Baseel
Security - Technology - Transformation

CUSTOMER CASE STUDY | SECURITY OPERATIONS

DEESHAA
The Right Direction

MARCH 2026

A unified SOC approach for a global technology and cybersecurity environment

Prepared for customer and stakeholder discussion | March 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 Kestrel's SOC capabilities align with Deeshaa Limited's published technology and cybersecurity service environment. Public sources reviewed do not disclose a Deeshaa-specific Kestrel 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, 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.

In an environment that combines technology delivery with cybersecurity and managed services, security operations benefit from a consolidated view of activity across endpoints, networks, servers, identity platforms, cloud workloads and business applications. Baseel Kestrel is designed to provide this operational foundation through centralised telemetry, contextual threat detection, investigation workflows, response orchestration and reporting.

ORGANISATION PROFILE AND OPERATING CONTEXT

Deeshaa Limited, 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 makes consistency of monitoring and incident handling an important consideration, particularly where infrastructure and security responsibilities span multiple platforms or customer environments.

For organisations delivering managed IT and cybersecurity services, operational visibility is not limited to identifying an isolated alert. Analysts also need to understand the affected asset, user, service, business context and potential exposure; preserve investigation records; and coordinate remediation with the appropriate technical owner.

SECURITY OPERATIONS PRIORITIES

01

Consolidated visibility

Bring together security events from endpoint protection, servers, network devices, firewalls, VPNs, identity services, cloud platforms and supported applications.

02

Alert quality and context

Correlate related events and apply behavioural analytics to help distinguish routine activity from potentially malicious behaviour.

03

Hybrid infrastructure coverage

Maintain a coherent monitoring approach across cloud, on-premises, containerised and hybrid environments.

04

Repeatable incident management

Establish clear triage, escalation, ownership, evidence capture and closure practices.

05

Risk-based remediation

Connect asset and vulnerability context to prioritise remediation according to exposure and operational importance.

06

Customer assurance and governance

Support reviews with consistent incident records, dashboards and compliance-oriented reporting.

KESTREL SOLUTION ALIGNMENT

Baseel Kestrel is positioned as a unified Security Operations Centre platform combining continuous monitoring, event correlation, threat detection, investigation, response and reporting. Supplied product materials describe rule-based, signature-based and behaviour-based analytics, UEBA, asset discovery, vulnerability management, case management, SOAR playbooks, threat intelligence and endpoint/network forensic capabilities.

OPERATIONAL PRIORITY	KESTREL CAPABILITY ALIGNMENT	POTENTIAL OPERATIONAL CONTRIBUTION
Cybersecurity services	Centralised security event collection; rule, signature and behaviour analytics; UEBA; threat intelligence enrichment.	A consolidated view of security signals and additional context for investigating suspicious user, endpoint and network activity.
Infrastructure and managed IT	Monitoring for supported Windows/Linux systems, network devices, firewalls, VPNs, IDS/IPS and application telemetry.	Improved visibility across distributed infrastructure and a more consistent basis for triage and escalation.
Cloud and hybrid services	Telemetry integration across supported cloud, on-premises and hybrid environments; asset inventory and vulnerability context.	A more complete picture of monitored assets and potential exposure across mixed infrastructure.
DevOps and container environments	Integration options described for GitHub/GitLab and container platforms such as Docker and Kubernetes, where configured.	Security events from software delivery and container environments can be considered alongside wider SOC telemetry.
Governance and assurance	Case management, investigation history, dashboards and compliance-oriented reporting.	More structured evidence for operational reviews, incident tracking and customer assurance activities.

ILLUSTRATIVE SOC USE-CASE LIFECYCLE

1. **Collect:** ingest agreed security telemetry from selected systems and platforms, with source ownership and retention requirements defined.
2. **Correlate:** associate related events and apply rules, signatures and behavioural analytics to identify patterns that warrant investigation.
3. **Prioritise:** enrich alerts with asset, identity, vulnerability and threat-intelligence context to support risk-based triage.
4. **Investigate:** create and manage cases, preserve relevant event context, and use endpoint or network forensic capabilities where available.
5. **Respond:** follow approved playbooks for escalation, containment and remediation, with automation applied only to authorised actions.
6. **Report:** provide operational dashboards and agreed summaries covering incidents, trends, response activity and outstanding risks.

EXPECTED OPERATIONAL VALUE

When the relevant data sources, integrations and operating procedures are implemented, the Kestrel capabilities described in the product materials can support the following outcomes:

- A more unified operational view of security activity across supported infrastructure and services.
- Improved investigative context through event correlation, UEBA and threat-intelligence enrichment.
- More consistent incident handling through documented cases, assigned ownership and repeatable playbooks.
- Better-informed vulnerability prioritisation through asset discovery and exposure context.
- More structured reporting 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 telemetry-source coverage, alert-to-case conversion, mean time to acknowledge, mean time to contain, vulnerability remediation ageing and incident closure quality.

RECOMMENDED IMPLEMENTATION AND GOVERNANCE CONSIDERATIONS

01
Confirm the in-scope business services, infrastructure boundaries, customer environments and operational responsibilities.

02
Prioritise data sources based on business criticality, security value, availability and integration readiness.

03
Define alert severity, escalation paths, incident ownership, response authority and out-of-hours procedures.

04
Agree data retention, access controls, evidence handling and reporting requirements before production onboarding.

05
Review use cases periodically to reduce noisy detections, address coverage gaps and reflect changes in the technology estate.

ABOUT BASEEL AND KESTREL

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 Kestrel-specific customer outcomes.

Baseel Kestrel is a Security Operations Centre platform. The supplied product materials describe capabilities spanning continuous monitoring, advanced threat detection, UEBA, incident response and containment, asset inventory and discovery, vulnerability management, SBOM and software supply-chain analysis, threat intelligence, case management, SOAR, forensic investigation, dashboards and compliance reporting. Deployment models described include cloud, on-premises, hybrid and private cloud.

CLIENT CONTACT

Seema Shintre, Managing Director · seema@deeshaa.biz

DEESHAA The Right Direction