



Cy4Gate

Mid & Small - Virtual 2023

June 2023



TABLE OF CONTENTS

- Our Growth
- Strategic pillars
- Governance and Shareholders
- Portfolio and markets
- Financial performance
- ESG
- Q&A
- Solutions and Services

Fast growing and attractive group...

2,85x

Shares price since IPO



JV between

ELETRONICA GROUP
Defence | Cyber | Security



2014

Start up



2019

Growth and acquisition of market share

2020 IPO

Listing on FTSE Italia Growth



2022

Capital Increase of 90 Millions for M&A



129%

Revenues CAGR 2022 vs IPO

2023

Listing on EURONEXT STAR Milan



... thanks to exceptional performance

Delivery on track on all Strategic pillars

Strategic pillars



360° Cyber vendor
"Made in Europe"



Tailormade solutions
for **Global Cyber Defence**



Superior **ethics & talent**
development



Partnerships and
M&A for **tech leadership**

Target



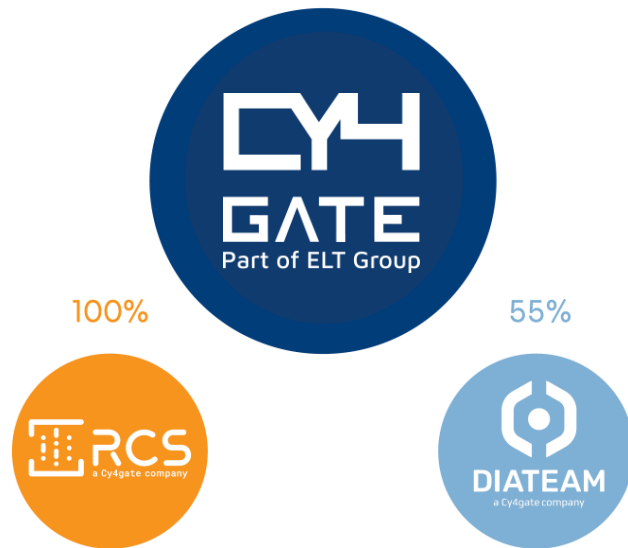
ESG



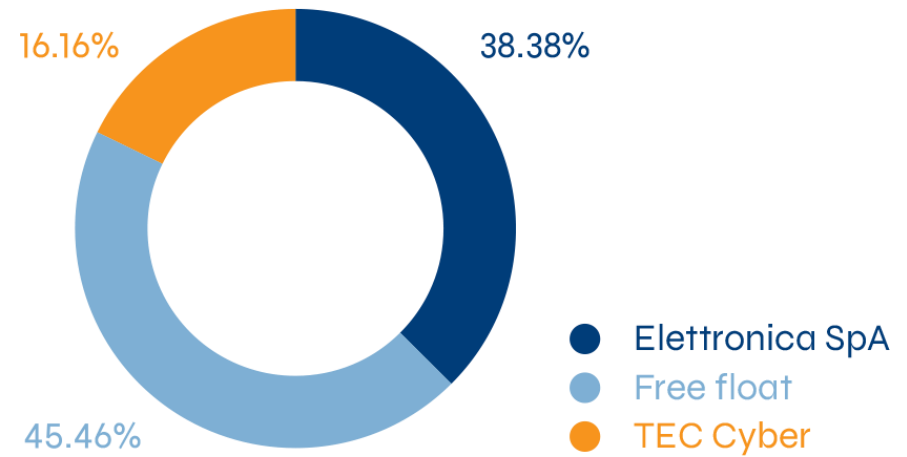
“ *To protect and empower people through reliable and leading edge solutions* ”

GROUP & SHAREHOLDERS

GROUP



SHAREHOLDERS



TEAM



Domitilla Benigni
CHAIRMAN



Emanuele Galtieri
CEO & General
Manager



Marco Latini
CFO & Investor
Relations Manager

Board of Directors



Domitilla Benigni Chairman	 	Emanuele Galtieri CEO & General Manager
Roberto Ferraresi Member	 	Maria Giovanna Calloni Independent Member
Cinzia Parolini Independent Member	 	Enrico Peruzzi Member
Alberto Luigi Sangiovanni Vincentelli Member	 	Paolo Izzo Member
Alessandra Bucci Independent Member		

Strategic and M&A Committee



CY4Gate is present in two main markets:

Cyber Intelligence & Cyber Security

PORTFOLIO OVERVIEW

CYBER INTELLIGENCE

Decision Intelligence

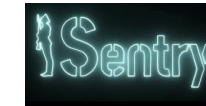


Forensic Intelligence



CYBER SECURITY

Cybersecurity Products



Cybersecurity Services



CYBER INTELLIGENCE

Cyber Intelligence solutions collect and analyze information available online and generate added value insight thanks to AI

Decision Intelligence



QUIPO is complete intelligence platform, based on AI technology, able to mix and match: several data sources, for timely and effective reaction to events

CONTINUOUS INTELLIGENCE
The Right Information, At The Right Time,
To The Right People, In The Right Way

Forensic Intelligence

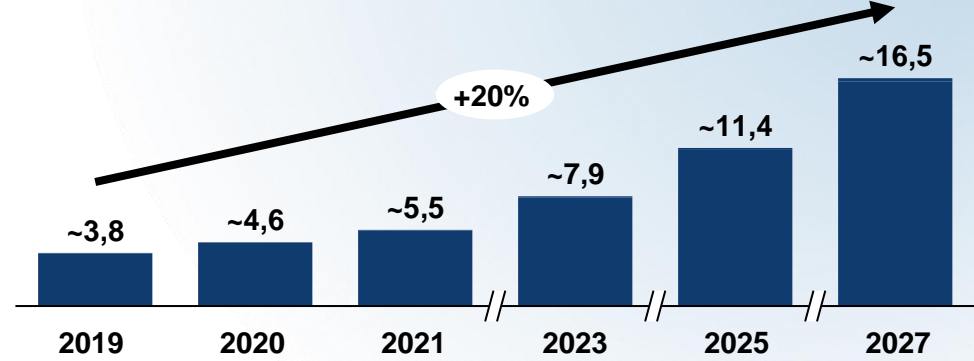


Support law enforcement agencies providing **customizable and easy-to-use Forensic Intelligence & data analysis solution**



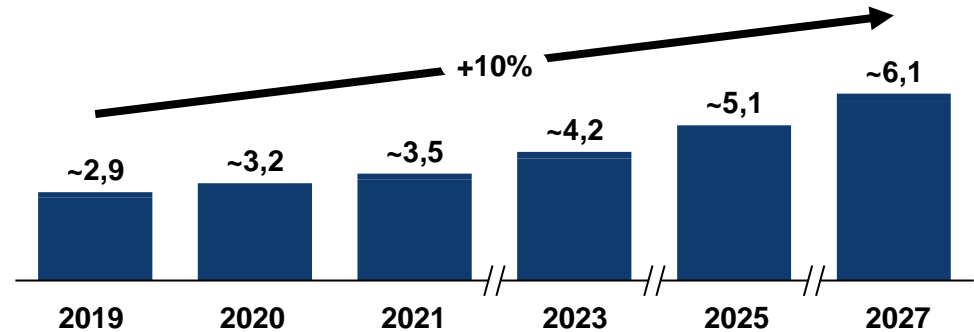
Global opensource intelligence (Osint) market

€ bln



Global forensic intelligence & data analysis

€ bln



Source: Markets & Markets, industry reports and expert interviews

Double digit growth



CYBER SECURITY

Cyber security solutions protect clients' information systems, enabling the detection of anomalies and generating response actions



Real time analytics (RTA) is a security information and event management (SIEM), advanced cyber security application that enables the analyst to detect cyber security anomalies and creates conditions to rapidly strike back.

Cybersecurity Products



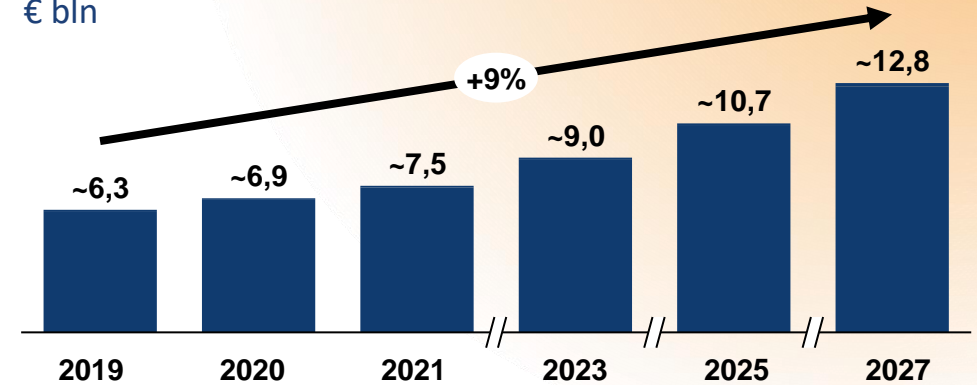
Pool of **Cyber Security services** covering the following topics:

- Red Teaming and Penetration Test
- Compliance Assessment
- Managed Detection & Response
- Incident Response & Malware Analysis
- Hands-on Cyber Training and Security Awareness
- Cyber Resilience Design for Critical Infrastructure

Cybersecurity Services

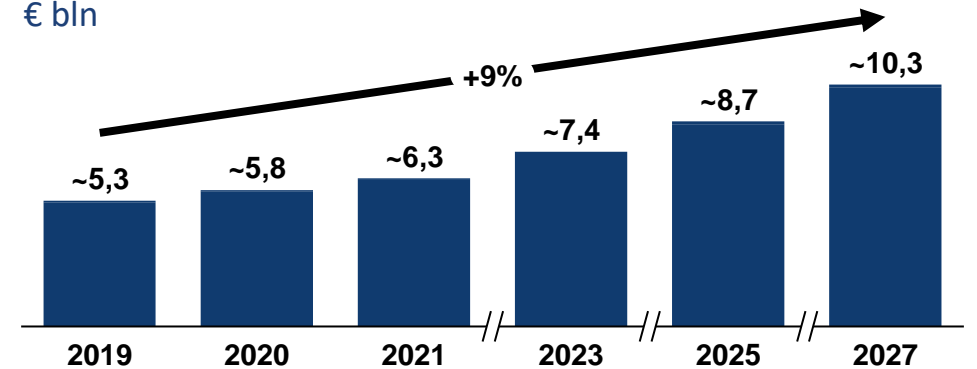
Global Cybersecurity Products¹ Market

€ bln



Global Cybersecurity Services² Market

€ bln



1. Includes Security Operations products such as SIEM, SOAR, UEBA, Threat Intelligence and related products
 2. Includes Penetration testing, Vulnerability management and related services

Source: IDC, industry reports and expert interviews

Enduring growth



MARKETS

GEOGRAPHICAL PRESENCE AND MARKETS SERVED

The company mainly operates in Italy, is also active in Spain and is increasing its presence in Germany and France. It also has a global presence, with clients in the Middle East, South East Asia, and Latin America.



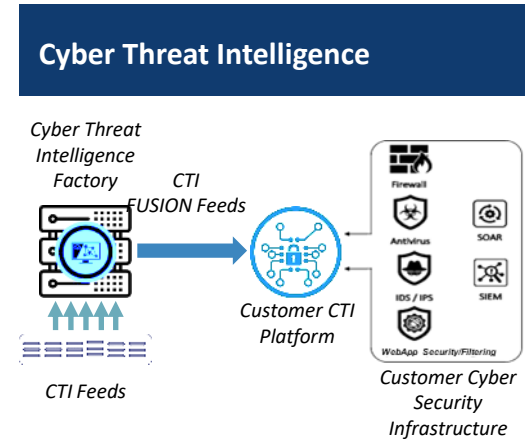
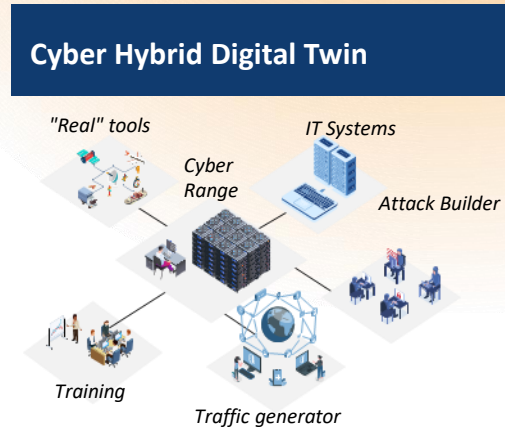
REVENUES BY GEOGRAPHIC AREA

Revenues by geographic area	2020		2021		2022	
	CY4GATE S.p.A		CY4GATE S.p.A		CY4GATE Group	
	€M	%	€M	%	€M	%
ITALY	10.7	86%	14.4	85%	41.2	63%
EXPORT	1.8	14%	2.6	15%	24.2	37%
TOTAL	12.5	100%	17.0	100%	65.4	100%

Note: Calculated on operating revenues, Cy4Gate 2022 pro-forma full year

4 new Cyber Security solutions

Example



Target customers

- SME

Large corporations & institutions

- Institutions

- Large companies and institutions

Key features

- Platform for “at scale” offering of **Cyber-incident management services**, through **dedicated e-commerce**, towards SMEs
- **Price based on the average man-days consumed**, also factoring the risk of realization

- Development/delivery **platform for simulation environments** (digital twin)
- Wide range of **functions** and possible **applications** such as:
 - Systems **cyber resilience testing** in a "secure" environments
 - **Research and development of attack mitigation** solutions
 - **Education and training** for advanced Cybersecurity capabilities

- **Device** capable of **scanning mobile devices for real-time attack detection** (e.g., unknown APT1 and unknown vulnerabilities)
- Presence of **software elements** (e.g., *core* license), usable through a hardware device ("mobile sweeper") that enables scanning
- **Multiple revenue models** available: purchase, rental and "perpetual", "pay-per-use" use

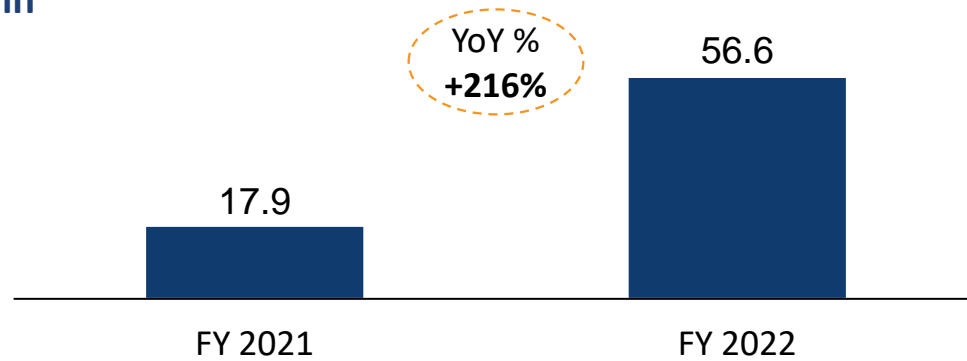
- **Cyber attack reprocessing/intelligence service** (with possible integration with SIEM), exploitable at tactical level
- **Integration and correlation of CTI Feeds** (commercial and Open Source) in the platform, then presented in **specific reports** providing a "**vertical**" view on **Cyber** threats (e.g., for selected industries)
- Possibility to access **different levels of customized service** (i.e., Silver Gold, Advanced)



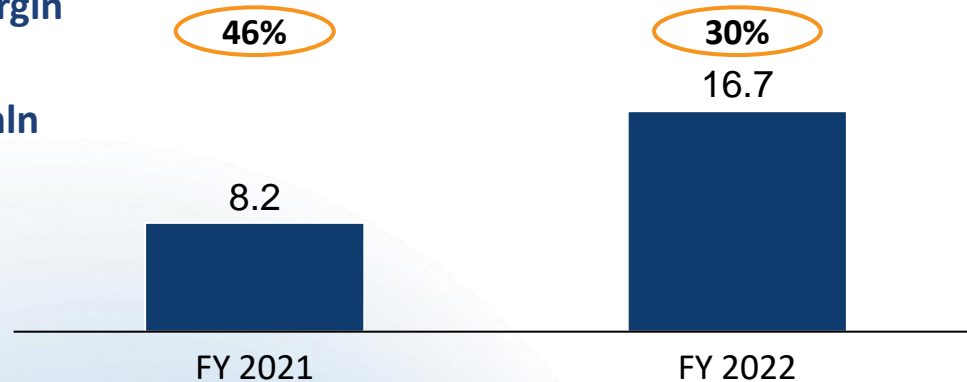
Financial performance

FY 2022 Key data¹

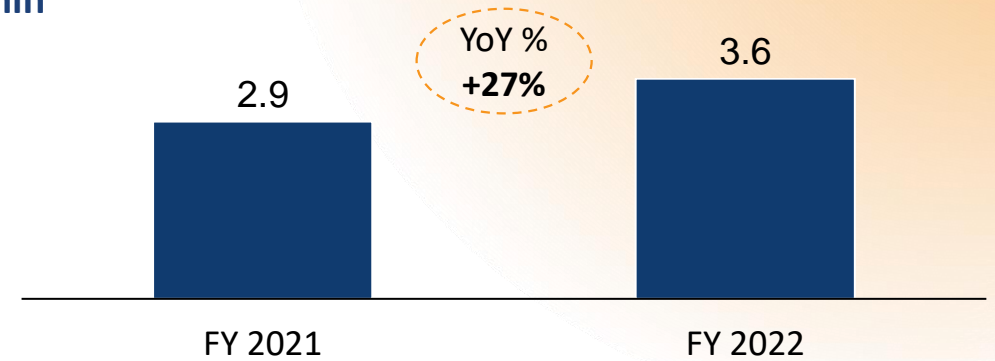
Revenues²
€ mln



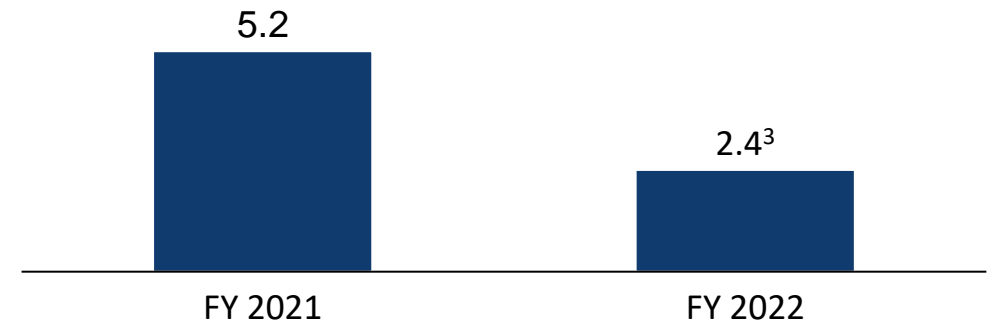
EBITDA
Margin
(%)
€ mln



R&D
€ mln



Net profit
€ mln

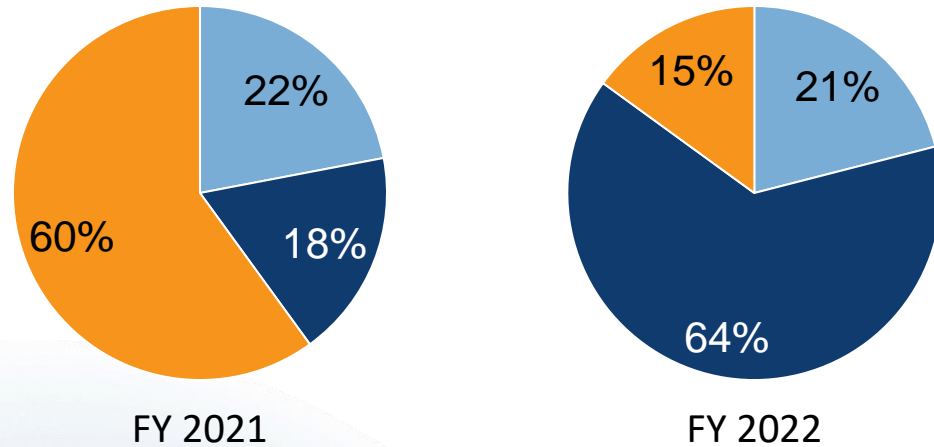


1. 2021 and 2022 economic data have been restated due to the transition from Italian GAAP (OIC) to International Accounting Standards (IFRS): 2021 financial results refer to Cy4Gate stand alone, 2022 financial results refer to Cy4gate Group (12 months of Cy4Gate + 9 months of RCS)
2. Includes other operating revenues
3. Includes D&A component determined by Purchase Price Allocation mechanism from RCS acquisition and other extraordinary items
4. Full Year 2022 Group consolidated Revenues and EBITDA are equal to €68 mln and €19 mln respectively

FY 2022 Revenues Breakdown

By Segment

Decision Intelligence Forensic Intelligence Cyber Security

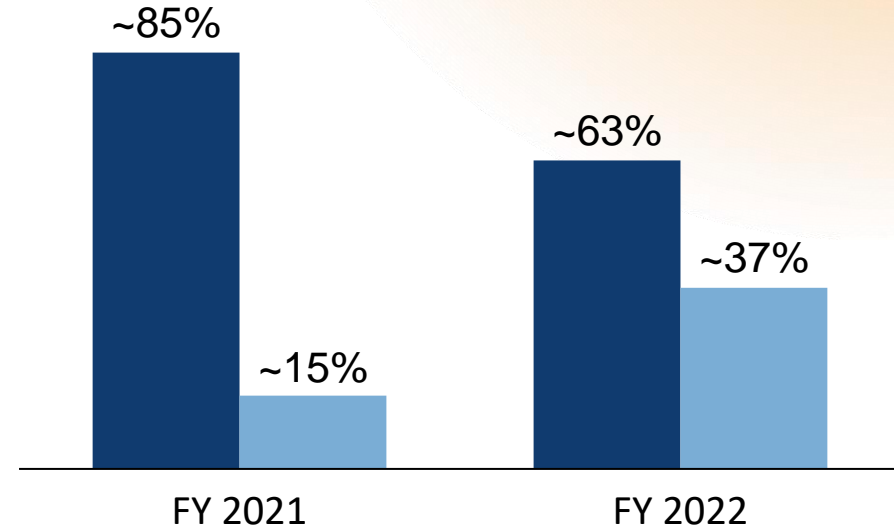


Forensic Intelligence revenues increased due to the acquisition of RCS and new Cy4gate projects

Note: Cy4gate Group results include 12 months of Cy4Gate + 9 months of RCS
Note: Calculated on operating revenues

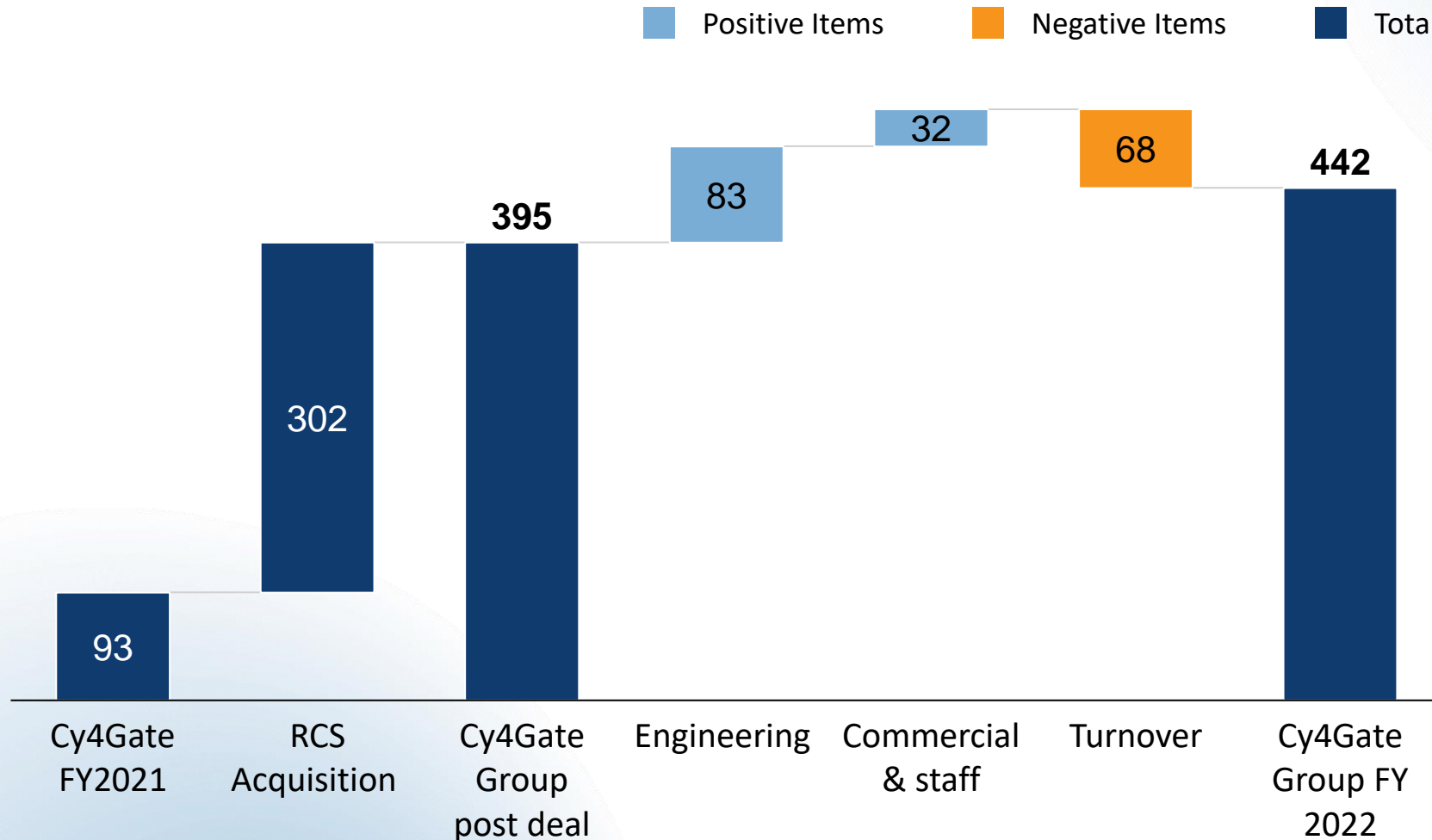
By Geographical Area

Italy Export



Expanded Group's presence in international markets

FY 2022 People Investment



- Large **increase of staff** from acquisition (~x4 total FTE), playing a pivotal role in the **Group strategy** to **access talent**
- Hiring **focus on engineering** to increase capabilities in core domains, with **positive net effect** on the organization post deal

1. Cy4Gate staff + RCS staff

ESG SUSTAINABILITY REPORT



Learn more

Our commitment for a greater sustainability

UN Global Compact & SDGs

By joining the United Nations Global Compact, CY4GATE shares, supports and applies the fundamental Ten Principles of the Global Compact in its sphere of influence and actively contributes to the achievement of the United Nations Sustainable Development Goals.

CY4GATE has included in 2023-2025 business plan investments to adopt its Social Report structured on the indications contained in the GRI (GRI 200, 300, 400) and GBS standards.

And, we will contribute to the achievement of the following 6 of the 17 goals of the 2030 Agenda for Sustainable Development.



Goal 4

To ensure **inclusive and equitable quality education and promote lifelong learning opportunities** for all



Goal 8

To promote **sustained, inclusive and sustainable economic growth**, full and productive employment and decent work for all



Goal 9

To build resilient infrastructure, and to promote **inclusive and sustainable industrialization and foster innovation**



Goal 12

To ensure **sustainable production and consumption patterns**



Goal 16

Relating to **Peace, justice and strong institutions**. Defence is a crucial component of security, and security constitutes the prerequisite for peace, prosperity, international cooperation, economic and social development.



Goal 5

To **achieve gender equality and empower all women and girls**, for operational efficiency and social inclusiveness, actively promoting the implementation of the Women Empowerment Principles.



Business ethic and human empowerment

Governance



- Solid corporate governance
- Sustainability-oriented strategies and policies
- Responsible business conduct
- Information security and privacy
- Transparency of information towards investors
- Prevention to corruption
- Prevention on anticompetitive behaviour



Environment



- Energy efficiency and emissions reduction
- Use of water resource
- Waste management



Human rights



- Respect for human rights
 - in the production and sale of products
 - in People management
 - in the gender equality and diversity empowerment
 - in the supply chain management



Business management



- Leadership in innovation
- Customer relationship management
- Responsible management of the supply chain



Relationship and working conditions



- People management and care
- People empowerment
- Occupational health and safety
- Equal opportunities and gender equality



Responsibility towards the community



- Protection and safety of the community
- IT security and critical infrastructure protection



Q&A



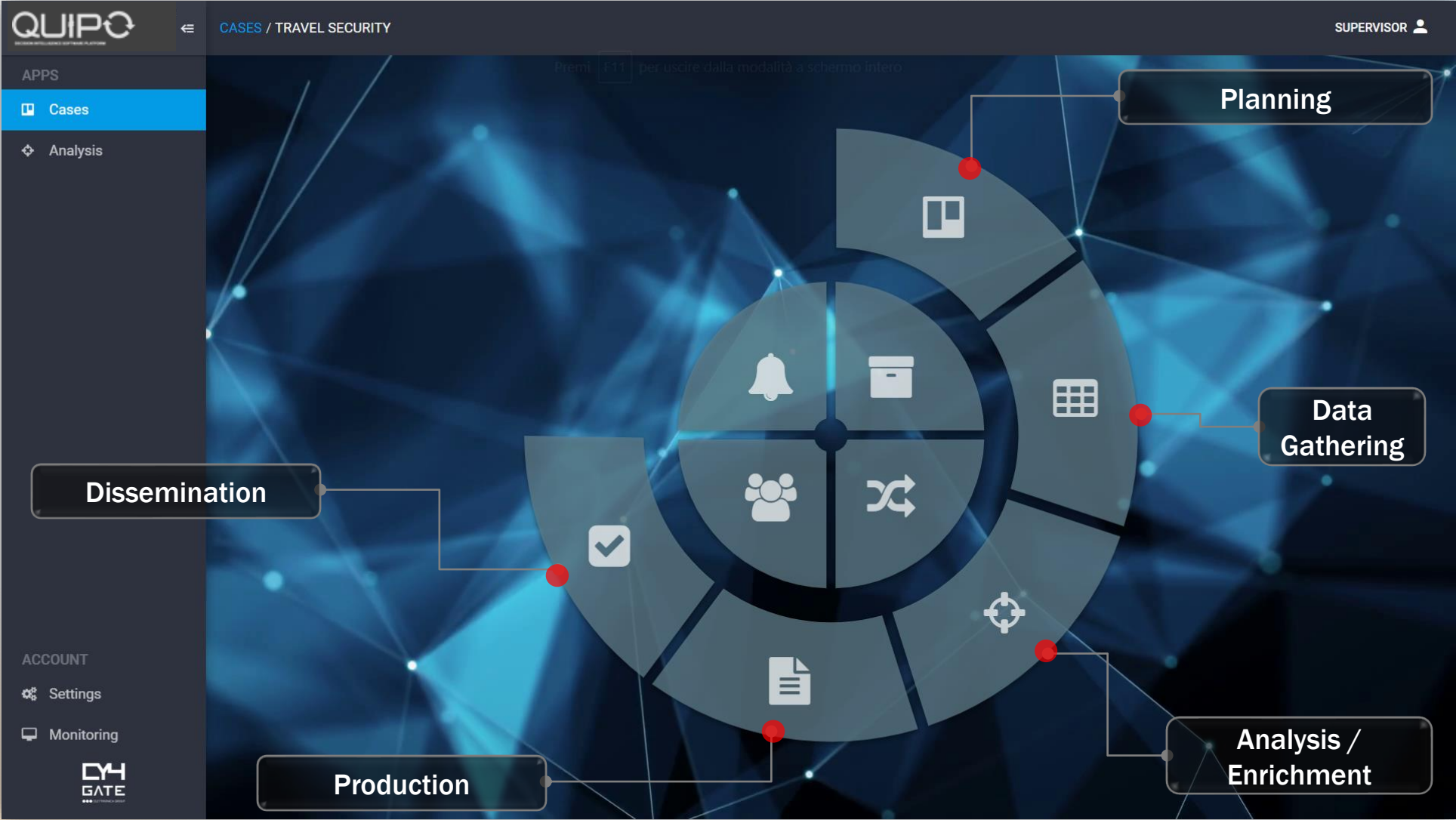
.....

THANK YOU

.....

Solutions and Services

QUIPO Automation for Decision Augmentation





QUIPO DECISION INTELLIGENCE

*The Right Information, At The Right Time,
To The Right People, In The Right Way*

QUIPO is a **Decision Intelligence** platform based on AI algorithms that transforms **data into knowledge** and provides **Decision Support** and **Decision Augmentation** more and beyond traditional solutions based on conventional IT technologies

Value drivers

Multilayer analysis in a unique solution

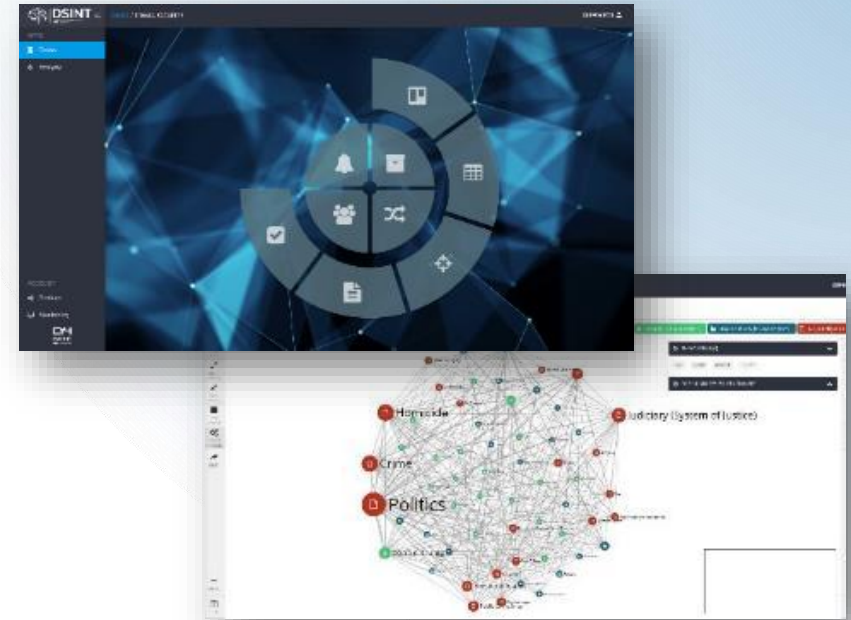
The integrated collection of multiple information assets (internal or external) enables the possibility to combine multiple analysis models (video tagging, audio tagging, semantic analysis, face recognition, location identification, feature detection, link analysis, etc.).

Prompt Information from large datasets

More effective real time access to external and internal information minimizes reputational risks, and a fraud and product development mitigates costs

Unique platform for Better Intelligence

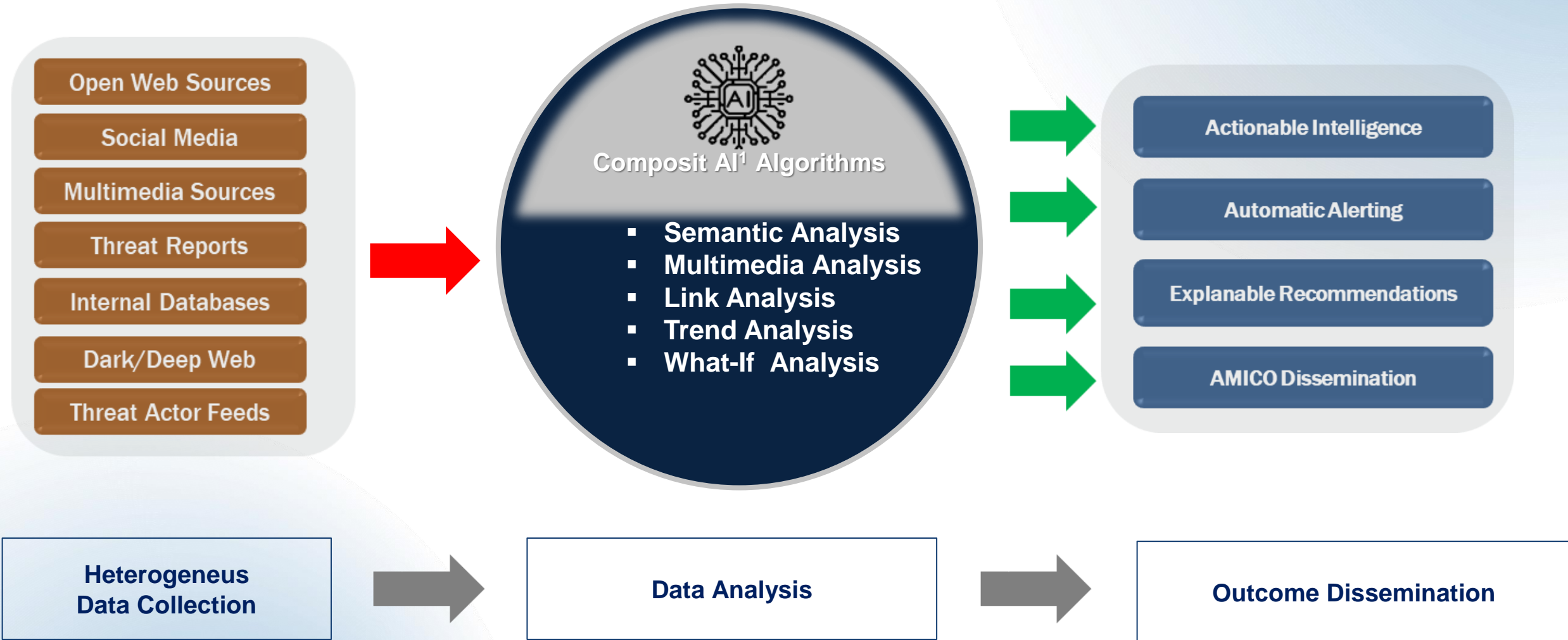
A central platform, specifically designed to support the intelligence cycle, help the possibility to improve the analysis, dissemination and production possibilities



How Is It Different?

- Fully **customizable software platform** specifically designed for the efficient **management of structured and unstructured data**
- **AI Technologies** to automate and augment the analysis activities. Different modules (semantic module, image tagging/face recognition modules, “anomalous behaviour” module) which works on machine learning, cognitive computing and deep learning
- **Multiyear experience in the intelligence domain and enterprises security** transformed into a platform that supports analysts from A to Z

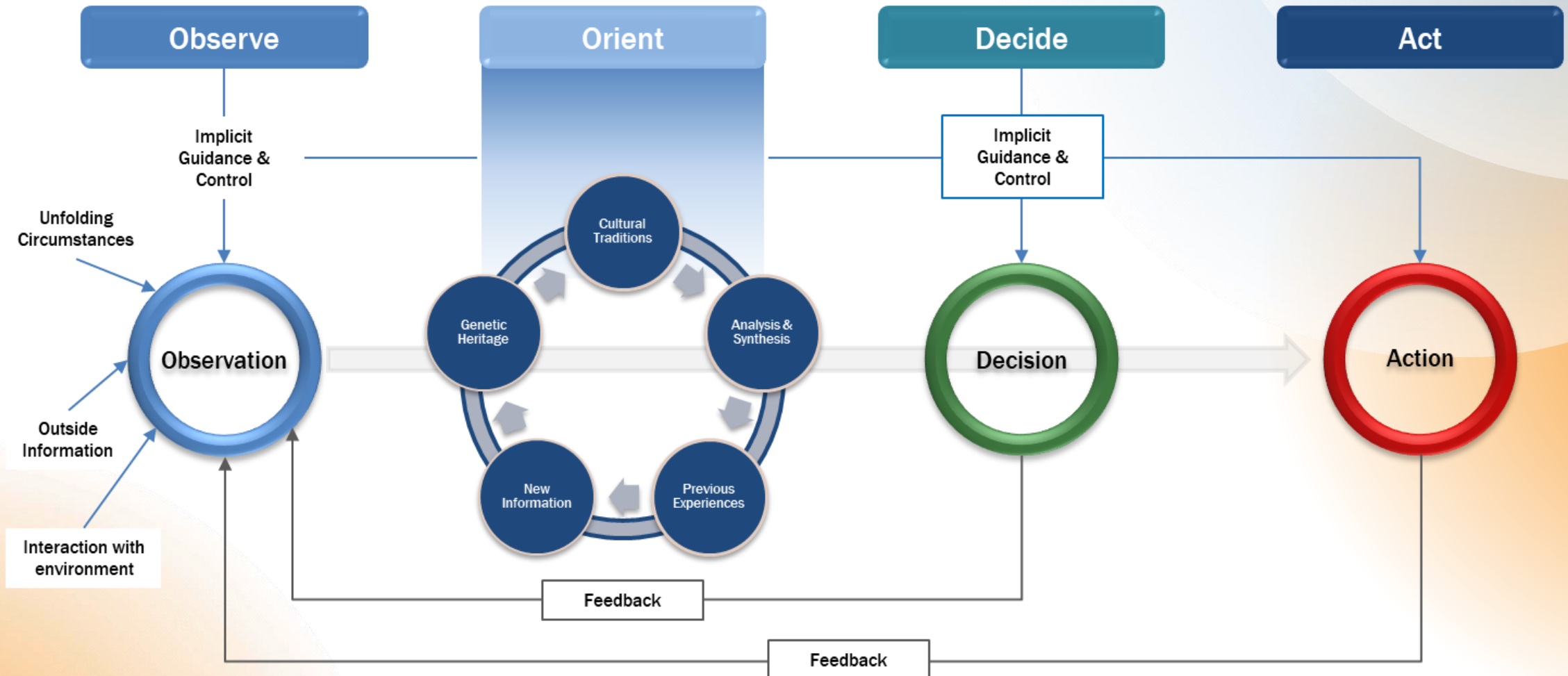
QUIPO Data Centric Intelligence Architecture



1. CY4 has been cited by Gartner as a cool vendor of composite AI (ref. Innovation Insight for Composite AI published 10 January 2022)

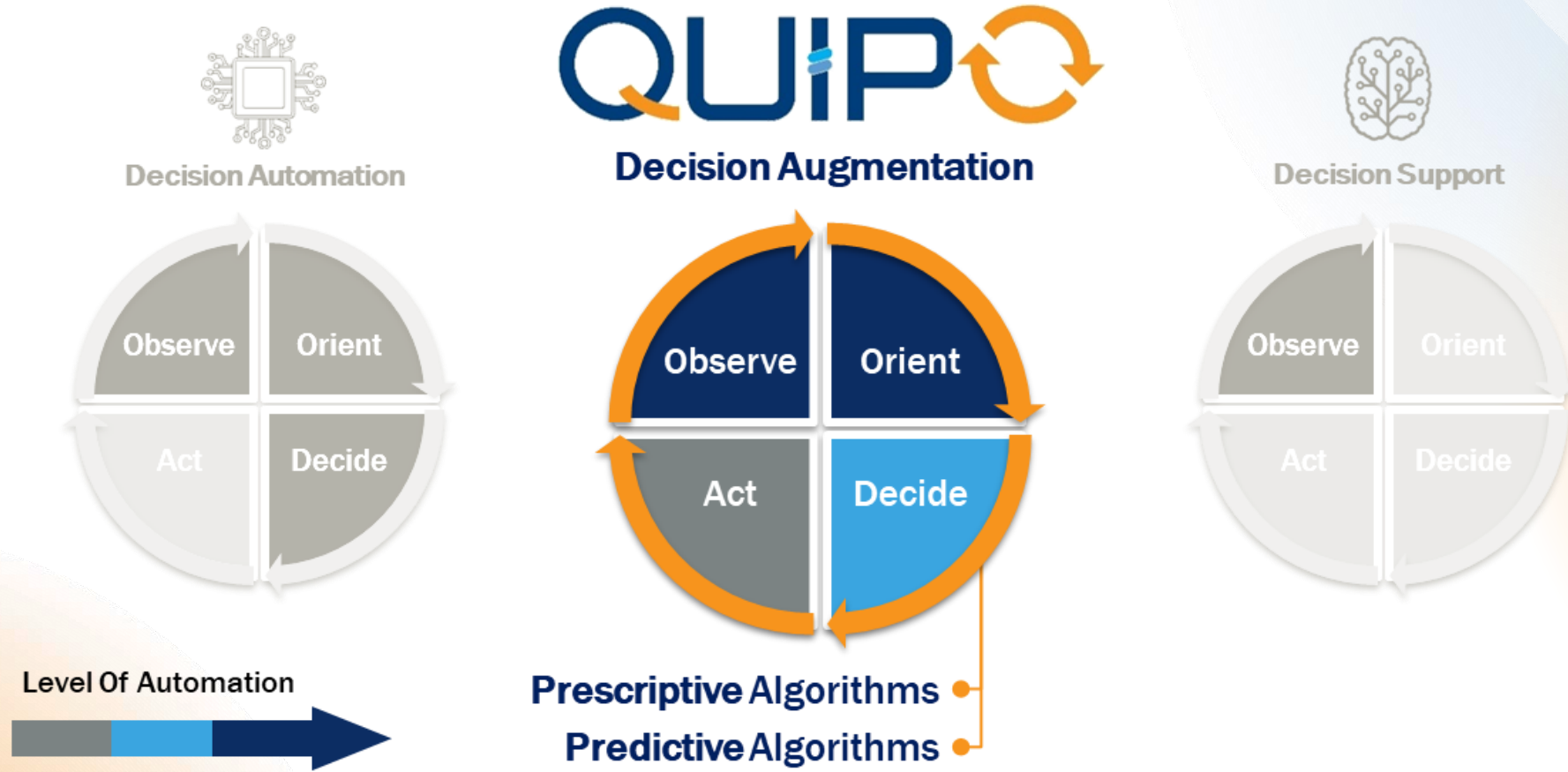
Observe – Orient – Decide - Act

Heterogeneous Information Collection + Data Valorisation + Data Analysis = Intelligence for a Decision



Decision Intelligence = Decision Augmentation

Use of **predictive algorithms** (what will happen) together with **prescriptive algorithms** (what to do) exponentially increase automation factor of the **decision phase** in an **Augmented Decision Process**



Gartner



RTA

Real Time Analytics

Upgrade your threat detection tools

RTA is a cyber security application framework that allows real-time ingestion, processing, enrichment and analysis of different kind of security events, aka Modern SIEM

RTA enables the analyst to detect anomalies and establishes the conditions to rapidly strike back

Value drivers

Sensors are everywhere

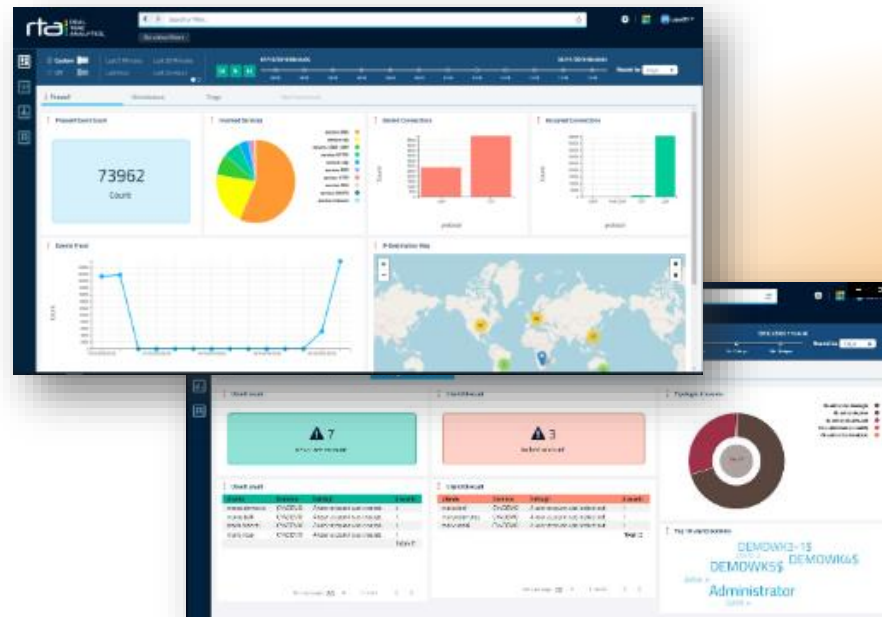
Smart collection and normalization of every sensor enables: understandable data meaning, rapid anomaly detection among billions of data. Raw Network traffic can be collected and analysed as well

More Enrichment → More Context → Better Insight

RTA enrich all events adding information on the execution context, the involved entities and the purposes of the action.

Drill down and Situation Awareness

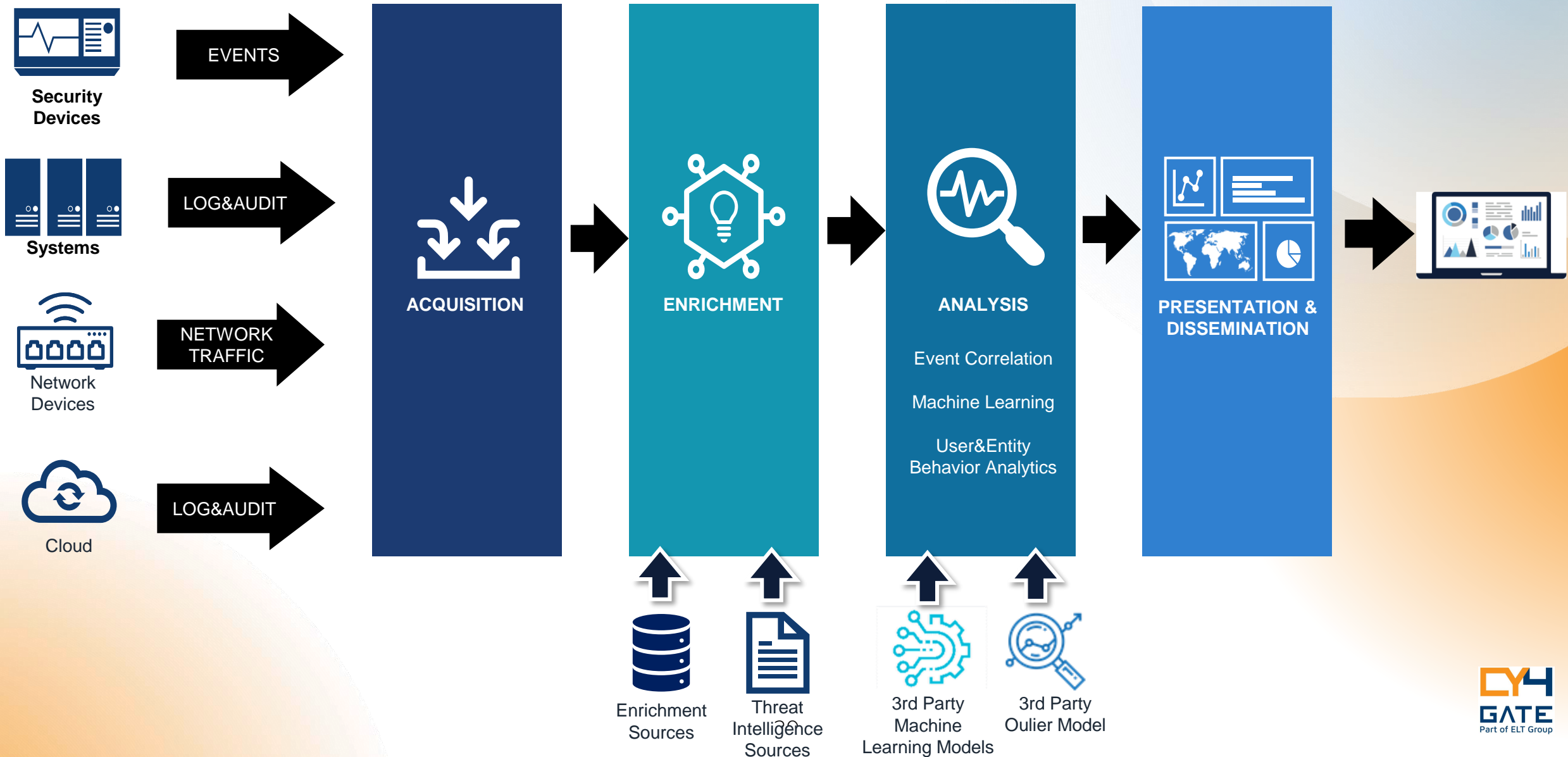
A single point of view for the Analyst allows more efficient browsing, helping to detect entities and their relationships. RTA is able to identify relationship network, through visualization tools allowing for a more accurate analysis of threats.



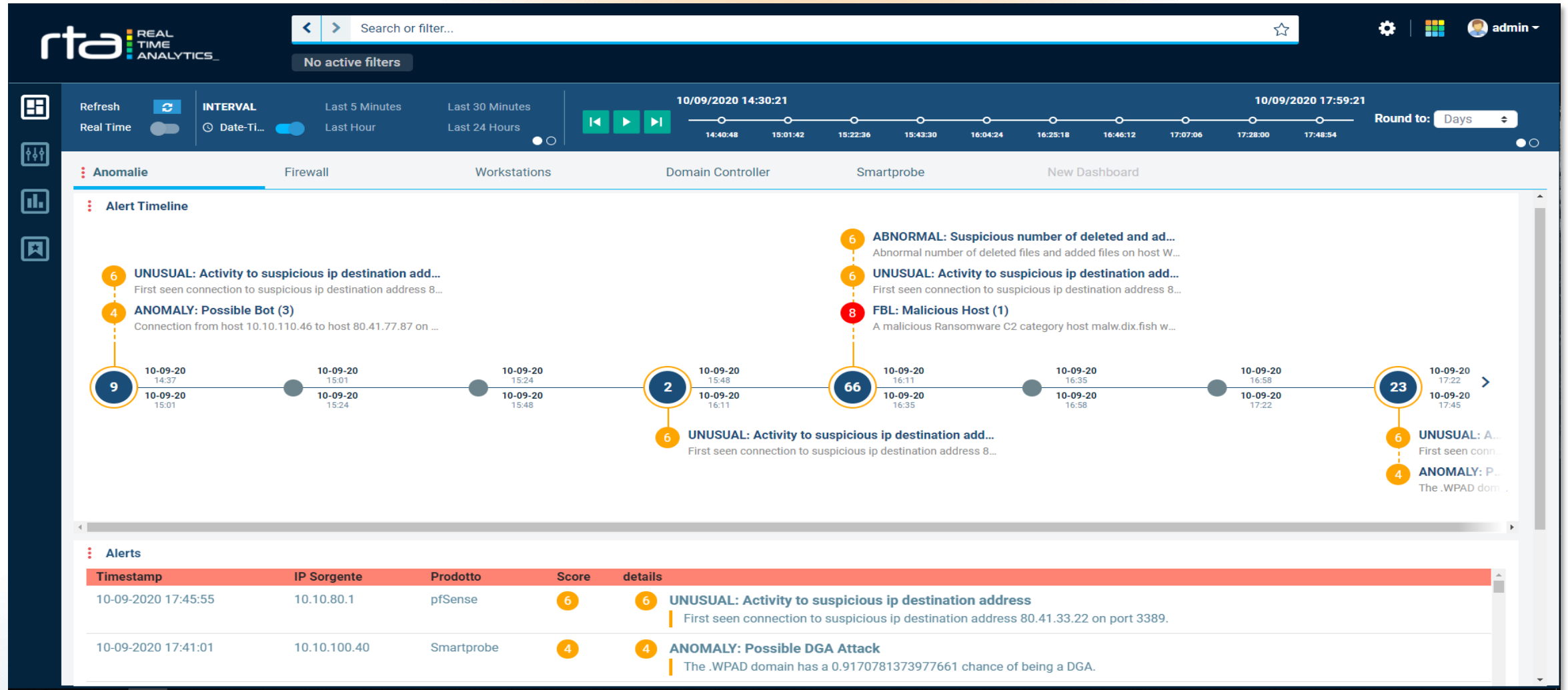
How Is It Different?

- **“Time Machine” approach**, which allows the analyst both to gather historical information (so to **“freeze the crime scene”**) and to flash forward to gather information regarding potential effects of occurring events
- **Composite Artificial Intelligence Technologies** boost RTA during the enrichment and correlation phase, allowing faster exploitation of information
- **Alarms are based on correlation, machine learning or behavioral rules** Alarms are operated by the indexing engine and then transferred to the graphical user interface which allows the analyst to perform several actions simultaneously to handle alarms

Solution Architecture (Processing)



RTA: Augmented Incident Management Process

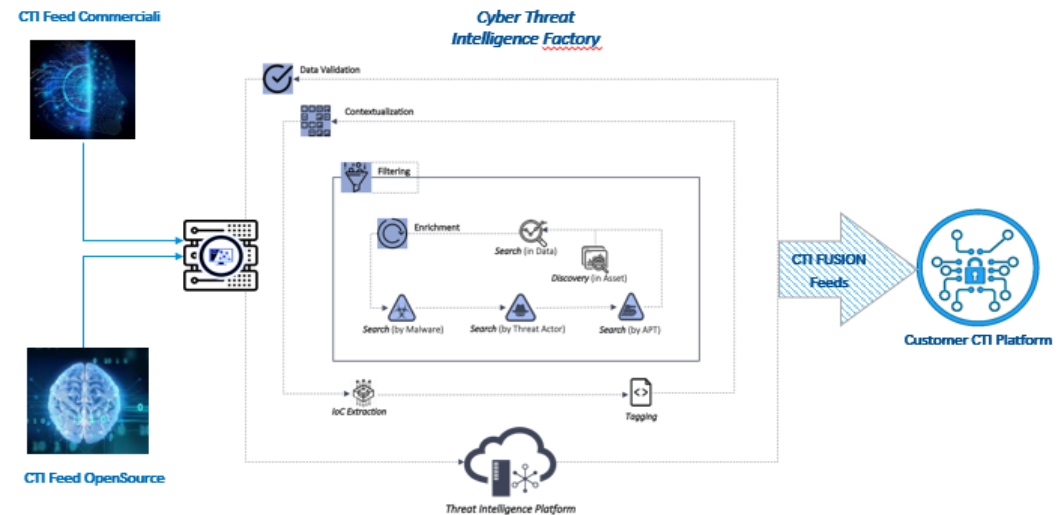


Cyber Threat Intelligence

The Cyber Threat Intelligence (CTI) Fusion Model developed by Cy4gate offers various advantages to a company with respect to a standard approach:

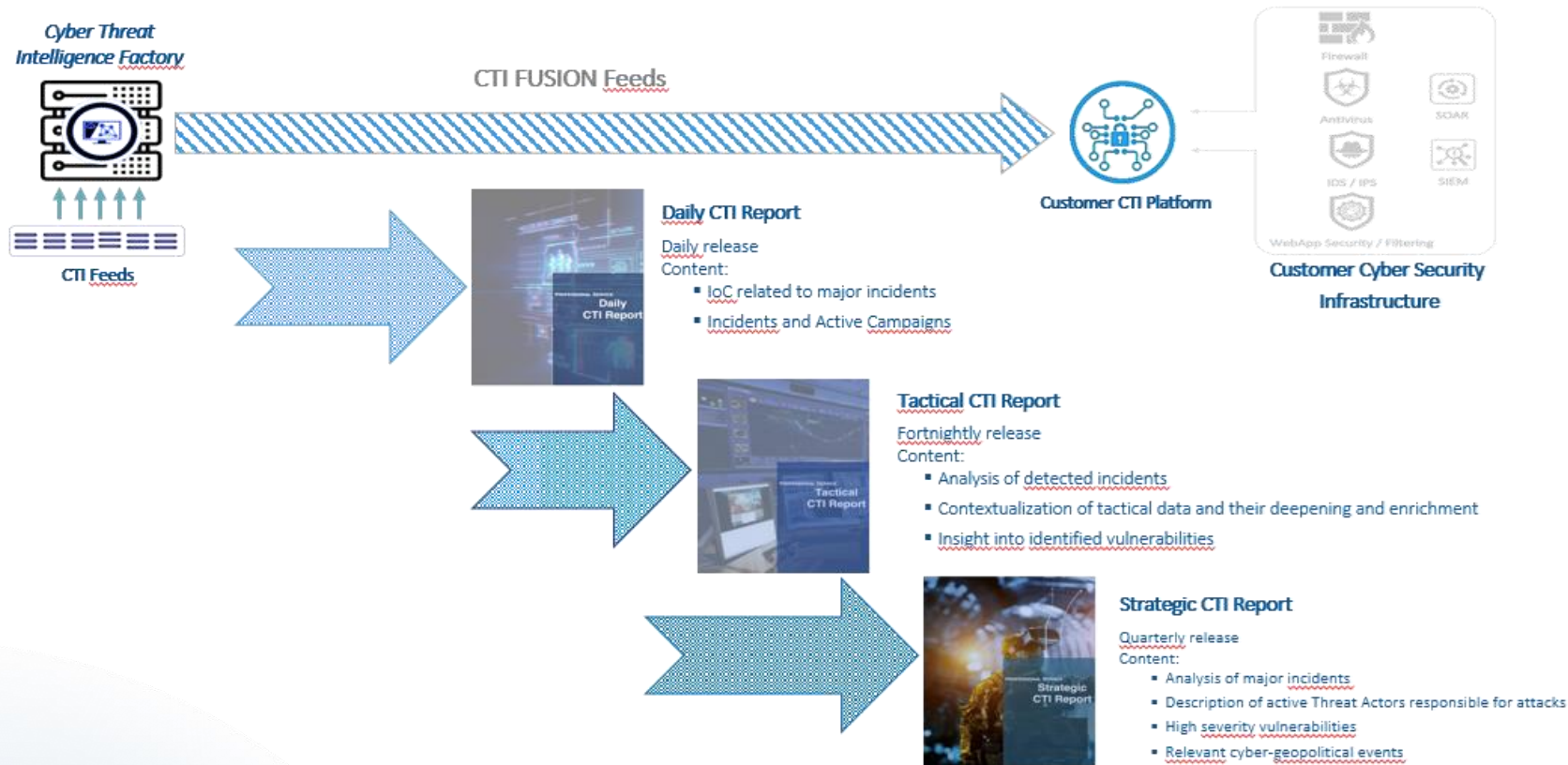
- ❑ Enable the company to approach CTI effectively while avoiding high investment costs for platforms and specialized skills, growing gradually and consciously in this area
- ❑ Make daily use of qualified CTI data sources (commercial and open source)
- ❑ Benefit from intelligence that is already processed and immediately usable through an optimized, enriched, and contextualized data type concerning the client's technological environment and its target market
- ❑ Receive periodic reports of various types with well-defined objectives

Caratteristiche	Silver	Gold	Advanced
Sharing Tactical Cyber Threat Intelligence across distinct protocols and services	●	●	●
Benefit from a fusion (Collection, Data Feed Processing and Dissemination) of intelligence data that allows it to be used for Security Defence	●	●	●
Sharing Contextualized Tactical and Operational Cyber Threat Intelligence	●	●	●
Using CTI Feeds related to specific industries	●	●	●
Daily CTI Report sharing with tactical type intelligence	●	●	●
Sharing CTI Report with operational type intelligence	○	●	●
Sharing the CTI Report with strategic type intelligence	○	●	●
Dedicated on-demand support	○	○	●



Cyber Threat Intelligence Fusion Service Delivery

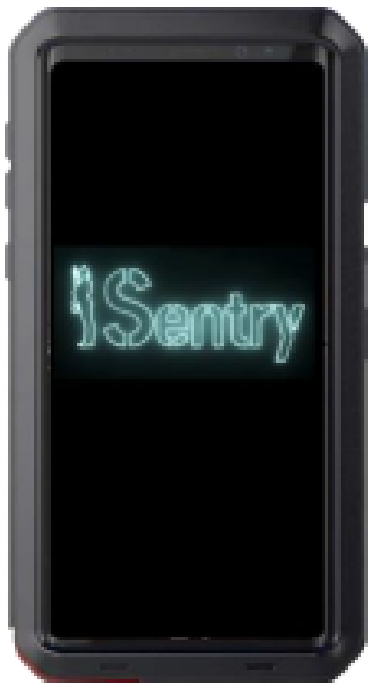
The Cyber Threat Intelligence, FUSION service, is delivered through both the sharing of already related CTI Feeds and through CTI Reports:



SENTRY Mobile APT-Detector

Sentry is a solution for the analysis and detection of malware on Android based devices in order to verify their compromise. Unlike an antivirus that analyzes threats against known items, Sentry detects by analyzing mis-configurations and anomalous behavior at the system level attributable to compromises by APT (Advanced Persistent Threat) agents.

It is a physical device or one that can be managed centrally via app and WiFi network which, once connected/installed on the device to be controlled, returns an output (OK/KO).



Sentry is structured in 3 main items:

- License for "Sentry Core"
- "Sentry Mobile Sweeper" Terminals
- "Sweep cartridge" scan instance packages



PRODUCT

WHAT'S A CYBER RANGE?

A virtual environment that enables organisations to simulate cyber combat training, system/network development, testing and benchmarking.

Learn
more



DIATEAM Hands-on Cyber Twin Solution

Solutions and Services

● Product ● Services



Hybrid Digital Twin

Virtual environment that enables simulated cyber-attacks, systems development, testing and benchmarking



Cyber training

Skills development training, in particular, threat recognition and management



Incident response

Emergency response for declared incident (e.g., ransomware, data leakage)



Test e Validation

Virtual environment with Hardware and Software in the loop to test networks and OT infrastructure and cyber defense tools.

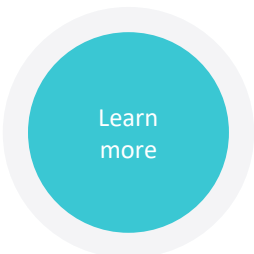


PRODUCT FEATURES

- Tailored environment
- User-friendly
- A powerful way of replicating existing information systems
- Demonstrative way to raise awareness
- Open Platform API
- Remotely run actions within the Cyber Range
- Improve your defensive posture by facing realistic threats
- USB Plug & Play
- Full content catalogue
- And much more

WANT TO KNOW MORE?

Click below for further info about our product features.



USE CASE

TESTING

Cyber Range offers the capability to test new technologies before implementing these in real life scenarios.

- Is the technology secure?
- What effect will the technology have?
- Run different scenarios
- Real-life & simulations



USE CASE

DIGITAL TWIN FOR DECEPTION

Clone your real-life network to:

- Evaluate vulnerabilities
- Optimise performance
- Test without risk

THE HONEY NET

This cyber digital twin enhances the capability to prevent attacks by luring real attackers to the clone network – 'honey net' – to observe, isolate and block further malicious cyber actions.



USE CASE

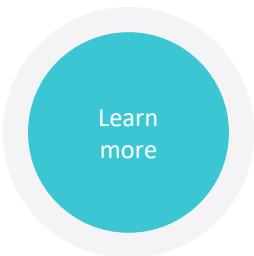
HYBRID DIGITAL TWIN FOR IT & OT INTEGRATION

Connect operations technology (OT) systems with information technology (IT) to prevent attacks on industrial sites.

- Crises simulation
- Test validation
- Safeguard the operation

WANT TO KNOW MORE?

Click below for further info on our IT & OT Connection.



USE CASE

MARITIME AND NAVAL ACTIVITIES

Our solutions meet an array of maritime and naval cybersecurity needs:

- Cyber training for cyber defenders and defence teams
- Offensive ops, because adversary emulation is essential for military operations.
- Cyber Lab, comprising experimentations and simulations of IT and OT assets for analysis, prototyping or research for attack and defend purposes.
- Experience with DEFNET cyber trainings, virtualisation of ports IT/OT systems, custom design of realistic APT scenarios, ashore and on-board cyber training for shipowners.
- Over a dozen scenarios enable a wide range of training on all aspects of cyber security.



USE CASE

TRAINING

Experiencing real-world threats in a safe environment is the key to cyber security within IT & OP.

- Recognise and handle threats
- Team building & process validation
- On site & online
- HR tool
- Understand employee behaviour
- Offensive ops

WANT TO KNOW MORE?

Click below for further info about our training.

Learn
more

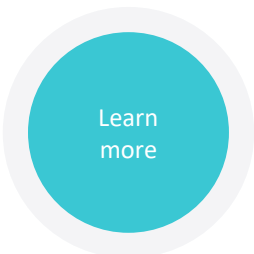


PRODUCT FEATURES

- Tailored environment
- User-friendly
- A powerful way of replicating existing information systems
- Demonstrative way to raise awareness
- Open Platform API
- Remotely run actions within the Cyber Range
- Improve your defensive posture by facing realistic threats
- USB Plug & Play
- Full content catalogue
- And much more

WANT TO KNOW MORE?

Click below for further info about our product features.



SERVICES

- Incident Response
- Technical Audit
- Research & Development
- CTF Builder



Learn
more



iSOC-CSIRT

Monitor, Withstand And Mitigate Cyber-attacks Against Your Network

Our Security Operation Center (SOC) mission is to continuously monitor and improve our customers' cyber security posture giving a full MDR (Managed Detection and Response) experience.

We can setup a full outsourced service sized according to the Customer infrastructure or support the Customer to deploy and integrate our technologies for a local Security Operation Center (SOC)

Value drivers

Be Prepared and Respond quickly

A SOC increase the effectiveness of the cyber-attack detection and response capabilities

Technology, Processes & People Combined Together

We combined best practices in class technical aspects with human resources, advanced expertise and policies

Full Outsourcing With Full Visibility

This model let you to have a SOC at the best conditions (minimum involvement and controlled cost).

This model supplies competent and operational people available 24/7



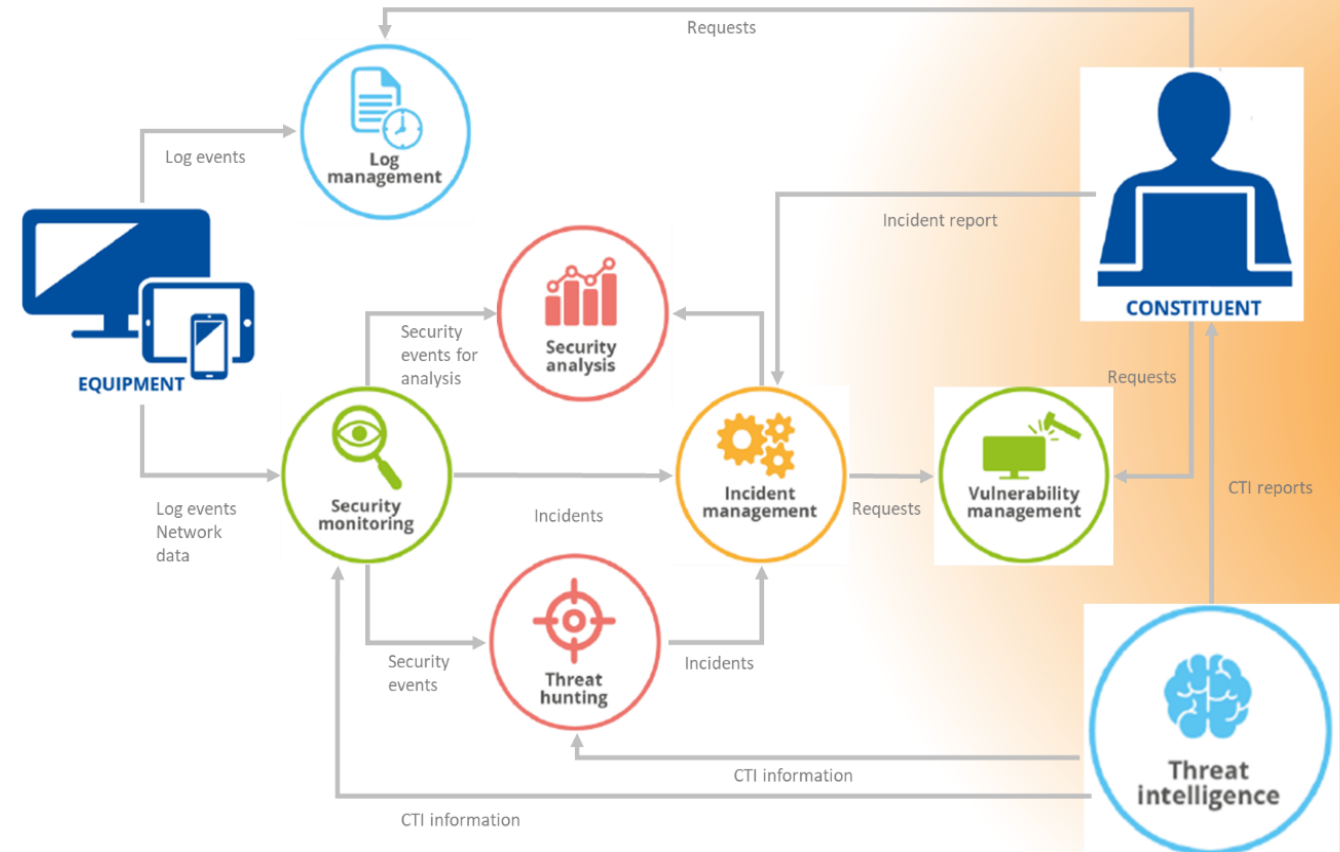
How Is It Different?

- **24/7 hardworking forces dedicated to preventing, detecting, assessing, and responding to the cyber threats and vulnerabilities.** Highly skilled and organized team with the mission of continuously monitoring and improving the security posture of an organization
- Huge amount of data ingested, analysed and enriched from cyber, IT/OT ecosystem
- Third parties tools integration with proper products and technologies for maximizing our security analysis.
- **Your SOC is our SOC. We use the same SOC we offer for defending our network**

MDR (Managed Detection & Response) Service

The SOC is a structure that centralises all information on the security status of a company's IT, offering an integrated MDR (Managed Detection & Response) service

The SOC, delivered 'as-a-service' solution, leverages the skills of the team of operators and security analysts and the best security technologies, including the proprietary RTA solution



ProntoCyber: a Fast and Ready-to-Go Cyber Solution

**INDUSTRIAL
SALES AND
DELIVERY
PROCESSES
TO REDUCE
TIME AND
COSTS**



- ✔ Digital Support
- ✔ Instant Rescue
- ✔ Continuous Awareness

IL PRONTO INTERVENTO DIGITALE

ProntoCyber è la prima piattaforma, dedicata a tutte le Aziende, che garantisce un supporto rapido ed efficace nella gestione dei Cyber-incidenti




PRONTOCYBER®
BY CY4GATE

Perché ProntoCyber®?

Non farti trovare impreparato: i Cyber attacchi sono sempre più diffusi e molto spesso sono le PMI ad esserne vittima. Dotarsi di un Pronto Intervento Digitale ti permette di minimizzare probabilità ed impatto degli attacchi cyber.

Cos'è ProntoCyber®?

- Pronto Intervento Digitale**
 - ✔ Cyber Expertise
 - ✔ Consulenza Legale Informatica
- Cyber Resilience**
 - ✔ Vulnerability Assessment
 - ✔ Penetration Test
- Cyber Awareness**
 - ✔ Cyber Education
 - ✔ Campagne Phishing





CY4GATE ACADEMY

Advanced knowledge, skills, capability

CY4Gate Academy provides recruiting, educational and training programs to address today's needs in intelligence, cyber intelligence and cyberwarfare.

Value drivers

Capability Oriented

Capability refers to the process of converting 'cyber knowledge' into specific results. "Cyber Knowledge", indeed, never transforms in cyber capability automatically because requires a combined hands-on and exercise oriented approach

Creating better staff

Your staff deserves the opportunity to learn, begin and grow a career in the cyber and intelligence fields

More Readiness → Better Security

Becoming prepared about threats and the best techniques to face them, will make it harder for a cybercriminal to access your data



How Is It Different?

- Some (successful) cybersecurity expert skills simply cannot be taught in a traditional classroom. This is why **we always offer Modern vocational training and skills education programs** through interactive scenarios, "cyber arenas" where to simulate real cyber competition, and challenges to solve real-world business and human competitions
- **"Learning elements, contents, and skills" together.** Bringing together all the best cyber security and cyber intelligence elements, **from those who are doing it, those who did it,** and those **who learned from it,** and delivering to your organization
- CY4GATE Academy offers an innovative **method for assessment inside and outside your organization**



DIGILAB

Prepare Your Cyber Mission!

The DIGILAB is a strategic asset, dedicated to perform digital activities for platform and system analysis, vulnerability management, attack pattern engineering

Value drivers

Beyond the Academic Approach

The building up of a lasting capability on all the aspects of Cyber Warfare can hardly be achieved by traditional education & training which is useful for the creation of individual competences, but not sufficient to establish a permanent capability. So, also for this reason we have DIGILAB that integrates our Cyber Academy offering

Tailored around the Customer

Every customer has his needs and for this reason each DIGILAB is a unique mix of education, training, labs and continuous support for preparing customer's missions

Focused on Teamworking

Final goal of a DIGILAB program is to train all the teams (Penetration Testing team, Intelligence Team, Malware reversing and exploiting team, Reversing team, Crypto-analysis team and so on) to understand how to approach a cyber mission and identify the right tools for each specific task



How Is It Different?

- We own **full penetration testing and validation capabilities** against complex systems to check the HW, SW, firmware. Also the wireless level
- We create **laboratories** and services for **malicious code analysis** and define a valid counter-strategy
- We can **reverse engineer** things to catch how a **device or algorithm works**

CFO & IR MANAGER

Marco Latini

marco.latini@cy4gate.com

IR ADVISOR

CDR Communication

Silvia Di Rosa silvia.dirosa@cdr-communication.it

Luca Gentili luca.gentili@cdr-communication.it

FOLLOW US:

