MAULEE FOUNDATION

Protecting donor, grant and beneficiary information for a mission-led charity

Maulee Foundation uses Baseel Kestrel to watch over the systems behind its grant-making, with clear visibility into threats and a proportionate way to respond.

SECTOR	LOCATION	PLATFORM	RELATIONSHIP
Non-profit, grant-making foundation	London, United Kingdom	Baseel Kestrel unified SOC	Supported by Baseel Partners LLP

The organisation

Maulee Foundation connects donors and charities to maximise social impact. It makes grants to registered charities in England and Wales, focusing on preventing or relieving poverty, supporting individuals in need and advancing education for disadvantaged people.

Its projects cover education, food security, vocational and digital skills, relief for people in need and support for disadvantaged communities.

The challenge

The Foundation works with donors, grant applicants, charity partners, volunteers, trustees and programme stakeholders. That means handling sensitive personal information, supporting documents, financial and grant records and governance material.

With a strong emphasis on due diligence, safeguarding and transparent reporting, protecting the confidentiality, integrity and availability of that information is central to its work and to stakeholder trust.

Security and resilience priorities

01
Stakeholder information
Safeguard donor, applicant, partner, volunteer and beneficiary information held in approved systems.

02
Identity and access oversight
Monitor sign-ins, privilege changes and access to sensitive records, limited to authorised roles.

03
Digital service protection
Keep watch over public websites, online forms, email and supporting infrastructure.

04
Grant record integrity
Protect and trace applications, assessment evidence, decisions and outcome reports.

05
Practical incident readiness
Triage, escalation, investigation and response workflows sized to the team's capacity.

06
Governance and accountability
Incident records and concise reporting for management and trustee oversight.

> *"Kestrel has strengthened our security posture with better visibility into threats and protection for sensitive organisational and beneficiary information — giving us greater confidence in our digital operations."*
>
> **— Chief Operating Officer, Maulee Foundation**

How Maulee uses Baseel Kestrel

PRIORITY	BASEEL KESTREL CAPABILITY	WHAT IT GIVES MAULEE
Donor and grant information	Audit, identity, endpoint, application and database events from systems that hold stakeholder and grant records.	Visibility into unusual access and support for investigating unauthorised activity.
Charity partner due diligence	Monitoring of access to partner records, governance documents and evidence, with case context retained.	Traceability and a consistent security view of information used in assessments.
Staff, trustee and volunteer accounts	Identity and behaviour analytics on sign-ins, privilege changes and anomalous access.	Early warning of unusual sign-ins, unexpected account activity and credential misuse.
Websites and online services	Web, server, network and endpoint telemetry from public-facing services.	Faster spotting and investigation of suspicious activity on engagement channels.
Governance and reporting	Case management, dashboards, audit-friendly records and compliance reporting.	Structured information that supports management and trustee oversight.

Scenarios Baseel Kestrel is set up to handle

A

Unusual access to grant records

An account opens far more grant files than usual. Behaviour analytics flags it, and the case keeps the investigation trail.

B

Compromised mailbox or credential

A suspicious sign-in or account change is detected, and correlated events show whether other systems are affected.

C

Threat to a public service

Unexpected activity around the website or an online form is triaged and routed to the right technical owner.

D

Malware or ransomware

Suspicious execution or lateral movement triggers investigation and approved containment and recovery playbooks.

E

Vulnerable key system

A vulnerability on a grant-administration system is ranked by asset criticality so the most important fix comes first.

What Maulee gains

- Clear visibility into security activity around donor, partner and grant workflows.
- Better context for reviewing unusual account behaviour and access to sensitive data.
- Structured incident handling with case records, owners and approved playbooks.

How the deployment is run

- Systems holding donor, grant, partner, staff and beneficiary data are classified by sensitivity.
- Data ownership, access, logging, retention and safeguarding requirements are confirmed.
- Identity, email, web, endpoint, server, cloud and network sources are onboarded first.

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.

Relationship disclosure: Maulee Foundation is supported by Baseel Partners LLP, which covers the Foundation's operational and logistical expenses.

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