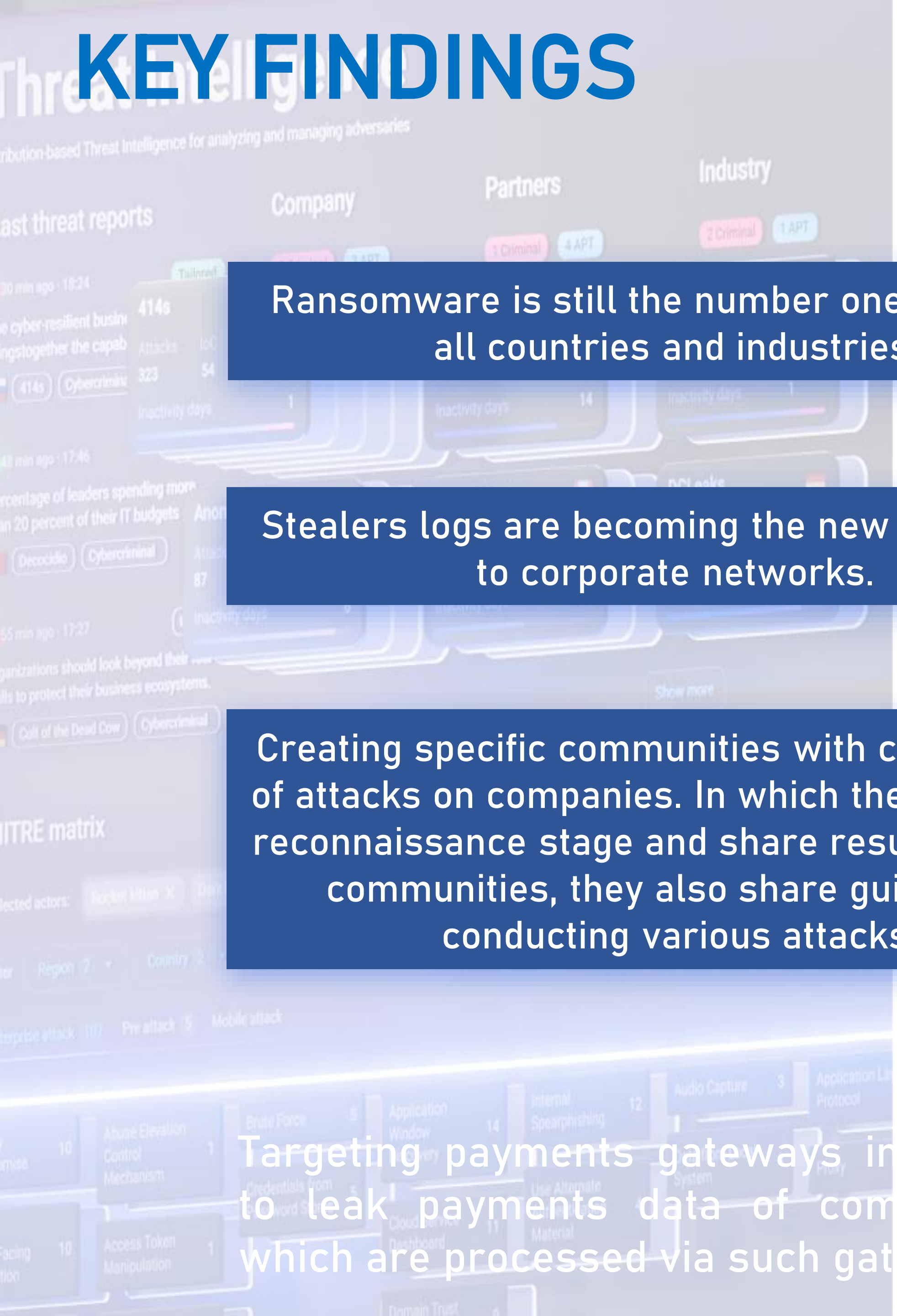
Cyber Threat Intelligence e Digital Risk Protection: il futuro è *hybrid*

DEEPCYBER
a Maggioli Group company

Advanced Intelligence, Protection, Antifraud.

KEY FINDINGS


Threat Intelligence
Attribution-based Threat Intelligence for analyzing and managing adversaries
Last threat reports
Company
Partners
Industry
MITRE matrix

Ransomware is still the number one threat for all countries and industries.

Stealers logs are becoming the new entry point to corporate networks.

Creating specific communities with coordination of attacks on companies. In which they are doing reconnaissance stage and share results. In such communities, they also share guides for conducting various attacks

Targeting payments gateways in to leak payments data of com which are processed via such gat

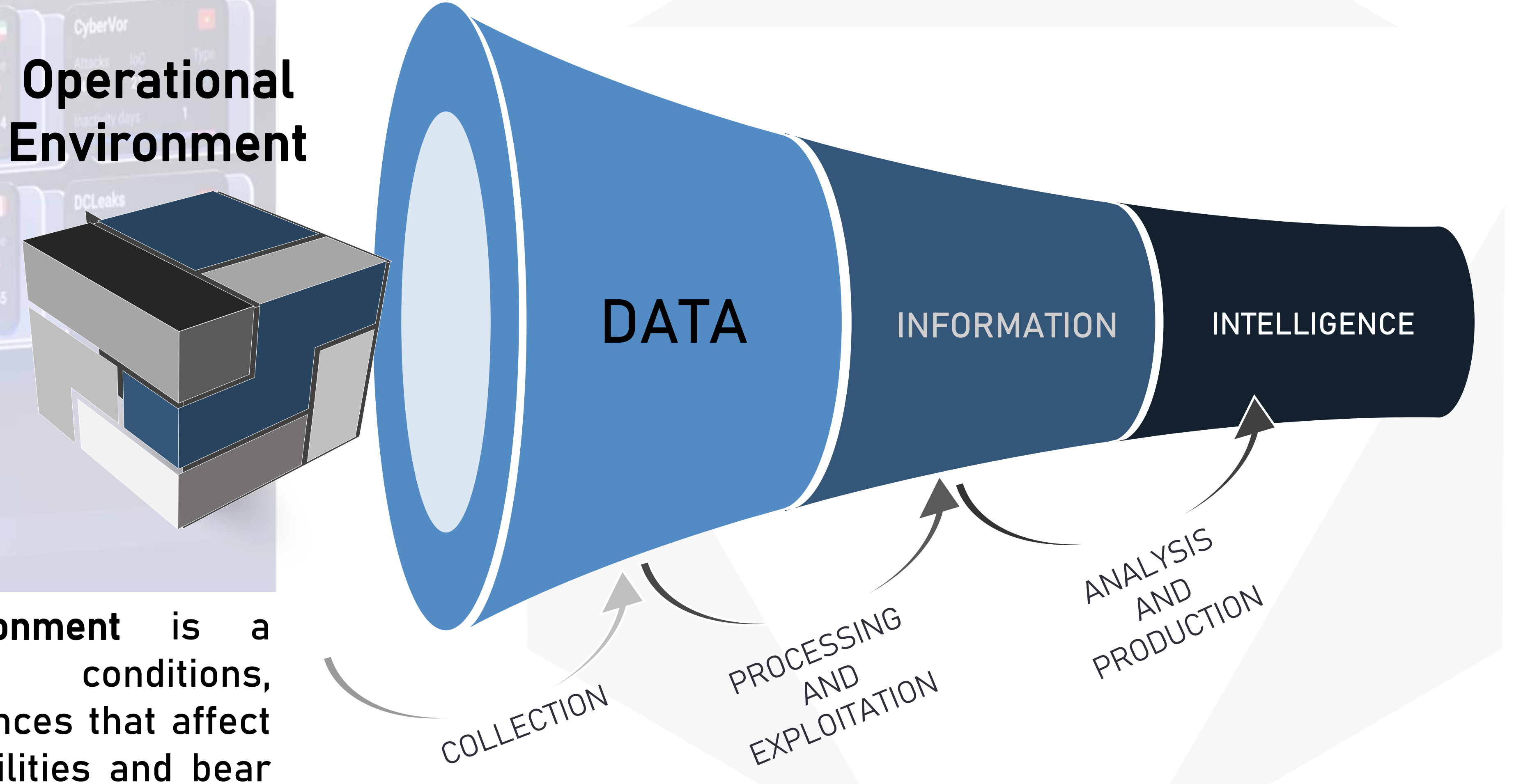
The number assesses sold to corporate network more than doubled.

The war has resulted in an increase in the activity of threat actor groups.

Using unprotected API for conducting DDoS attacks and collecting DBs

Increased activity of national-state actors which are targeted Industrial sector and Government sector. In most cases they use Phishing emails and RAT for espionage purposes. In cases of Industrial companies – they use wiper malware.

Back to Origin



The **Operational Environment** is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the ‘commander’

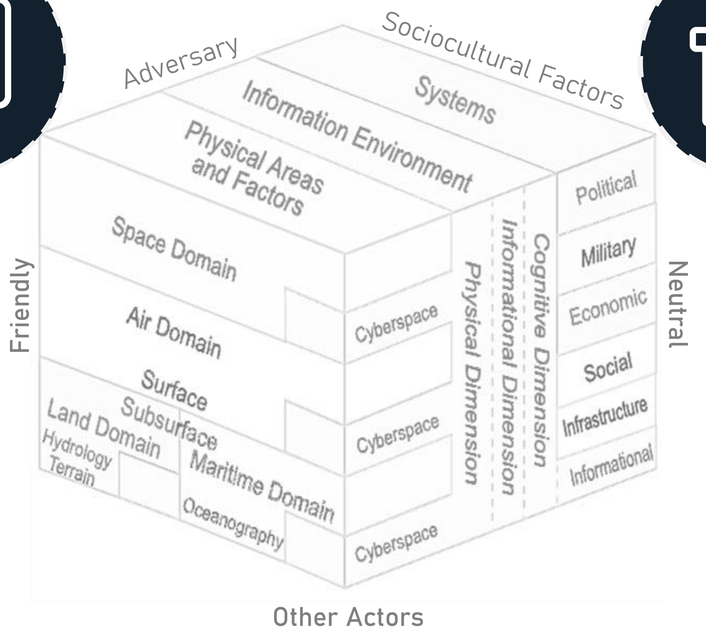
Relationship of Data, Information, and Intelligence (Joint Publication 2-0, 2013)

“Know yourself and know your enemy… “

TLP: CLEAR

4 Determine Adversary Courses of Action

- Analysis of Adversary Capabilities
- Adversary capabilities in relative probability of adoption l b. Vulnerabilities



Operational Environment (OE)

1 Define the OE

Determining the dimensions of the Operational Environment by identifying the significant characteristics of the operational environment and gathering information relating to the operational environment and the adversary (i.e. the mission)

3 Evaluate the Adversary

- Adversary military situation
- Adversary unconventional & information operations situation
- Adversary Capabilities

2 Describe the Impact of the OE

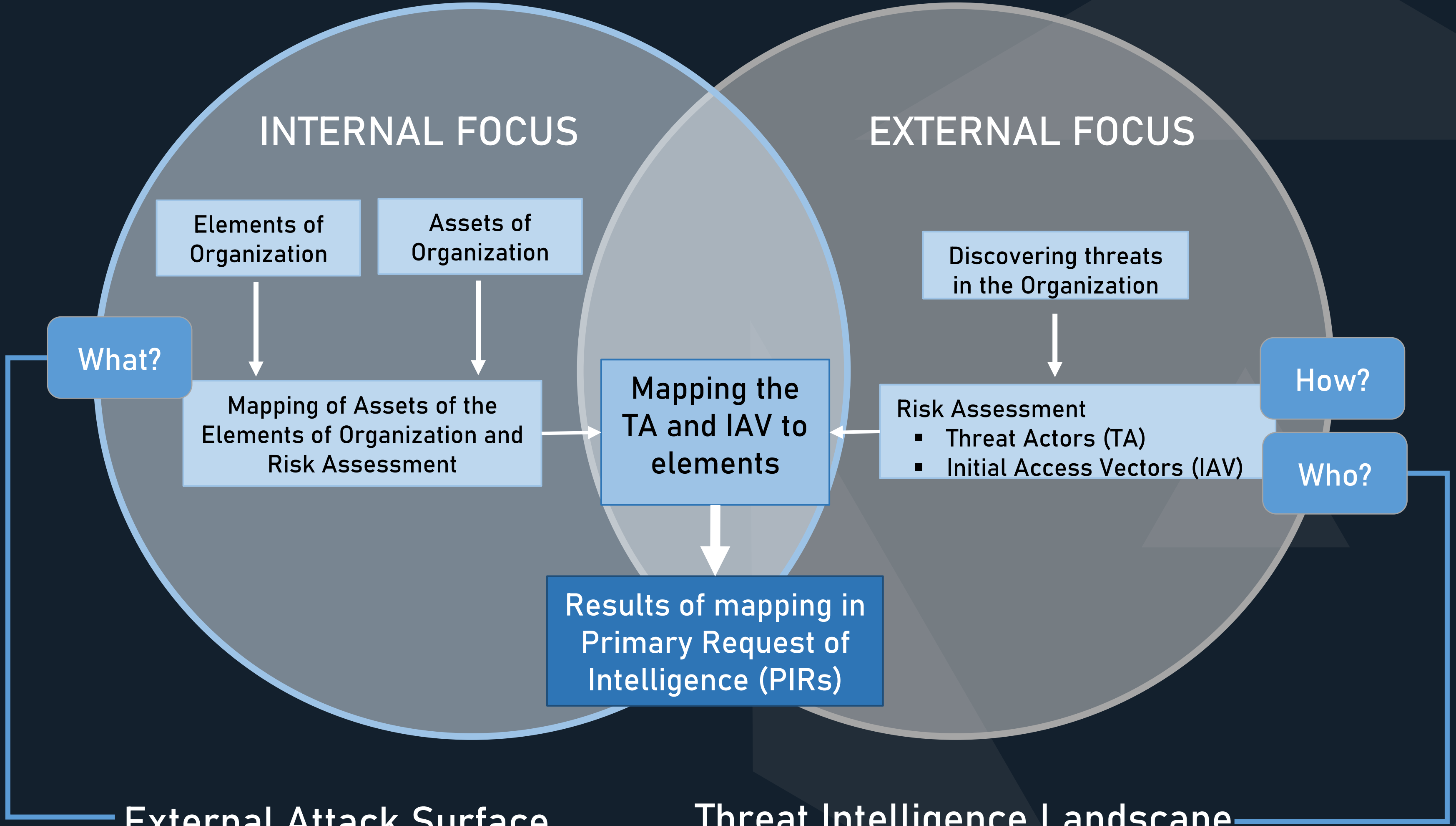
Characteristics of the operational area

Joint Intelligence Preparation of the Operational Environment (JIPOE)

CYBERSECURITYITALIA

Digital Risk Protection Services

TLP: CLEAR


INTERNAL FOCUS
EXTERNAL FOCUS
Elements of Organization
Assets of Organization
What?
Mapping of Assets of the Elements of Organization and Risk Assessment
Mapping the TA and IAV to elements
Discovering threats in the Organization
Risk Assessment
▪ Threat Actors (TA)
▪ Initial Access Vectors (IAV)
How?
Who?
Results of mapping in Primary Request of Intelligence (PIRs)

External Attack Surface

An external attack surface is the entire area of an organization or system that is susceptible to an attack from an external source.

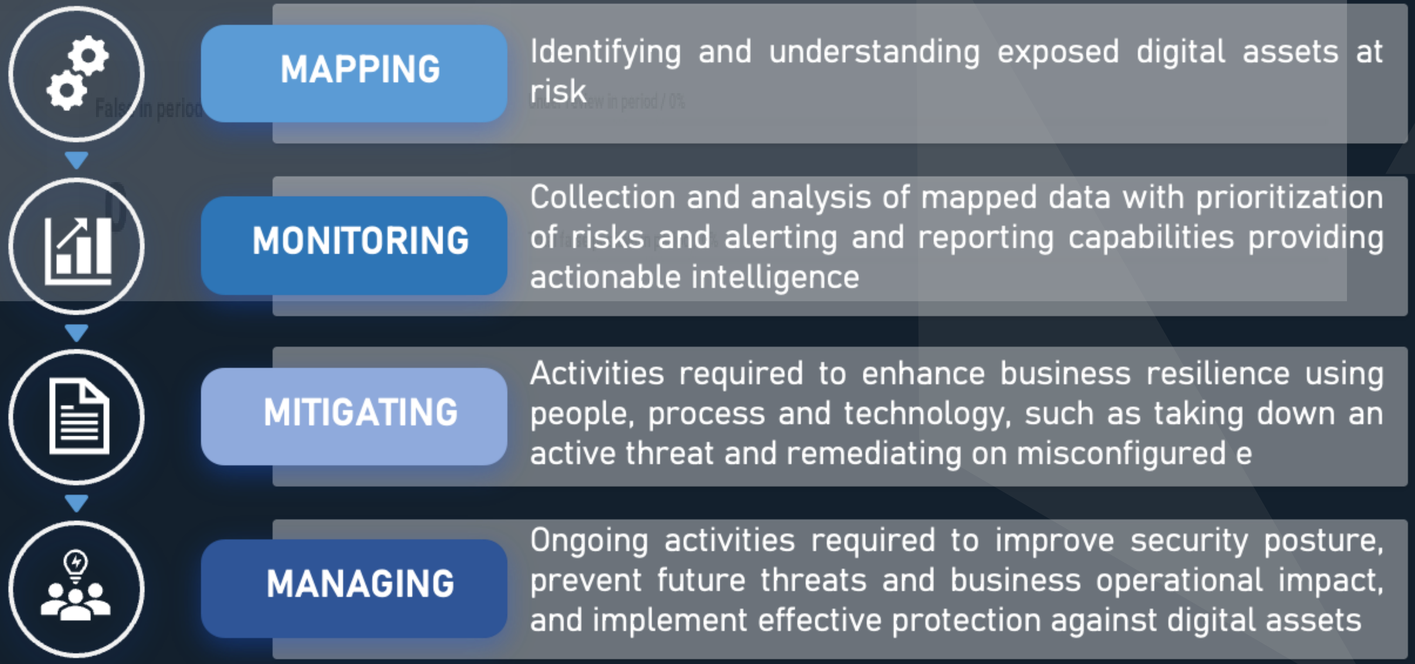
Threat Intelligence Landscape

The threat landscape is the entirety of potential and identified cyberthreats affecting a particular sector, group of users, time period, and so forth.

Digital Risk Protection Services

TLP: CLEAR

> The **Digital Risk Protection Services** (DRPS) are technologies and services developed to protect critical digital assets and data from external threats. These solutions provide visibility into the open (surface) web, dark web and deep web sources to identify potential threats to critical assets and provide contextual information on threat actors and the tactics and processes utilized to conduct malicious activity



MAPPING Identifying and understanding exposed digital assets at risk

MONITORING Collection and analysis of mapped data with prioritization of risks and alerting and reporting capabilities providing actionable intelligence

MITIGATING Activities required to enhance business resilience using people, process and technology, such as taking down an active threat and remediating on misconfigured e

MANAGING Ongoing activities required to improve security posture, prevent future threats and business operational impact, and implement effective protection against digital assets

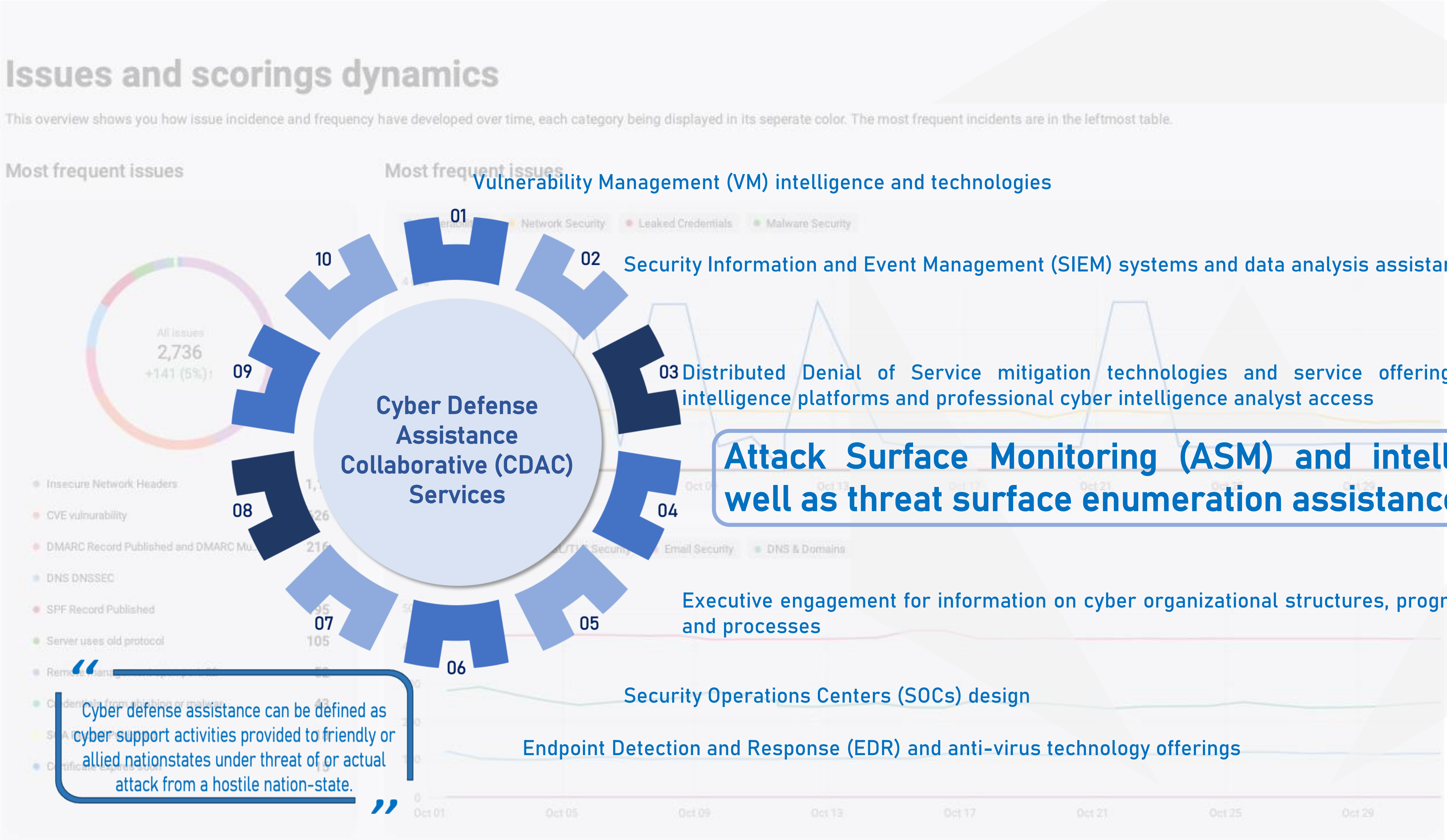
Digital Risk Protection Services provides support in four areas

DRPS Use Cases

- Digital footprinting through mapping exposed digital assets
- Brand protection
- Account takeover
- Fraud campaigns
- Data leakage detection

CYBERSECURITYITALIA

Attack Surface Monitoring as First Effective Defence



Issues and scorings dynamics

This overview shows you how issue incidence and frequency have developed over time, each category being displayed in its seperate color. The most frequent incidents are in the leftmost table.

Most frequent issues

All issues
2,736
+141 (5%)

- Insecure Network Headers
- CVE vulnerability
- DMARC Record Published and DMARC Mu...
- DNS DNSSEC
- SPF Record Published
- Server uses old protocol

Most frequent issues

Cyber Defense Assistance Collaborative (CDAC) Services

01 Vulnerability Management (VM) intelligence and technologies

02 Security Information and Event Management (SIEM) systems and data analysis assistance

03 Distributed Denial of Service mitigation technologies and service offerings Access to intelligence platforms and professional cyber intelligence analyst access

04 **Attack Surface Monitoring (ASM) and intelligence, as well as threat surface enumeration assistance**

05 Executive engagement for information on cyber organizational structures, programs, policies, and processes

06 Security Operations Centers (SOCs) design

07 Endpoint Detection and Response (EDR) and anti-virus technology offerings

08

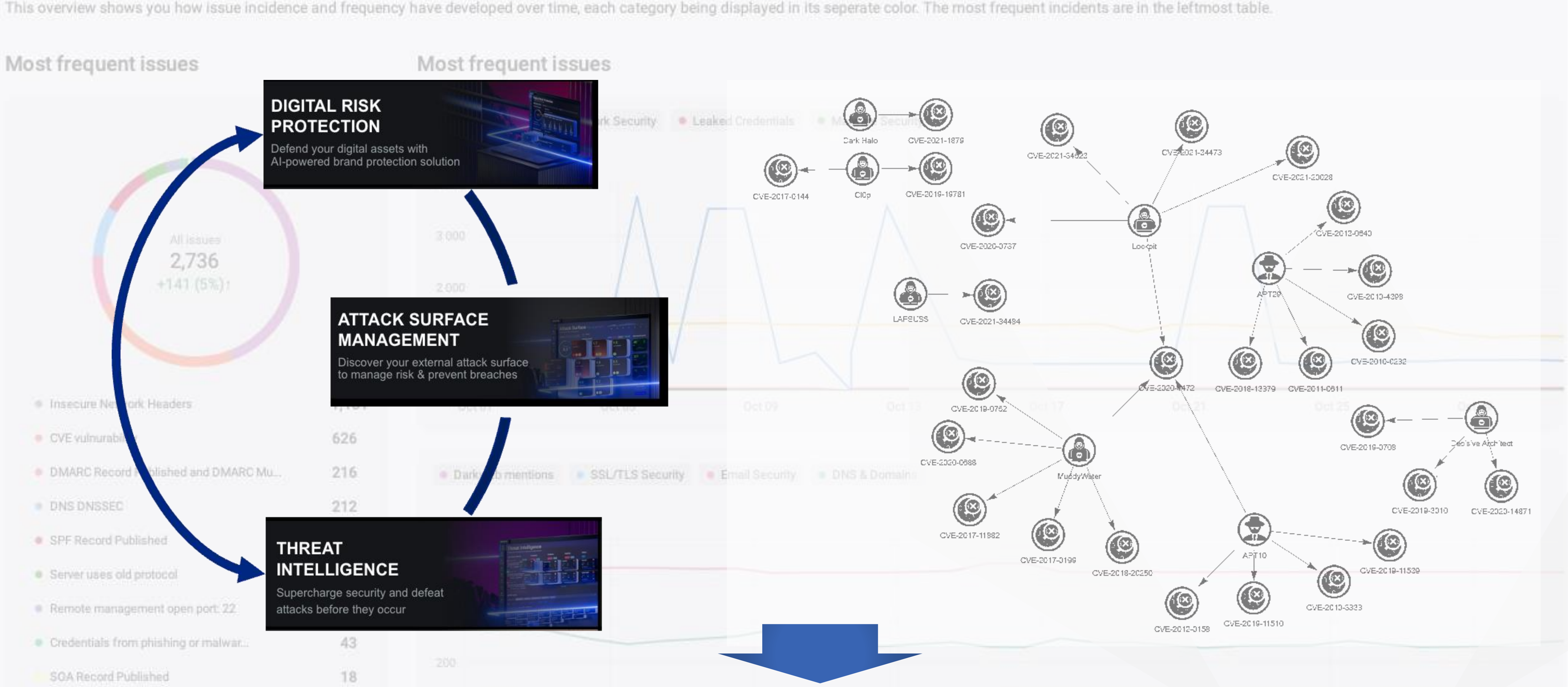
09

10

> "Cyber defense assistance can be defined as cyber support activities provided to friendly or allied nationstates under threat of or actual attack from a hostile nation-state."

Gain visibility into risk factors is the key

Gain visibility into risk factors impacting the extended enterprise and supply chain by mapping your attack surface and monitoring deep and dark web activity.



DIGITAL RISK PROTECTION
Defend your digital assets with AI-powered brand protection solution

ATTACK SURFACE MANAGEMENT
Discover your external attack surface to manage risk & prevent breaches

THREAT INTELLIGENCE
Supercharge security and defeat attacks before they occur

Attack Surface Intelligence