
DuskRise
Cyber Act Forum
2024
Unleashing the power of threat intelligence
Stay one step ahead to protect your brand, customers and nation.
FORMBOOK
Qakbot
See all
Three months | Six months | Year
OTT
NOV
SET
AGO
LUG
GIU
MAG
APR
FEB
Dridex
LokiBot
4
5
3
6
7
8
9
10
EWR
Recent Sharp
TinyNuke Targeting
Kimsuky: Mar: Kimsuky AP
TrickBot Targeting Update Septe
TinyNuke Targeting Update Septembe
Kimsuky: Mar: Kimsuky APT Group targets the

Alicia Fawcett, Director of Cyber Threat Intelligence

Director of Threat Intelligence at DuskRise, leading the Cluster25 team focused on cybersecurity posture improvement and strategic initiatives for national security, defense, academia, and critical infrastructure. Expertise in geopolitics, disinformation, threat intelligence, security and cybersecurity policy. Former cybersecurity consultant at McKinsey & Co., specializing in threat intelligence, strategic compliance, data protection, and risk management. Work experience at the U.S. Department of State, U.S. Intelligence, Capitol Hill think tanks, Uber, and international media on open-source analysis. Esteemed professor at the University of Economics, Prague, training future leaders in cybersecurity, combining academic insight with real-world implementation.

Cyber Norms podcast, The Carnegie Council on Ethics in International Affairs

Academia, Alicia Fawcett

LinkedIn

Carnegie Council Podcast

Disinformation Fellow

Chinese Discourse Power, Atlantic Council

Alicia.Fawcett@duskrise.com

Cybersecurity is Political. Data is Power.

Knowledge is power, so harnessing the power of knowledge is intensively POLITICAL

National security, nationalism, political participation, political contentions, conflict, violence, and war.

Processing, manipulation, exploitation, augmentation of information

Interaction of people and information.

Characterized by decentralization interests.

Cyber Threat Intelligence supports the protection of values: nonmaleficence, privacy, and trust.

Why is data in Cyberspace so complex?

Capability-vulnerability paradox

Connective realities

High degree of anonymity

Closing the power gap between states and non-state actors.

“complexity is the enemy of security”- Bruce Schnieder

Finding the balance in Cyber Disorder

Actors, institutions and social arrangements.

Low barriers to entry

Absence of great power cooperation, emergence of malicious proxy actors

Power vacuum between cyber actors and private public institutions

Collaboration between technology companies, government agencies, and civil society is crucial to mitigating the impact of cyber threats in Italian Cyberspace.

Who are the actors?

Rogue nations

Terrorists

Non-state actors

Cyber mercenaries: attractive to nation-states as

Two important categories of non-state actors in cyberspace:

- non-state actors with highly structured networks
- Individuals with more lightly structured networks (no hierarchy)

Current and Emerging Threats

- Social Media Manipulation
- Phishing and Spoofing
- Deepfakes
- Hacking and Data Breaches
- Malware and Ransomware
- Influence Operations

Unparalleled Threat Visibility

Cluster25's team continuously scans the **Clear**, **Deep**, and **Dark Web** to capture **new indicators of compromise**, **emerging threats**, **relevant malicious actors**, **evolving tactics**, and **targeted campaigns**. The information gathered provides **real-time alerts**, **proactive responses**, and **customized reports** that help protect the infrastructure and resources of DuskRise's clients, from Intergovernmental Organizations to SMEs.

The C25 Platform

DuskRise's Cyber Threat Intelligence activities converge in the proprietary **C25** platform, analyzing a large amount of data from different channels: **OSINT** (Open Source Intelligence), **CLOSINT** (Restricted Access Sources and Clandestine Channels), and **HUMINT** (Intelligence obtained from data collected and provided by human sources and interpersonal contacts).

C25: Intelligence modules and services

A modular platform designed for complete, relevant and accessible coverage.

Global Threat Intelligence Module

A unique solution designed to protect organizations from security threats and vulnerabilities, featuring two main components: Intelligence and Feed. The Intelligence component offers insights into threats and vulnerabilities, while the Feed provides a real-time perspective on emerging threats, including an "Early Warning" service.

Hunting and Investigate Module

The Hunting and Investigate section of the Cluster25 Platform delivers a suite of investigation and analysis tools aimed at malware detection. This includes retro-hunting with YARA rules, automated behavioral analysis through sandboxing, gene analysis, and tailored analysis services for examining suspicious artifacts.

Exposure Intelligence Module

Cluster25's Exposure Intelligence offers a comprehensive monitoring solution for protecting one's assets from external threats.
Composed of four areas: Surface Intelligence, Risk/Identity Intelligence, Typosquatting, Domain Squatting, Takedown Service, and VIP Monitoring Service

Tailored Intelligence Services

DuskRise offers tailored services such as Platform on Premise and Cyber Surveillance. Platform on Premise provides dedicated infrastructure with three instances sized according to customer needs. Cyber Surveillance service monitors the digital perimeter, detecting botnet and high-level malware infections, leakage of sensitive information and external credentials with access to corporate resources.

Neglecting Compromised Data leads to distrust

If neglected, it could undermine citizen’s trust and confidence in the digital infrastructure, in policy makers and in state authorities.

Data flows are important to malicious actors can undermine cybersecurity- ie. Information operations (IO), propaganda (disinfo)

IP Netflow

IPv4 to IPv4 traffic monitoring focuses on observing and analyzing the metadata associated with network packets exchanged between two systems, rather than the actual content (payload) of the transmitted data. This approach is particularly useful for understanding the characteristics of network traffic without violating privacy or encountering legal issues related to accessing sensitive data.

The monitoring will check for any traffic directed to command and control centers, or exfiltration centers, crossing it with detectable network anomalies (traffic spikes), defining possible ongoing attack scenarios.

Only a few IPV4 addresses will be monitored at a time for a given period, and large amounts of data will not be stored.

Cross-referencing this information with the C25 platform's informational database will allow for the creation of detailed and reliable reports.

IP Netflow

Flow Data Collection and Data Analysis

Metadata Capture: Using proprietary tools, metadata on traffic flows are collected, including source and destination IP addresses, port numbers, protocols used, packet size and count, and so on.

IPv4 Address Filtering: During data collection, filters can be set to focus exclusively on data flows involving communications between specific IPv4 addresses. This allows for a focus on traffic relevant for analysis.

Traffic Volume: The volume of traffic between the monitored IPv4 addresses is analyzed, assessing the amount of data transmitted over a given period. This can help identify unusual traffic patterns or potential network congestions.

Connections and Sessions: The frequency and duration of connections between IPv4 addresses are examined, providing information on network relationships and service usage.

Protocol Types: By analyzing the protocols used (TCP, UDP, ICMP, etc.), the nature of the communications can be understood (for example, web traffic, file transfers, streaming).

IP Netflow

Monitoring, Reporting e Privacy

Data Visualization: The collected information is often displayed through interactive dashboards that allow for easy interpretation of data and rapid identification of anomalies or trends.

Alarms and Notifications: Alarms can be set up based on specific criteria (such as exceeding a certain traffic threshold) to be alerted in real time of potential problems or suspicious activities.

Periodic Reports: Generation of periodic reports that provide an overview of traffic trends, useful for network capacity planning and security strategies.

Privacy Respect: Since the analysis focuses on metadata and not content, the risk of privacy violations is reduced. In summary, this form of IPv4 traffic monitoring provides an in-depth view of network usage and performance, while maintaining a high level of respect for user privacy.

OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)

COVERT SHORES www.hisutton.com bellingcat

“Data loss” turns into “data leak” turns into loss of trust

Ways your data could be compromised:

Resource exhaustion

Resource segregation failure

Abuse of high privilege roles

Management interface compromise

Intercepting data in transit, data leakage

Insecure deletion of data

Distributed denial of service (DDoS)

Economic denial of service (EDoS)

Encryption and key management (Loss of encryption keys)

Undertaking malicious probes or scans

Compromise of the service engine

Cyber Surveillance

The Cyber Surveillance service, integrated into the Exposure Intelligence module of the C25 platform, will be a surveillance tool easily settable through a wizard (Simple data entry and configuration tool with easy access). By entering information such as domain, email, IP addresses and tags, a surveillance engine will be created for each of the connected assets, funneling the collected information into a monitoring dashboard that allows for perfect visibility.

Cyber Surveillance

Continuous surveillance service, 24/7, to monitor the digital perimeter, detecting botnet and high-level malware infections, vulnerabilities, and credential theft of external personnel with access to company resources and employees. It will **monitor** web forums (Dark Web and Deep Web) for information on potential data thefts and **identify** any improper use of client information (Domains, brands, etc.), reducing the risk of phishing email spam and data breaches through the Domain Squatting service. It will also be possible to receive preemptive information on potential planned DDoS attacks.

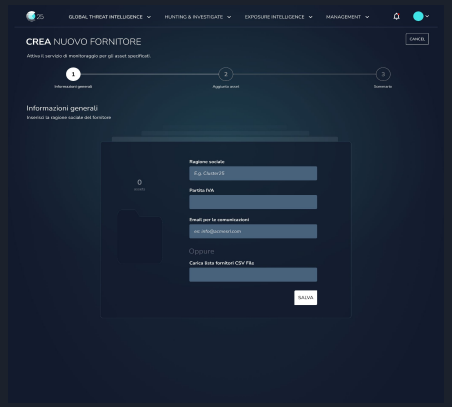
Quarterly reports will be provided to inform the client of the exposure level and email notifications in case a new exposure is discovered.

Access limits will be defined based on the number of employees of the client.

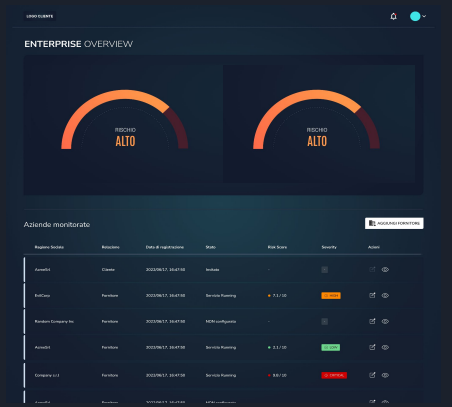
CTI – Supply Chain Security Monitoring

The Process

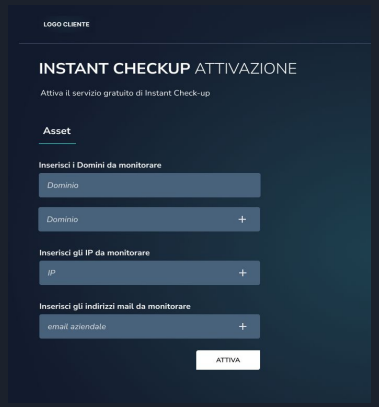
Data Input
Enterprise Customer



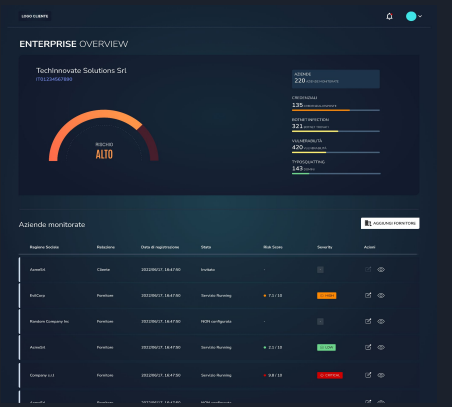
Monitoring&Analysis
Enterprise Customer



3rd Party Activation

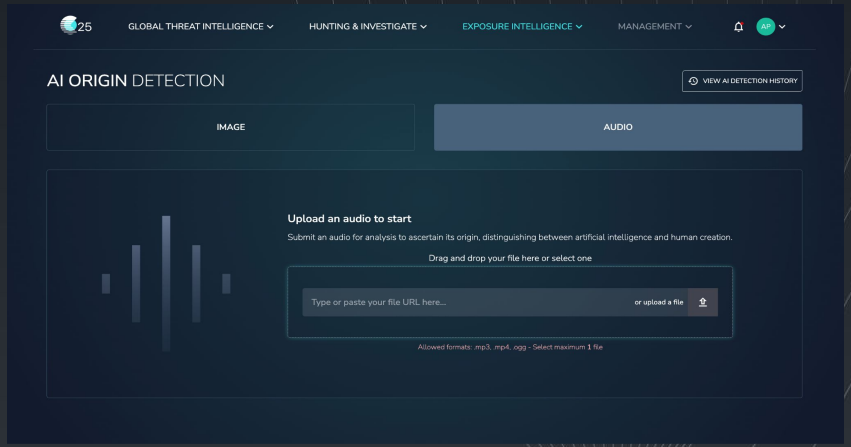


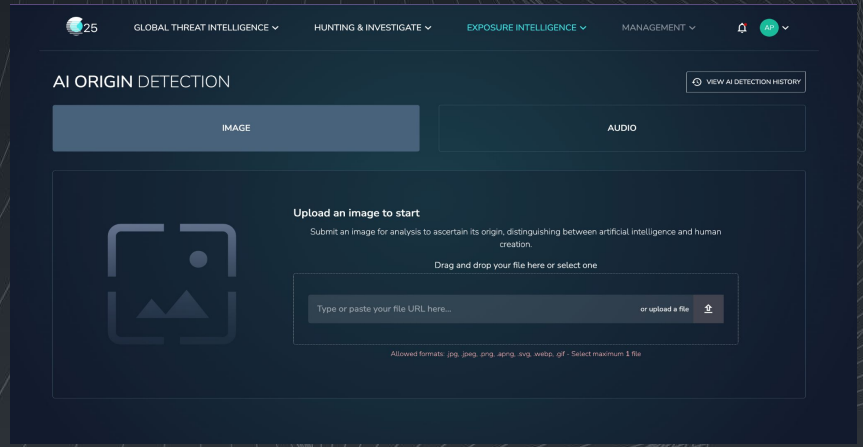
Instant Check-Up



AI Detection

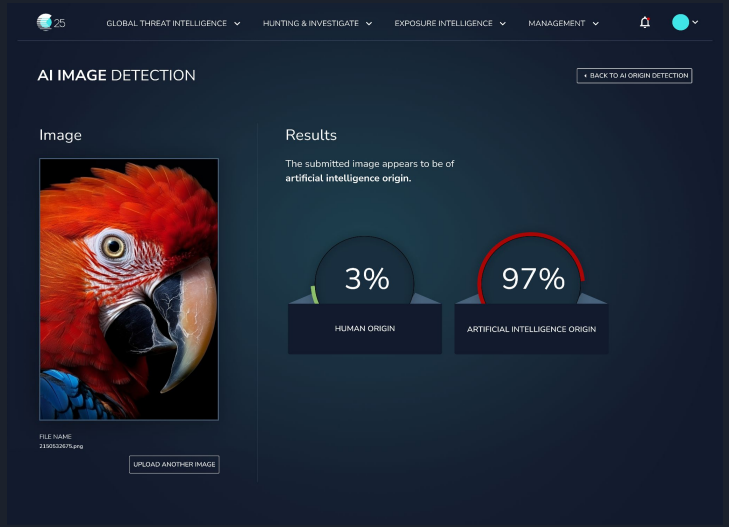
AI Detection is an advanced tool for detecting certain types of deep fakes, specifically images and audio generated by artificial intelligence. This tool is essential for navigating the information age, where distinguishing between real and artificial has never been so critical. Its deep analysis capabilities ensure that the truth is always within reach.

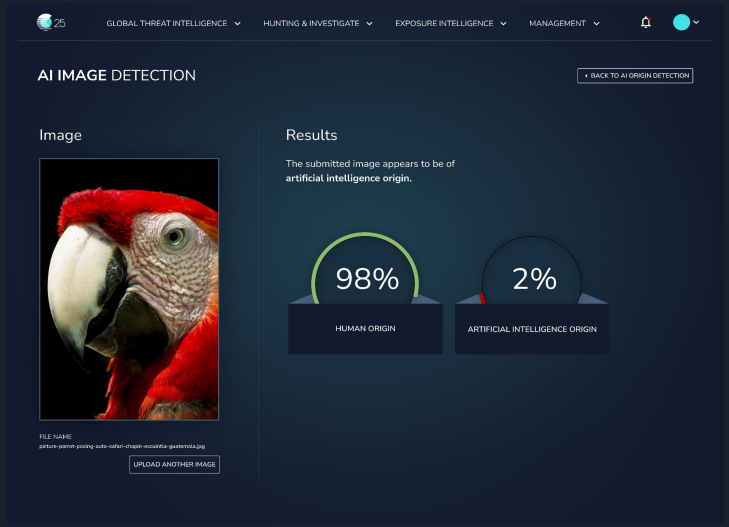




AI Detection

The tool displays the probability that the uploaded assets are real or not, using sophisticated algorithms to provide a quick and accurate analysis.
The process is simple: the user uploads their file and lets AI Detection do the rest.






Thank You
DuskRise
Cyber Act Forum
2024
Most Targeted Countries
Total Thr
Latest Threa
1
2
3
4
5
New Threat De
New Threat Detected
New Threat Detected Title 1N
New Threat Detected Title 1New Thre
New Threat Detected Title 1New Threat..