Maulee
Uniting Hearts, Transforming Lives

MAULEE FOUNDATION

Strengthening cyber resilience for a mission-led grant-making organisation

Prepared for customer and stakeholder discussion | March 2026

SECTOR
Non-profit / grant-making foundation

LOCATION
London, United Kingdom

ORGANISATIONAL CONTACT
Mrinmayee Nistane, Chief Operating Officer

GENERAL CONTACT
insights@maulee.org

CASE STUDY PERSPECTIVE

This document maps Baseel Kestrel's SOC capabilities to the information-security and operational needs suggested by Maulee Foundation's published mission and governance model. Public sources reviewed do not establish a Kestrel deployment scope or measured security outcomes for Maulee; the solution narrative is therefore presented as a relevant capability alignment, not as a verified implementation claim.

01 EXECUTIVE OVERVIEW

Maulee Foundation is a non-profit organisation whose published mission is to connect donors and charities and maximise social impact. Its website describes grant-making to registered charities in England and Wales, with a focus on preventing or relieving poverty, supporting individuals in need and advancing education for disadvantaged people.

The Foundation's activities involve donors, grant applicants, charity partners, volunteers, trustees and programme stakeholders. Its public materials place emphasis on due diligence, safeguarding, governance, transparent financial practices and impact reporting. These responsibilities make the protection, availability and integrity of information important to the continuity of its charitable operations and the confidence of its stakeholders.

Baseel Kestrel's unified SOC model is relevant to this operating context because it is designed to consolidate security telemetry, identify suspicious behaviour, support structured investigations, coordinate response actions and provide operational reporting.

02 ORGANISATION PROFILE AND OPERATING CONTEXT

Maulee's public information describes a grant-making and charitable support model that includes assessing charitable purpose, evidence of need, public benefit, safeguarding and governance. Its published projects reference areas such as education, food security, vocational and digital skills, relief for people in need and support for disadvantaged communities.

These activities can involve sensitive personal information, supporting documents, financial and grant records, governance material and communications across multiple stakeholder groups. A proportionate security programme should therefore consider both technical threats and the operational controls needed to preserve confidentiality, maintain reliable records and respond appropriately to incidents.

03 SECURITY AND RESILIENCE PRIORITIES

1. **Stakeholder information protection:** safeguard donor, applicant, charity-partner, volunteer and beneficiary-related information held in approved systems.
2. **Identity and access oversight:** monitor authentication activity, privilege changes and access to sensitive records, with access limited to authorised roles.
3. **Digital service protection:** maintain visibility into public-facing websites, online forms, email and supporting infrastructure.
4. **Grant and due-diligence record integrity:** support the protection and traceability of application records, assessment evidence, decisions and outcome reports.
5. **Practical incident readiness:** establish clear alert triage, escalation, investigation and response workflows suited to the organisation's operating capacity.
6. **Governance and accountability:** retain incident records and produce concise reporting that can support management and trustee oversight.

04 KESTREL SOLUTION ALIGNMENT

Baseel Kestrel is designed to provide centralised security monitoring and response capabilities across supported endpoints, servers, networks, applications and cloud environments. Product materials describe event correlation, rule-, signature- and behaviour-based detection, UEBA, asset discovery, vulnerability management, case management, guided playbooks, SOAR, forensic investigation and reporting.

OPERATIONAL PRIORITY	KESTREL CAPABILITY ALIGNMENT	POTENTIAL OPERATIONAL CONTRIBUTION
Donor and grant information	Centralise relevant audit, identity, endpoint, application and database events from systems that store or process approved stakeholder and grant records.	Improve visibility into unusual access patterns and support investigation of potentially unauthorised activity.
Charity partner due diligence	Monitor access to partner records, governance documents and supporting evidence; retain relevant incident and case context.	Support traceability and a more consistent security view around information used in assessment and oversight workflows.
Staff, trustee and volunteer accounts	Apply identity and behavioural analytics to authentication events, privilege changes and anomalous access patterns.	Help identify unusual sign-ins, unexpected account activity and potential misuse of credentials.
Websites and online services	Monitor available web, server, network and endpoint telemetry associated with public-facing services.	Support earlier identification and investigation of suspicious activity affecting online engagement channels.
Malware and service disruption	Correlate endpoint, server and network events; use threat intelligence and forensic capabilities where integrated.	Provide investigation context for suspected malware, ransomware indicators or disruption affecting critical services.
Governance and reporting	Use case management, dashboards, audit-friendly records and compliance-oriented reporting.	Provide structured operational information that can complement existing governance and oversight processes.

05 ILLUSTRATIVE NON-PROFIT SECURITY SCENARIOS

A **Unusual access to grant records**

A user account accesses an unusually large number of grant files or accesses records outside its normal pattern. Identity and behavioural analytics can help surface the activity for review, while case management preserves the investigation trail.

B **Compromised mailbox or credential**

A suspicious sign-in or account change is detected in an integrated identity or email environment. Correlated events can help analysts assess whether other systems or records may be affected.

C **Threat against a public-facing service**

Unexpected web-server, endpoint or network activity is observed around a public website or online form. Centralised telemetry can support triage and coordination with the responsible technical owner.

D **Potential malware or ransomware activity**

Endpoint and server events indicate suspicious execution or lateral movement. Investigation and approved response playbooks can help organise containment and recovery actions.

E **Vulnerability affecting a key system**

An asset or vulnerability finding indicates exposure in a system supporting grant administration or stakeholder engagement. Asset context can help prioritise remediation according to criticality.

06 EXPECTED OPERATIONAL VALUE

Subject to implementation, integration and appropriate operating procedures, Kestrel's documented capabilities can support the following value areas:

- Improved visibility into security activity affecting systems that support donor, charity-partner and grant-related workflows.
- Better context for reviewing unusual account behaviour and access to sensitive information.
- More structured incident handling through case records, ownership, investigation history and approved response playbooks.
- A clearer basis for prioritising technical remediation through asset and vulnerability information.
- More consistent security reporting to inform management oversight and operational risk discussions.

OUTCOME MEASUREMENT

Any statement of realised benefit should be supported by agreed evidence.

Relevant measures may include coverage of critical systems, number and quality of actionable alerts, time to acknowledge and contain incidents, vulnerability remediation timelines, incident closure completeness and completion of periodic access reviews.

07 IMPLEMENTATION AND GOVERNANCE CONSIDERATIONS

01	Identify systems that process donor, grant, partner, staff and beneficiary-related information, and classify them according to sensitivity and business importance.
02	Confirm data ownership, authorised access, logging availability, retention periods and any applicable privacy or safeguarding requirements.
03	Prioritise integrations for identity services, email, public-facing web infrastructure, endpoints, servers, cloud services and network security controls.
04	Define incident severity, escalation contacts, decision rights and approval requirements for containment or account actions.
05	Ensure reporting is proportionate and useful to management and trustee oversight, without exposing unnecessary personal or confidential information.

08 ABOUT BASEEL AND KESTREL

Baseel Partners describes itself as 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 800+ clients and 2,000+ projects; these are company-published corporate profile figures and should not be read as Kestrel-specific outcomes.

Maulee's website separately states that Baseel Partners LLP covers the Foundation's operational and logistical expenses. This is an organisational support arrangement disclosed by Maulee and is not, by itself, evidence of a Kestrel deployment.

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

100+
countries served

800+
clients

2,000+
projects