ORYXLABS

DATARIG360

FUELING SECURITY INSIGHTS

PRODUCT BROCHURE

INTRODUCTION

Global cybercrime costs are projected to reach $10.5 trillion annually by 2025[1], while 93% of business leaders expect daily AI-based cyberattacks in 2025[2]. Organizations face unprecedented threats targeting their domain and certificate infrastructure.

$10.5
TRILLION
ANNUAL CYBERCRIME COST

93%
DAILY AI ATTACKS

204
DAYS
AVERAGE BREACH DETECTION TIME

$4.88
MILLION
AVERAGE BREACH COST

1,298
AVERAGE WEEKLY CYBERATTACKS

- **Proactive Threat Detection**
  Traditional reactive security fails against sophisticated adversaries who conduct extensive reconnaissance using automated tools, with one in four attacks exploiting vulnerabilities in public-facing applications[3]
- **Certificate Security Gaps**
  SSL certificate-related security issues expose websites to data interception and man-in-the-middle attacks[4], while unauthorized certificate issuance through Certificate Transparency logs enables convincing phishing campaigns

KEY TRENDS DRIVING THIS MARKET

- **AI Integration Acceleration**
  76-89% of organizations have integrated AI into their cyber defense mechanisms[2], with AI-based security systems blocking 95% of phishing attacks[2] and reducing response time by 35-60%.
- **Automated Intelligence Focus**
  Organizations recognize that 400 million terabytes of data are generated daily[5], driving demand for automated solutions that can process vast intelligence datasets in real-time.
- **Proactive Defense Evolution**
  With North American organizations facing 1,298 cyberattacks per week[6] and 25% of attacks targeting public-facing applications[3], the shift from reactive to predictive defense strategies has become critical for organizational survival.

[1] Cybersecurity Statistics in 2025 - https://www.micromindercs.com/news-announcement/cybersecurity-statistics
[2] 100+ Cybersecurity Statistics and Facts for 2025 - https://zerothreat.ai/blog/cybersecurity-statistics-and-facts
[3] IBM X-Force 2025 Threat Intelligence Index - https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
[4] The Crucial Role of SSL Certificate Monitoring in Ensuring Cybersecurity - https://www.cloudns.net/blog/the-crucial-role-of-ssl-certificate-monitoring-in-ensuring-cybersecurity/
[5] Threat Intelligence Market Size, Size, Growth & Latest Trends - https://www.marketsandmarkets.com/Market-Reports/threat-intelligence-security-market-150715995.html
[6] Threat Intelligence Market Size, Share & Growth Report 2030 - https://www.grandviewresearch.com/industry-analysis/threat-intelligence-market

OUR SOLUTION

Our DATARIG360 platform provides threat-intel data at scale in a Data-as-a-Service (DaaS) model, enabling organizations to make data-driven decisions and fostering innovation for data-driven applications and services related to cyber security.

DOMAIN INTELLIGENCE DATA

Our domain intelligence capability provides comprehensive visibility into the global domain ecosystem through continuous collection and analysis of registration data, DNS records, WHOIS information, and historical changes.

The platform monitors domain ownership details including registrant information, contact data, and organizational affiliations while tracking registration and expiration dates to identify potential risks. Advanced DNS analysis reveals complete subdomain structures, mail server configurations, and IP address relationships that expose hidden infrastructure connections.

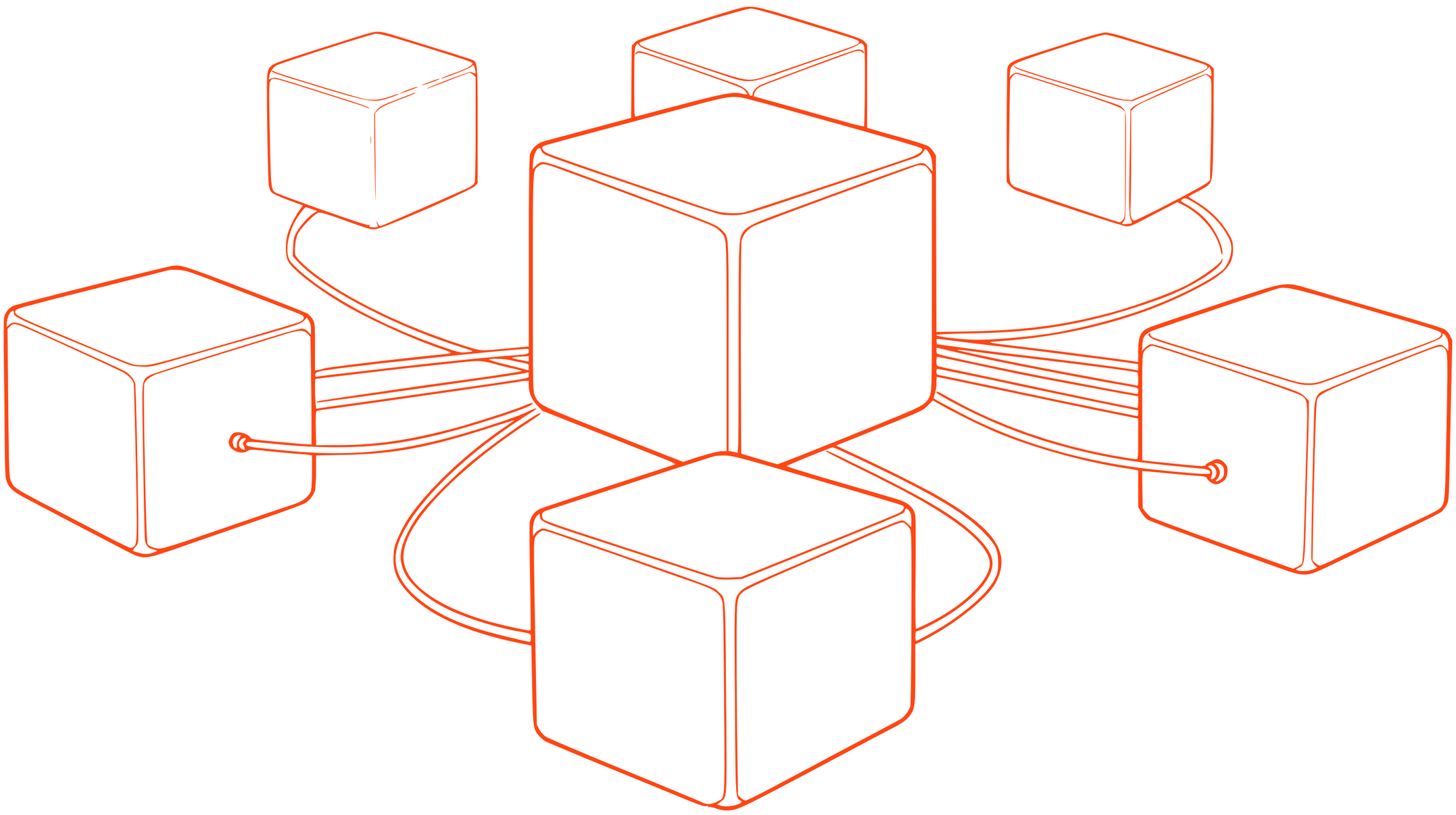
The system automatically correlates domain data with threat intelligence feeds to detect typosquatting, trademark abuse, and phishing infrastructure while providing risk assessments based on domain age, reputation, and associated IP addresses.

CERTIFICATE INTELLIGENCE DATA

Our certificate intelligence monitoring delivers real-time visibility into SSL/TLS certificate issuance and management across the internet through comprehensive Certificate Transparency log analysis.

The platform continuously monitors all public Certificate Transparency logs to detect unauthorized certificate issuance for monitored domains, providing immediate alerts when certificates are issued without proper authorization. Advanced certificate analysis examines issuer information, validity periods, cryptographic algorithms, and subject alternative names to identify potential security weaknesses or fraudulent certificates.

The system tracks certificate lifecycles including issuance, renewal, and expiration dates while maintaining detailed records of certificate chains and trust relationships.



FEATURES

DATARIG360 delivers two core capabilities designed to streamline intelligence operations and enhance security team efficiency through automated data management, distribution and intuitive visualization.

» **Comprehensive Intelligence Dashboard**

Our platform delivers a unified, interactive dashboard that consolidates domain and certificate intelligence into actionable insights. The dashboard provides real-time visibility into domain and certificates security trends through customizable visualizations and filtering capabilities. Users can monitor domain registration patterns, certificate issuance anomalies, and threat actor infrastructure through intuitive charts and tables that support drill-down investigations.

Advanced analytics panels display key performance indicators including newly registered domains, and certificate transparency alerts. The interface enables security teams to quickly identify emerging threats through automated risk scoring and contextual threat intelligence integration.

» **Automated Data Export Scheduling**

The platform features flexible and automated export scheduling that enables organizations to deliver and integrate intelligence data at regular intervals for seamless integration with existing security tools. Users can configure recurring exports on daily, weekly, or monthly schedules to ensure continuous data flow to SIEM platforms, threat intelligence platforms, and analysis tools. Most commonly used format is CSV which allows ease of ingestion into myriad of downstream platforms.

Secure delivery options encompass SFTP, and API endpoints with encryption capabilities to protect sensitive intelligence data during transit. The system provides export configuration management for organizing predefined settings tailored to specific organizational use cases.

BENEFITS

Our delivery intelligence platform provides measurable business value through four critical advantages that can be used to transform security operations and enhance organizational resilience leveraging data as a valuable asset.

» **Early Threat Detection and Prevention**

Identify malicious domains and unauthorized certificates before they impact operations, enabling proactive defense and reducing incident response time.

» **Enhanced Security Posture and Compliance**

Maintain continuous visibility and comprehensive audit trails to support regulatory requirements and strengthen overall risk management.

» **Operational Efficiency and Optimization**

Automate domain analysis and certificate monitoring tasks to free security teams for critical high-priority investigations and efficiently streamline daily workflows.

» **Strategic Business Impact**

Leverage actionable intelligence to inform executive decision-making, improve customer trust, and drive competitive differentiation.

ORYXLABS

WHO WE ARE

ORYXLABS was founded in Abu Dhabi in 2020 with a passion for cybersecurity-focused engineering.

A proudly diverse staff hailing from 22 different countries with backgrounds ranging from national defense to world-renowned top software engineering organizations joined together to develop best-in-class security solutions.

We leverage research and innovation to provide solutions in four key areas:

- Cyber Security Assessment
- Monitoring
- Prevention
- Improvement

When combined, ORYXLABS solutions provide a holistic approach to situational awareness and attack mitigation.

WEBSITE

Scan to view

VIDEO

Scan to view

OUR MISSION

Our mission is to equip cybersecurity teams with first-in-class intelligence and technical solutions that continuously assess, monitor, and improve environments to mitigate ongoing or future attacks.

WHY US

As an agile and innovative company focused on cybersecurity, we pride ourselves on crafting highly tailored solutions to meet our clients' exact needs, not "one size fits all" products like our competitors in the domain.

With our combined experience in deep learning, AI, vulnerability research and big data, and partnerships with world-renowned subject matter experts, you can rest assured our solutions are built and run on information that is timely and accurate.

COMPANY AWARDS

2025

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2024

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2023

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2022

Top CyberSecurity Solutions Provider Middle East

Enterprise Security

ORYXLABS

21st Floor, Aldar HQ
Al Raha Beach
P.O. Box: 33289
Abu Dhabi, UAE

oryxlabs.ae