Solution Overview

HELIOS

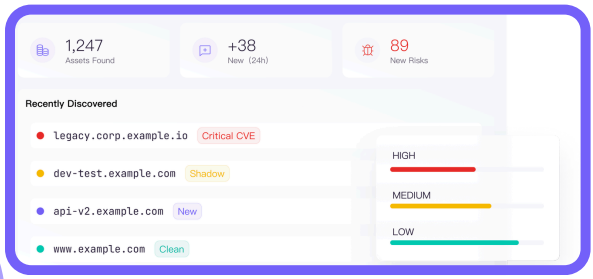
AI-Powered External Attack Surface Management Platform

No Blind Spots. No Surprises.

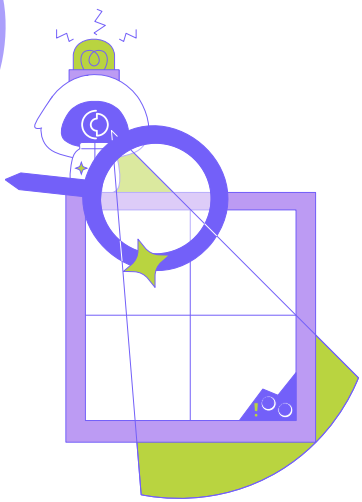
Adversaries continuously map your external attack surface. HELIOS ensures you know your internet-facing assets, exposures, and risks before they become entry points.

Today, an organization's digital footprint extends far beyond its traditional perimeter. Security teams often lack visibility into unknown or unmanaged assets across cloud, SaaS, and internet-facing environments, creating blind spots that significantly increase the risk of compromise.

HELIOS continuously discovers internet-facing assets, identifies exploitable exposures, and monitors for external compromise across open sources and the dark web, giving organizations the same view of their attack surface as adversaries. AI gives these capabilities a depth that traditional discovery tools cannot match.



Asset attribution identifies assets organizations did not know existed, even when ownership is not immediately obvious. Breach content analysis determines whether leaked data found on the dark web is organizationally relevant and how critical the exposure is, a judgment only AI can make at scale. Together, they elevate HELIOS from a discovery tool to an intelligence platform.



AI CAPABILITIES IN HELIOS

Internet Asset Attribution:

Analyzes website content, digital certificates, favicon hashes, and metadata to determine whether internet-facing assets belong to the target organization, surfacing unknown assets that traditional discovery methods miss.

Breach Content Analysis:

Analyzes leaked credentials, documents, and other exposed data from open sources and dark web repositories to determine organizational relevance and assess the significance of the exposure.

TARA AI:

The Autonomous CTEM Agent behind HELIOS. Use natural language to investigate assets and exposures while TARA AI continuously prioritizes risks and recommends follow-on actions.

WHAT IS EASM ?

External Attack Surface Management (EASM) helps organizations understand exactly what adversaries can see, reach, and potentially exploit across their internet-facing environment. Using an outside-in approach, EASM continuously discovers, inventories, and monitors external assets to identify unknown assets and exploitable exposures before they become entry points for attack.

Product Highlights

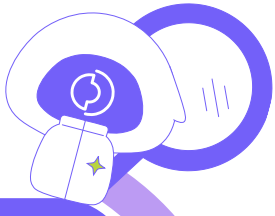
Asset Discovery
Continuously discover internet-facing domains, subdomains, IPs, and services, with full visibility into asset relationships and how your external attack surface evolves over time.

Data Breach Discovery
Continuously monitor open sources and the dark web for leaked credentials, emails, and sensitive documents, delivering early warning before adversaries can exploit them.

Risk Assessment
Identify exploitable exposures, vulnerabilities, and shadow IT with AI-powered prioritization that surfaces the risks most likely to be exploited by adversaries.

Reporting and Insights
Track changes across your external attack surface with evidence-based reporting that helps security teams and leadership understand external risk and prioritize remediation over time.

Platform Advantages



Flexible Delivery
Choose between periodic assessment reports or full platform access, allowing organizations to consume external attack surface intelligence in the way that best supports their security operations.

Accuracy at Scale
Internet Asset Attribution and Breach Content Analysis reduce false positives by confirming asset ownership and exposure relevance, enabling teams to focus on genuinely critical risks.

Rapid Time to Value
HELIOS delivers actionable results within 24 hours of onboarding, providing immediate visibility into the external attack surface without lengthy deployment or integration.

Continuous Risk Management
HELIOS continuously monitors for new assets, open ports, misconfigurations, and emerging exposures, ensuring risks are identified before adversaries can act on them.

> **HELIOS** *has given us the adversary's perspective, uncovering risks we didn't know were exposed and clear guidance to reduce them before they could be exploited.*
>
> —— **Head of Information Security, Leading Asian Aerospace Group**

www.digidations.com
info@digidations.com

digiDations is an AI Native cybersecurity company helping organizations move from hoping their defenses will hold to knowing they will through Autonomous Cyber Defense.