

Evaluation of Kartos

CyberSuite Hackathon Challenge
Presentation

kartos®

Incident Response

Continuous Threat Exposure
Management



Co-funded by
the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.



01

Introduction to Enthec and Kartos

05

Hackathon Evaluation Process

02

Purpose of the Challenge

06

Expected Outcomes

03

Key Functionalities of Kartos

04

Target Users and Use Cases



About Kartos

- Developed by **Enthec**, Kartos is an **automated and continuous threat exposure management platform**.
- Monitors an organization's **digital footprint** across the **Surface Web, Deep Web, Dark Web, and social media**.
- Provides real-time alerts about threats such as **phishing, credential leaks, brand impersonation, and third-party risk**.
- 100% **non-intrusive** and **AI-driven**, minimizing false positives and delivering actionable insights.



Objective:

To assess and validate Kartos' capabilities during the CyberSuite Hackathon through hands-on testing.

Specific Goals:

- Evaluate the **accuracy of threat detection** and **false positive management**.
- Assess the **usability and clarity** of dashboards and reports.
- Collect participant feedback to guide **future product improvements**.
- Measure **overall user satisfaction** and readiness for broader deployment.



- **Threat Intelligence:** Detection of phishing, data leaks, and impersonation campaigns.
- **External Attack Surface Management (EASM):** Identification of exposed assets and vulnerabilities.
- **Third-Party Risk Monitoring:** Continuous evaluation of suppliers and partners.
- **Cyber Risk Scoring:** Real-time scoring based on exposure and risk levels.
- **AI Contextual Tagging:** Reduces false positives, improving precision of results.



Cybersecurity Analysts – Threat monitoring and incident validation.

CISOs / Security Managers – Strategic visibility and reporting.

SOC Teams – Continuous external monitoring.

Risk & Compliance Officers – Third-party and regulatory risk management.

Government and Critical Infrastructure – Proactive cyber threat intelligence.



Testing Activities:

- Participants will access **Kartos**.
- Perform **digital risk and threat exposure monitoring** using test domains and assets.
- Analyze and classify detected threats and reports.
- Submit structured feedback on usability, accuracy, and performance.

Expected Outputs:

- Completed **evaluation forms** and **feedback reports**.
- Recommendations for improving detection accuracy, dashboard usability, and alert prioritization.



Objective:

Demonstrate Kartos' reporting and analysis capabilities through a predefined user session, focusing on the visualization of outcomes rather than setup or configuration.

Structure:

1. Login with predefined demo account
2. Explore dashboard overview
3. Explore risk scoring and vulnerabilities
4. Review exportable report



Hackathon Flow - Step 1: Login

Action:

1. Access Kartos using the demo account. Use your preconfigured product. Click on **1** **“Go to Kartos using this profile >”**

URL: login.enthec.com User: hackathon@cybersuiteproject.eu

The image shows two side-by-side screenshots from the ENTHEC platform. The left screenshot is the login page, featuring a circular profile picture of a person in a helmet, the text 'LOG IN TO ENTHEC', and input fields for 'Email' (containing 'hackathon@cybersuiteproject.eu') and 'Password' (masked with dots). A red 'Login' button is at the bottom, along with the 'ENTHEC' logo. The right screenshot is the 'Dashboard' page. It has a sidebar with 'Dashboard', 'Settings', and 'Logout' options. The main content area shows a 'Choose a product' section with a dropdown menu displaying 'HACKATHON'. Below this is a summary card for the 'Hackathon Enterprise' product, showing '1 TOTAL PRODUCT DOMAINS', '0 UNIQUE DOMAINS TO ASSIGN', '0 NUMBER OF SWAPS', and '1 PROFILE'. A red circle with the number '1' highlights a 'Go to Kartos using this profile >' link. At the bottom, there is a 'FAVOURITE LIST NEW LIST (1 DOMAIN)' section showing 'kriper.org' with 'SEC 68' and 'REP 78' scores.

Hackathon Flow - Step 2: Explore Dashboard



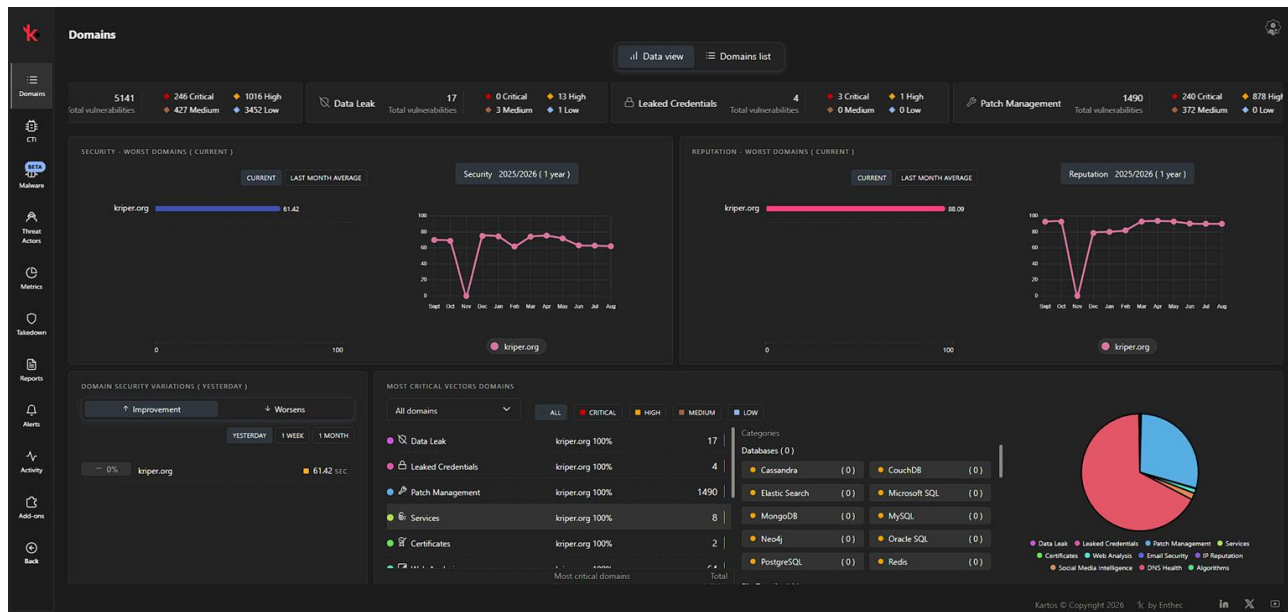
HACKATHON26

Action:

Navigate through the main dashboard to understand the organization's threat exposure.

Purpose:

Present Kartos' visual summary of risks, active alerts, and monitoring coverage.



Dashboard Overview Explanation

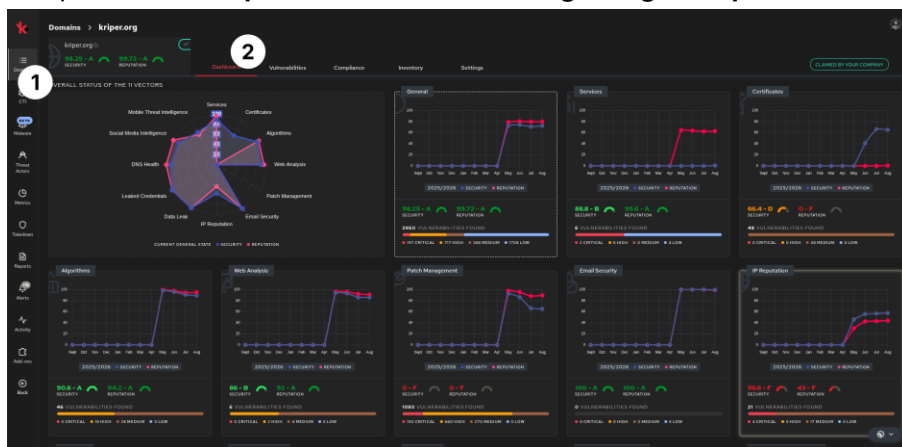
- The **first block** provides a **summary of all active vulnerabilities** detected across monitored domains.
In this case, as only one domain is being analyzed, it shows its vulnerabilities across different vectors.
- The following charts display the **Security Score** and **Reputation Score**, along with their **monthly evolution**, allowing users to track overall performance trends.
- Below, the dashboard highlights **domains that have improved or worsened** compared to previous checkpoints — yesterday, one week ago, and one month ago.
- The **Critical Vectors** section shows which vectors are most affected, including **count and severity filters** for deeper analysis.
- The **Domain Details** panel lists each domain's **number of IPs and subdomains**, including **hosting locations**.
- Finally, the **Alerts section** summarizes notifications triggered by configured monitoring rules.



Hackathon Flow - Step 3: Explore risk scoring and vulnerabilities

Domain Dashboard View

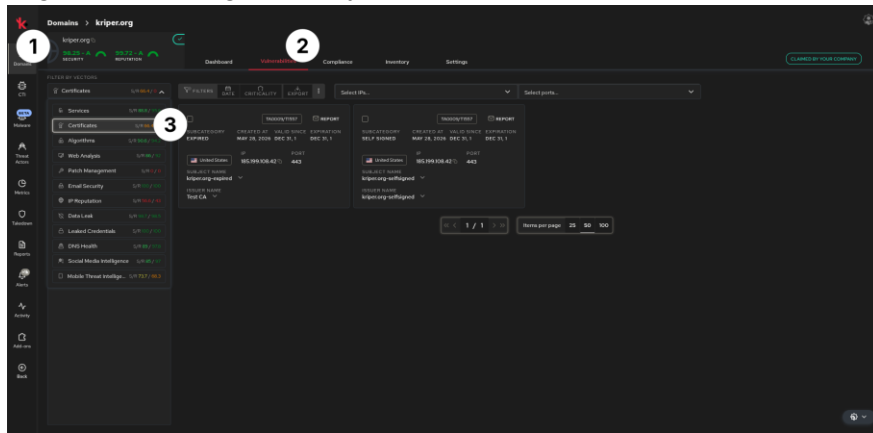
- Within a specific domain, users can access a **dedicated dashboard** showing detailed charts for both **Security** and **Reputation Scores** across **eleven vectors**, as well as the **overall score**.
- These visualizations display the **evolution of each score over time**, offering insight into how the domain's security posture changes.
- The dashboard also summarizes the **number and severity of vulnerabilities** detected within each vector, highlighting which areas are **most critical** and require immediate attention.
- This view provides a **comprehensive understanding of digital exposure** and supports prioritization of remediation efforts.



Hackathon Flow - Step 3: Explore risk scoring and vulnerabilities

Vector-Level Exploration

- Users can **navigate through individual vectors** (e.g., web, email, infrastructure, leaks, brand) to explore specific vulnerabilities in detail.
- Each vector includes **multiple filters** — by severity, type, source, or detection date — enabling precise and efficient analysis.
- Vulnerabilities are displayed as **interactive cards** containing key information such as description, impact, and related assets.
- This granular view helps analysts **drill down into the root cause** of each issue and understand its context within the organization's digital ecosystem.



Hackathon Flow - Step 4: Review Exportable Report

- **Action:**
Open or download a **final PDF or visual report** generated by Kartos.
- **Purpose:**
Demonstrate how Kartos delivers actionable intelligence for CISOs and analysts.

The screenshot displays the 'Reports' section of the Kartos interface. On the left is a dark sidebar with navigation icons and labels: Reports (1), Alerts, Activity, Add-ons, and Back. The main content area has a top navigation bar with four numbered callouts: 1 points to the 'Reports' label in the sidebar; 2 points to the 'Select the report type' dropdown menu (currently set to 'Executive report'); 3 points to the 'Select a domain' dropdown menu (currently set to 'kripier.org'); and 4 points to the 'Download PDF' button. The report content for 'kripier.org' (EMISSION DATE: SEP 23, 2024) includes a title 'Real-time monitoring of threat exposure', a paragraph about the report's scope, another paragraph about threat exposure analysis, and a 'Kartos Scores' section with a color-coded bar chart. At the bottom, a 'General data' section shows '98.25 - A SECURITY' and '99.72 - A REPUTATION' with corresponding green progress indicators and a line graph.

kartos®

Thank you for your attention!



Enthec Solutions



Miguel Selma



mselma@enthec.com



enthec.com



Co-funded by
the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.