LECS

Protect your future today

The World's First Plug & Play Cyber Security BlackBox

Company and Brand

History

ISO 27001 ISO 9001

- 2018 - Foundation of **EVOLUTION CYBER**

- 2020 - Patent Grant and International PCT Extension

- 2022 - Acceleration Program with Cassa Depositi e Prestiti and VC

- 2023 - Start of distribution in 8 countries, EU and non-EU

- 2024 - Bridge Round +1,5Mln con CDP e Azimut

- 2025 - Opening of the national research center and internationalization

Awards

| Vincitori CDP Forward Factory 2022	Global Ventures @Zurich on KickStart	Winners of the Italian Lifestyle Nana Bianca Acceleration Program	Among the best startups at the Enterprise Europe Network @EU PRAGUE	Finalisti TIM Cyber Challenge	Partner EIT Manifacturing

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

The paradox

- Networks not secure by **default**
- Vulnerable **Supply-chain**
- Missing **internal** control
- Struggles with management using **traditional measures**.
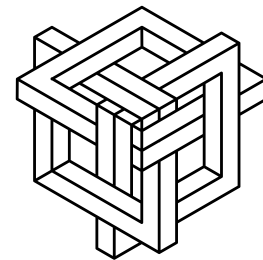
- Missing **response** to attacks
- Thousands of **logs** to analyze
- Needs for **expertise**, time, and personnel
- Excessive **costs**

Effects

Undetected vulnerabilities

Failure to Manage Logs and Penalties

Poor visibility, control and response

Low ROI

The Proliferation of Ransomware in 7 Minutes

Imagine a scenario where your company or a client is completely blocked for days, with no access to data and no way to recover.

With LECS you can prevent this scenario

The World's First Plug & Play Cyber Security BlackBox

LECS

AUTOMATIC

- No **configuration** needed
- Inspired by military **Blackboxes**
- 2 in 1 - Network Debugging and Security
- Automatic **updates**
- **24/7** network monitoring

INTERNAL

- It operates in **stealth** mode
- Protects where firewalls and EDR cannot
- Physical Resilience for **LOG**
- **360°** analysis of all individual connections

IT/OT PROTECTION

- Unique Energy **Countermeasure**
- Defends **all types of devices:**
  IoT, Server, 4.0 Machinery, Mobile
- Implementable in **critical** and/or industrial **environments** *(SCADA etc..)*
- Automatic and fast **response**

COMPLEMENTARY

- Can be integrated into any **environment** and with any **vendor**
- **Stand Alone**, it does not rely on existing network devices
- Possible **integration** with SIEM / SOAR via **API**

AI at the service of LECS

SPECTO
Detection Engine

- Hidden Analysis & Logging Classification
- Real Time Action
- Parallel analysis of all connections
- Does not slow down or stop operations

TIRESIA
Threat Forecast

- Threat prediction
- Continuous learning from the LAN
- Grows with the client's network
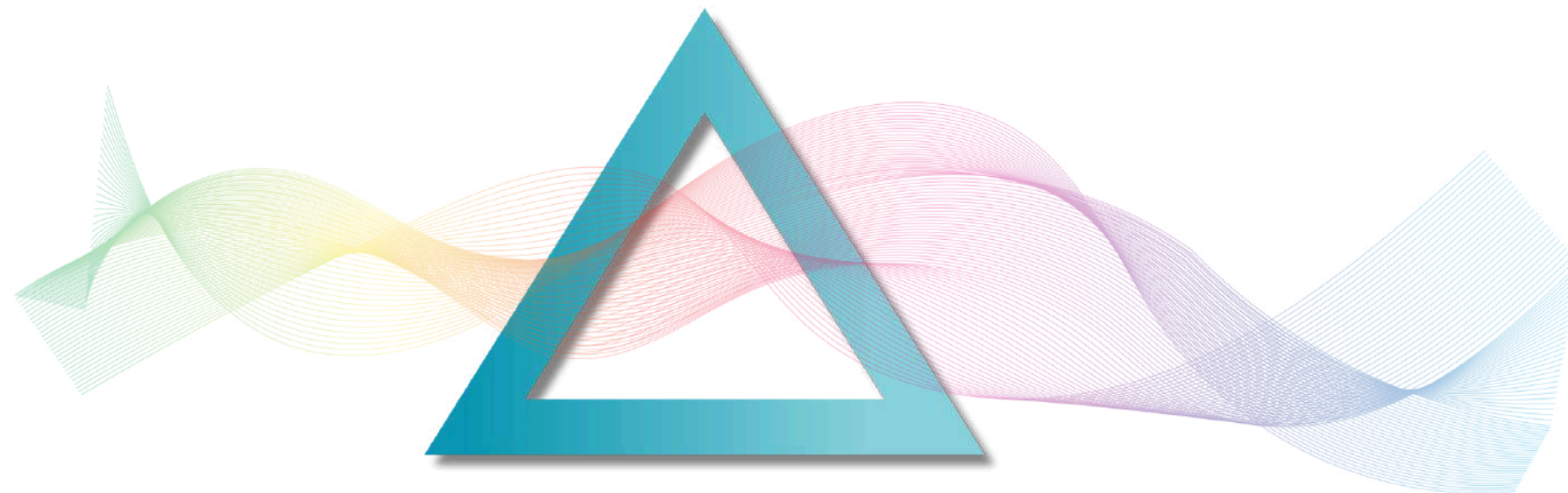
RAISES
Autonomous Response

- Adaptive procedural response
- Physical Air-Gap OSI Layer 0
- DEFCON Classification

The Detection

Tires-IA, the Neural Network that grows in the LAN

The 3 Engines of LECS:

AI Analysis

Static   Heuristic

Analyzes the **network spectrum**, detects **morphological** and **entropic** anomalies using the triangulation of **3 engines**

Ratings and false positives

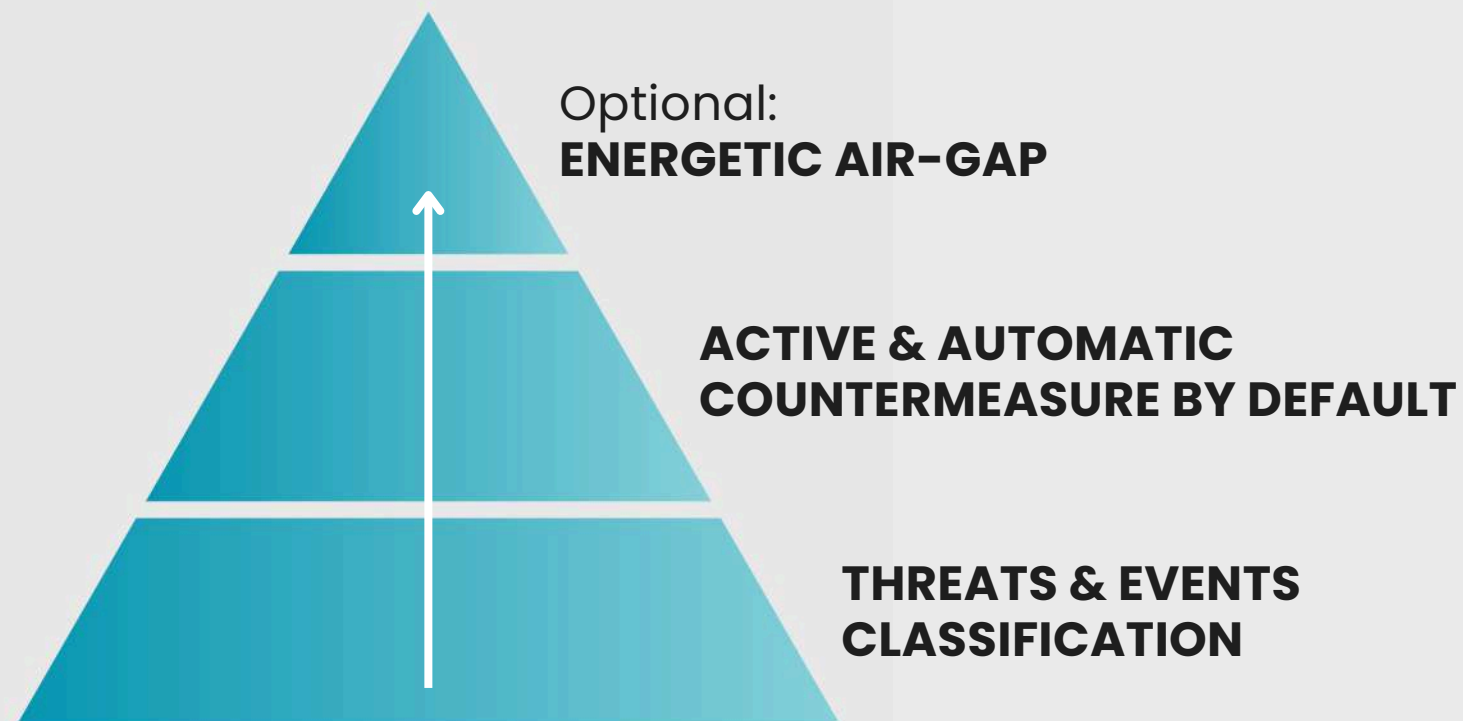LECS engines provides an extremely low false positive rating.

After over **5 years** in production environments, LECS has not reported any false positives for **critical levels**.

Statistics

+ 20% of monitored hosts compared to existing solutions

+ ∑(hosts traffic) + 550% of analyzed connections

- 87% False Positives in the LOGS

+ 10% types of anomalies

Dynamic response

The system **responds** in a **calculated and measured** way based **on the type and severity** of the threat, **instantly**

Optional:
ENERGETIC AIR-GAP

ACTIVE & AUTOMATIC COUNTERMEASURE BY DEFAULT

THREATS & EVENTS CLASSIFICATION

*HACL : Hidden Analysys Classification Logging

Engine Levels

01 + **CLASSIFICATION**

HACL* dynamically classifies threats based on every possible variable.

02 + **AUTOMATIC RESPONSE**

Software **procedures** for **automatic** threat mitigation.

03 + **AIR-GAP COUNTERMEASURE**

It operates electrically through a cyber-physical **actuator**, creating a real isolation bubble.

Dashboard
Multi-Level
Notifications

Ai Based

Time is precious.
The multitenant notification system
**allows for greater support and
services from IT consultants**

WELCOME TO YOUR LECS DASHBOARD

PARTNER

SIGN IN

USER

SIGN IN

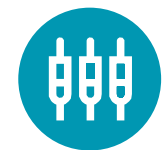| Automatic and Manual Reporting | Simplified visualization and natural language | Advanced Multi-Tenant Level for IT/ OT Manager | Use of AI & ML for a clear and simplified view | Sending emails and messages | APIs for SIEM/SOAR SOC integration |

Installation in
10 Minutes

Connect it to the network

Register it on the platform

Installation completed

Lecs is already active!

① Network **Defense**

24/7 Monitoring
Protection of all devices
Attack prediction
Active countermeasures

② Network **Control**

Network problem check
Online devices check
Network behavior analysis
Automatic updates

③ Log **Notarization**

Event LOGs with private blockchain technology
that enhance threat traceability, support
certification and regulatory compliance, and is
also useful for insurance purposes.

Introduction to the **Blockchain**

LECS Logs are certified, resilient, and secure. They are encoded with the DLT protocol and recorded in a Blockchain that encrypts them, ensuring integrity, date certainty, and making the log content mathematically immutable.

Blockchain Advantages:

- Eliminates the need for external **digital signatures**

- Reduces **fraud risks** by ensuring traceability

- Thanks to encryption, it **ensures** security and immutability, preventing **tampering**
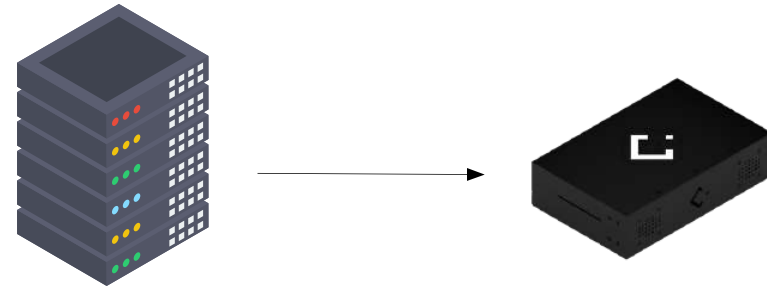
Compliance:

Integrity

Confidentiality

CIA triad

Availability
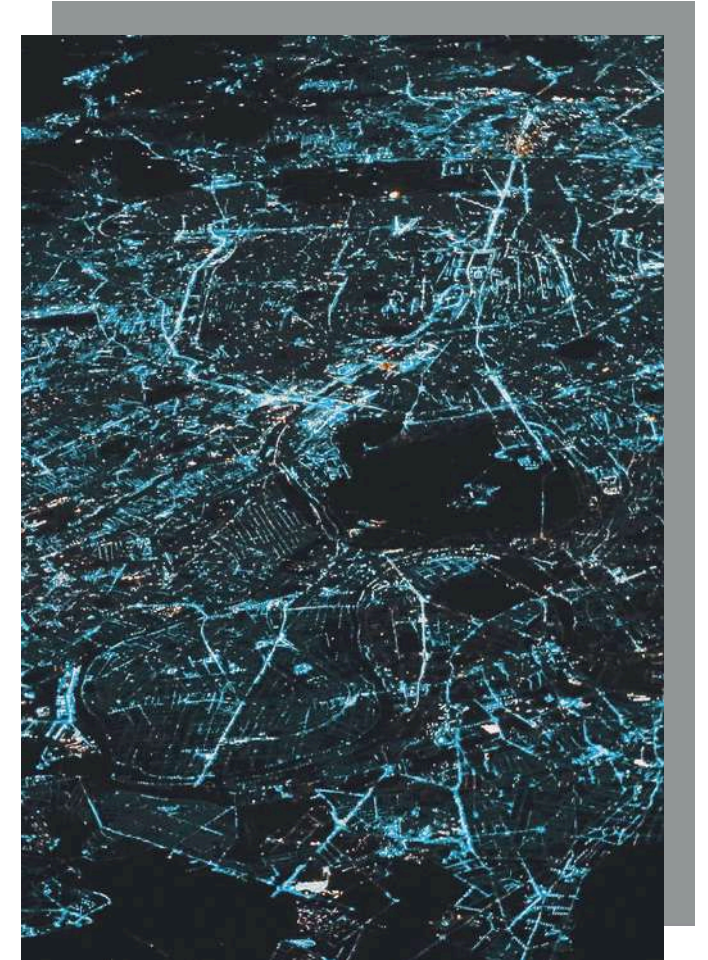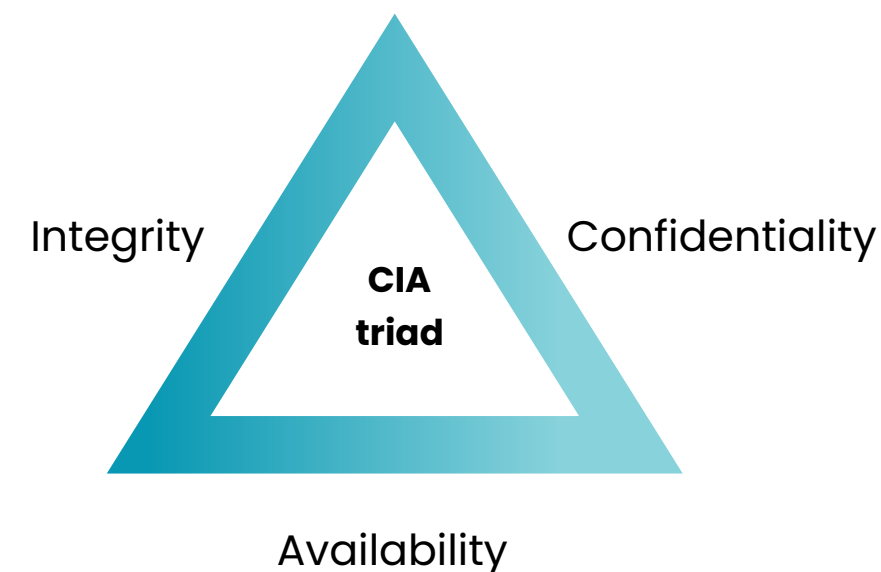
LECS supports in the legal, insurance, banking and healthcare sectors.

ISO 9001
ISO 27001
GDPR EU
NIS2
DORA
IEC 62443

LECS in Your Network

Polling

- **Local** detection management
- User **privacy** compliance
- Operates **without internet**, no slowdown

No impact on bandwidth consumption

Armored Blackbox

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

* PPS: Ports Protocols & Services
* RCE: Remote Code Execution
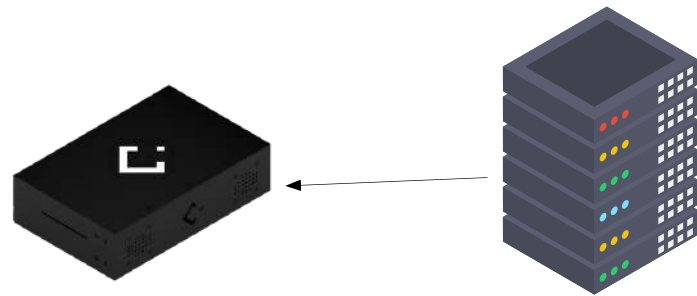
Updates

LECS chooses the **best timing** to perform updates

ADVANTAGES:

- Hard to detect
- Enhanced security
- No push (update cannot be forced)

RCE*

Brute Force

DoS

Credential Theft
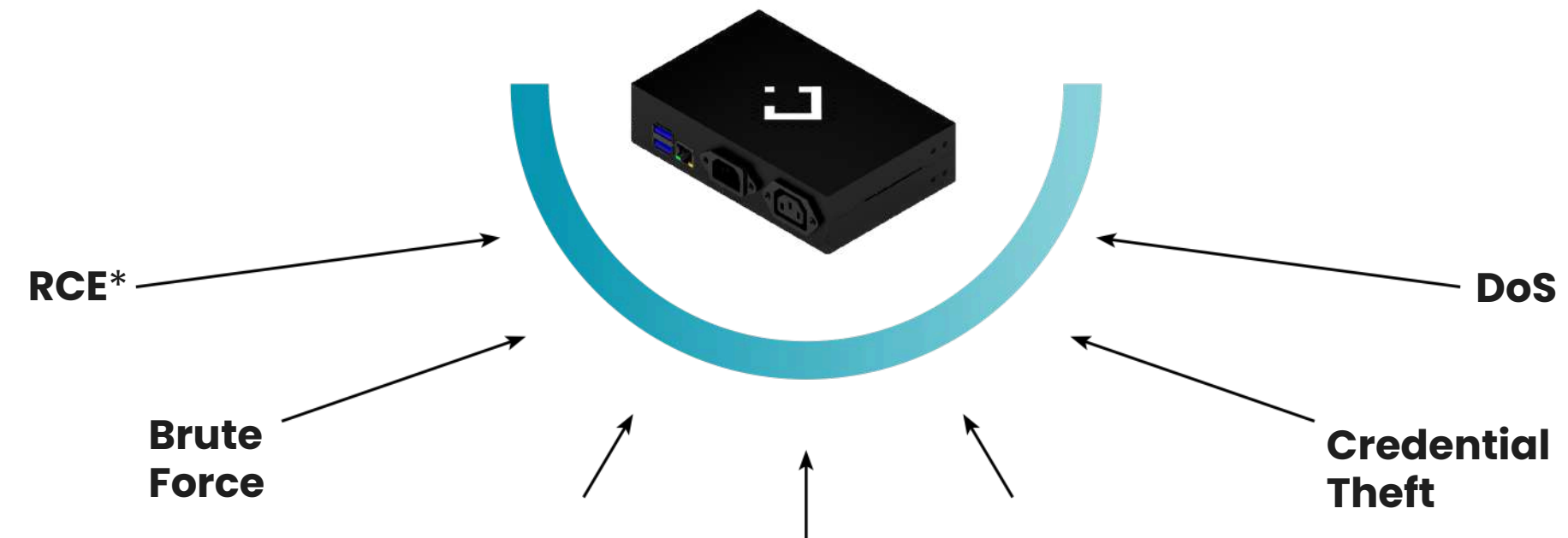
FIRMWARE SECURITY
The internal components of LECS are layered, ensuring local defense

Energy Barrier

To block an attack you must act quickly and on multiple fronts

AIR GAP Physical

Example:

Temporary **Cut-Off** of a backup system is a great strategic choice

NO Ecosystems required
LECS is completely **stand-alone** in its response

LECS can secure an entire network in the safest possible way by temporarily shutting down the switch with an automatic electric actuator, as an alternative to a software procedural system.

Threats are designed to **bypass** EDR or perimeter systems and attempt to disable security services.

LECS acts energetically **only if necessary** and for the minimum time required to prevent the threat's action.
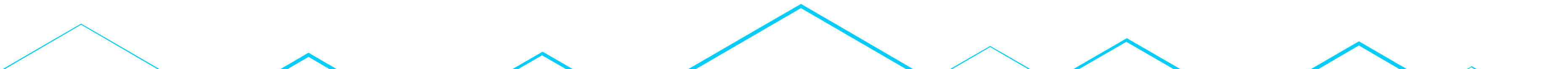
Strengths

Placing **LECS** at multiple points in the network creates a protection **Grid** that monitors traffic between hosts, which represent the surface. All connections, including external ones, are analyzed **securing the ENTIRE AREA**.
LECS integrates well with existing Firewalls or EDR systems, adding an extra **Layer** of security.

K.P.I.

Characteristics	Competitor	LECS Technology
Installation Time and Difficulty	Complex, often prolonged and with operational blocks	Quick in 10 minutes. Simple and without interrupting work
Plug & Play	NO	YES
EDR Network Protection	Protects only devices with operating system	Provides complete protection for all types of devices, even those without an operating system.
Military inspired Air-Gap	NO	YES
Implementation and Maintenance	Expensive and complex ecosystems	Simplified and easy implementation and maintenance
LOG Management	Cloud-only solutions, difficult to interpret.	High resilience, local, in LAN &/or Cloud depending on the model. Log interpretation and analisys made easy thanks to AI.
Additional Features	NO	YES, it includes a network and security control system in a single Black Box. Log Notarization.
Scalability and Modularity	Very difficult to scale and adapt.	Device for every type and size of company & environment. Scalable and easily integrable with SIEM, SOAR and SOC via API.
Integration with other security devices	Requires design and planning for integration	Installable alongside other systems without causing any operational disruption

Validated Technology

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

Operations Director of 1 PoC
Corporate

"LECS provided me with immediate visibility into areas where it wasn't possible before."

IT Manager of 1 PoC
Industry

"It's extremely 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 layer of security to the machinery with a very quick approach."

OT Manager of 1 PoC
Corporate

Technology present in:
19 countries

Conversion Rate from NFR:
85 %

Successful PoC:
› 80 %

Customer Satisfaction:
99 out of 100

Renewal Rate:
93 %

Validations:
in every environment

Critical industrial environments and supply chains, including sectors such as Pharmaceuticals, Aerospace, Automotive, Currencies.

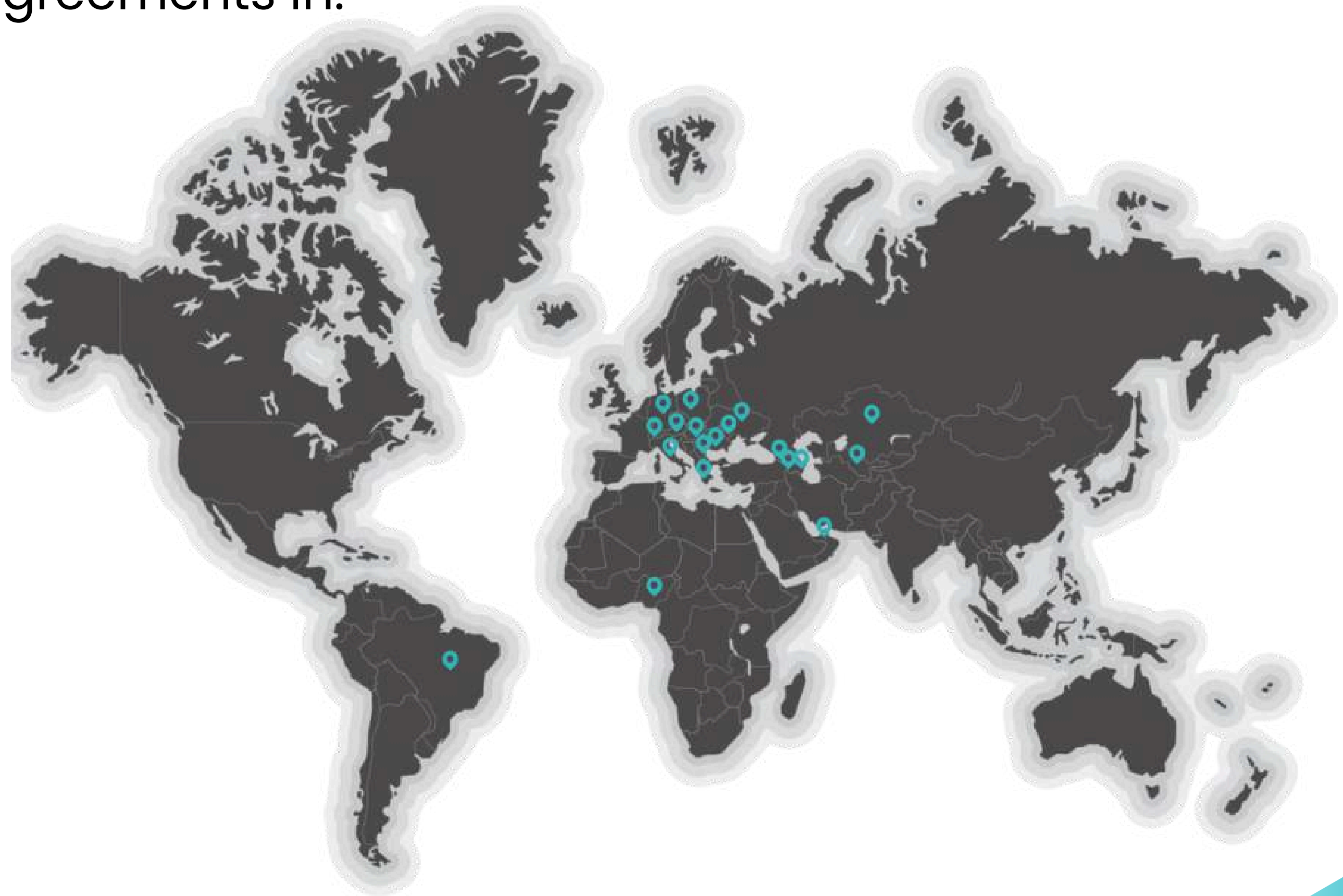# Distribution agreements in:

- Germany
- Austria
- Switzerland
- Poland
- Moldova
- Romania
- Bulgaria
- Greece
- Hungary
- Ukraine
- Armenia
- Italy
- Nigeria
- Georgia
- Kazakhstan
- Azerbaijan
- Uzbekistan
- United Arab Emirates
- Brazil

Business Model

Simple and Scalable System

Hardware Appliance

with a license that includes

Updates

- **Daily** Updates
- Release of new **engines** and analysis tools
- Updates for the **AI** and its **neural networks**
- Protection updates from Global Intelligence sources and against threats from the **dark/deep web**

Report & Notifications

- Instant **notifications** via chat and e-mail
- Weekly **reporting**, manageable and viewable from the Dashboard
- Through **API**, export of LECS Logs to integrate them into other platforms or aggregators

Warranty & Log Retention

- **Hardware** Warranty guaranteed for the entire duration of the license
- **Replacement** Warranty in case of obsolescence
- **Log retention** for a specified number of days, varying by license type and extendable upon request

Physical Products

Each company has **different cybersecurity needs** based on its technological infrastructure and the sector in which it operates.

LECS BUSINESS

- Ideal for **small** companies with few network nodes
- Software procedural countermeasure
- **Tires-IA Lite** Detection Engine

LECS CORE 2P / 4P

- Ideal for **medium-sized** companies, including those in manufacturing
- Software procedural countermeasure
- **Multi-port** for Detection, **4P** for multiple Network
- **Tires-IA Advanced** (2P) and **Elite** (4P) Detection & Analysis & Neural Network

LECS ENTERPRISE 2.0

- Ideal for **small/medium** sized companies, including those in manufacturing
- Software procedural countermeasure
- Hardware **Air-Gap** countermeasure
- **Tires-IA Advanced** Detection & Analysis Engine

THE ONLY VERSION WITH ENERGY COUNTERMEASURE

LECS CORE SFP

- Ideal for **large** enterprises, including those in manufacturing
- Software procedural countermeasure
- **Multi-port** for Detection across multiple Networks
- **SFP Fiber** ports for backbones
- **Tires-IA Ultra** Detection & Analysis & Neural Network

LECS EMBEDDED / SAAS

Customized version. **Virtual** or hardware, fully integrable into machinery.

LECS CUSTOMIZED

Customized version. Perfect for mission-critical environments and specific virtualized implementations.

N.B. Data of LECS can be collected in cloud datacenter based in Italy or OnPremise inside customers network

Virtual products

LECS technology is also available in virtualized mode through these environments:

Vm Ware   Proxmax   Hyper V

ALL LECS PRODUCTS CAN collect logs

In Cloud   *or*   On Premise

Certifications and Patents

Patented Technology and Certified Excellence - LECS

Patented Technology

ISO-9001 Certification

ISO-27001 Certification

Compliance NIST Framework 1.1

Compliance NIST Framework SP800

Compliance NIS-Directive

ACN Certification - Request process initiated

Patented technology

A network protection system and its security procedure with international PCT extension. Below are the differences between **LECS** and other solutions. **LECS is complementary to other security solutions**.

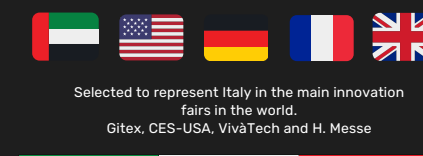| Characteristics	LECS	Antivirus	Firewall	IPS
Plug & Play	✓	✗	✗	✗
Unique Energy Countermeasure	✓	✗	✗	✗
Active protection for devices, IoT and Industrial OT	✓	✗	✓	✓
Completely stealth approach	✓	✗	✗	✓
Physical LOG storage	✓		✗	✗
Innovative internal protection (POV type)	✓		✓	✓
Parallel installation, without steps and downtime	✓		✗	✓
Zero technical knowledge needed for maintenance	✓	✓	✗	✗
Blackbox Approach	✓		✗	✗
Intuitive Dashboard	✓		✗	✗

The highest security standards

LECS
Protect your
future,
now!

LECS is a product of
Cyber Evolution S.r.l.
Via Erasmo Mari 57/s
63100 Ascoli Piceno

Tel: +39 0736 652614
Mail: info@cyberevolution.it
Web: https://lecs.io

"Become a partner in an innovation that has been revolutionizing Cyber Security, offering your clients proactive and intelligent defense. Together, we can transform Cyber Security into a competitive advantage."

Partners and Awards:

eit | European Institute of Innovation & Technology

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

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