

CyberEvolution

LECS Technology

" Cyber Security becomes useful when it is accessible "



Company & Brand

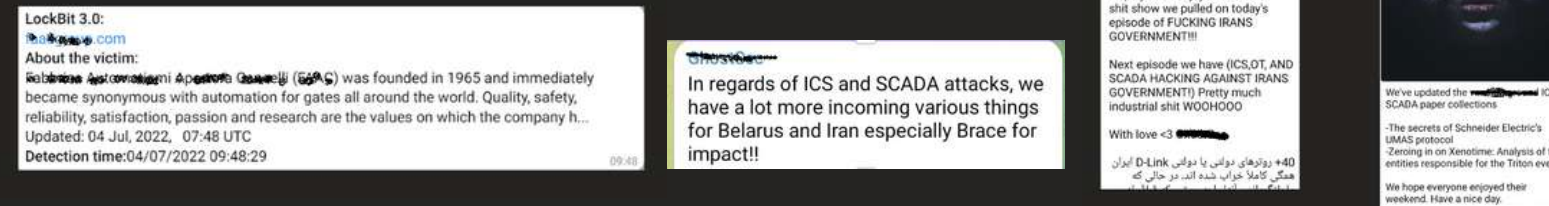


- **Company:** To date, it has 3 locations:
 - 1 **production** site
 - 1 location for **research and development**
 - 1 location for **administrative offices**
- **Team:** **Multidisciplinary** team with Cyber Security focus, Researchers, Software Engineers, Penetration testers, developers.
- **Experience:** thanks to our team's know-how and more than 10 years' background in cyber security, we have been successfully providing high-tech solutions to enterprises, industries, professionals and public administrations for more than 5 years.
- **Mission:**

*"Innovating the future of Cyber Security,
providing an accessible, automatic and universal response."*

The Problem

Reality



Real screens from our R&D of criminal organisations targeting critical infrastructure

CYBER THREATS ARE ALWAYS GROWING IN NUMBER AND IMPACT
DESPITE
SOPHISTICATED SECURITY MEASURES ARE ALREADY IN PLACE

What is the issue?

Current defense systems are not sufficient and are
too complex to install and maintain, thus leaving significant protection holes

Reasons

Unsecured networks by structure

Costs, implementation time, and complexity

Entire supply chain vulnerabilities

Are required Specific and advanced skills required

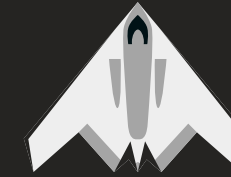
Automatic



- **No configuration** required
- Inspired by **blackboxes** used in aeronautics
- Network Monitoring and Classification
- 2 in 1 **Network Debugging & Security** Checks
- **Automatic** daily updates

The solution

Internal



- **Stealth** and **interior** point of view
- It **protects** where **firewalls** and **EDRs** cannot
- **Physical resilience** for LOG
- **Reports** all network errors
- Makes **prediction** of anomalies

Protection IT & OT



- Unique **Energy Countermeasure**
- Defends **every type of device**, from IoT to Server
- Implementable in **critical** and/or **industrial** environments (SCADA etc.)
- **Simplifies** Cyber Security Management

LECS

THE FIRST
CYBER SECURITY
BLACKBOX
PLUG & PLAY
TO THE WORLD.

Complementary



Full **integrability** and **compatability** in any type of implementation environment.



Made & Data
in Italy



For Industry
4.0

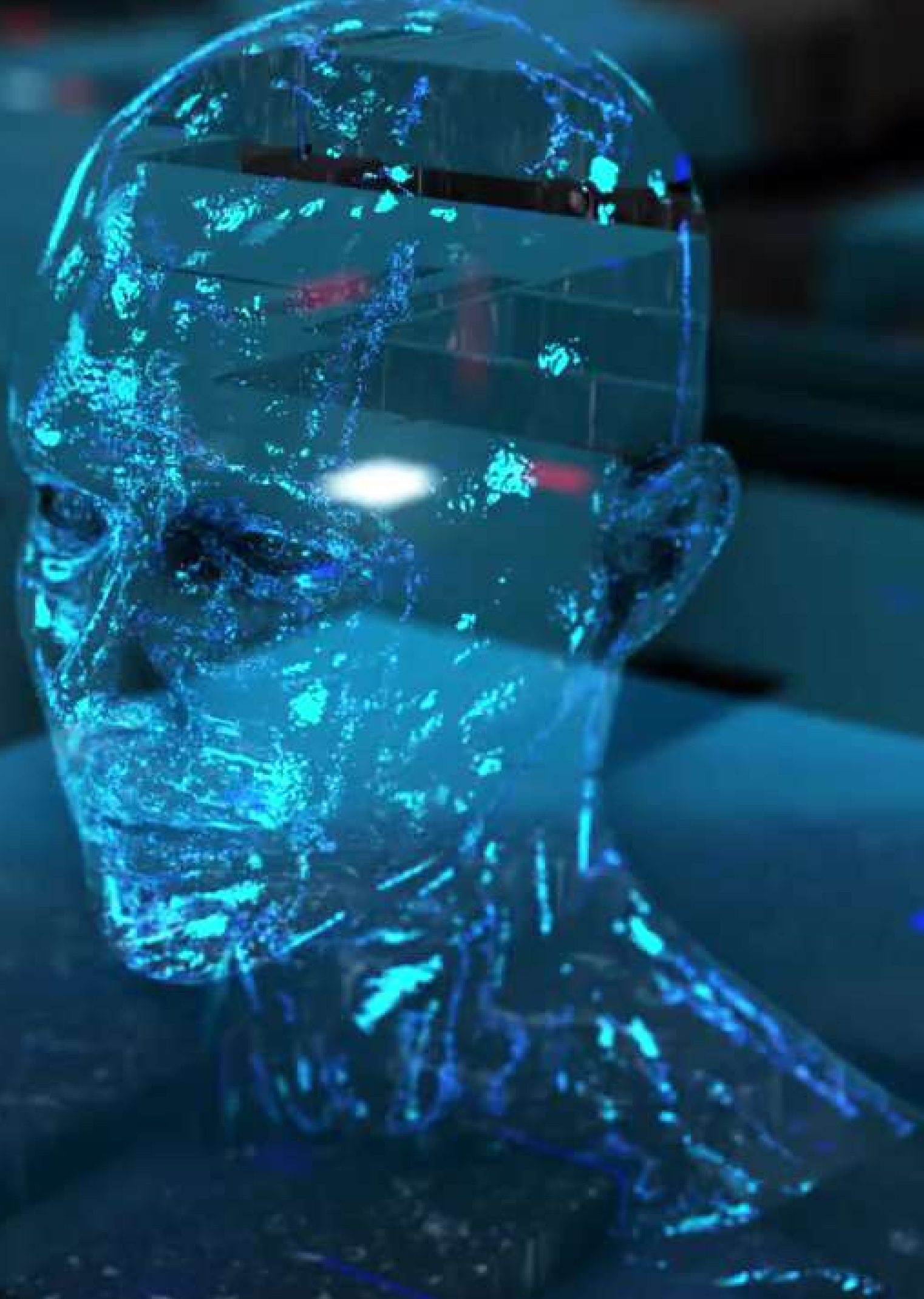


GDPR/16



Compliance Support

Tiresia Engine



Technology

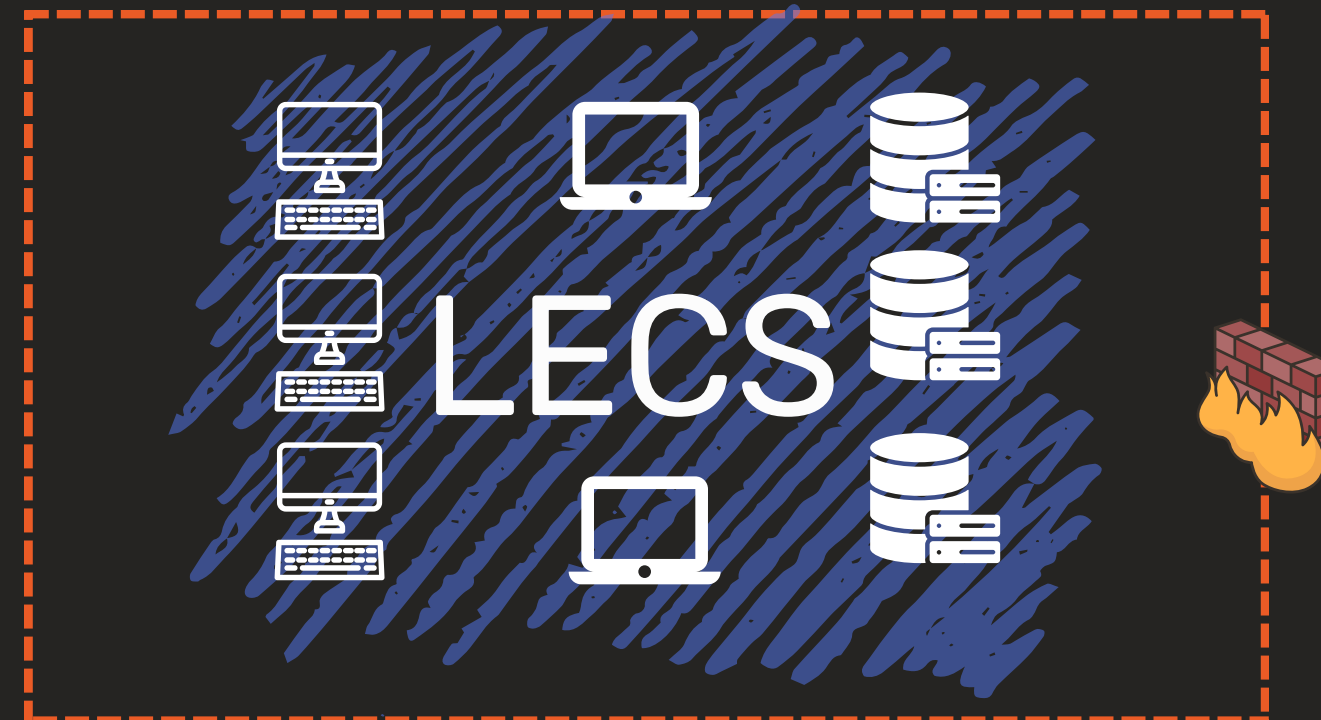
Tiresia Engine

Not only Artificial Intelligence.

We use a concatenation of 3 different POVs and different engines for the same threat thus succeeding in performing advanced detection of dangerous and invisible lateral movements.

*Protection where **firewalls** and **antivirus** cannot.*

we cover the entire surface of the net, not just the perimeter,
providing comprehensive protection,
even in the "darkest" and hidden areas where threats proliferate most.



Legend:

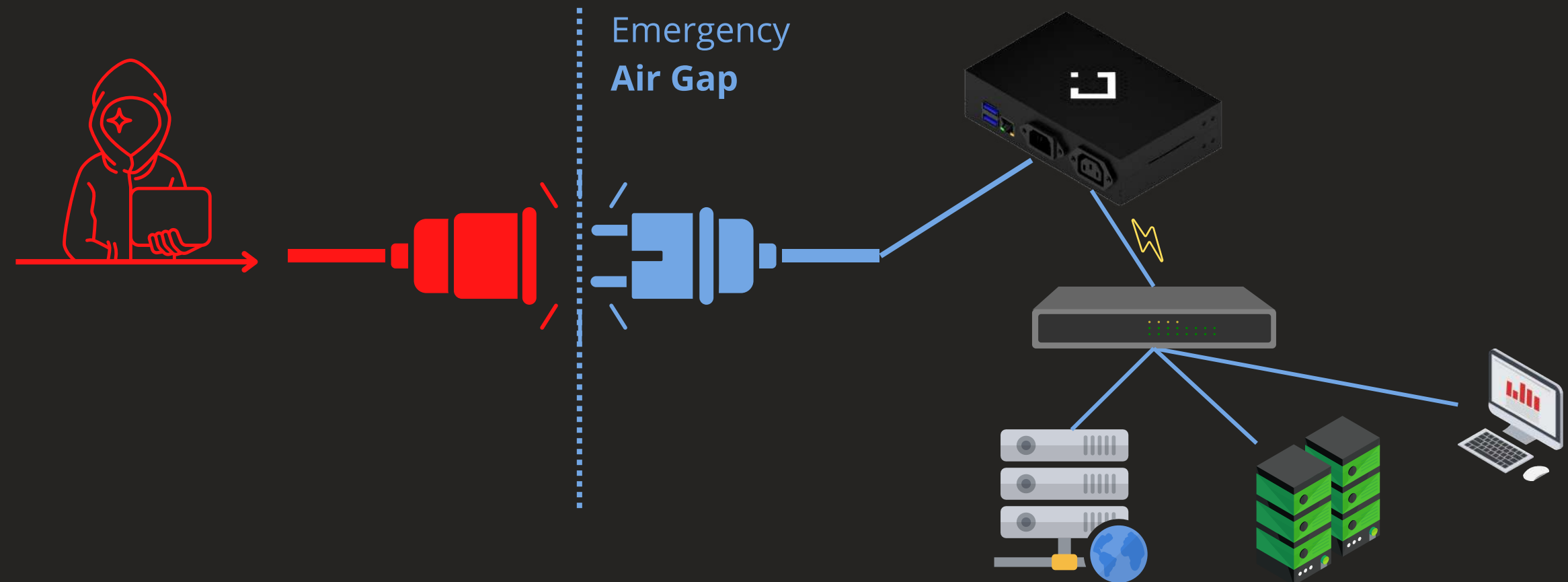


Firewall
Perimeter protection
only

LECS
Protection of the entire
surface and all devices
inside

Physical Defense

In case of **extremely dangerous** attacks such as **data exfiltration on C2 servers** or a **ransomware attack**, LECS can **armor** an entire network in the most secure way possible using an automatic electrical actuator as an **alternative** to a **software procedural** system.

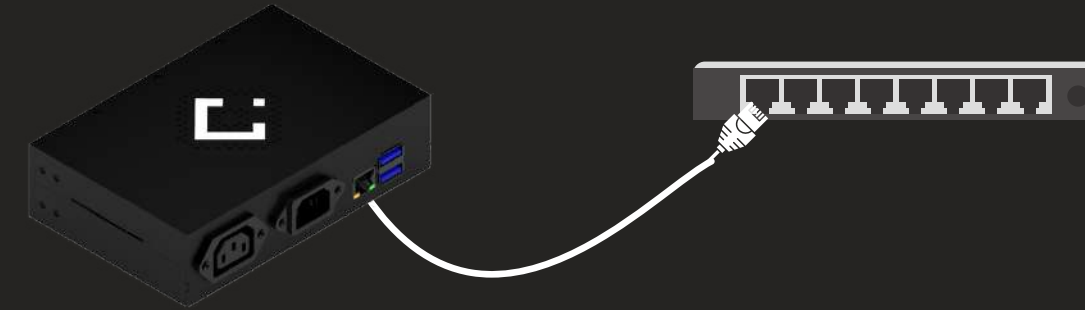


That's cause threats arise to make bypasses of EDR systems, perimeter, and/or shut down security services.

The only way to block them, is to act rapidly and concurrently.

Installation in 10 minutes

1) **Plug it in:**



2) **Register it on the platform**
in 3 minutes



3) **You've completed the installation**

LECS has already activated:

Network defense

- 24/7 monitoring
- Protection of all devices
- Prediction of attacks
- Active countermeasure



Network control

- Checking network problems
- Online device control
- Network behavior analysis
- Automatic updates

Notarization

Of LOG events with private blockchain technology
to improve threat **tracking** and better support **certifications**, **regulations**, and is also useful
for **insurance** purposes.

NOTIFICATIONS


Time is precious.

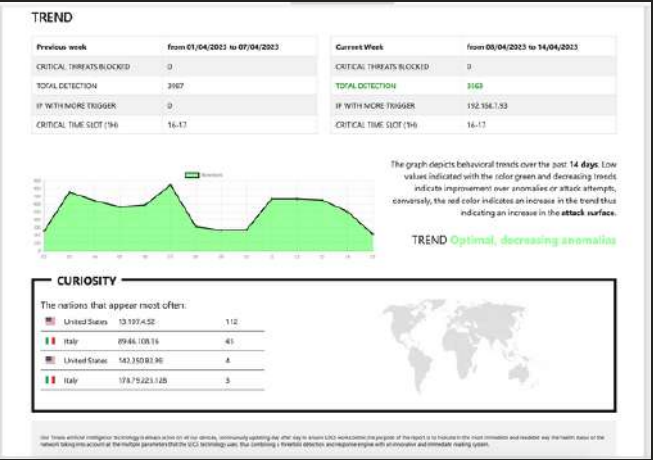
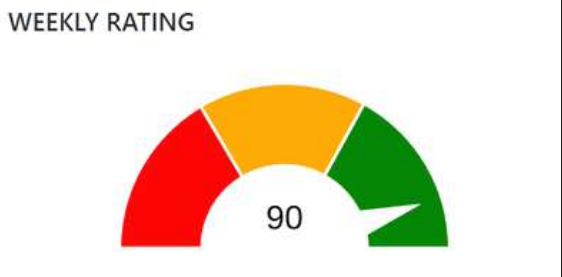
That's why the notification and dashboard system
is completely automatized
in order not to waste it

SECURITY, COMPRENSIBLE

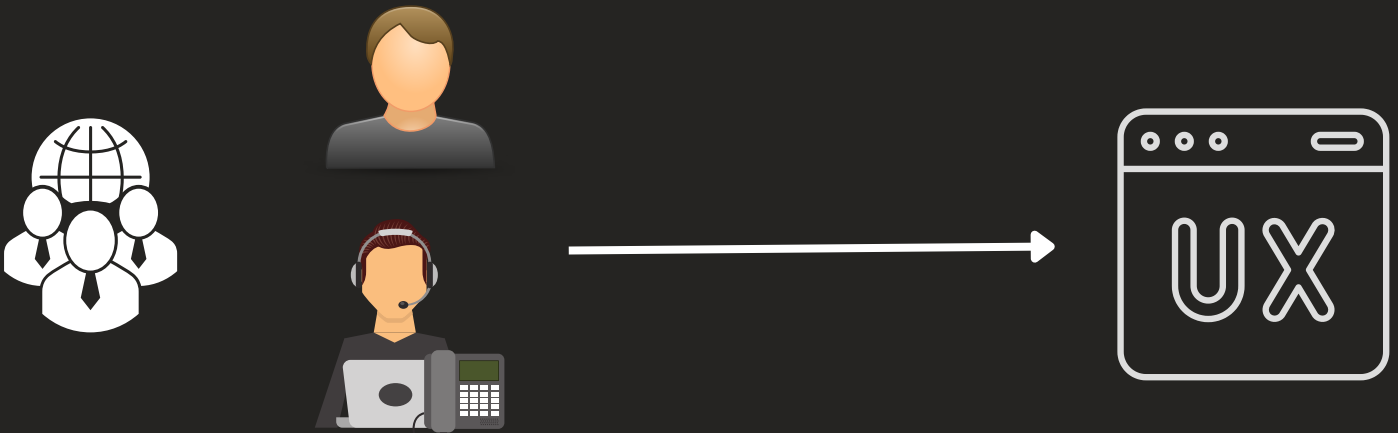
1° in World
The user can interact direct
with **LECS**.
In the easiest way possible.




Report for every
people.
Easy readings

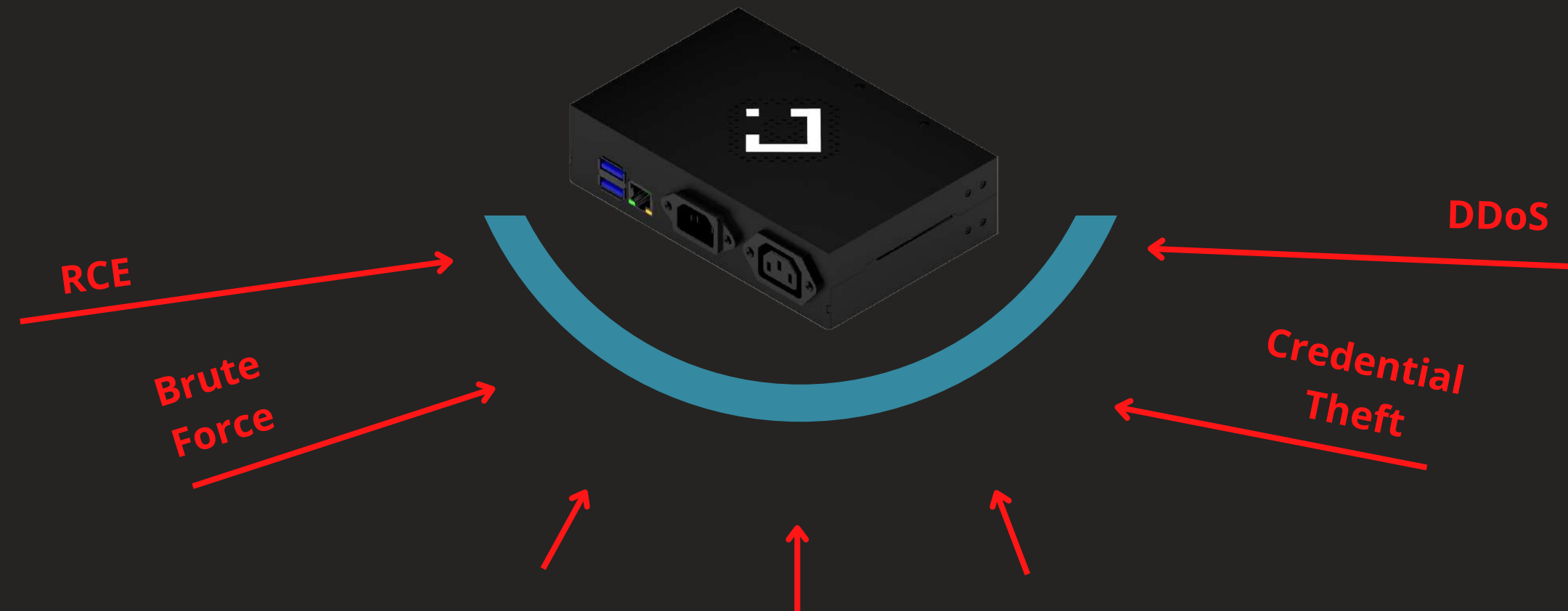


Multi-tenant



The Blackbox Approach

LECS **non è direttamente attaccabile**, al contrario di altri sistemi configurabili che spesso espongono PPS, come i firewall o altri ecosistemi



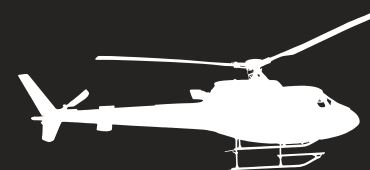
It acts like a real black box with the 'addition of active countermeasure actions:

Analyze
Record
Act.

Critical Systems

If implemented in
Strategical or Crytical enviroments,
LECS has the advantage of
being **completely stand-alone**
not slowing down the network flow

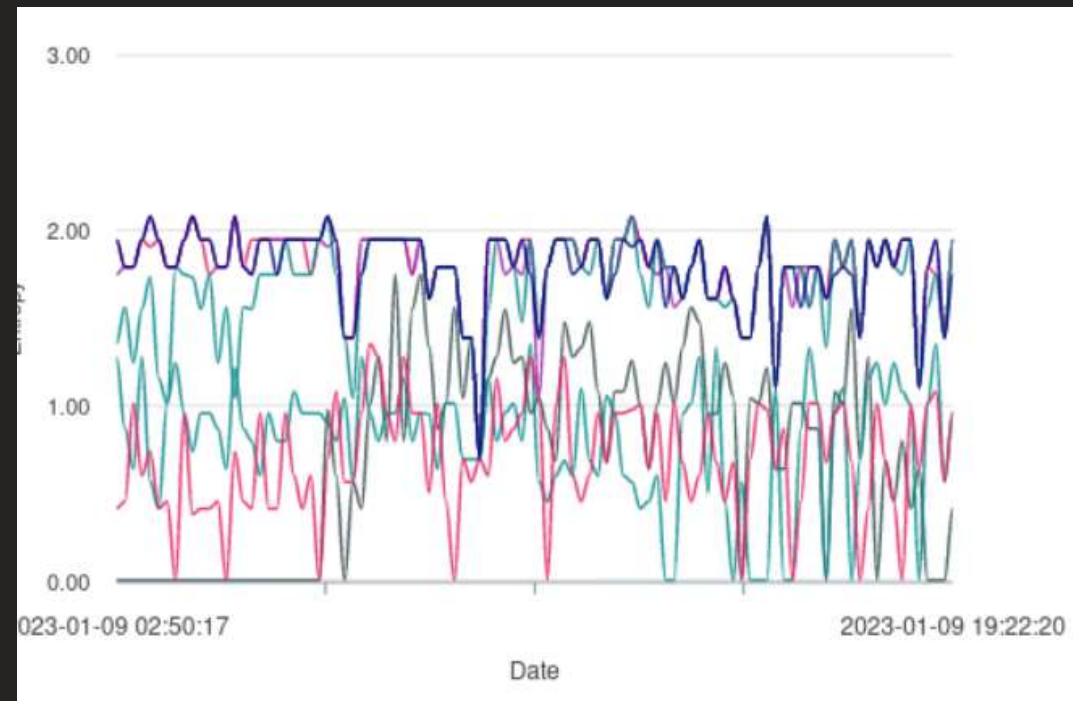
It does not require any Internet and/or Cloud connection.
It can rely on an **internal server/agent**
in order to display security LOGs and notifications



Predictive

Far superior than detection

Thanks to the union of **complex mathematical functions**
and cluster models,
the risk and type of future threat can be calculated.



This enables LECS to mitigate and/or anticipate 0-day threats.
object of University thesis with honorable mention



Not only the perimeter

LECS is able to collect data of movements **hidden and nested in unknown internal networks**

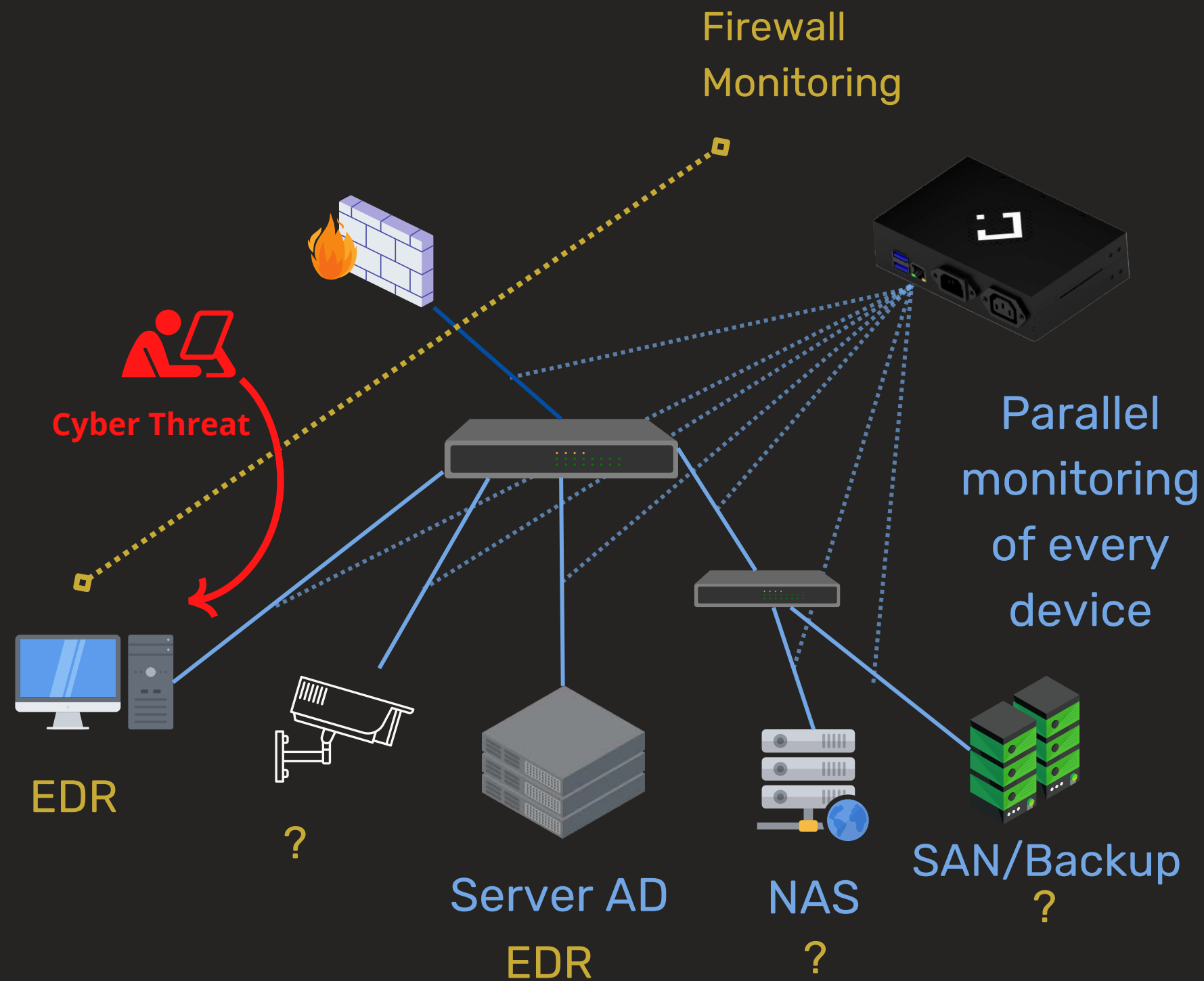
The implementation of various LECS in different network nodes creates a GRID and grants the system the **capacity to oversee the network**.

This feature, combined with EDR and Firewalls, manages the whole AREA of the network



LECS

The most dangerous threats are designed to bypass EDR and Firewall systems,
but are vulnerable in internal pivots.



Measured Performance

**+ 20% of monitored hosts vs.
present**

+ Σ (hosts) , in this case ~ 550 % of connections

- 87% Noise in LOGs (~38 / ~300) in 1 hr.

+ 10 Types of anomalies / time

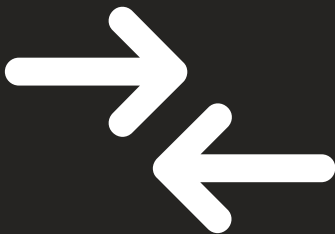
On field Test @PoC @F.F. e Cdp Program - Ott 22

CONCRETE ADVANTAGE

EXAMPLES AND TTP UNDER EXAMINATION

Cyber Threat Kill Chain

TA0007 Discovery	
T1046 Network Service Discovery	Both Advanced Port Scanner and NetScan have been used to discover local network infrastructure devices and services running on remote hosts. Active Directory queries for remote systems have been performed by ADFind.
T1057 Process Discovery	Process Explorer, Process Monitor and PCHunter have been utilized to discover any anti-malware or monitoring software and terminate it.
T1082 System Information Discovery	LockBit 2.0 enumerates system information such as hostname, shares, and domain information.
T1614 System Location Discovery	Attempts to check the language settings.
TA00008 Lateral Movement	
T1021 Remote Services	Although Cobalt Strike has many capabilities beneficial to threat actors in ransomware attacks, it was mainly seen in LockBit 2.0 investigations acting as a command and control beacon, a method of lateral movement and a tool for downloading/executing files.
T1021.002 Remote Services: SMB/Windows Admin Shares	LockBit 2.0 has been known to self-propagate via SMB.
TA0010 Exfiltration	
T1030 Data Transfer Size Limits	In some cases, LockBit 2.0 will limit the data transfer sizes to fly under the radar of any monitoring services a client may have set up.
T1041 Exfiltration over C2 Channel	MEGASync is the leading way for LockBit 2.0 affiliates to exfiltrate data from clients with it being occasionally replaced by RClone.

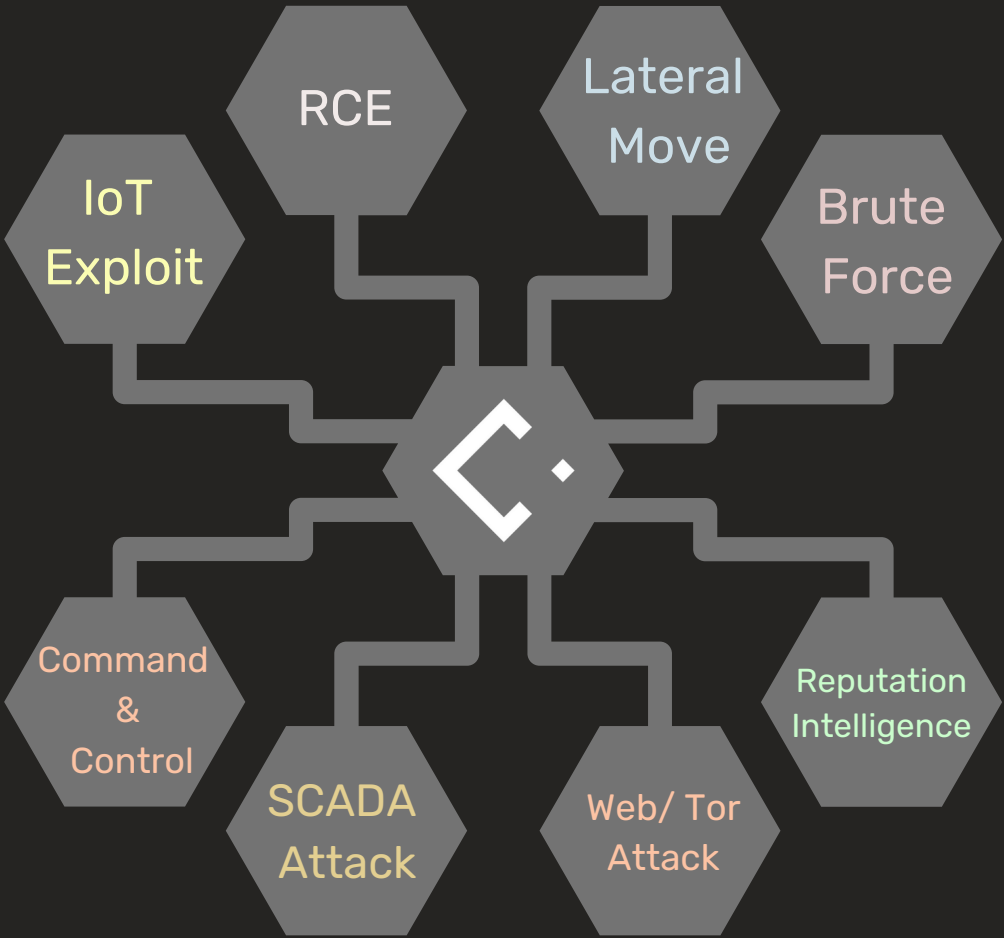


LECS

BENEFITS, LOG AND COUNTERMEASURE	
LATERAL MOVEMENTS	Truncating the Kill-Chain when the threat loses its obfuscation
FLOW CONTROL	Traffic monitoring not only useful for security purposes but also for internal traffic analysis (noise, optimization, debugging...)
EXFILTRATION BLOCK	Countermeasure literally allows a specific segment or host to be locked up, preventing data leakage.
LESS TIME FOR RECOVERY	With containment, Recovery times are significantly lowered.
FIND THE SOURCE OF PROBLEM	Optimized time and quantity of LOG for TH Operations.
CERTIFIED LOG	Accident demonstration, in compliance with many international certifications

Source:
<https://unit42.paloaltonetworks.com/lockbit-2-ransomware/>

INFOGRAFIC DETECTION



RCE / Attack / Malware

Thousands of services and vendors supported
With many and up-to-date CVE > 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...

Network Recon Category

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

- 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

• 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...

LECS: Why is it so **unique**?

Features	Competitor	LECS Technology
Implemetation times	From many hours to entire working days	10 minutes
Plug & Play	NO	YES
EDR Network Protection	Protects only devices with Operating System	Complement and protect all kinds of devices even without OS
Military inspired Air-Gap	NO	YES
Maintenance and Implementation	Expensive ecosystems	Minimal implementation and maintenance costs
LOG Management	Only Cloud	High resilience, local, internal LAN or/and Cloud depending on model
Features additional	NO	YES, debug and security control system
Scalability and modularity	Very Hard	from Embedded to HW Appliance

LECS is complementary to all solutions and actively complements firewall, antivirus and EDR in management and detection.



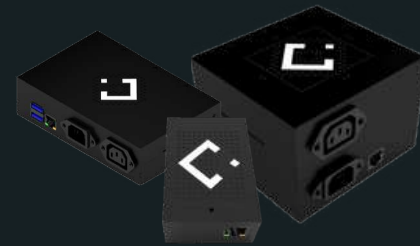
TECHNOLOGY VALIDATED IN:

*Critical industrial environments and supply chains, including sectors such as.
Pharmaceutical, Aerospace, Military supplies and more*

Business Model

B2B : Distributors and Resellers

Products:



- **Hardware Appliance:**

- 3 device models on the market to cover all targets:
 - Studios and Professionals
 - SMEs and Corporate
 - Industries and Public Administrations

- **Virtual Appliance:**

- Integration with manufacturing systems/processes and V-Servers
- Embedded/custom models

Licenses:



- **Annual recurring license that includes:**

- Daily updates to threats
- Maintenance of security LOGs
- Releasing new updates and features
- Weekly network status reports
- Instant notifications in case of dangerous threats
- Email notification of any threats in the World of Cyber

Products



LECS Business

Version that has a
Procedural
countermeasure
Software
Compact design.
Anodized aluminum
body.



LECS Plus

Version with hardware
countermeasure.
Cubic design.
Anodized aluminum body.
IEC13-14 220v shucko
sockets



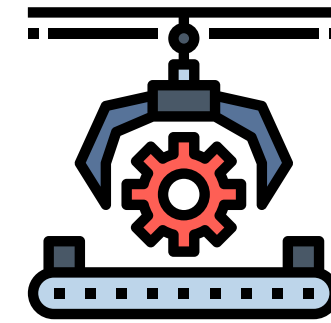
LECS Enterprise

Perfect for large
enterprise industry,
govern. Has powerful
hardware with 2 motors
for thorough inspection
and debugging of the
network



LECS Custom

Customized version.
1U rack implementation.
Anodized aluminum
body.
Customizable
countermeasures.



LECS Embedded

Customized version.
Virtual or hardware
implementation for
has become fully
integrable into
machinery.

IT SupplyChain / Retail
Segments

Industrial Segments
and Corporate



Validated Technology

Some recent **successful PoCs**:

► "LECS highlights a latent need, demonstrating current critical issues and providing an immediate response."

Operations Director of 1 PoC Corporate

► "LECS has provided me with immediate visibility in areas where it was not possible before."

IT Manager of 1 PoC Industry

► "It is very useful that LECS allows you to have both network debugging and cybersecurity control."

Sw Design e Manager of 1 PoC Industry

► "It adds an important level of safety in machinery with a very rapid approach."

OT Manager of 1 PoC Corporate

Reviews of Critical industrial environments and supply chains operating in the sectors
Pharmaceutical, Aerospace, Manufacturing Environments, Military



Corporate growth

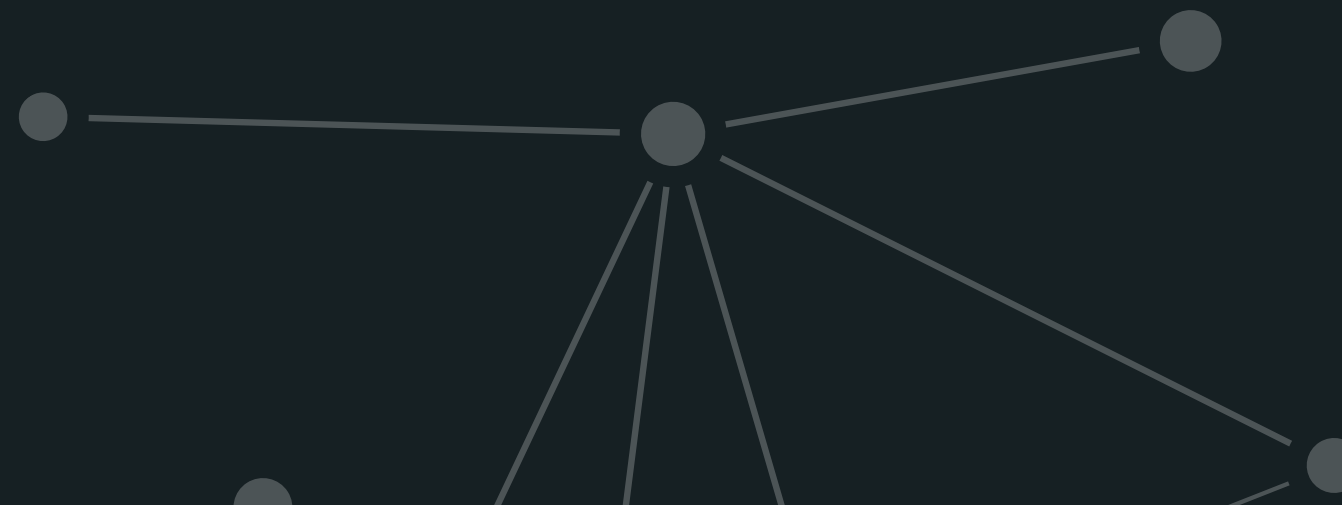
Numbers don't lie:

To date:

- Over **Hundred of Clients** including:
 - **6 Big Corporate**
 - **2 Relevant Multinazionali**
 - **Public administration**
- **5 successful PoCs** active with big Corporate
- **1 Successful PoC** in use case University (Thesis)
- **100% of customers**, to date, have renewed the fee
- **30%** of customers, purchased **another** LECS

Current asset:

- **New production site and R&D owned**
- **Current team:** 10, growing rapidly
- **20 Years of Intellectual Property**
- **Open contacts** with:
 - France
 - Germany
 - Dubai (Emirates)
- **Distribution/Reseller agreements:**
 - Italy
 - 2 Contract of Export Extra UE



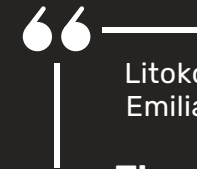
Awards



Selected at ForwardFactory 2022 with major
Corporate and Cassa Depositi e Prestiti



Best startup @EU Praga



Litokol with its Information Systems was 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 along with other excellences in various fields of application.



Selected to represent **Italy**
in the **World's** leading innovation fairs.
Gitex, CES- USA, VivàTech and H. Messe

https://www.linkedin.com/posts/litokol-s%2Ep%2Ea%2E_cyberevolution-activity-6995378352664526848-pNbT?utm_source=share&utm_medium=member_desktop



265 k€ Concessed Grant
Found for LECS technology and
related product



300k€ VC Round Investing
First Round completed.



Finalist Ai4Gov 2022
Contest AI in Governatives Env.



Master & Institutional Summit
Testimonial as **successful technology**
to Master and Events as ITASEC21,
Roma Security Summit



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



1° Classify Grant 30 k€
Region Marche Innovative Startup
Innovative Project Cyber Security
LECS.



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



Several Istitutional Awards
from Italian Governments

Auth. Res.



Contacts and Social



" Cyber Security becomes useful when it is accessible "



<https://lecs.io>



<https://www.linkedin.com/company/cyber-evolution-srl/>



<https://www.facebook.com/CyberEvolutionSrl>



<https://www.instagram.com/cyberevolutionsrl/>



<https://www.youtube.com/@cyberevolution574>



info@cyberevolution.it