

CyberSuite Hackathon Challenges Template

Challenge Title:

Comprehensive Evaluation of Kartos: Automated Digital Risk Protection and Threat Intelligence Platform

Challenge Context and Purpose:

This challenge focuses on evaluating **Kartos**, an advanced **Digital Risk Protection (DRP)** and **Threat Intelligence** solution developed by **Enthec**. Kartos automatically and continuously monitors an organization's digital footprint to detect threats, vulnerabilities, and data exposures across the **surface web, deep web, dark web, and social networks**.

The purpose of this challenge is to assess how effectively Kartos identifies and classifies digital threats such as phishing campaigns, brand impersonation, credential leaks, and third-party risks. Participants will explore its capabilities in **External Attack Surface Management (EASM)**, **Third-Party Risk Assessment**, and **Cyber Threat Scoring**.

By conducting this evaluation, the goal is to validate Kartos' real-time intelligence accuracy, the elimination of false positives through AI-based contextual tagging, and the usability of its dashboards and reports. Insights gathered will support Enthec's continuous improvement process, enhancing the platform's analytical precision, automation, and user experience for cybersecurity professionals.

Goals of the Challenge:

- Assess the **accuracy and efficiency** of Kartos' automated threat detection system.
- Evaluate the **usability and clarity** of its dashboards and reports for cybersecurity analysts.
- Verify the platform's **ability to minimize false positives** using AI contextual tagging.
- Measure the **effectiveness of Kartos' scoring and prioritization of risks**.
- Gather expert **feedback and improvement recommendations** to enhance performance and usability.

Key Tasks for Participants: *List the main tasks participants will perform to test and evaluate the solution.*

Examples:

- Access the Kartos environment and review its main features.
- Configure digital risk monitoring using the provided simulated domains and assets.
- Analyze detected threats, exposed data, or suspicious activities reported by Kartos.
- Evaluate results related to **phishing detection, credential leaks, brand impersonation, and third-party risk**.
- Assess the clarity and precision of the generated alerts and reports.

CyberSuite Hackathon Challenges Template

- Complete the feedback form summarizing observations and recommendations.

Feedback and Evaluation Requirements: *Describe the feedback participants are expected to provide.*

Participants are expected to provide:

- A detailed evaluation form highlighting **strengths, weaknesses, and improvement opportunities**.
- Qualitative feedback on **usability, interface design, and alert prioritization**.
- Insights into **false positive reduction, threat relevance, and response accuracy**.
- Comments on how Kartos could better support analysts in real-world cybersecurity monitoring.

Deliverables: *Clearly state what participants are expected to submit.*

- A **summary document** outlining key findings and suggested improvements.
- Supporting evidence such as **screenshots or notes** from testing sessions.

Resources and Tools Provided: *List any tools, documentation, datasets, or other resources participants will need to effectively test and evaluate the solution.*

- Access credentials to Kartos' instance.
- A user guide and quick-start manual describing main features and workflows.
- A dataset of simulated digital assets (domains, brands, credentials) to monitor.
- A feedback and evaluation form template.

Estimated Time Requirement: *Provide an estimated amount of time participants will need to complete the challenge (e.g., hours, days).*

Approximately **4–5 hours** to complete all assigned tasks and prepare the final feedback report.

Contact Point (Optional): *Provide a point of contact for any questions related to this challenge (name, email, etc.).*

Email: support@enthec.com

Organization: Enthec Solutions