DEESHAA LIMITED

# One view of security across a multi-platform managed-services business

Deeshaa Limited runs its security operations on Baseel Kestrel, bringing monitoring, detection, investigation and response for a diverse technology estate into a single console.

| SECTOR | HEADQUARTERS | RELATIONSHIP | PLATFORM |
|---|---|---|---|
| IT, cyber security and technology consulting | Gibraltar, serving clients in 50+ countries | Baseel customer for over a year | Baseel Kestrel unified SOC |

## The organisation

Deeshaa Limited is an international technology and consulting organisation that helps clients in more than 50 countries with governance and strategy, cloud, data, cyber security, infrastructure and applications, and managed IT and security services.

Its work spans technology partnerships with Microsoft, AWS, AT&T, IASME, Tenable and SonicWall, along with infrastructure security, Cyber Essentials technical audits, GDPR, IoT security, Microsoft DevOps and data-centre services.

## The challenge

A service model this broad means security events arrive from many platforms and customer environments. Analysts need more than an isolated alert: they need the affected asset, user, service and business context, a preserved investigation record, and a clear route to the right technical owner.

Deeshaa wanted consistent monitoring and incident handling across all of it, without adding another set of disconnected tools.

## Security operations priorities

**01**
### Consolidated visibility
Security events from endpoints, servers, network devices, firewalls, VPNs, identity services, cloud platforms and applications in one place.

**02**
### Alert quality and context
Correlated events and behavioural analytics that separate routine activity from genuinely suspicious behaviour.

**03**
### Hybrid coverage
One monitoring approach across cloud, on-premises, containerised and hybrid environments.

**04**
### Repeatable incident handling
Clear triage, escalation, ownership, evidence capture and closure for every incident.

**05**
### Risk-based remediation
Asset and vulnerability context that ranks fixes by exposure and business importance.

**06**
### Customer assurance
Consistent incident records, dashboards and compliance reporting for service reviews.

> *"Kestrel brings a structured, proactive approach to security monitoring and threat management — with integrated detection, vulnerability management, and operations that improve visibility and response to emerging risks."*
>
> **— Managing Director, Deeshaa Limited**

## How Deeshaa uses Baseel Kestrel

| PRIORITY | BASEEL KESTREL CAPABILITY | WHAT IT GIVES DEESHAA |
|---|---|---|
| **Cyber security services** | Centralised event collection; rule, signature and behaviour-based analytics; UEBA; threat intelligence enrichment. | A single view of security signals, with the context to investigate suspicious user, endpoint and network activity quickly. |
| **Infrastructure and managed IT** | Monitoring for Windows and Linux systems, network devices, firewalls, VPNs, IDS/IPS and application telemetry. | Visibility across distributed infrastructure and a consistent basis for triage and escalation. |
| **Cloud and hybrid services** | Telemetry from cloud, on-premises and hybrid environments, with asset inventory and vulnerability context. | A complete picture of monitored assets and their exposure across a mixed estate. |
| **DevOps and containers** | Integrations with GitHub, GitLab, Docker and Kubernetes. | Events from software delivery and container platforms analysed alongside wider SOC telemetry. |
| **Governance and assurance** | Case management, investigation history, dashboards and compliance reporting. | Structured evidence for operational reviews, incident tracking and customer assurance. |

## From telemetry to closed case

**01**
### Collect
Agreed telemetry flows in from in-scope systems, with source owners and retention defined.

**02**
### Detect
Rules, signatures and behavioural analytics surface patterns worth a look.

**03**
### Triage
Alerts are enriched with asset, identity, vulnerability and threat intelligence context.

**04**
### Investigate
Cases preserve event context, with endpoint and network forensics on hand.

**05**
### Respond
Approved playbooks drive escalation, containment and remediation.

**06**
### Recover and report
Dashboards and summaries cover incidents, trends, actions and open risks.

## What Deeshaa gains

- A unified view of security activity across its infrastructure and services.
- Richer investigations through correlation, UEBA and threat intelligence.
- Consistent incident handling with documented cases, clear owners and repeatable playbooks.
- Sharper vulnerability prioritisation from asset discovery and exposure context.
- Structured reporting for service reviews, governance and customer assurance.

## How the deployment is run

- In-scope services, infrastructure and customer environments are defined up front.
- Data sources are onboarded in order of business criticality and security value.
- Severity, escalation paths, ownership and out-of-hours procedures are agreed.
- Retention, access control, evidence handling and reporting are set before go-live.
- Detections are reviewed regularly to cut noise and close coverage gaps.

### About Baseel Kestrel

Baseel Kestrel is the unified security operations platform from Baseel Partners LLP (Baseel Group). It brings SIEM, Case Management, Hunt Management, UBA, Baseel Osprey (software supply-chain security) and the Baseel Owl threat intelligence add-on into one console, with cloud, on-premises, hybrid and private-cloud deployment. It is sold as a commercial subscription, licensed per asset.

Baseel Partners LLP (Baseel Group) is a global IT and consulting group serving 800+ clients in 100+ countries, with operations across the UK, Europe, the Middle East and Asia. Baseel Partners LLP is certified to ISO/IEC 27001 and is a CREST member company.

**baseel.com/products/security-products/baseel-kestrel** · contactus@baseel.com · +44 (0) 20 4540 0111