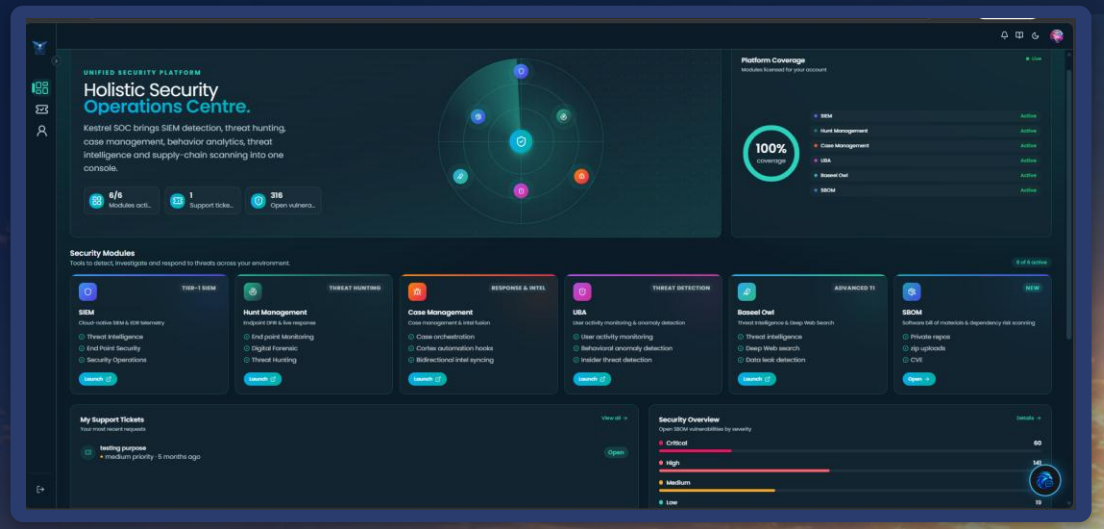
BASEEL KESTREL

AI-Powered Security Operations Center & Continuous Risk Intelligence



Kestrel Security Operations Dashboard — live SOC posture in one view

One Platform. Complete Visibility. Smarter Security.

SIEM | Hunt Management | Case Management | UBA Guard | Baseel Owl | SBOM

Product Overview • Platform Walkthrough • November 2026

Baseel
Security - Technology - Transformation

THE CHALLENGE & OUR ANSWER

Security teams are drowning in silos and noise

Fragmented tooling

No shared context — 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.

Manual response

Inconsistent, slow 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 KESTREL ANSWER

Telemetry in. AI analysis. Automated response — in one console that covers cloud, on-prem, endpoints, applications, containers and the software supply chain.

6	24/7	360°
integrated modules	continuous monitoring	environment coverage

10,613 of 31,879 alerts triaged by AI — a 33.3% cut in alert volume reaching analysts.

PLATFORM ARCHITECTURE

Six modules. One console. Full-spectrum coverage.

01 **Collect**
Endpoints, cloud, identity, apps & code repos

02 **Analyze**
AI correlation, risk scoring, MITRE mapping

03 **Respond**
Cases, playbooks, runbooks & live forensics

SIEM
TIER-1 DETECTION

Cloud-native SIEM & EDR telemetry, compliance packs, IT hygiene and cloud security.

Hunt Management
THREAT HUNTING

Endpoint DFIR & live response — fleet-wide hunts, artifact collection, offline collectors.

Case Management
RESPOND & INVESTIGATE

AI triage, alert browser, L1/L2/L3 cases, playbooks, runbooks and SOC reporting.

UBA Guard
UEBA + ABA

Behavioural baselines, anomalies, attack chains and AI-agent behaviour analytics.

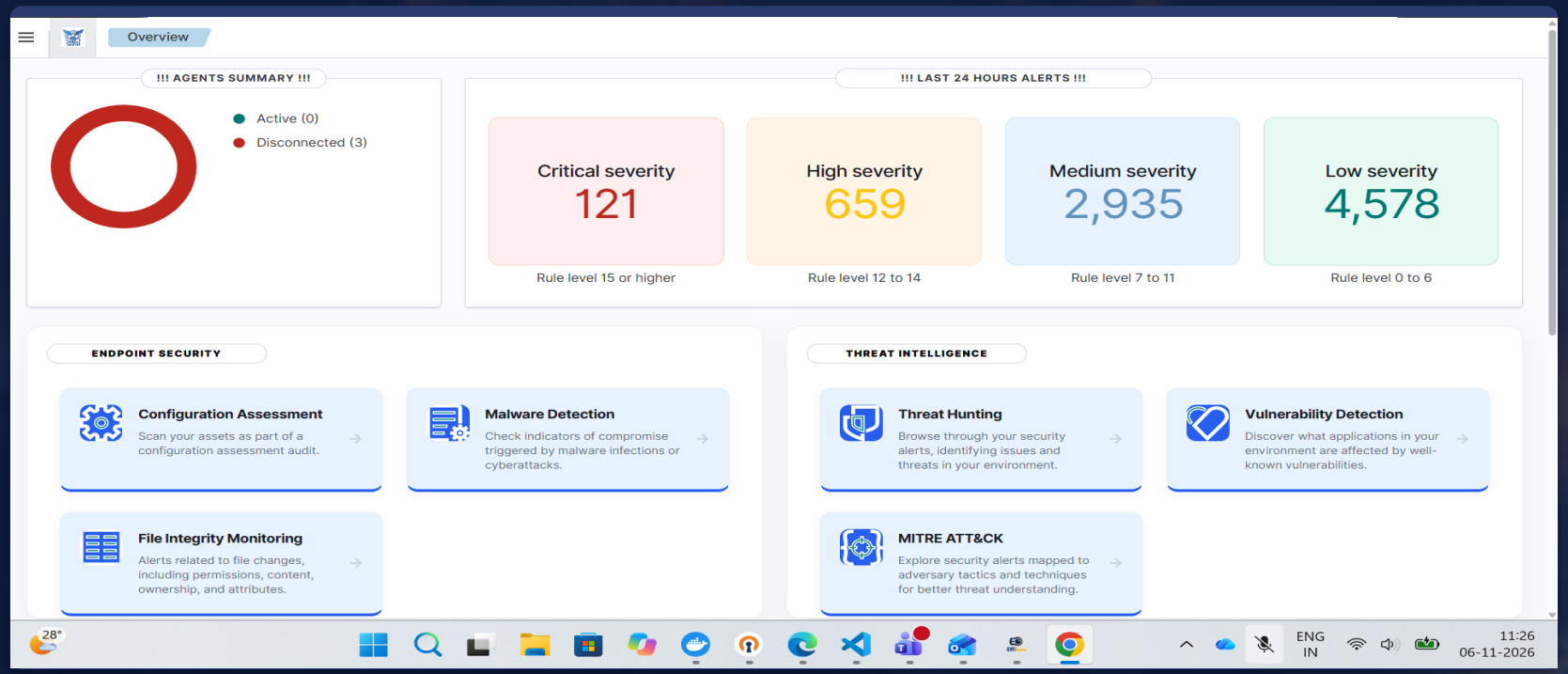
Baseel Owl
THREAT INTELLIGENCE

Deep-web intel: 1,182 intrusion sets and 894K+ indicators correlated with telemetry.

SBOM
SUPPLY-CHAIN RISK

SBOM generation, CVE/GHSA correlation, license violations and per-project risk scores.

Unified detection across endpoint, cloud & compliance



SIEM overview — log-source health and 24-hour alert severity bands by rule level

Endpoint security Configuration assessment · Malware detection · File integrity monitoring
Threat intelligence Threat hunting · Vulnerability detection · MITRE ATT&CK mapping

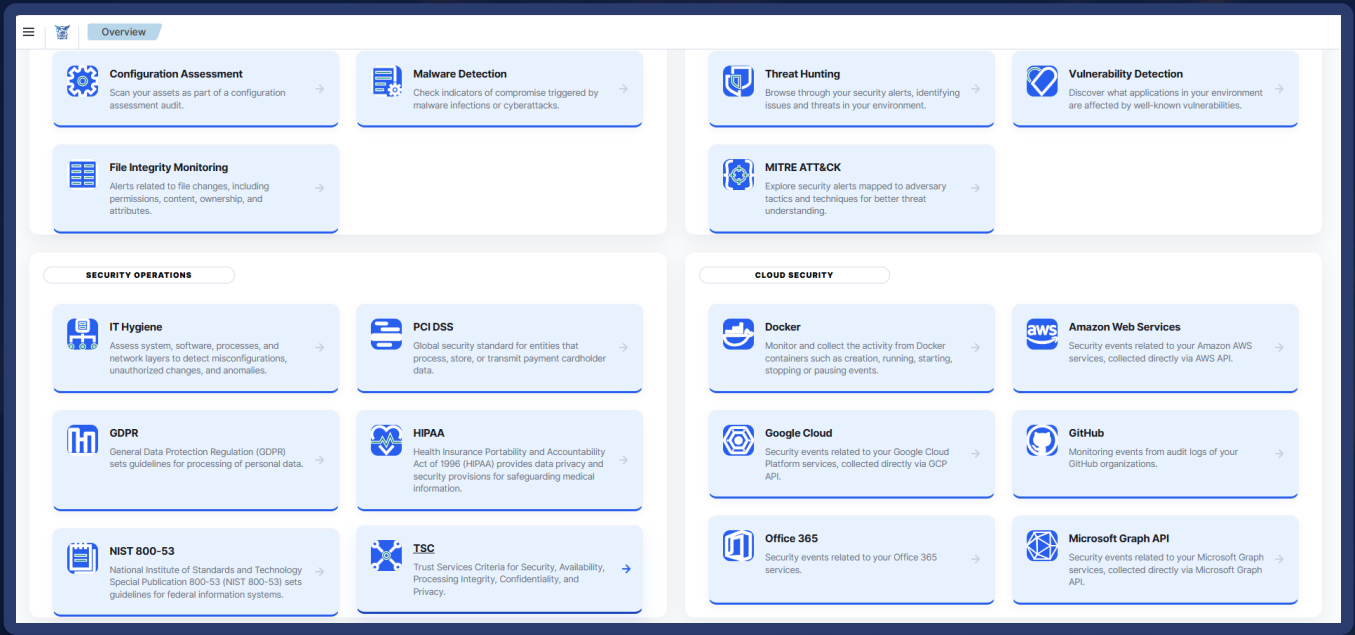
10
Critical alerts (24h) — rule level 15+

660
Medium alerts (24h) — rule level 7–11

7,152
Low alerts (24h) — rule level 0–6

2 / 0
Log sources active / disconnected

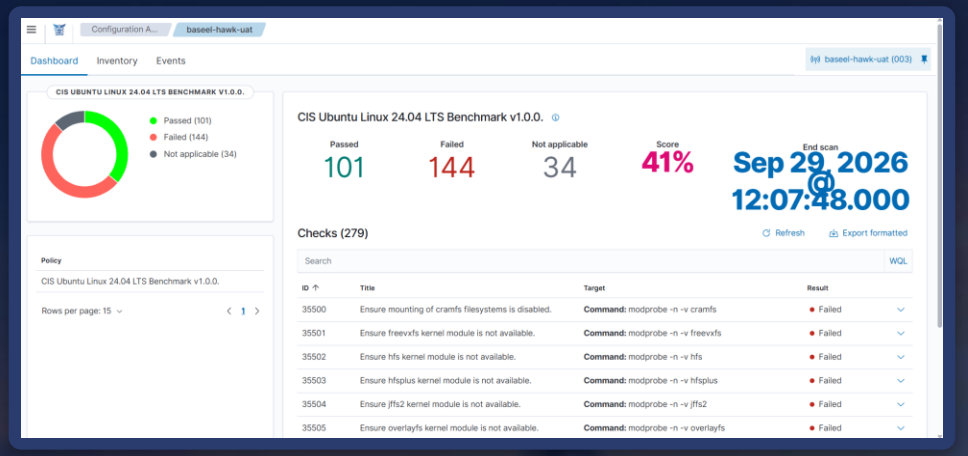
Compliance, cloud security & IT hygiene in one view



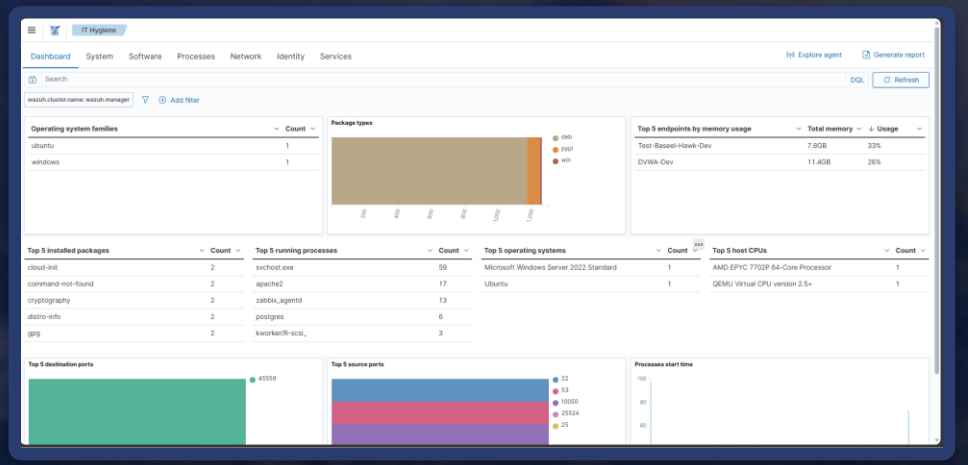
Built-in compliance packs and native cloud connectors

PCI DSS · GDPR · HIPAA · NIST 800-53 · TSC · CIS

AWS · Google Cloud · Docker · GitHub · Office 365 · MS Graph

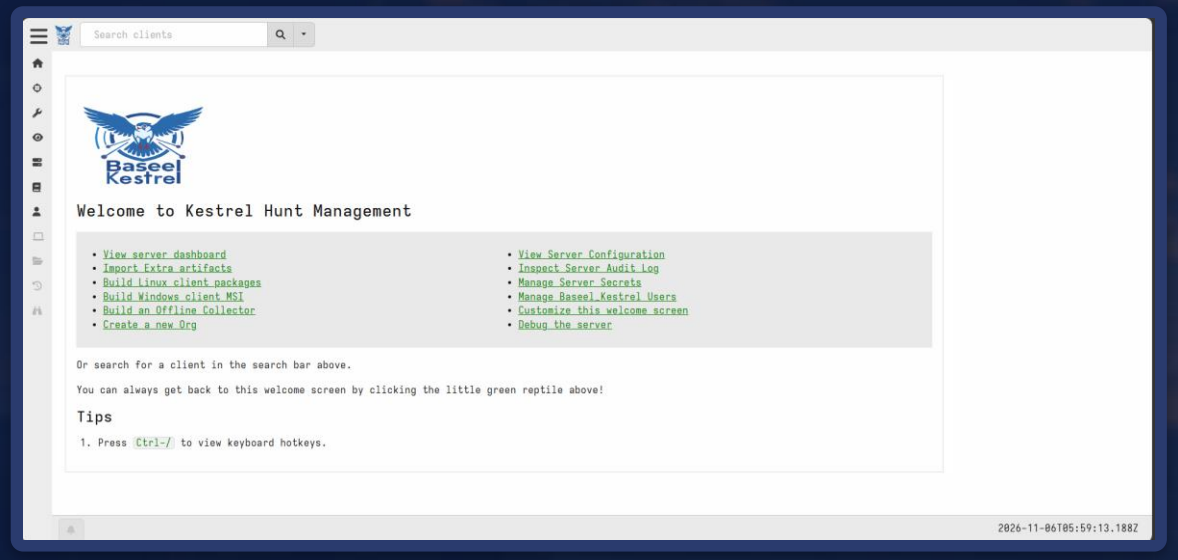


CIS Ubuntu 24.04 benchmark — 279 checks scored per host

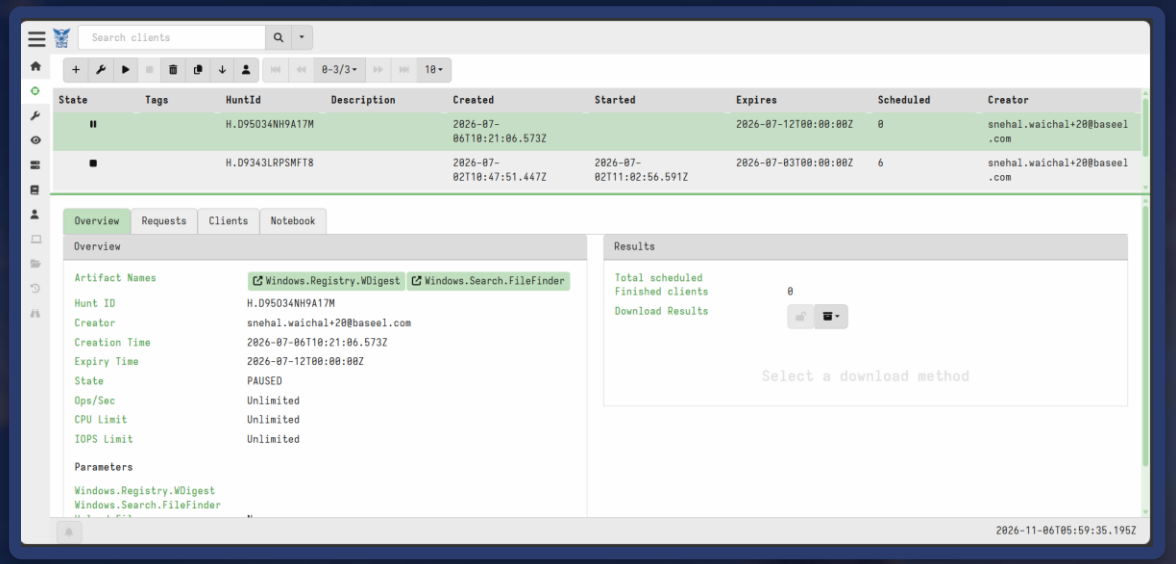


IT Hygiene — OS, packages, processes, ports, memory

Endpoint DFIR & live response at fleet scale



Kestrel Hunt Management console — server, clients, packages and orgs



Fleet hunts — e.g. Windows.Registry.WDigest + Windows.Search.FileFinder

Fleet-wide hunts

Schedule artifact hunts across every endpoint with CPU, IOPS and expiry controls.

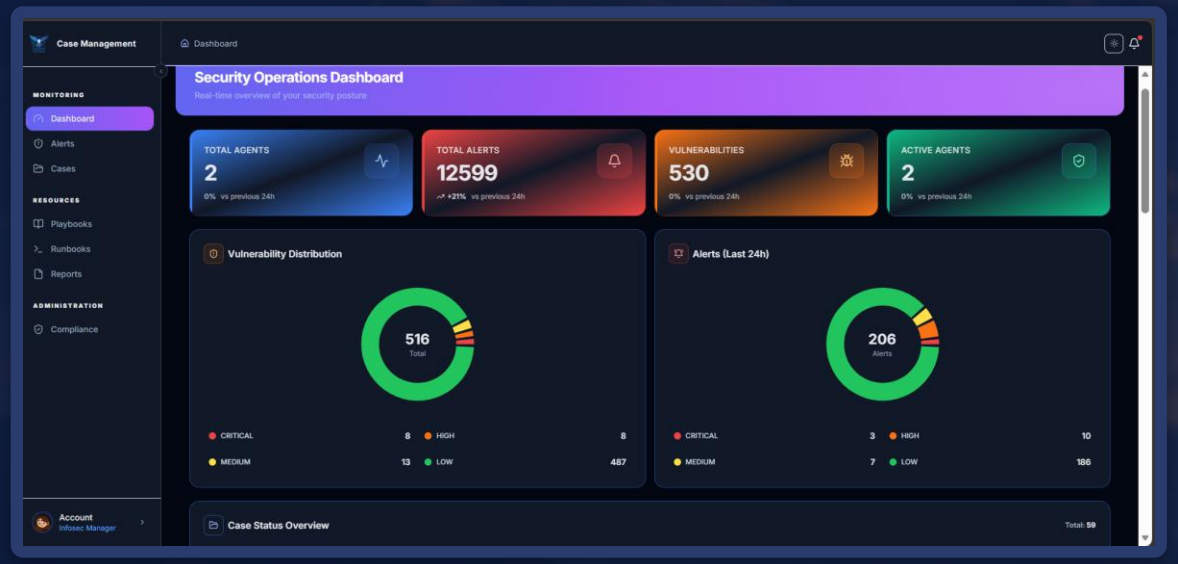
Deploy anywhere

Build Windows MSI and Linux client packages, or offline collectors for air-gapped hosts.

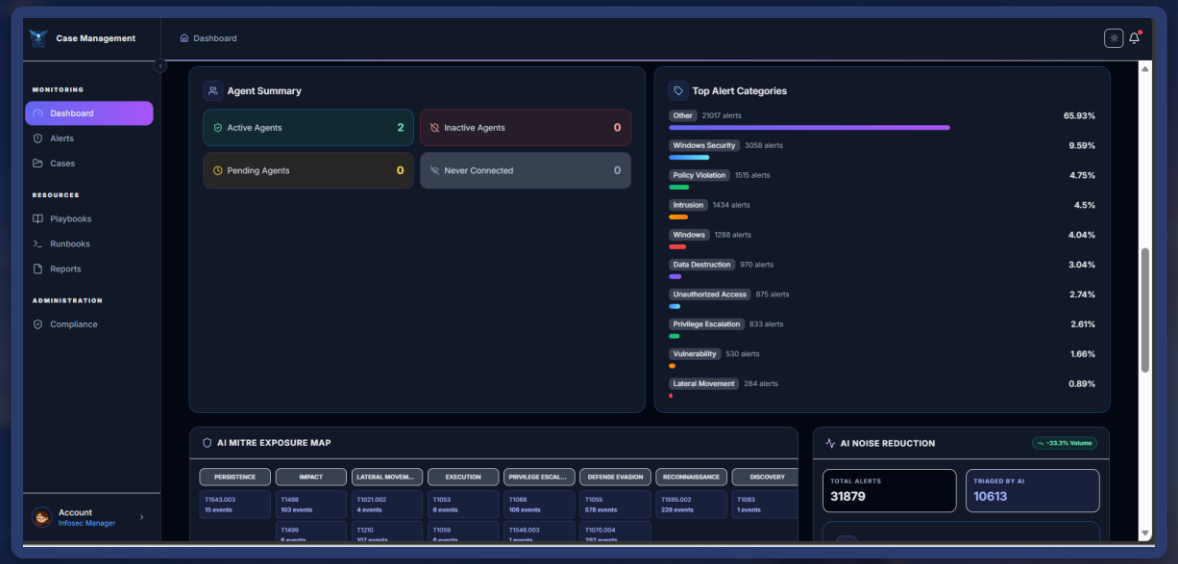
Live forensics

Collect artifacts, run notebooks and download evidence straight into a case.

Real-time SOC operations with AI triage built in



Security Operations Dashboard — agents, alerts & vulnerabilities



Top alert categories, AI MITRE exposure map & AI noise reduction

12,599
total alerts tracked (+21% vs previous 24h)

530
vulnerabilities across monitored agents

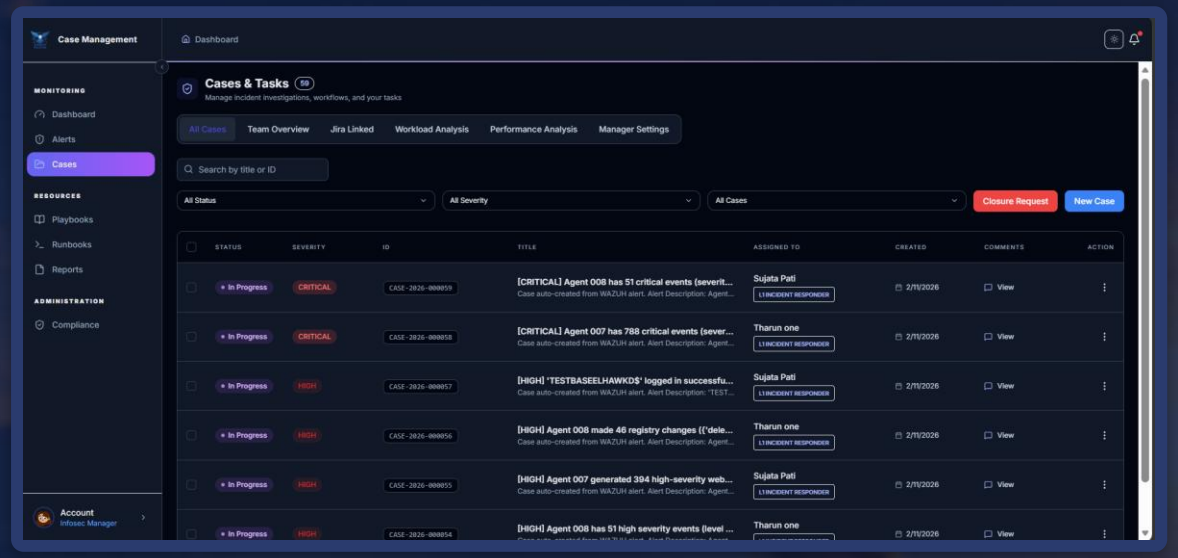
10,613
alerts auto-triaged by AI

–33.3%
alert volume after AI noise reduction

From alert to resolved case — triaged, assigned, tracked



Alert Browser — AI-driven triage with severity and top-rule analytics



Cases & Tasks — 59 cases auto-created from SIEM alerts

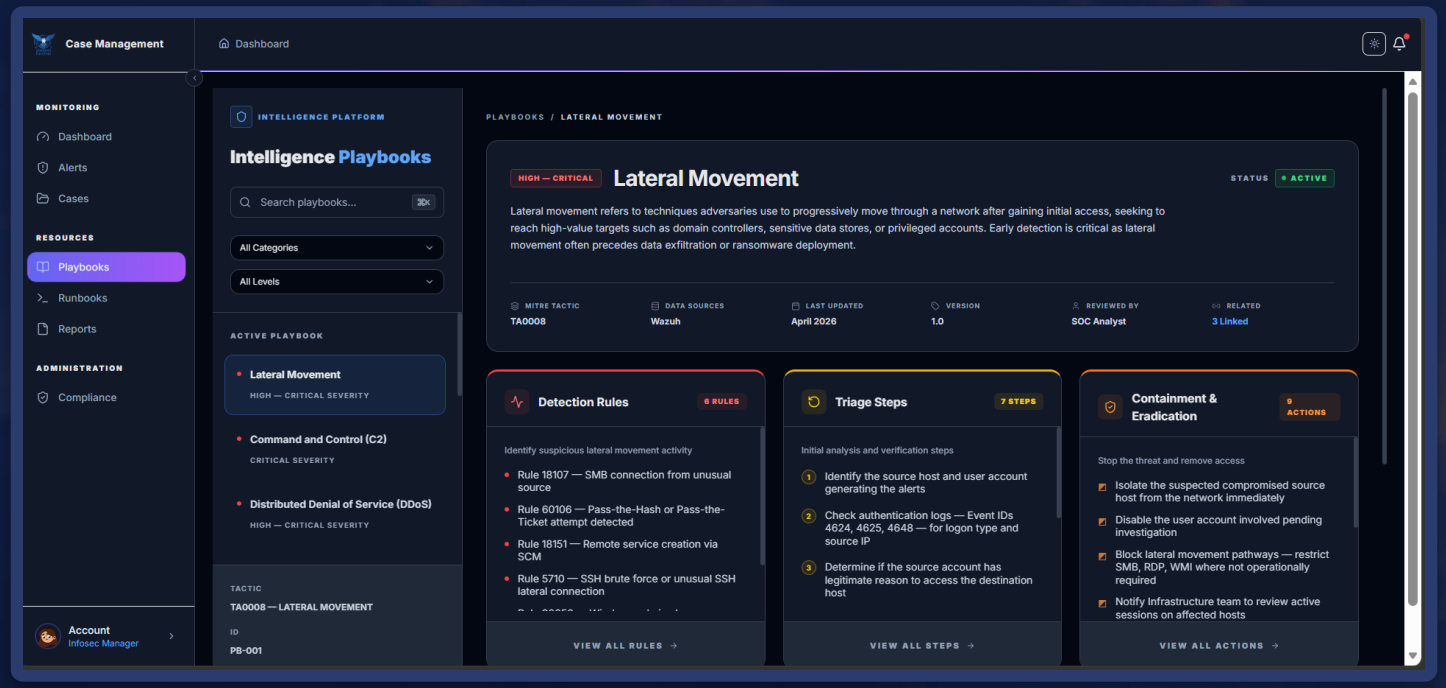
Five analytics views Alert browser, machine analytics, rule analytics, health check, anomaly browser

Filter in seconds By status, severity, agent ID or rule ID — then export or create alerts

Tiered ownership Cases routed to L1 responders, L2 triage and L3 threat hunters

Built for managers Jira linking, workload & performance analysis, closure requests

Guided response with playbooks, runbooks & reporting



Intelligence Playbook PB-001 — Lateral Movement (MITRE TA0008)



Reports & Analytics — 30-day SOC view

MITRE-mapped playbooks Lateral movement, C2, DDoS — rules, triage, containment, recovery

Runbooks Step-by-step workflows executed live from the case

SOC reporting Alert trend, severity mix, MTTD / MTTC / MTTR and SLA tracking

6 detection rules

7 triage steps

9 containment actions

User, entity & AI-agent behaviour analytics



Security Overview — behavioural risk posture, activity by hour and behaviour categories

34/100
behavioural posture (elevated)

768
events processed · 10 decoders

11
anomalies · 4 behaviour types

2
attack chains (multi-stage hosts)

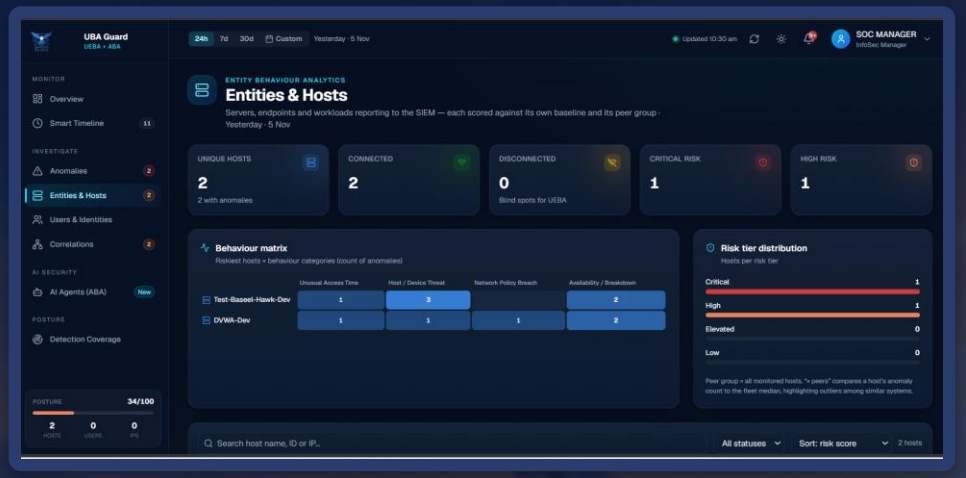
Smart Timeline 11 correlated events, in order
Correlations Links users, hosts and source IPs

NEW AI Agents (ABA) — the same baselining and anomaly detection, applied to AI agents operating in your estate.

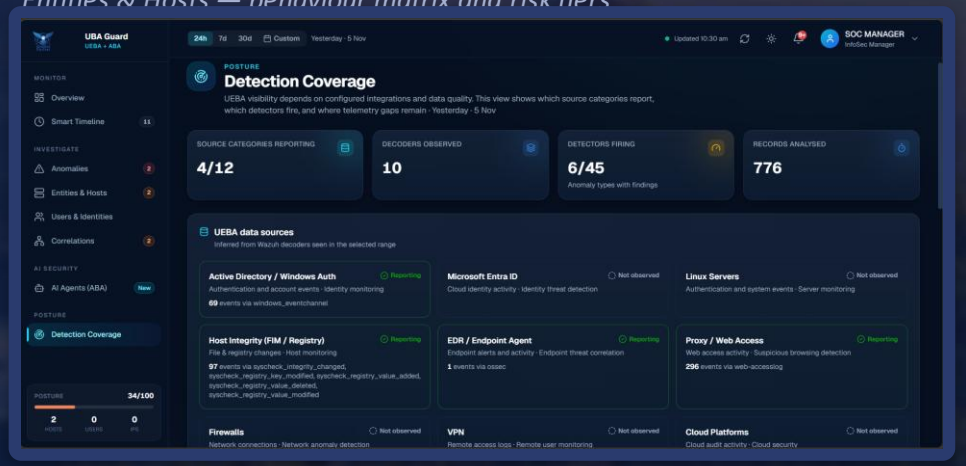
Investigate anomalies, entities and detection coverage



Anomalies — hour-of-day severity stack, filterable by behaviour



Entities & Hosts — behaviour matrix and risk tiers



Detection Coverage — which sources report, where gaps remain

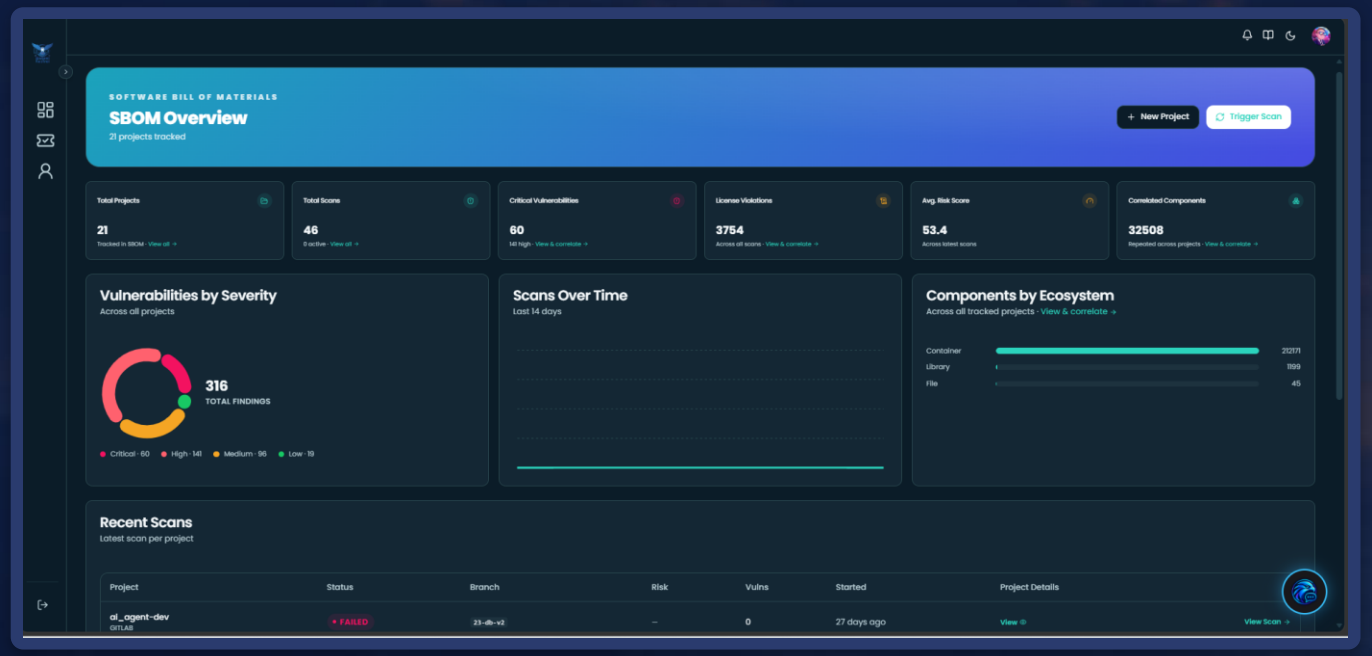
807 events evidenced

4/12 source categories reporting

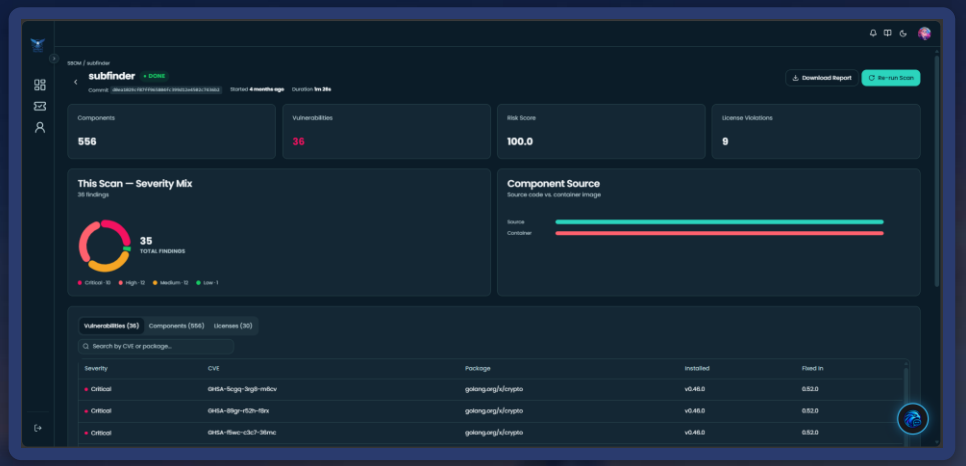
6/45 detectors firing

776 records analysed

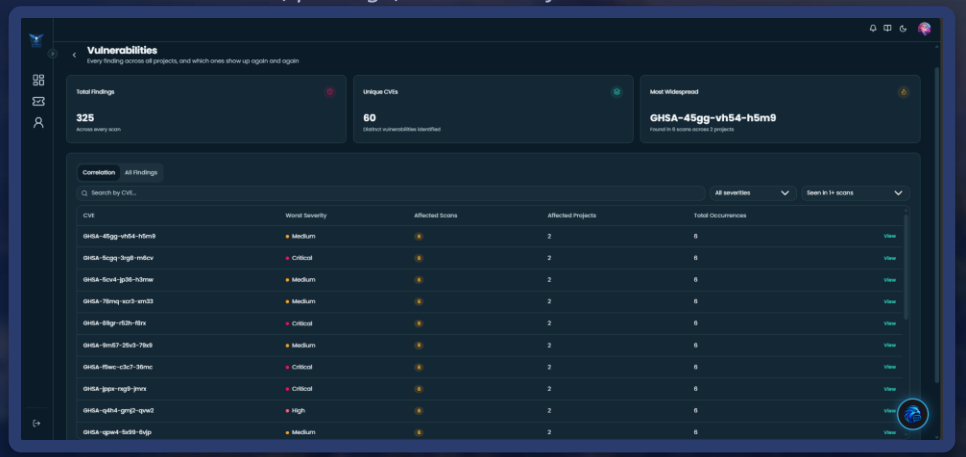
Software supply-chain risk, scanned and correlated



SBOM Overview — 21 projects, severity mix, components by ecosystem



Per-scan detail — CVE, package, installed vs fixed version



Cross-project correlation — which CVEs recur, and where

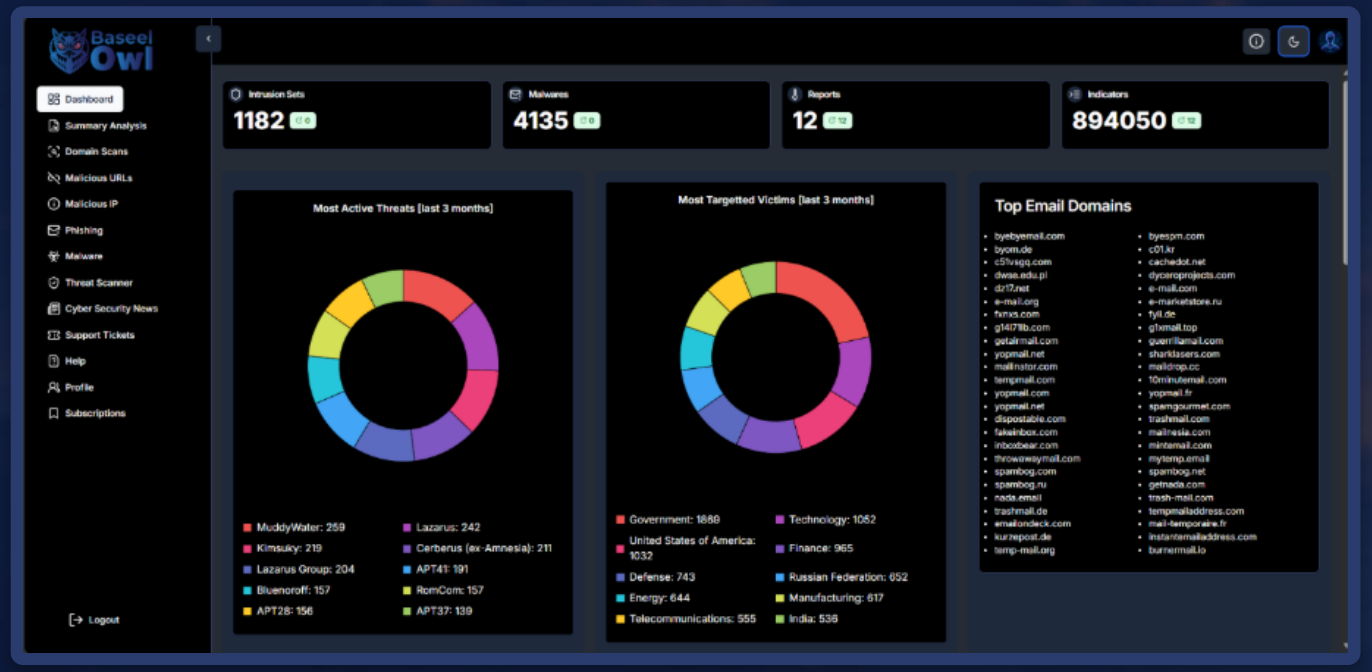
316 vulnerability findings

60 critical (141 high)

3,754 license violations

32,508 correlated components

Threat intelligence that plugs into what you run



Baseel Owl — most active threat groups, targeted sectors, phishing domains

1,182
intrusion sets

4,135
malware families

894K+
indicators correlated

INTEGRATIONS

Cloud	Microsoft Azure · AWS · Google Cloud
Identity	Entra ID · Active Directory · LDAP · Okta
Endpoint	Defender · CrowdStrike · SentinelOne
DevSecOps	GitHub · GitLab
Containers	Docker · Kubernetes · OpenShift
Log sources	Syslog · Firewalls · VPN · IDS/IPS
Threat intel	STIX/TAXII · MISP · commercial feeds

DIFFERENTIATORS

Why organisations choose Kestrel

- Integrated AI-powered SOC platform
- Built-in SBOM & supply-chain security
- AI risk scoring, false-positive scoring & AI remedies
- UEBA plus AI-agent behaviour analytics
- Guided playbooks & runbooks for analysts
- Native case management with rich reporting
- Compliance-ready: PCI DSS, HIPAA, GDPR, NIST, CIS
- Extensible integrations with your stack

DEPLOY THE WAY YOUR BUSINESS NEEDS

Cloud
Fully managed SaaS

On-premises
Inside your infrastructure

Hybrid
One view across both

Private cloud
Dedicated environment

ISO 27001 Certified | CREST Certified | SOC 2 Compliant | Secure SDLC Practices | Experienced SOC Team | Customer-Centric Support

Secure your business with Baseel Kestrel

See every module live on your own data. Request a personalised demo and a specialist will reply within one business day.

EMAIL
contactus@baseel.com

WEB
www.baseel.com

PHONE
+44 20 4540 0111