NETHOPE CONNECTED

NET HOPE CONNECTED

Digital protection and cyber resilience

NOVEMBER 2026

CUSTOMER CASE STUDY | THREAT INTELLIGENCE

An intelligence-led approach to external cyber threats across the humanitarian ecosystem shifts cybersecurity from a generic, reactive chore into a targeted, mission-critical defence strategy.

Prepared for customer and stakeholder discussion | November 2026

SECTOR	ORGANISATION	PROGRAMME CONTEXT	RELATIONSHIP
Humanitarian, development and nonprofit technology	NetHope / NetHope Connected	Digital protection, cyber resilience and threat information sharing	Prospective solution alignment; no deployment asserted

CASE STUDY PERSPECTIVE

This case study describes how Baseel Owl's threat intelligence capabilities can align with NetHope Connected's published digital protection and non-profit cyber resilience frameworks. Because publicly available sources do not disclose a specific partnership, deployment, or independently verified security performance results between NetHope and Baseel Owl, these use cases are presented as a solution-alignment narrative rather than quantified implementation claims.

01 EXECUTIVE OVERVIEW

NetHope is a global consortium connecting humanitarian, development and conservation organisations with technology and funding partners. Through NetHope Connected and its digital protection work, it supports nonprofits in strengthening digital capacity, cyber resilience and responsible technology use.

For organisations working in humanitarian contexts, cyber incidents can disrupt services, expose sensitive information and undermine trust. Threats may include phishing infrastructure, compromised accounts, malicious indicators, exposed internet-facing assets and impersonation of trusted organisations or programmes.

Baseel Owl is designed to provide an outside-in intelligence view through indicator enrichment, external attack surface discovery, brand protection, breach intelligence, watchlists and curated threat information. When integrated with Baseel Kestrel, relevant findings can be routed into SOC investigation and response workflows.

02 ORGANISATION PROFILE

NetHope Connected describes itself as a global community and digital programme designed by, for and with nonprofits. Its model combines learning resources, peer connection and practical guidance to help small and mid-sized organisations strengthen digital capacity at their own pace.

NetHope's published Global Humanitarian ISAC and Digital Protection programme focus on helping humanitarian organisations understand context-specific threats, share relevant information and strengthen their ability to respond. A complementary intelligence platform would need to fit existing member-led sharing and coordination practices rather than replace them.

The core opportunity for Baseel Owl is to empower authorised teams to investigate external indicators, monitor approved organisational assets and brands, and establish structured hand-offs to the appropriate security owners.

03 THREAT INTELLIGENCE PRIORITIES

01
Shared threat visibility

Bring relevant external indicators, campaigns and threat context into a consistent view for authorised analysts and participating organisations.

02
Faster indicator verdicts

Check suspicious URLs, IP addresses, file hashes and domains against configured intelligence sources rather than relying on disconnected manual lookups.

03
External attack surface awareness

Discover and track approved internet-facing domains, subdomains and services to understand what an external attacker may see.

04
Brand and phishing protection

Identify lookalike domains, fake websites and suspicious online activity that may impersonate an organisation or programme.

05
Credential exposure awareness

Identify when organisational email addresses or domains appear in known breach data and support appropriate owner follow-up.

06
Governed collaboration

Separate organisations and teams, control access, preserve audit records and route findings to accountable owners.

04 OWL SOLUTION ALIGNMENT

Baseel Owl's supplied product materials describe IOC intelligence, malicious indicator databases, external attack surface management, domain and OSINT reconnaissance, brand protection, social media monitoring, breach intelligence, AI-summarised threat news, watchlists, notifications, and integration with Baseel Kestrel. The mapping below represents a potential fit for NetHope's published context; it is not a claim of an existing implementation.

SERVICE AREA	OWL CAPABILITY ALIGNMENT	POTENTIAL OPERATIONAL CONTRIBUTION
Threat intelligence and sharing	IOC intelligence, malicious indicator databases, watchlists and threat context.	Support consistent indicator triage and provide contextual findings for sharing through agreed NetHope/member channels.
Digital protection	Attack surface discovery, domain scanning, Web Recon and subdomain discovery.	Improve visibility of authorised internet-facing assets and help teams prioritise exposed services for review.
Brand and phishing protection	Lookalike domain detection, fake website identification and social mention monitoring.	Provide earlier warning of possible impersonation affecting participating organisations or programmes.
Identity and data exposure	Breach Intelligence and Breach Lookup for organisational emails and domains.	Help teams assess potential credential exposure and coordinate account-owner follow-up.
SOC integration	Kestrel integration, Slack/email notifications and structured findings.	Create a path from intelligence discovery to SOC triage, assignment, escalation and response tracking.
Governance	Multi-tenant access controls, roles and audit logging.	Support separation of participating organisations and traceability, subject to agreed data-sharing rules.

POSITIONING NOTE Owl should complement—not replace—NetHope's Global Humanitarian ISAC, member-led information-sharing arrangements, incident coordination, capacity-building programmes or existing security controls.

05 ILLUSTRATIVE THREAT INTELLIGENCE LIFECYCLE

1 **COLLECT**

Aggregate intelligence from approved external sources and threat feeds, alongside domains, brands, assets and indicators that each participating organisation has authorised for monitoring.

2 **ENRICH**

Check URLs, IP addresses, file hashes and domains against configured intelligence sources to return reputation, detection context and supporting details.

3 **MONITOR**

Track approved watchlists, possible lookalike domains, attack-surface changes, social mentions and breach intelligence for findings requiring review.

4 **PRIORITISE**

Assess findings by severity, confidence, asset importance and likely impact so analysts focus on the most relevant exposures first.

5 **ACT**

Share relevant findings through approved channels and, where configured, route cases into Kestrel for investigation, assignment and response tracking.

6 **REPORT**

Provide dashboards and summaries of indicators investigated, exposures found, actions taken, accountable owners and open risks.

06 EXPECTED OPERATIONAL VALUE

When the relevant monitoring scope, integrations, data-sharing permissions and operating procedures are in place, Owl could support the following outcomes:

- ✓ A more consistent intelligence review process for authorised analysts.
- ✓ Earlier awareness of malicious infrastructure, phishing domains and possible brand impersonation.
- ✓ Better visibility of internet-facing assets and changes that may warrant remediation.
- ✓ More structured assessment and follow-up of potential credential exposure.
- ✓ Clearer hand-off from intelligence discovery to incident triage and accountable action.
- ✓ Better evidence for programme reviews, governance discussions and member-facing reporting.

07 OUTCOME MEASUREMENT

To convert expected value into verified results, agree a baseline and reporting period for measures such as:

Time to indicator verdict	Authorised domains and assets monitored
Lookalike-domain detection-to-action time	Credential exposure response time
Watchlist match volume	% of findings assigned to an owner
% closed with a recorded outcome	Report only where the underlying data is available and collection is approved.

08 RECOMMENDED IMPLEMENTATION AND GOVERNANCE

01

Confirm scope

Agree the participating organisations, brands, domains, assets, user groups and asset owners. Obtain explicit authorisation before monitoring.

02

Define sharing rules

Specify what intelligence may be shared, with whom, at what confidence level and under which confidentiality and handling markings.

03

Protect sensitive data

Set controls for personal data, breach intelligence, retention, access, cross-border processing and incident evidence.

04

Integrate with existing workflows

Map Owl findings to existing ISAC and member processes; avoid creating conflicting incident-coordination channels.

05

Pilot and measure

Begin with a limited, consented pilot. Validate alert quality, false-positive handling, operational workload and measurable outcomes before scaling.

09 ABOUT BASEEL AND OWL

Baseel Partners is a global IT and consulting group. Its threat intelligence platform, Baseel Owl, provides IOC enrichment, external attack surface management, domain and OSINT reconnaissance, brand protection, social media monitoring, breach intelligence, cybersecurity news, watchlists, notifications, multi-tenant access controls, and seamless integration with the Baseel Kestrel SOC.

CLIEN CONTACT
Nino Hares
Virtual Chief Information Security Officer
Nino.Hares@nethope.org

DOCUMENT STATUS

Prepared for discussion as a prospective solution-alignment case study. NetHope organisational context is based on the NetHope Connected case study supplied by the user and public programme descriptions. Owl capabilities are based on Baseel product materials. No NetHope deployment, partnership, endorsement or measured customer result is implied.

PUBLICATION REFERENCE

NetHope Connected, "AI Ethics and Readiness Lab for Egyptian NGOs — Educuality, Egypt," October 2026. The supplied publication is used as the source for NetHope Connected visual identity and organisational framing.