Baseel
Security - Technology - Transformation

CUSTOMER CASE STUDY | THREAT INTELLIGENCE

DEESHAA
The Right Direction

NOVEMBER 2026

An intelligence-led approach to external threats for a global technology and cybersecurity environment

Prepared for customer and stakeholder discussion | November 2026

SECTOR	HEADQUARTERS	RELATIONSHIP	CLIENT CONTACT
IT, cybersecurity and technology consulting	Gibraltar; international client reach	Baseel service relationship: over one year	Seema Shintre, Managing Director seema@deeshaa.biz

"CASE STUDY PERSPECTIVE"

This case study describes how Baseel Owl's threat intelligence capabilities align with Deeshaa Limited's published technology and cybersecurity service environment. Public sources reviewed do not disclose a Deeshaa-specific Owl deployment design or independently verified security performance results; accordingly, the use cases below are presented as a solution-alignment narrative rather than quantified implementation claims.

EXECUTIVE OVERVIEW

Deeshaa Limited is an international technology and consulting organisation headquartered in Gibraltar, serving clients in more than 50 countries. Its published portfolio spans governance and strategy, cloud, data, cybersecurity, infrastructure and applications, and managed IT and security services. The organisation's public materials also reference capabilities associated with infrastructure security, Cyber Essentials-related technical audits, GDPR, IoT security, Microsoft DevOps and data-centre services.

Many of the threats facing a technology and managed-services provider originate outside its own network: impersonating domains, phishing infrastructure, leaked credentials, exposed internet-facing assets and fast-moving attack campaigns. Baseel Owl is designed to give security teams this outside-in view through indicator enrichment, external attack surface discovery, brand protection, breach intelligence and curated threat news, delivered from one API-driven platform.

ORGANISATION PROFILE AND OPERATING CONTEXT

Deeshaa Limited operates a broad, multi-disciplinary service model supported by technology partnerships and capabilities that include Microsoft, AWS, AT&T, IASME, Tenable and SonicWall. The breadth of this environment means that the organisation's own brand, domains and people, and those of its clients, can present a wide external footprint to potential attackers.

For organisations delivering managed IT and cybersecurity services, intelligence is most useful when it answers practical questions quickly: is this indicator known to be malicious, is a lookalike domain impersonating the brand, have staff or client credentials appeared in a breach, and which internet-facing assets are exposed? Answers need to be recorded, shared with the right owner and acted on consistently.

THREAT INTELLIGENCE PRIORITIES

01

Faster indicator verdicts

Check suspicious URLs, IP addresses, file hashes and domains against trusted intelligence sources from one place, rather than across several separate tools.

02

External attack surface visibility

Discover and track internet-facing domains, subdomains and services to understand what an attacker can see and reach.

03

Brand and domain protection

Identify lookalike domains, fake websites and suspicious social media activity that could be used to impersonate the organisation or its clients.

04

Credential exposure awareness

Find out when organisational email addresses or credentials appear in known breach data so that resets and user follow-up can begin early.

05

Emerging threat awareness

Keep analysts and stakeholders informed of new campaigns, malware and vulnerabilities through curated news, watchlists and a geographic threat view.

06

Governed, multi-tenant access

Separate organisations and teams, apply role-based access and maintain audit records so intelligence work can be reviewed and evidenced.

OWL SOLUTION ALIGNMENT

Baseel Owl is positioned as a threat intelligence platform for SOC analysts, threat researchers and security organisations that need centralised, automated intelligence. Supplied product materials describe IOC enrichment, malicious indicator databases, external attack surface management, domain and OSINT reconnaissance, brand protection, social media monitoring, breach intelligence, AI-summarised threat news, watchlists, Slack and email notifications, and integration with the Baseel Kestrel SOC platform.

SERVICE AREA	OWL CAPABILITY ALIGNMENT	POTENTIAL OPERATIONAL CONTRIBUTION
Cybersecurity services	IOC Intelligence for URLs, IPs, hashes and domains; malicious IP, URL, phishing and malware databases; automated enrichment from multiple trusted intelligence sources.	Quicker, more consistent verdicts during triage and fewer manual look-ups across separate intelligence tools.
Infrastructure and managed IT	AttackLens external attack surface management, Web Recon, domain scanning and subdomain discovery.	A clearer inventory of internet-facing assets and a basis for prioritising exposed services for remediation.
Brand and client protection	Lookalike domain detection, fake website identification, social media and mention monitoring.	Earlier warning of impersonation and phishing activity targeting the organisation or the clients it serves.
Identity, data and GDPR	Breach Intelligence and Breach Lookup for organisational email addresses and domains.	Supports credential resets, user follow-up and data-exposure discussions under GDPR-related obligations.
SOC integration and governance	Single sign-on from Baseel Kestrel; watchlists; Slack and email alerts; multi-tenant organisations, role-based access and audit logging.	Intelligence available alongside SOC operations, with structured records for service reviews and customer assurance.

ILLUSTRATIVE THREAT INTELLIGENCE LIFECYCLE

1. **Collect:** aggregate intelligence from agreed external sources, threat feeds and news, alongside the domains, brands and assets nominated for monitoring.
2. **Enrich:** look up indicators against trusted intelligence sources to return reputation, detection and context details for each URL, IP, hash or domain.
3. **Monitor:** track watchlists, lookalike domains, attack surface changes, social mentions and breach data for matches that need attention.
4. **Prioritise:** assess findings by severity, asset importance and likely impact so that analysts focus on the most relevant exposures first.
5. **Act:** share findings through Slack, email or the Kestrel SOC workflow and coordinate remediation with the responsible technical or business owner.
6. **Report:** provide dashboards and summaries of indicators investigated, exposures found, actions taken and open risks.

EXPECTED OPERATIONAL VALUE

When the relevant monitoring scope, integrations and operating procedures are in place, the Owl capabilities described in the product materials can support the following outcomes:

- A single, consistent source of threat intelligence for analysts, instead of research spread across multiple tools.
- Earlier awareness of brand impersonation, phishing domains and fake websites.
- Better visibility of internet-facing assets and the exposure they present.
- Faster response to credential exposure through breach intelligence.
- More structured intelligence records for service reviews, governance discussions and customer assurance.

OUTCOME MEASUREMENT

To convert these expected value areas into verified customer results, agree a baseline and reporting period for measures such as time to indicator verdict, monitored domain and asset coverage, lookalike-domain detection-to-action time, credential exposure response time, watchlist match volume and the share of findings closed with a recorded outcome.

RECOMMENDED IMPLEMENTATION AND GOVERNANCE CONSIDERATIONS

01
Confirm the brands, domains, client environments and user groups in scope for monitoring and who owns each.

02
Prioritise monitoring based on business criticality, public exposure and the likelihood of impersonation.

03
Define severity levels, notification channels, escalation paths and who may act on each type of finding.

04
Agree access controls, data retention and handling of breach and personal data before production use.

05
Review watchlists and monitoring scope periodically to reduce noise and reflect changes in the estate.

ABOUT BASEEL AND OWL

Baseel Partners, a global IT and consulting group serving clients across more than 100 countries, with regional strengths in the UK, India and the Middle East. Baseel's website reports a corporate footprint of 800+ clients and 2,000+ projects; these are company-published profile figures and are not Owl-specific customer outcomes.

Baseel Owl is a threat intelligence platform. The supplied product materials describe capabilities spanning IOC enrichment, malicious indicator databases, external attack surface management, domain and OSINT reconnaissance, brand protection, social media monitoring, breach intelligence, AI-summarised cybersecurity news, watchlists, a geographic threat map, Slack and email notifications, multi-tenant access control with audit logging, and Baseel Kestrel SOC integration.

CLIENT CONTACT
Seema Shintre, Managing Director · seema@deeshaa.biz

DEESHAA The Right Direction