CyberEvolution

LECS Appliance and LECS Embedded technology

An unique advanced NDR-IPS technology

" Cyber Security becomes useful when it is accessible "

2023

The growth

Certifications

ISO 9001

ISO 27001

To date:

- Among our clients in addition to numerous SMEs:
  - **International Manufacturing Companies**
  - **4 Major Multinationals**
  - **Public administrations**

- **97% of customers have renewed the subscription to date**

- **30% of customers have purchased another LECS**

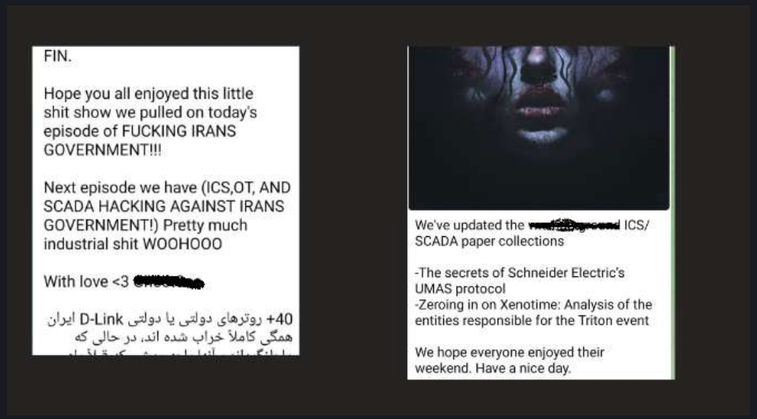
Presence in 10 main countries

Europe, South America, Arab Countries

Sectors and target markets where we are currently present:
currency, machinery manufacturers, automotive, energy, food, cosmetics, mechanical, hydraulic, production environments and supply chain...

CYBER EVOLUTION

Are Firewalls and Antivirus enough?



The Paradox

CYBER THREATS ARE ALWAYS GROWING IN NUMBER AND IMPACT

DESPITE

THERE ARE ALREADY SOPHISTICATED SECURITY MEASURES IN PLACE

The needs

95% of companies are “small”

+ 65%

is the growth of cyber incidents in Italy in 2023

+ 25%

is the growth of incidents affecting the Manufacturing sector

CLUSIT Report 2024 Data

LECS

HARDWARE VERSION

Embedded Version p.22

The solution

AUTOMATIC

- **No configuration required**
- Inspired aeronautics
- Network monitoring
- 2 in 1
- **Automatic daily updates**

INTERNAL

- Stealth approach
- Protects where other can’t
- Physical resilience
- Report all network errors
- It predicts anomalies

PROTECTION IT & OT

- Cyber Physical
- **Defends every type of device**
- Can be implemented in critical and/or industrial environments (SCADA etc..)

LECS

THE FIRST CYBER SECURITY **BLACKBOX PLUG & PLAY** IN THE WORLD

COMPLEMENTARY

Full integration and **compatibility** in any type of implementation environment.

Ministero dello sviluppo economico

Patented System

Made & Data in Italy

Compliance Support

NIST National Institute of Standards and Technology U.S. Department of Commerce

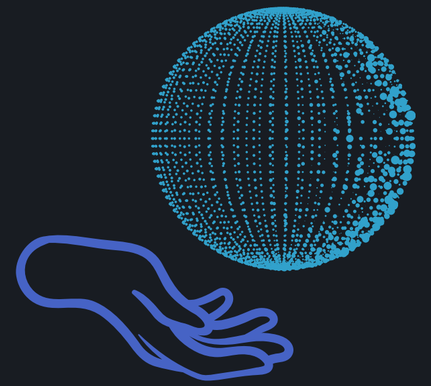
CE

CYBER EVOLUTION

Technology

LECS has the mission of
centralize and innovate the most complex technologies
used in areas
Aerospace and Military

Armored Blackbox



Making top-level approaches for Cyber Defense accessible to the entire and very large IT and OT market.

LECS

INSIGHTS FOR INSIGHTS
TIRESIA ENGINE

Embedded Version p.22

CYBER EVOLUTION

Network Deep Inspection

Definition:

Detailed **bit-for-bit** analysis of the contents of data packets passing through a network, not limiting itself to the header but **examining both packet payload and entire data streams.**

HEADER
+
PAYLOAD

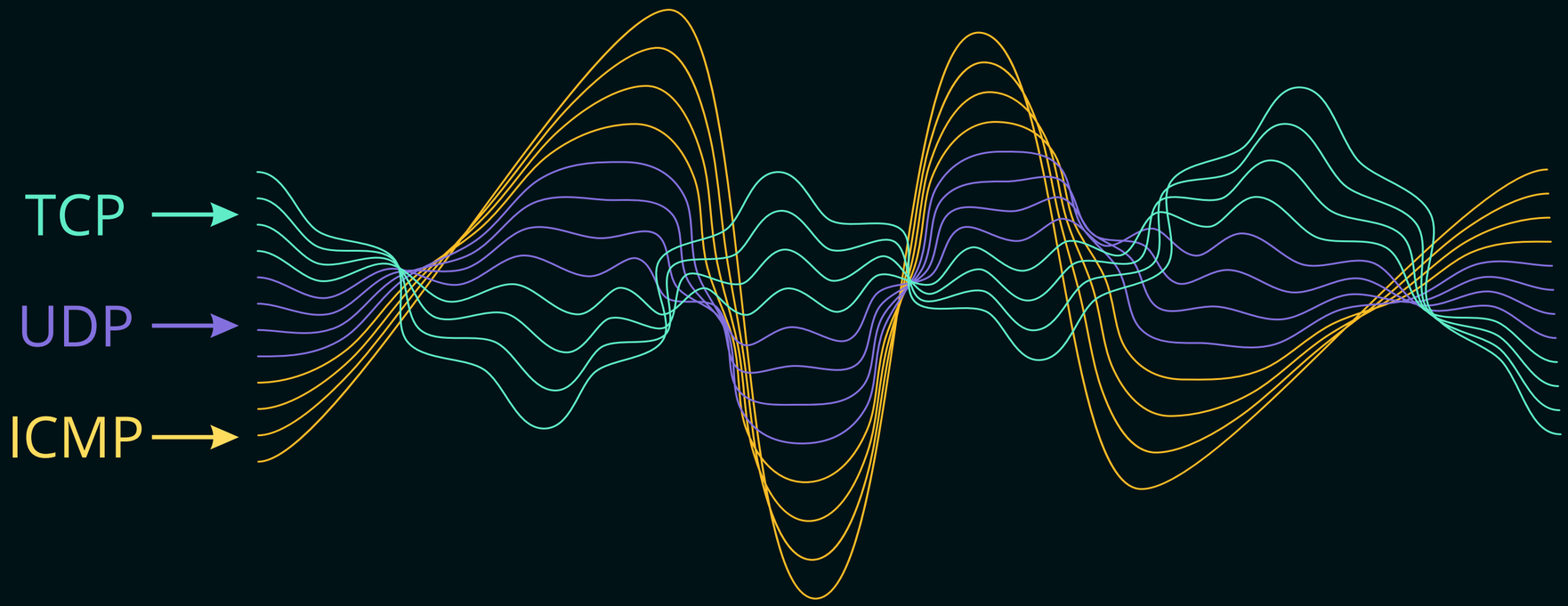
```
0000  d8 ec e5 5e ce 84 50 eb  f6 b9 7a 58 08 00 45 00   ···^··P· ··zX··E·
0010  00 29 fb 07 40 00 80 06  00 00 c0 a8 07 5b 8e fa   ·)··@··· ·····[··
0020  91 bc f6 73 14 6c 81 05  04 30 a3 3f 3b 40 50 10   ···s·l·· ·0·?;@P·
0030  04 00 e8 d5 00 00 00                              ·· ····· ···
```

IN-DEPTH
ANALYSIS

CYBER EVOLUTION

Technology

We use innovative techniques
beyond the current state of the art



We analyze the spectrum of the network, to capture morphological or entropic anomalies.

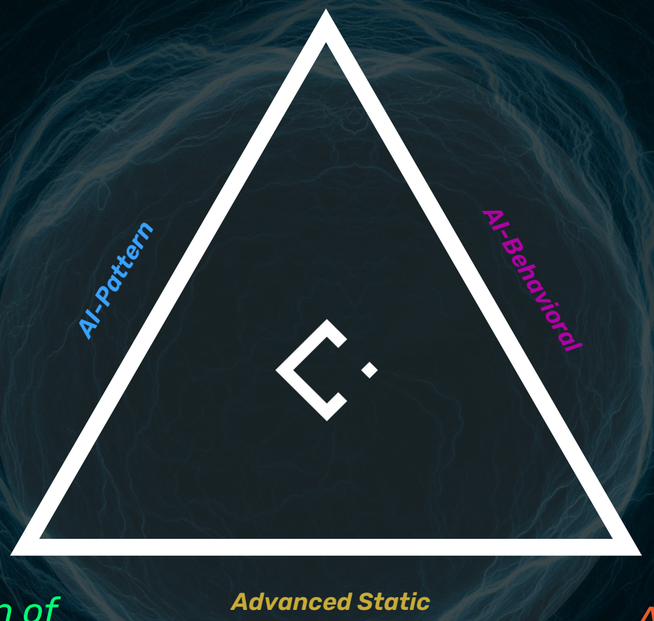
CYBER EVOLUTION

At Detection

By biunivocally combining all possible types of detection, we obtain a dynamic monitoring system optimized for the threat

AI Vision

Matching and Correlation for advanced DataAnalysis

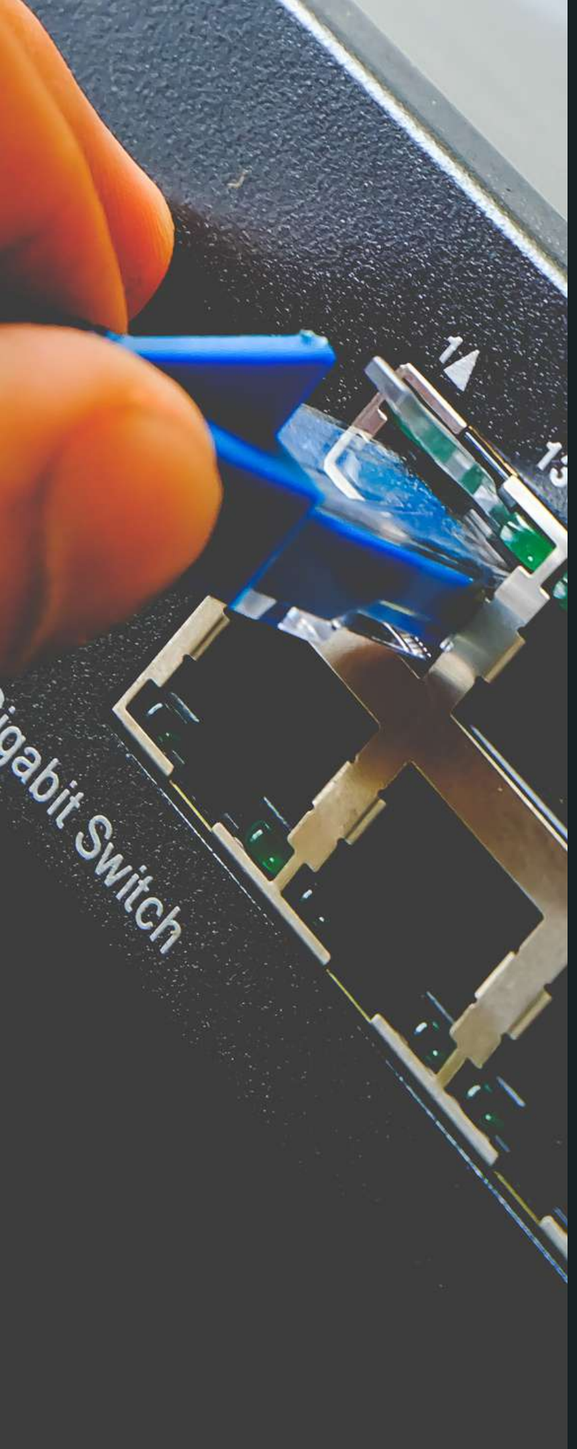


Pattern

Extremely fast match recognition of know threat

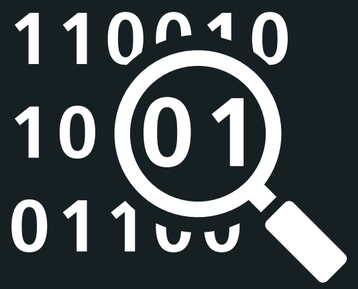
Behavioral

Awarded advanced statistic and mathematical algorithms for analyze traffic morphology



Not just safety

LECS, unlike other solutions, has the ability to carry out checks relating to the infrastructure, becoming a debugging tool for the network.



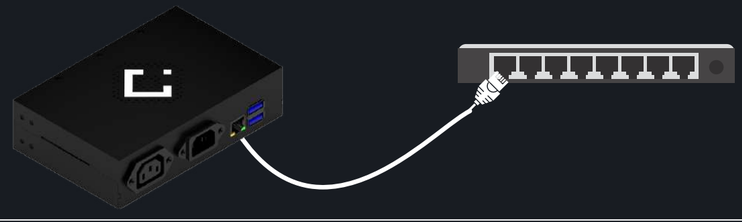
With bit-by-bit analysis, LECS also monitors the vital parameters of the network highlighting
delays, flow errors, broadcasts, unstable connectivity.

👇

All in the same Dashboard.

Installation in 10 minutes

1) **Connect it:**



2) **Register it on the platform**

3) **You have completed the installation**

LECS has already activated:

Network defense < > **Network control**

LOG notarization

with private Blockchain technology to improve threat tracking and better support certifications and regulations

Legal and assurance.
as 62443, GDPR EU, ISO and many more.

CYBER EVOLUTION

Protection and dynamic responses

OPTIONAL: AIR-GAP COUNTERMEASURE

If connected, it acts electrically via cyber-physical actuator to create a real isolation bubble, as per critical procedures.

AUTOMATIC DEFAULT COUNTERMEASURE

Procedural software threat mitigation techniques, implemented automatically and without human interaction.

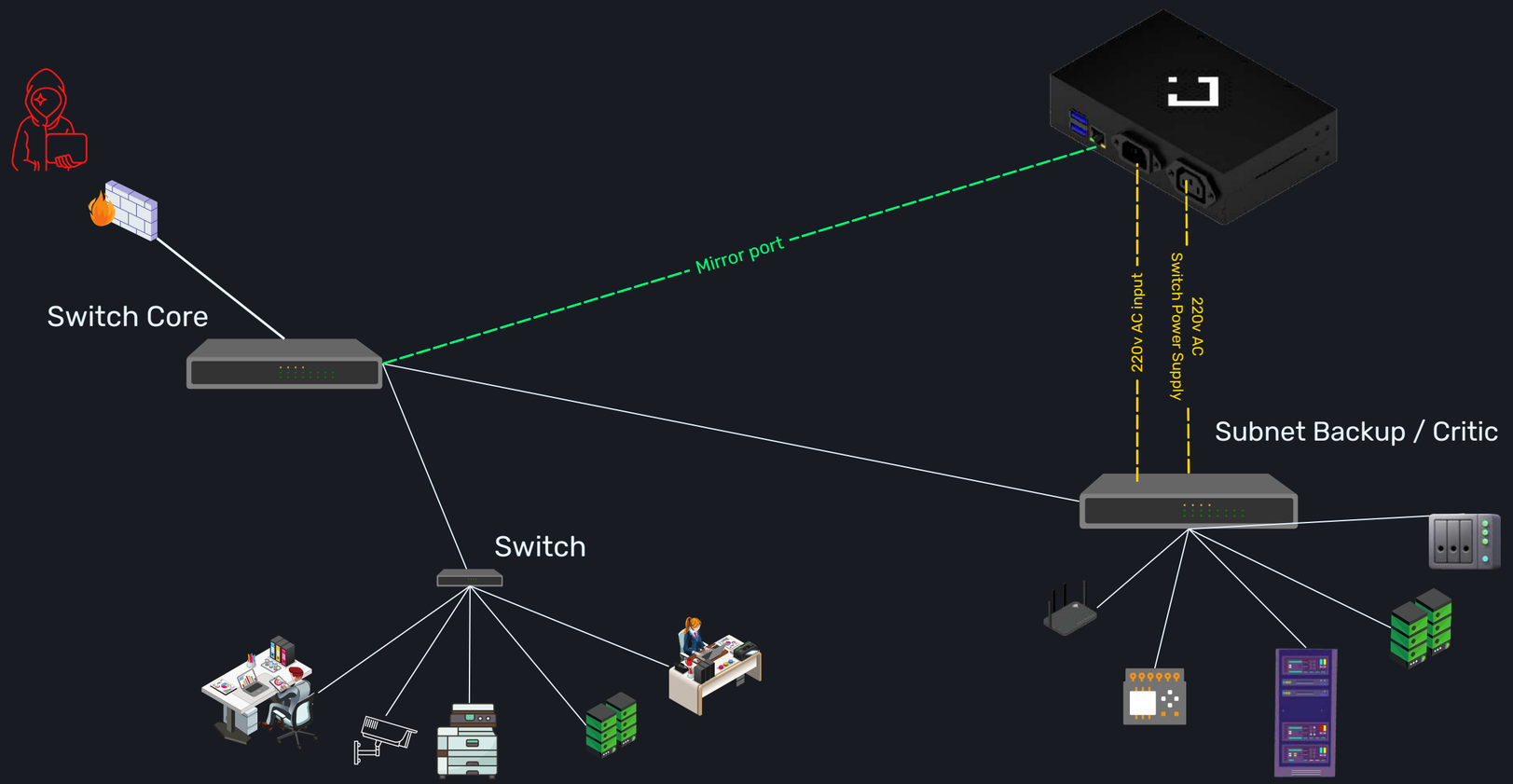
LECS works on multiple levels of the ISO/OSI stack to deal with different types of threats and without sending "commands" to other appliances.

SPECIFIC CLASSIFICATION TRIGGER

In the event of particular anomalies, LECS begins to perform more detailed monitoring of particular and noteworthy movements.

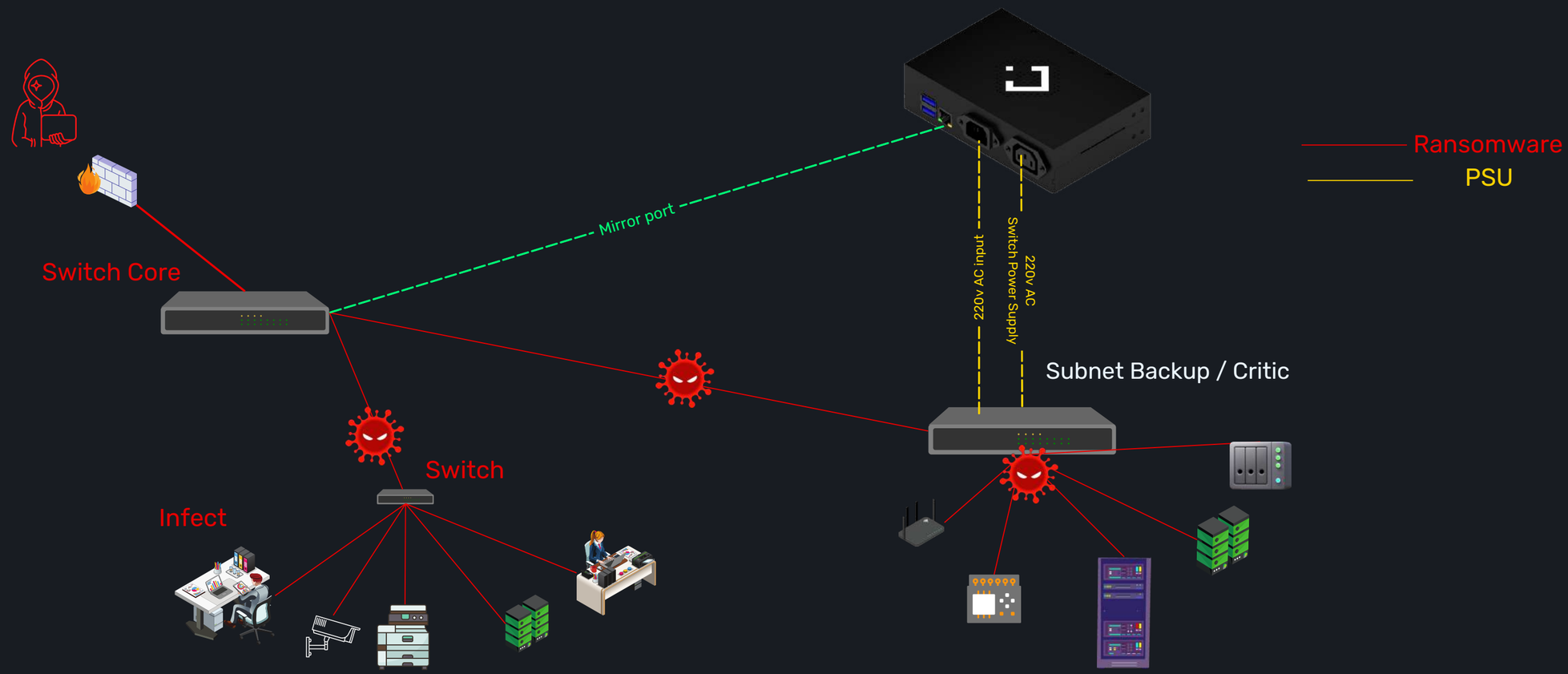
The system responds in a calculated and measured way to the type and severity of the threat almost instantaneously

Countermeasure: Initial State



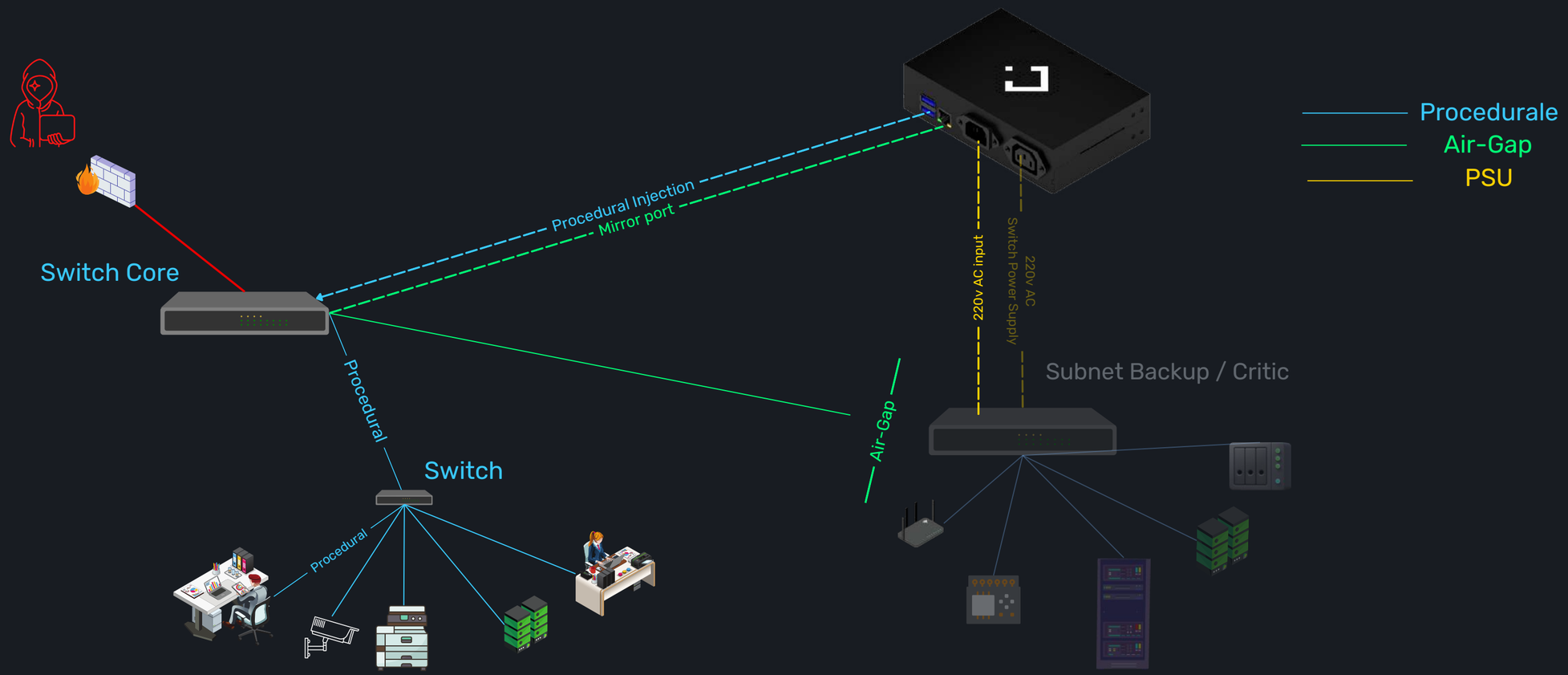
This is an example wiring diagram of LECS.
DIfact it is mounted as a detection in the Core and as an Air-Gap countermeasure on the backup switch.

Countermeasure: Without LECS



During an attack, such as ransomware, the myanccia starts performing lateral movements to infect new hosts and perform data exfiltration.

Countermeasure: WITH LECS

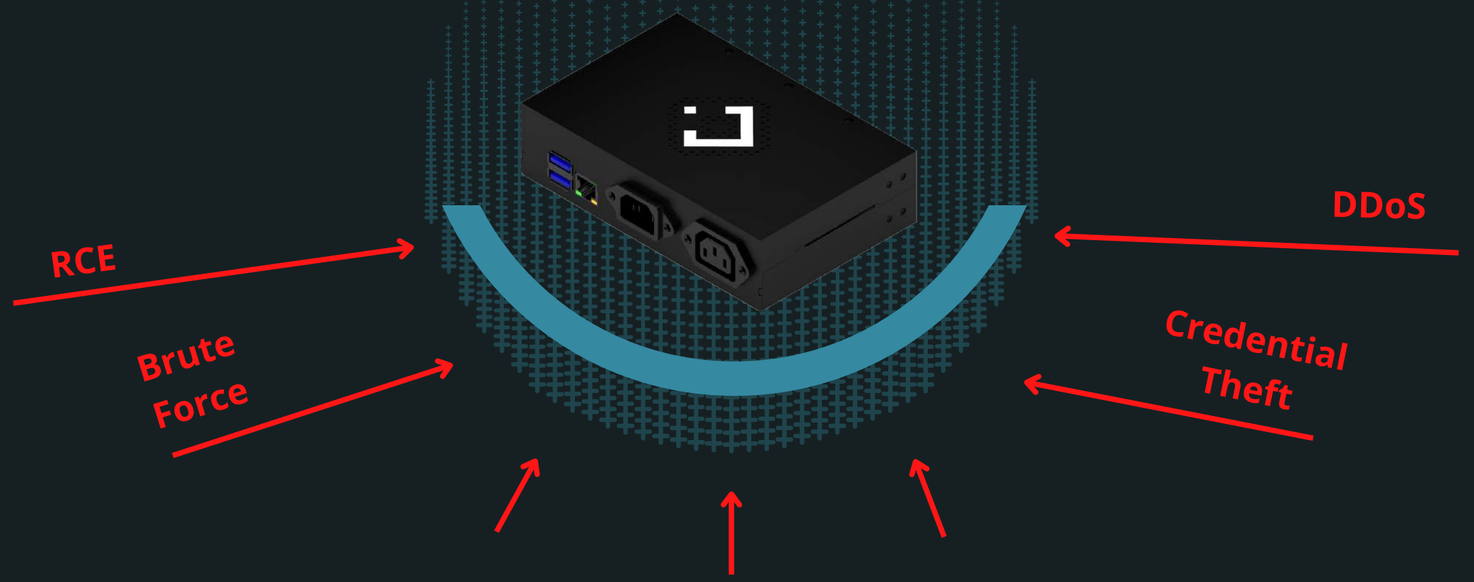


The DOUBLE intervention of LECS, allows in this case to reach both the switch hosts with hosts and to put the critical backup system in Air-Gap mode.

Aeronautics-inspired technology

Black box

LECS is not directly attackable, unlike other configurable systems that often expose PPS, such as firewalls or other ecosystems



It behaves like a real black box with the addition of active countermeasure actions:

Analyze Record Act

MULTI-LEVEL NOTIFICATIONS

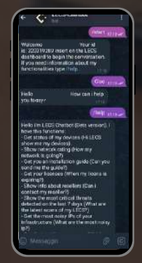
Visualization
simplified with chat

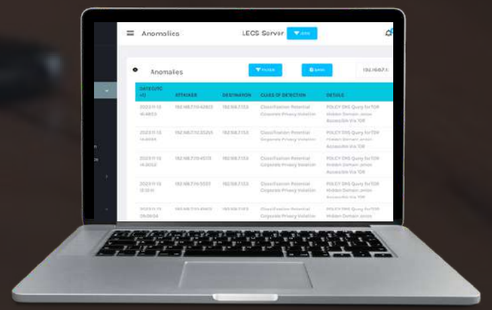
Automatically highlights key events.
It uses a natural language interface, the first in the world for this field.

Advanced level
multi - tenant per
IT/OT Manager

It goes deep into the network, allowing the SOC/NOC manager to monitor every technical and debugging aspect.

The first system in the world interfacing with *natural language*





Blockchain

Logs are highly resilient, as they are written and encoded in dedicated memory areas

Thanks to DLT's unique algorithms, it ensures with mathematical certainty that the LOG content is unchanged

Why?

Compliance and Security supporting aspects

legal, insurance and banking.

Es. 62443, GDPR EU, ISO and many more.

AWARDS:

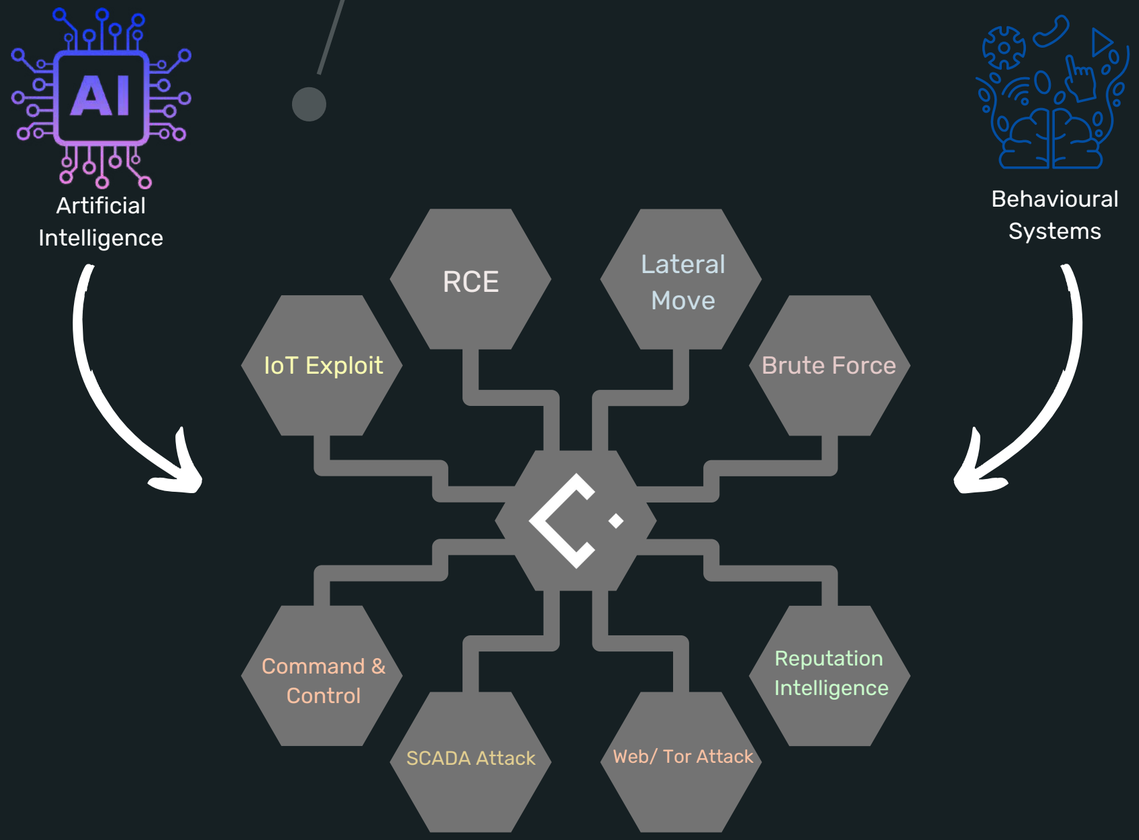
Award technology for thesis at Politecnico di Ancona with honor mention.

Competitor & LECS

Features	Competitor	LECS
Implementation	Required configurations	Plug&Play, nessun know how richiesto
Costs	High, suitable for a limited market	Contents, scalable from SME to Corporate
Hardware appliance approach	Appliance to configure and expensive. Possible remote control	Armored black box approach, inspired by aerospace technology. No services exposed or needed
Learning and detection	Required for AI	Not required, 3 different detection engines
Response to threats	Software	From procedural software to AirGap CyberFisico with patented procedures
Network Debugging functionality	NO	Yes, native specific system for net Infrastructure debugging
LOG integrity	Locale/Cloud	Highly resilient cloud and local with DLT Notarization (honorable mention at Politecnico AN)
False positives	Many, being based entirely on AI	Thanks to the triple engine, false positives are almost non-existent

CYBER EVOLUTION

DETECTION INFOGRAPHIC



RCE / Attack / Malware

Thousands of supported services and vendors
With many and updating CVEs > 9 CVSS Score

- SMB
- DNS
- FTP
- Laravel
- QNAP
- SolarWinds
- Various DBMS
- Microsoft Service...

- **Powershell**
  - Lateral Movement
  - Weel-Know base64 Command-Invoke
  - C2C
  - Kerberos

- **SQL Injection**
  - MSSQL
  - MySQL
  - noSQL
  - ..Other DB

- **Malware**
  - Adware_PUP
  - Loader
  - Various Payload [doc,pdf, Java..]
  - IOC of APT [Advanced Persistence Threat]
  - Many more...

- **IoT Exploit**
  - Router
  - Firewall
  - IP Camera
  - A lot of Network device...

- **Weak Credentials/ Config**
  - Default login
  - Clear traffic
  - Weak TLS/SSL
  - Many more...

- **Brute Forcing**
  - Dictionary Attack
  - Pure Brute Force
  - Mask Attack
  - SMTP Brute...

Network Recon Category

Hundreds of detectable attack categories, and Gathering Ops in different classification:

- Stealth Scan
- Aggressive Port Scan
- OS Fingerprinting
- Service Scan
  - Service Enumeration
  - Port triggering
- Slow Scan
- Fragmented Scan
- Kerberos
- Intra-Extra Net Conn. [TCP,UDP,SNMP..]
- Many more...

- **Industrial Scan - SCADA**
  - Modbus
  - SIEMENS
  - PcVue
  - DATAC...

Some Example:
- Mirai scan
- Tool: Zmap, MassScan, Hydra...
- Malware: Varius Ransomware scan
- HTTP Verbs
- UpnP Scan, VoIP....

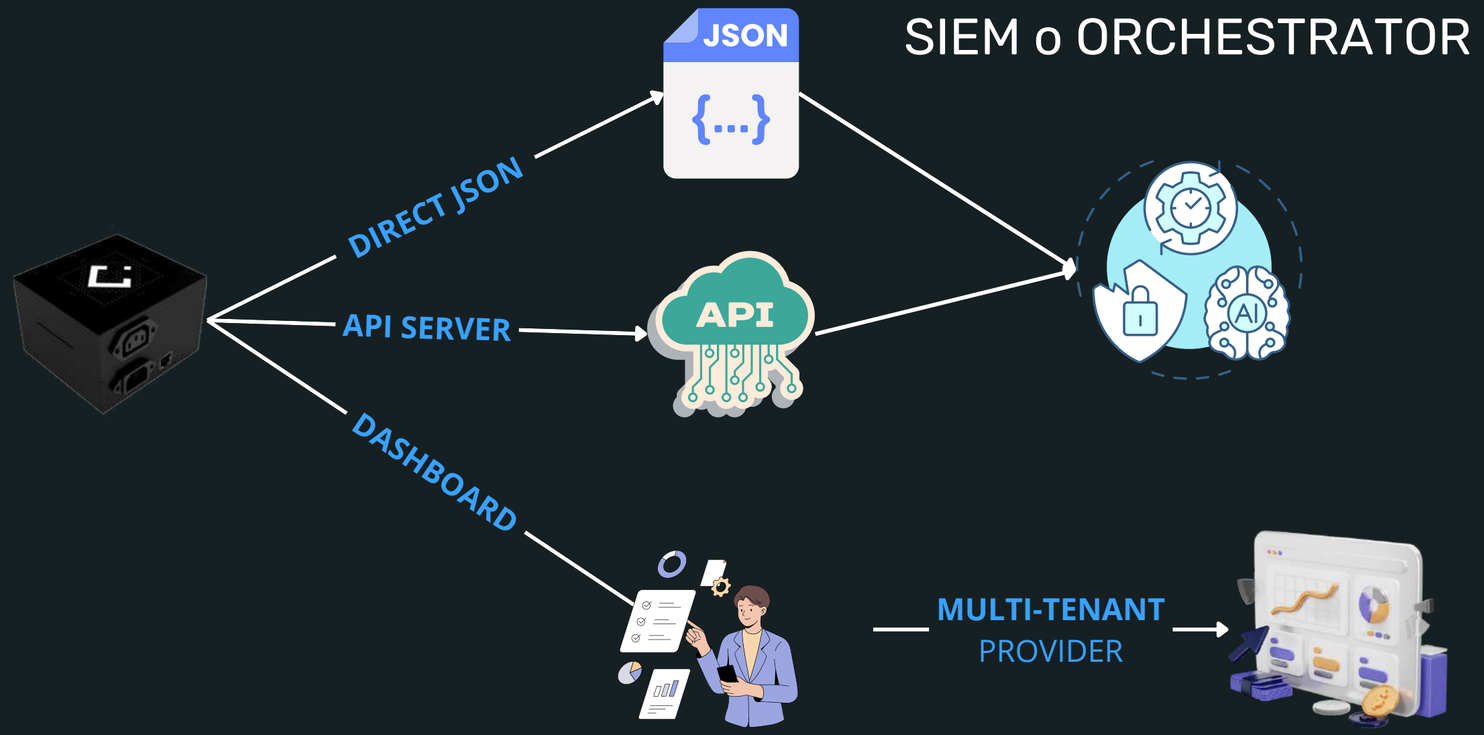
DOS Attack

- GreatCannon
- LOIC
- Flood [NTP, HTTP...]
- IRC Based...and many

CYBER EVOLUTION

Integrations

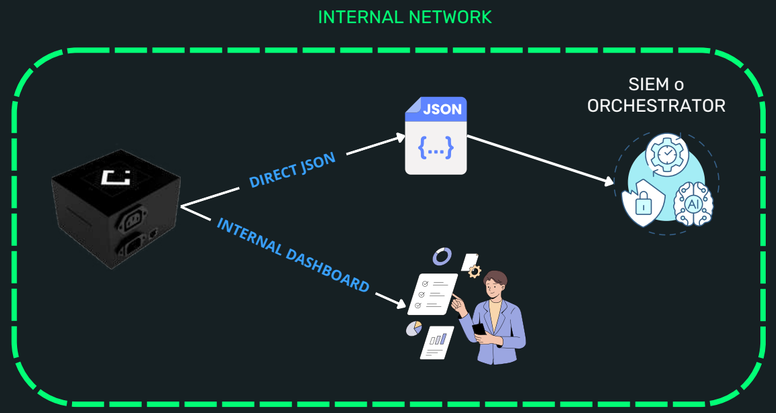
LECS, being a technology by nature, allows you to interface with third parties via API or sending data in JSON to SIEM/SOAR systems



Critical Environments

Extremely versatile stand-alone technology.
It does not require an Internet connection or software and
uses an internal server for viewing security LOGs and notifications with support for existing SIEMs.

Updates and features:
manageable completely locally



INTERNET NOT REQUIRED

AGENT SOFTWARE NOT REQUIRED

MARKET AND VALIDATION

LECS Business

Excellent for small companies with few network nodes.
Software procedural countermeasure.
Compact design with anodized aluminum body.

LECS Plus

Excellent version for medium-sized companies.
Equipped with procedural and hardware countermeasure.
Cube design with alloy body.
Shucko IEC13-14 220v sockets

LECS Enterprise

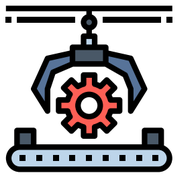
Ideal for medium-large companies.
Supports more hosts and traffic bandwidth than Plus.
Design for 1 U and a half U rack.
Supports industrial protocols
Procedural and hardware countermeasure with Shucko IEC13-14 220v sockets

LECS Core

Perfect for rack deployments with multiple switches and separate logical networks.
Supports countermeasures and detection on 3 ports.
Capacity 7 times greater than the Enterprise.
Supports ICS protocols.
Multi-port procedural countermeasure.
4 port of 2.5 Gb/s

LECS Virtualized

Virtualized version of LECS engines.
Possibility of custom versions with Docker.
Deployable directly as RAW disk in many operating environments such as VMWare and Hyper-V and many others.



LECS Embedded

Custom version built to measure on the customer.
Features unique integration features based on the environment and customizable cyber-physical responses for OT environments.

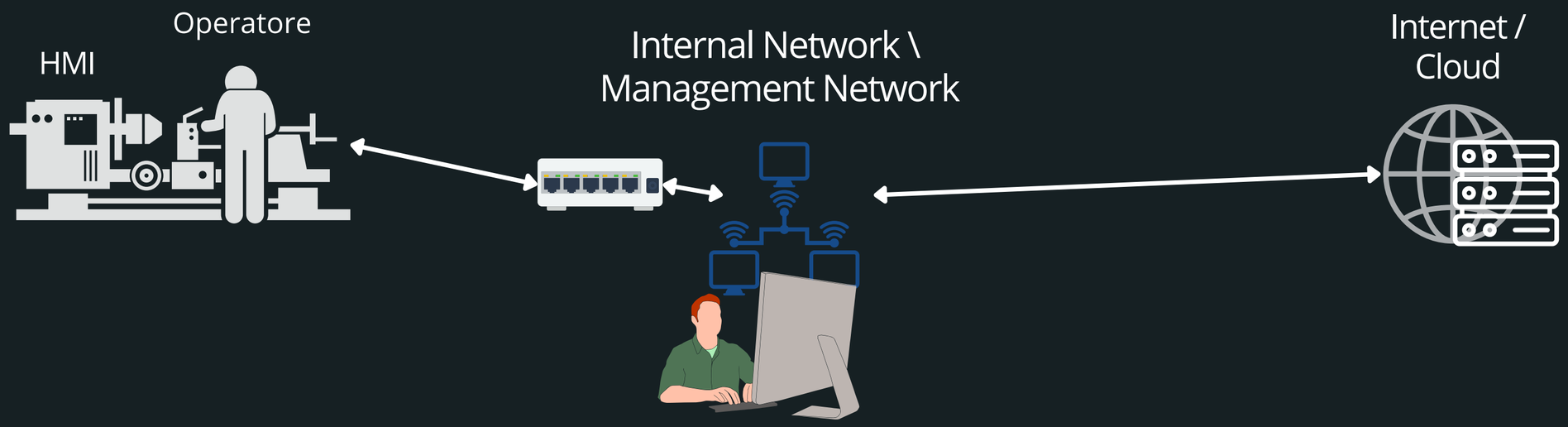
IT segments

Industrial Segments/ICS

LECS

VERSIONE
EMBEDDED

PoV di un **utente**



Industria 4.0 (connessa)

PoV di un **attaccante**

Rischio

HMI
Comrpomessa

Cyber Fisico

Pivot

Network Attack

Network attack

PPS
esterne

Phishing

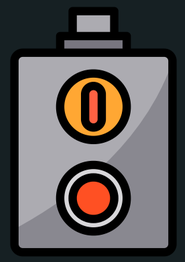
Download
malevoli

Spear phishing /
Whealing

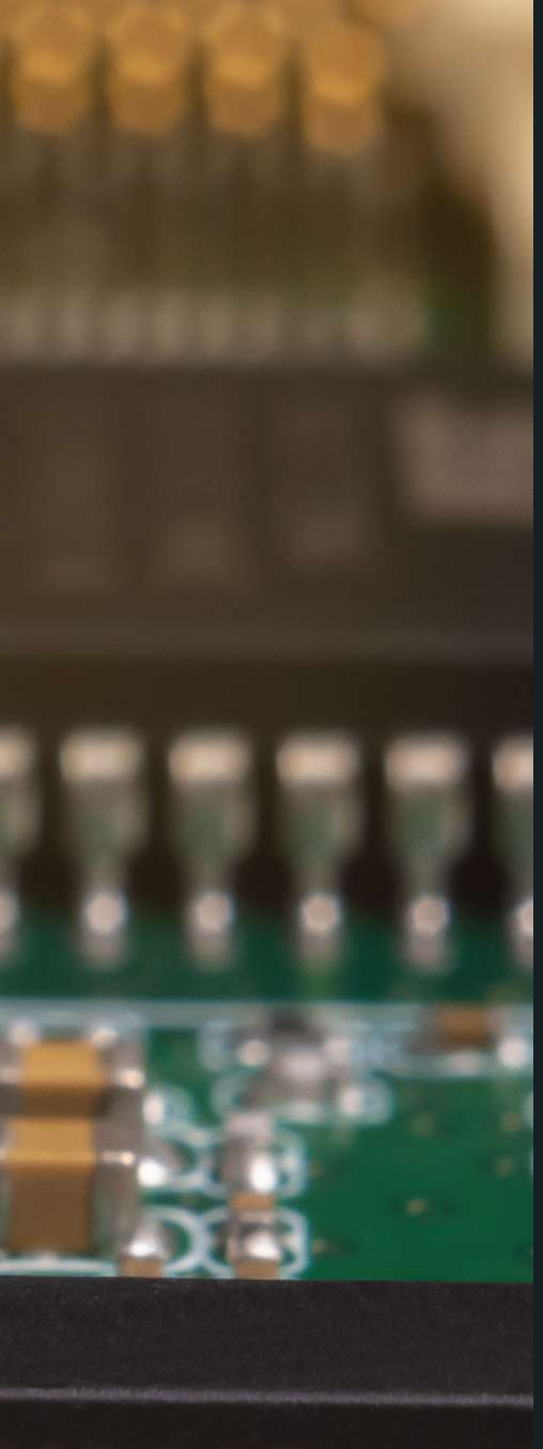
Protection touches reality

LECS uses cyber-physical actuators to:

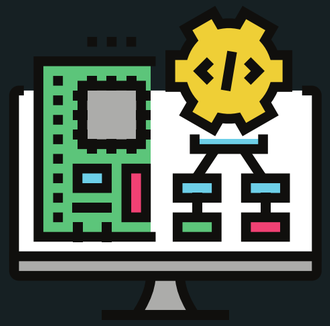
- Block the cyber threat
- Safeguard the machine and interfaces thanks to real actions
- Safeguard operators from physical accidents



It acts physically at any level, intervening promptly based on the type of machine or infrastructure.



What is LECS Embedded



Cyber-Protection Algorithms
specific for Industry and IoT

Multi-HW

arm32 arm64 x86
x64...

Multi-SW Edge

Container Local Virtualization
and much more

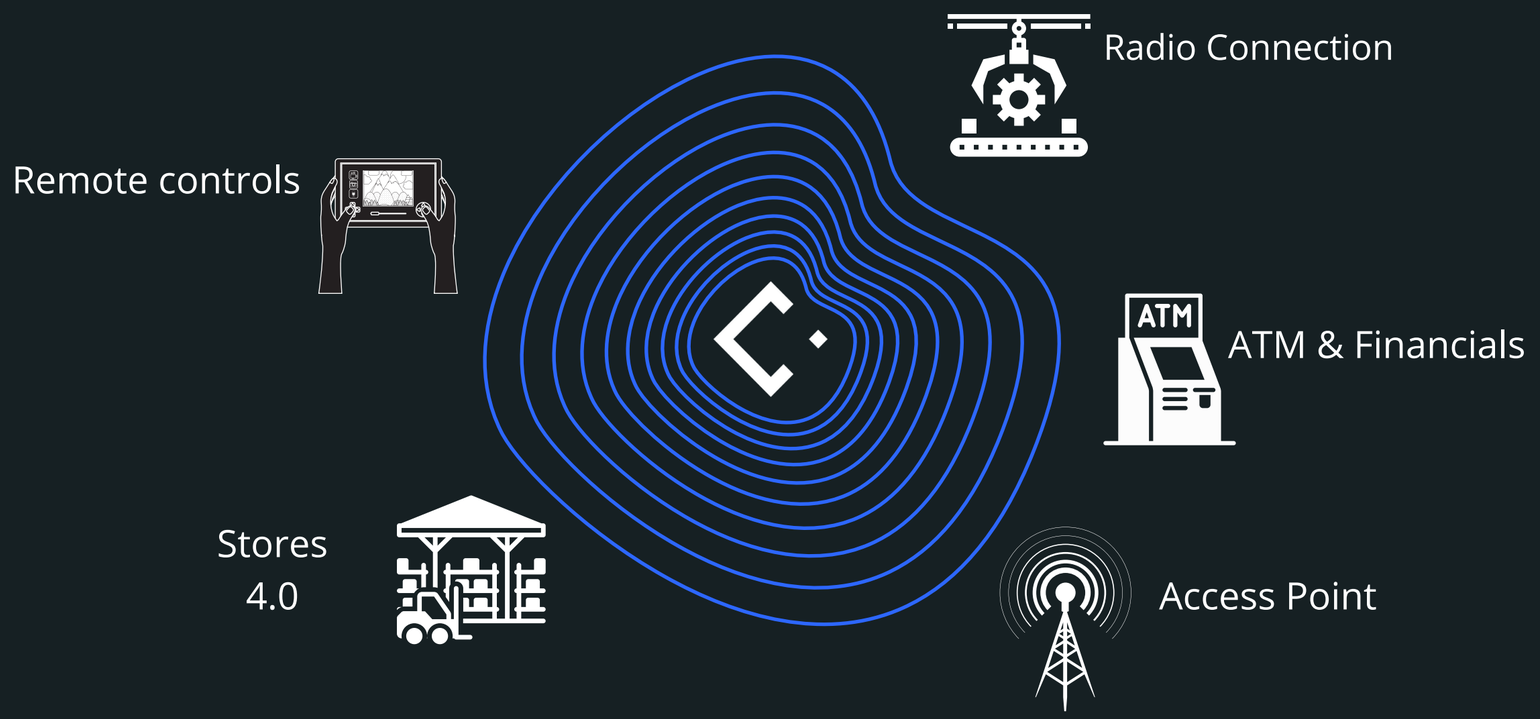
Backend

Integration
servers and/or digital
services already present

CYBER EVOLUTION

Versatility

LECS also protects what is connected by radio frequency



Many technologies supported from 802.11 to Low-Frequency

Main Awards

Winner at ForwardFactory 2022 with important Corporate and Cassa Depositi e Prestiti

Gestore e Co-investitore: GELIFY
Ecosystem Enabler: Manufacturing, INDUSTRIO
Ecosystem Enabler & Investitore: auxiell, AZIMUT LIBERA L'IMPRESA
Corporate Partner & Investitori: Angelini Industries, comer industries, scm group, VIS, POGGIPOLINI
cdp Rete Nazionale Acceleratori

Winner at Global @Zurich

kick» start

ITALIAN LIFESTYLE
Acceleration program in Florence
WINNER
PROMOSSO DA: INTESA SANPAOLO INNOVATION CENTER, nana bianca, FONDAZIONE CR FIRENZE

enterprise europe network

The best startups @EU Prague

> Litokol with its Information Systems has been a testimonial for Confindustria Emilia-Romagna and Unindustria Reggio Emilia, partners of the startup Cyber Evolution. The startup's solutions in the field of Cybersecurity have met with considerable success and have represented Italy together with other excellences in various fields of application.

TIM
Selected by TIM as one of the top 6 Italian companies out of 100 operating in cyber security during the TIM Cyber Challenge competition

Partner:
eit | European Institute of Innovation & Technology

890 k€ Granted Found for LECS technology and related product

300k€ VC Round Investing
First Round completed.

Selected to represent Italy in the main innovation fairs in the world.
Gitex, CES-USA, VivàTech and H. Messe

Hidden Treasures Cyber Security 2021 SWG – Startup Wise Guys Estonia as best B2B Italian Cyber Security

Masters & Institutional Summits Testimonial as successful technology to Master and Events as ITASEC21, Rome Security Summit

Italian Angels for Growth
Winner Italian Business Angels for Growth 2020 @ WMF2020

Several Institutional Awards from Italian Governments

POLITECNICO DI MILANO
Finalist Ai4Gov 2022 AI contest in Governmental Env.

REAL CASE with LECS