Baseel Owl

BASEEL OWL

See Every Threat. Triage in Seconds.

Powered by the Owl Threat Intelligence Engine — real-time intelligence aggregation with automated multi-vector triage, built for SOC teams who can't afford to miss a signal.

- Real-time Intelligence Aggregation
- Automated Multi-vector Triage
- High Confidence Detection & Enrichment
- Actionable Insights for Faster Response



ENTERPRISE CYBER THREAT INTELLIGENCE PLATFORM

AGGREGATE	DETECT	TRIAGE	PRIORITIZE	RESPOND
Multiple Intelligence Sources	Advanced Threat Detection	Automated Multi-vector Analysis	Contextual Risk Scoring	Faster, Smarter Decisions

Baseel
Security - Technology - Transformation

Why Cyber Owl

01 / EXECUTIVE SUMMARY

Baseel's Cyber Owl unifies fragmented threat data into one intelligence platform, powered by the proprietary **Owl Threat Intelligence Engine**. Built for SOC teams, CISOs and government security units, it aggregates, correlates and scores threats in real time — turning raw indicators into decisions your team can act on in **seconds, not days**.

90+
Reputation engines consulted in a single query

10
Modules on one analyst dashboard

02 / THE PROBLEM

Siloed, manual security tools can't keep pace with coordinated, multi-vector attacks.

01 **Speed**
Threats outrun manual review

02 **Fragmentation**
Intel scattered across disconnected tools

03 **Reactive posture**
Reactive security means costly breaches

04 **No correlation**
No standard way to link IOCs to actors

03 / THE SOLUTION

Cyber Owl converts scattered signals — IPs, URLs, hashes, domains, phishing indicators — into **standardized, engine-mapped intelligence**, live on one analyst dashboard.

04 / ARCHITECTURE — HOW IT WORKS



Key features

01 **Dashboard**
One command view — live counts of intrusion sets, malware, reports & indicators, plus most active threats, most targeted victims and top email domains

02 **Summary analysis**
Deep-dive attacker–victim relationships, STIX 2.1 containers, A–F reliability and confidence scoring (0–3) — validate before you act

03 **Domain scans**
Automated subdomain, mail server, host & DNS discovery — expose your attack surface first

04 **Malicious URLs**
Continuously updated inventory of URLs built to deliver exploits or host landing pages

05 **Malicious IP**
Live-tracked IPs tied to C2 servers, spam operations and DDoS infrastructure

06 **Phishing**
Detects deceptive email accounts, spoofed sender domains and fake landing pages targeting your brand

07 **Malware**
Centralized registry of malware binaries, signatures and threat classifications

08 **Threat scanner**
Query any IP, domain, URL or hash across 90+ AV engines — AI-generated verdict, confidence score & remediation runbook, mapped to MITRE ATT&CK

09 **Cyber security news**
Curated global & regional advisories, vulnerability alerts and threat actor reporting — in the same dashboard

10 **Plan**
Standard, Professional and Enterprise packages with real-time credit tracking and rate-limit control

Differentiators

Proprietary Owl Threat Intelligence Engine
Standards-based (STIX 2.1) mapping of intrusion sets, malware and indicator relationships — built natively into the platform.

90+ engine reputation scoring
Every verdict in a single query.

AI Investigator
Raw score → executive narrative → remediation runbook, automatically.

Flexible credit model
Spend scales with real investigation volume, not flat seats.

Single pane of glass
Domain, IP, URL, hash, phishing and news in one dashboard.

Use cases, packaging & next step

	Use Case	Problem	Baseel Owl	Outcome
01	**Threat intelligence alignment**	Local IOCs disconnected from global actor tracking	The Owl Engine structures and maps assets natively	**Unified adversary visibility**
02	**Attack surface mapping**	Unknown subdomains mean unknown risk	Automated Domain Scan	**Full exposure map in minutes**
03	**Reputation triaging**	A suspicious hash or URL needs an instant answer	Threat Scanner with AI Investigator	**Verdict and action plan in seconds**
04	**Targeted IP & URL blocking**	C2 and scam infrastructure evolves daily	Live malicious IP, URL and phishing feeds	**Always-current firewall blocklists**

DEPLOYMENT OPTIONS

- **Baseel-hosted SaaS**
  Fastest onboarding, continuous feed updates
- **Private cloud tenancy**
  Dedicated instance in your region for data residency and remove this and restricted network - from deployment options
- **On-premise / restricted network**
  For government and regulated environments

PACKAGING

Standard	Professional	Enterprise
Core dashboard, feeds & scanner credits	Adds AI Investigator & domain scans at scale	Full engine access, integrations & custom limits

REAL-TIME CREDIT TRACKING · RATE-LIMIT CONTROL

Tool video

NEXT STEP

Book a live Cyber Owl walkthrough

Bring one suspicious indicator and one domain — we will triage them live on the platform in under 15 minutes.

Email
ContactUs@baseel.com

Phone
+44 20 4540 0111

Baseel Owl

Baseel
Security - Technology - Transformation