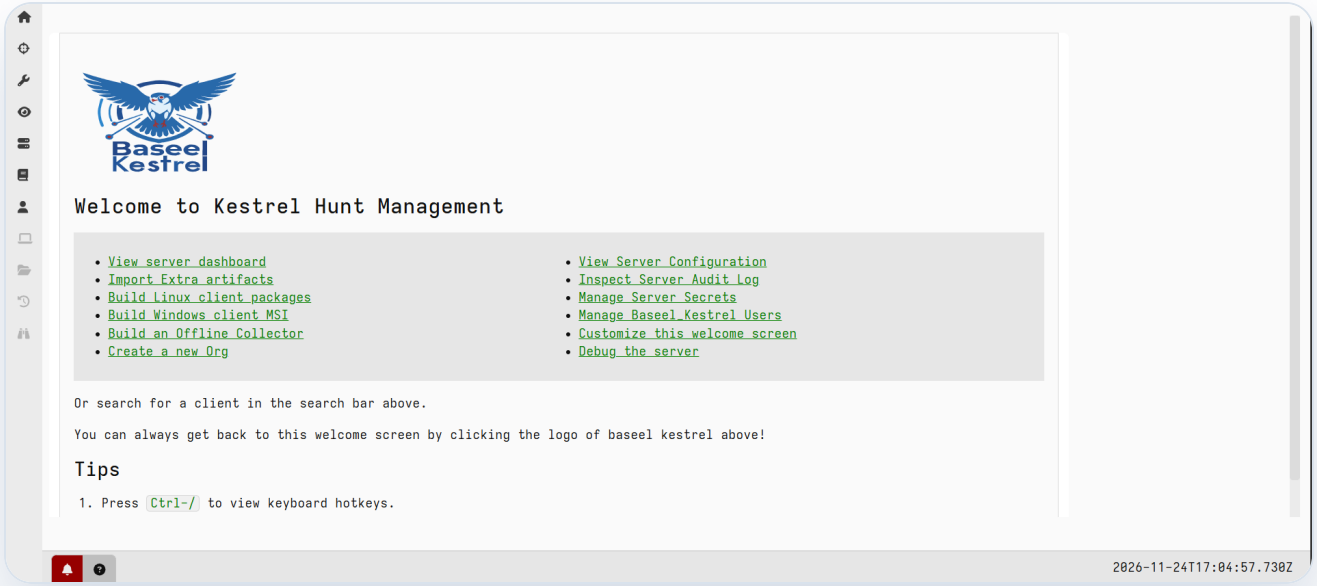
Real-time SOC operations with AI triage built in



- **AI-assisted triage** with severity, false-positive scoring and noise reduction
- **Tiered ownership:** cases routed to L1 responders, L2 triage and L3 threat hunters
- **MITRE-mapped playbooks** and step-by-step runbooks run from the case
- **SOC reporting:** alert trends, MTTD, MTTC, MTTR and SLA tracking
- **Jira linking** and workload views for SOC managers

MODULE · HUNT MANAGEMENT

Endpoint DFIR and live response at fleet scale



- **Fleet-wide hunts** across every endpoint, with resource and expiry controls
- **Deploy anywhere:** Windows and Linux agents, plus offline collection for air-gapped hosts
- **Live forensics:** collect evidence in minutes and attach it straight to a case
- **Built for response:** pivot from a SIEM alert or UBA anomaly into a targeted hunt

MODULE · UBA

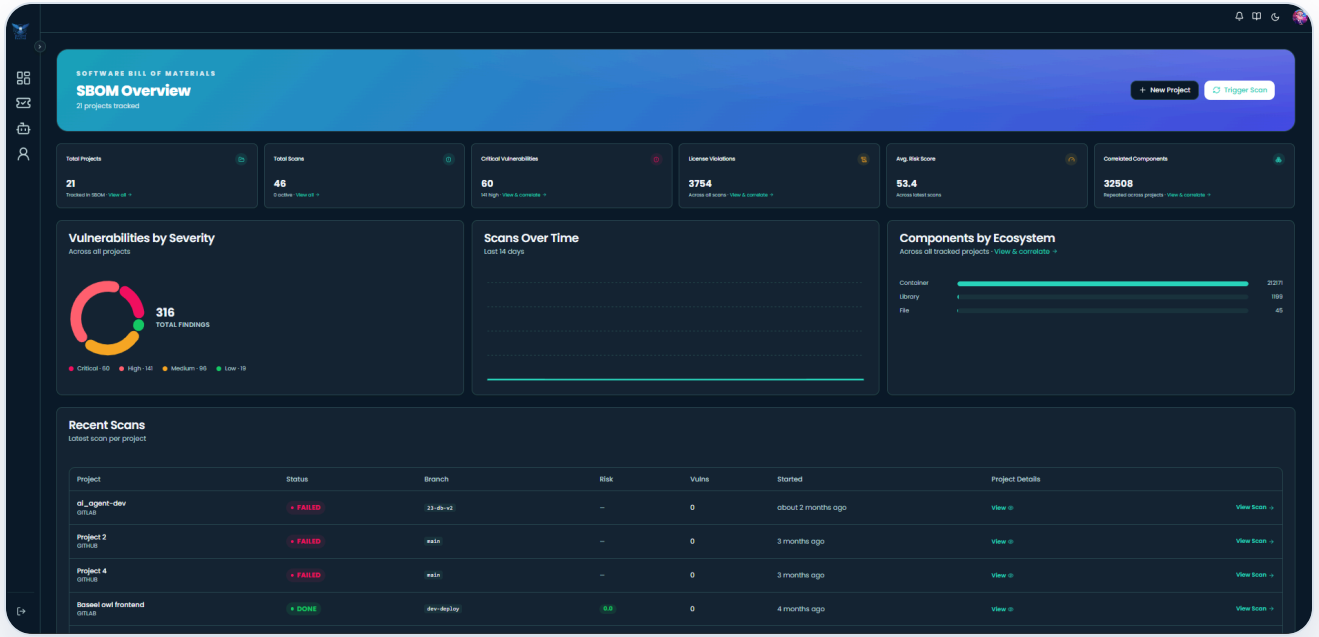
User and entity behaviour analytics



- **Behavioural baselines** for every user, host and source IP
- **Anomaly detection** for off-hours access, privilege misuse and unusual data movement
- **Attack chains** that link multi-stage activity across hosts
- **Risk posture** scored 0–100, with insider-threat alerting
- **Detection coverage** showing which sources report and where gaps remain

MODULE · BASEEL OSPREY

Software supply-chain risk, scanned and correlated



- **SBOM generation** from private repositories and source archives
- **Vulnerability matching** against CVE and GHSA advisories, with fixed versions
- **Licence risk** checked against your licence policy
- **Cross-project correlation** traces one vulnerable library everywhere it is used
- **Risk score** from 0 to 100 for every scan

MODULE · BASEEL OWL PAID ADD-ON

Threat intelligence in the context of your organisation



- **Threat intelligence:** malicious IPs, URLs, phishing and malware, mapped to threat groups
- **Deep web search** for mentions of your organisation and brands
- **Data-leak detection** for exposed credentials tied to your domains
- **Attack surface and brand protection** against look-alike domains and impersonation
- **Enriched investigations** inside SIEM and Case Management

INTEGRATIONS

Works with the tools you already run

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

WHY BASEEL KESTREL

Built for how your business runs

- Integrated, AI-powered SOC platform
- Built-in SBOM and software supply-chain security
- AI risk scoring, false-positive scoring and suggested remediation
- Guided playbooks and runbooks for analysts
- Native case management with rich reporting
- Extensible integrations with your existing stack

DEPLOYMENT AND LICENSING

Cloud (fully managed SaaS), on-premises, hybrid or private cloud. Sold as a commercial subscription, licensed per asset.

ISO/IEC 27001

Certified (Baseel Partners LLP)

CREST

Member company

SOC 2

Controls aligned with Trust Services Criteria

NIST CSF

Security practices aligned

SECURE DEVELOPMENT

Peer-reviewed, tested and SBOM-tracked

SUPPORT

Experienced SOC team, customer-centric support

NEXT STEP

Secure your business with Baseel Kestrel

See every module on your own data. Request a personalised demo and a specialist will come back to you within one business day.

WEB
baseel.com/products/security-products/baseel-kestrel

EMAIL
contactus@baseel.com

PHONE
+44 (0) 20 4540 0111