LECS

Proteggi il tuo futuro, oggi

La prima BlackBox di cyber
security Plug & Play al mondo

Cyber Logic Central
SOC

CerebroSec

TECNOLOGIA E INNOVAZIONE PER UNA SICUREZZA INFORMATICA INARRESTABILE

LECS, tecnologia brevettata.

Immagina un futuro in cui le minacce di cyber attacchi sono solo un ricordo lontano. Un futuro sereno, senza preoccupazioni o emergenze da affrontare, in cui puoi crescere e raggiungere tutti i tuoi obiettivi professionali. Con LECS questo futuro è oggi.

Indice »

Benvenuti in un mondo dove la **tecnologia** e **l'innovazione** convergono per forgiare un **futuro di sicurezza** senza compromessi. Benvenuti in LECS.

Semplicità e Potenza: la difesa Cyber alla tua portata

Le minacce informatiche aumentano sempre di più in termini di numero e di impatto, nonostante siano già state adottate sofisticate misure di sicurezza.

QUAL È IL PROBLEMA?

Gli attuali sistemi di difesa si rivelano insufficienti e troppo complessi da installare e mantenere, lasciando così buchi di protezione non indifferenti.

Ragioni

- Reti non sicure per struttura
- Intere supply-chain vulnerabili
- Specifiche ed avanzate skills
- Misconfigurazioni
- Controllo interno mancante
- Fatica nella gestione della detection con misure tradizionali
- Problemi nel rispondere prontamente alle minacce
- Migliaia di log da analizzare (perdita di tempo e difficoltà di analisi)
- Mancanza di tempo e personale
- Costi troppo elevati per soluzioni avanzate di security

Cosa significa questo per un'azienda?

Vulnerabilità non rilevate:
- Problemi già presenti in reti
- non sicure
- Possibile esposizione ad attacchi
- Blocchi produttività
  Perdita dati sensibili

Mancata Gestione dei Log e sanzioni:
- Richiederebbe personale
- aggiuntivo
- Skill specifiche di settore
  Sanzioni dovute da normative GDPR

Scarsa visibilità, controllo e risposta:
- Interi segmenti e ambienti
- non protetti
- Poca percezione delle minacce
- Impossibilità di rispondere e mitigare gli incidenti cybernetici
  Perdita dati sensibili

Scarso ROI:
- Con le attuali soluzioni non si è
- certi del proprio status di security
  Non sono più giustificati gli investimenti in soluzioni tradizionali già fatti, poiché incompleti
- Quanto costerebbe a un'azienda restare fermi per settimane oltre al danno di immagine con i propri clienti?

Immagina uno scenario in cui la tua azienda è completamente bloccata per giorni, senza accesso ai tuoi dati e senza possibilità di ripristino. Cosa faresti? Quanto ti costerebbe questo blocco? Noi possiamo prevenire questo scenario in pochi minuti e senza bisogno di personale specializzato.

LA PRIMA **BLACKBOX DI CYBER SECURITY** PLUG & PLAY AL MONDO

LECS è il primo dispositivo innovativo di sicurezza informatica Plug & Play al mondo che protegge qualsiasi rete LAN, infrastrutture in Cloud e impianti industriali dagli attacchi e dalle minacce informatiche più pericolose grazie alla sua tecnologia brevettata a livello internazionale.

Questo è LECS. Il più potente e intelligente sistema di sicurezza informatica.

LECS è una tecnologia unica che raccoglie tutte le peculiarità di soluzioni IPS, NDR, Honeypot e ti supporta attivamente a rispondere prontamente alle minacce e a monitorare lo stato di salute della tua rete.

ZERO KNOWLEDGE SECURITY NETWORK LECS ha un'architettura zero knowledge e non ha bisogno di manutenzione. Analizza il traffico, i movimenti interni ed esterni alla rete e una volta rilevata un'anomalia, la classifica ed agisce in base al grado di gravità con una risposta modulata all' attacco. LECS è il partner ideale per il rilevamento di movimenti laterali, ransomware e data-exfiltration.

Ha **3 sedi** e un **team multidisciplinare** focalizzato sulla cyber security, con ricercatori, ingegneri del software, penetration tester e sviluppatori che lavorano in sinergia con esperti di finanza e amministrazione. I suo interno sono presenti membri che collaborano attivamente alla divulgazione della cultura di Cyber Security attraverso Enti, testate nazionali e internazionali, webinar grazie al **know-how** e al background di oltre 10 anni esperienza nel settore della cyber security, l'azienda ha realizzato con successo soluzioni di altissimo profilo tecnologico, che hanno **ottenuto importanti sovvenzioni e supporto da acceleratori nazionali,** rafforzando così il suo ruolo di pioniere nella sicurezza informatica.

I nostri traguardi

- Vincitori CDP Forward Factory 2022
- Vincitori al Global @Zurich di KickStart
- Vincitori del programma di accelerazione Italian Lifestyle Nana Bianca
- Tra le migliori startup all'Enterprise Europe Network @EU PRAGA
- Finalisti TIM Cyber Challenge
- Partner EIT Manufacturing

LECS è la soluzione

Automatico

Non è necessaria alcuna configurazione. Ispirato alle blackbox utilizzate in aviazione per garantirti una sicurezza militare. Con il monitoraggio e la classificazione della rete integrati in un'unica soluzione, Lecs offre un approccio 2 in 1: Debug della rete e controlli di sicurezza. Aggiornamenti automatici quotidiani.

Protezione IT & OT

Contromisura energetica unica nel suo genere. Difende ogni tipo di dispositivo, dall'IoT al Server Implementabile in ambienti critici e/o industriali. Semplifica la gestione della sicurezza informatica.

Complementare

La produttività rimane inalterata: il dispositivo lavora in stealth con gli altri sistemi di sicurezza già presenti.

Interno

Punto di vista invisibile e interno. Protegge dove i firewall e gli EDR non arrivano. Resilienza fisica per LOG e logica interna. Segnala tutti gli errori di rete. Prevede le anomalie.

Blockchain

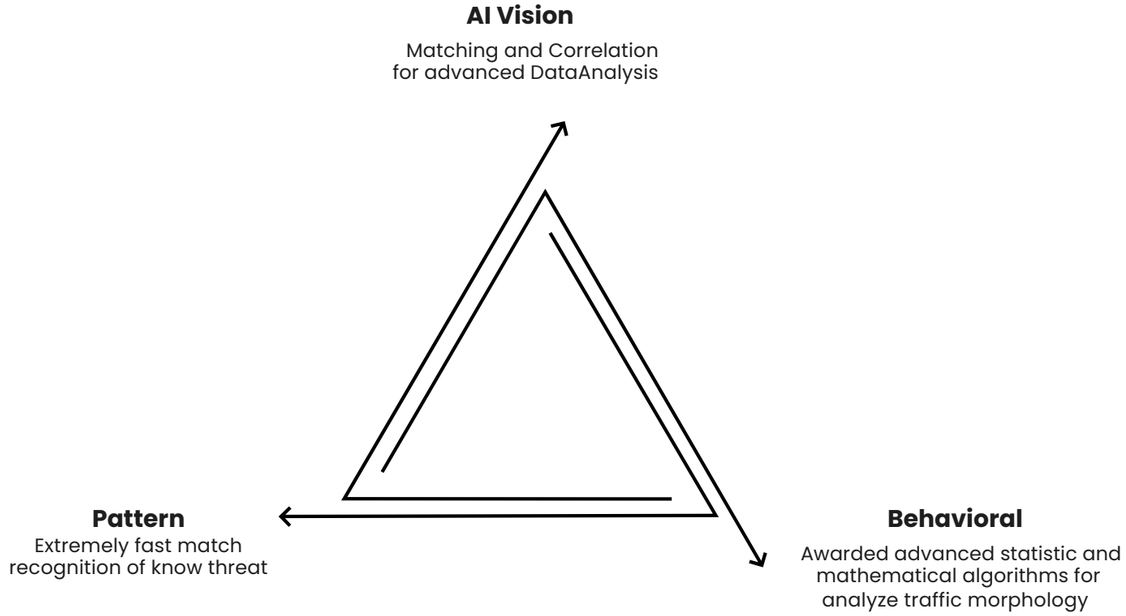
Ogni LOG rilevato dal dispositivo viene validato all'interno della propria blockchain.

Privacy

Garantisce gli standard alle normative europee e internazionali sul trattamento dati.

Come fa analisi LECS: Detection

Unendo biunivocamente tutti i tipi di detection possibili, otteniamo un sistema dinamico di monitoraggio ottimizzato alla minaccia.



Rating e falsi positivi

AI contrario di sistemi basati puramente su IA, ciascun livello di questi motori influsce sullo **score** della minaccia con metriche differenti abbattendo così a livelli minimi il numero di falsi positivi. Statisticamente, ad oggi, LECS non ha riportato falsi positivi in ambienti produttivi per i livelli critici.

+ 20% di host monitorati rispetto alle soluzioni presenti + Σ(host), in questo caso - 550% delle connessioni - 87% Rumore nei LOG (-38/-300) in 1 ora + 10 tipi di anomalia / tempo

Risposta dinamica

LECS usa tecniche innovative al di là dello stato dell'arte attuale. Si avvale di una concatenazione di 3 differenti Point Of View per una stessa minaccia riuscendo cosi a eseguire detection avanzata di pericolosi e invisibili movimenti laterali.

Optional: AIR-GAP CONTROMISURA

Se connesso, agisce elettricamente tramite un attuatore cYber-fisico per creare una vera bolla di isolamento, come da procedure critiche.

CONTROMISURA AUTOMATICA DI DEFAULT

Tecniche di mitigazione delle minacce software procedurali, implementate automaticamente e senza interazione umana.

LECS opera su più livelli dello stack ISO/OSI per affrontare diversi tipi di minacce e senza inviare "comandi" ad altri dispositivi.

TRIGGER DI CLASSIFICAZIONE SPECIFICA

In caso di particolari anomalie, LECS inizia a eseguire un monitoraggio più dettagliato di movimenti particolari e notevoli.

Il sistema risponde in modo calcolato e misurato in base al tipo e alla gravità della minacciaquasi istantaneamente.

01+

CLASSIFICAZIONE SPECIFICA PER L'ATTIVAZIONE

In caso di particolari anomalie, LECS inizia a eseguire un monitoraggio più articolato di movimenti particolari e degni di nota.

02+

CONTROMISURA AUTOMATICA DI TRAFFIC FREEZING

Tecniche procedurali software per la mitigazione delle minacce, implementate automaticamente e senza interazione umana.

03+

CONTROMISURA AIR-GAP

Quando è collegato, agisce elettricamente tramite un attuatore cyber-fisico per creare una vera e propria bolla di isolamento, come da procedure critiche.

LE AI AL SERVIZIO DI LECS

LECS usa tecniche innovative al di là dello stato dell'arte attuale. Si avvale di una concatenazione di 3 differenti Point Of View per una stessa minaccia riuscendo cosi a eseguire detection avanzata di pericolosi e invisibili movimenti laterali.

SPECTO

Motore di Rilevamento

Specto, il modello di **Hidden Analysis Classification Logging (HACL)** è il cuore delle operazioni di detection e gestione completamente automatica delle minacce in real-time. Il suo approccio stealth permette di **rimanere nascosto e di lavorare parallelamente alla rete**, senza ostacolare la normale operatività, il tutto mentre l'evoluto algoritmo analizza e classifica in tempo reale le minacce e anomalie sulla rete.

TIRESIA

Previsione delle Minacce

Tutte le operazioni sono supportate dall'algoritmo intelligente Tiresia, che continuamente **apprende e migliora non solo la detection, ma anche le previsioni future di attacco**. Essa infatti è la prima intelligenza digitale che supera la prevenzione stessa, effettuando vere e proprie predizioni di cyber threat forecast, aumentando in questo modo notevolmente le capacità di detection dell'intero ecosistema.

RAISES

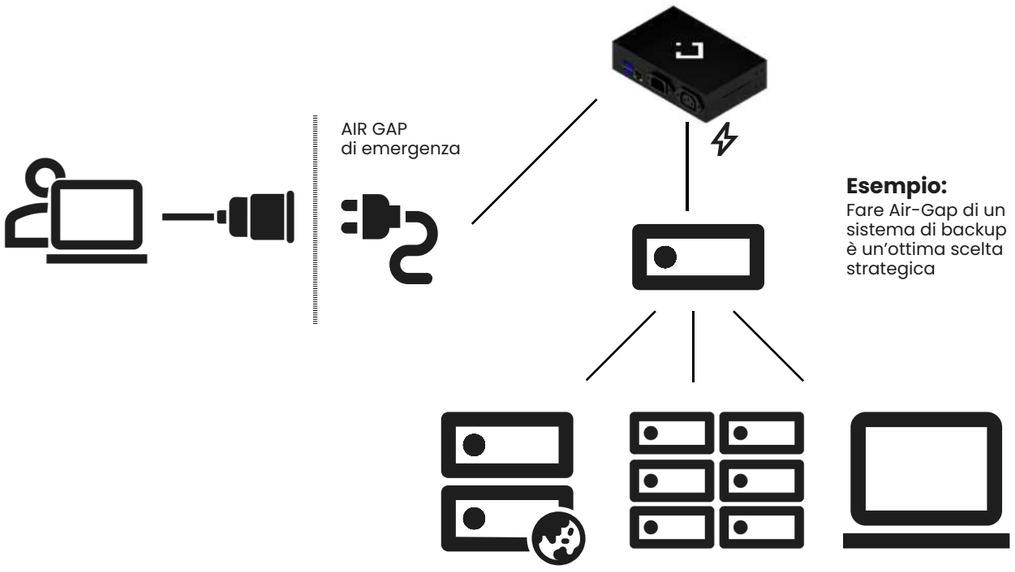
Risposta Autonoma

Nel caso in cui venisse rilevata una criticità ad alto rischio, interviene Raises con una risposta procedurale e adattiva per isolare e mettere in sicurezza il segmento di rete bersaglio.

BARRIERA ENERGETICA

In caso di attacchi estremamente pericolosi, esfiltrazione dati su server di C2 o ransomware in corso, LECS può blindare un'intera rete nel modo più sicuro possibile utilizzando un attuatore elettrico automatico in alternativa ad un sistema procedurale software.

Questo perchè le minacce nascono per fare bypass di sistemi EDR, perimetrali e/o spegnere i servizi di sicurezza. L'unico modo per bloccare, è agire subito e parallelamente.



Esempio:
Fare Air-Gap di un sistema di backup è un'ottima scelta strategica

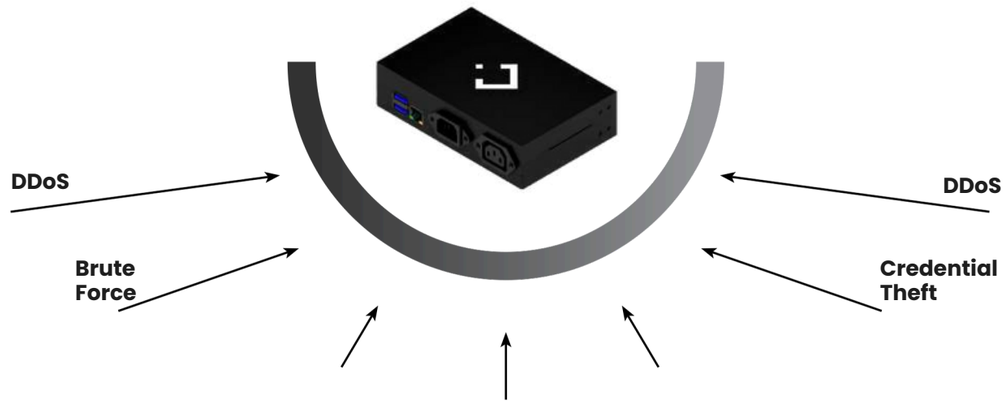
BLACKBOX

LECS non è direttamente attaccabile, al contrario di altri sistemi configurabili che spesso espongono PPS, come i firewall o altri ecosistemi Si comporta come una vera e propria scatola nera con l' aggiunta di azioni attive di contromisura:

Analizza

Registra

Agisce



INSTALLAZIONE IN 10 MINUTI

Ampia capacità di risposta, sia preventiva durante le fasi di Recon che di risposta durante i movimenti laterali e di Exploit.

Collegalo alla rete

Registrala sulla piattaforma

Installazione terminata

Il tempo è prezioso. Per questo il sistema di notifiche e dashboard completamente automatico non porta via tempo all'IT Manager o ai SOC.

Lecs è già attivo!

Difesa della rete

Monitoraggio 24/7
Protezione di tutti i dispositivi
Previsione degli attacchi
Contromisure attive

Notarizzazione

di eventi LOG con la tecnologia blockchain privata per migliorare la tracciabilità delle minacce e supportare meglio la certificazione, i regolamenti normativi ed è utile anche a fini assicurativi.

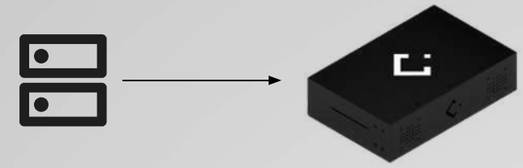
Controllo della rete

Controllo dei problemi di rete
Controllo online dei dispositivi
Analisi del comportamento della rete
Aggiornamenti automatici

MAGGIORI DETTAGLI

Approccio Polling

Il rilevamento è gestito localmente, nessun pcap o raw inviato ai server per l'analisi. Massima privacy garantita e nessuna latenza.



POLLING=NESSUNA CONNESSIONE CONTINUA

VANTAGGI:

Operazione a bassa latenza senza internet, nessun rallentamento

Aggiornamenti LECS sceglie il momento migliore per eseguire gli aggiornamenti in modo autonomo e con un mix di forti crittografie. Inoltre, gli aggiornamenti sono calibrati sul dispositivo stesso e quindi unici.

VANTAGGI:

Difficile rilevare l'uso della banda, sicurezza - non spingere

SICUREZZA DEL FIRMWARE

I componenti interni di LECS sono stratificati assicurando una difesa locale.

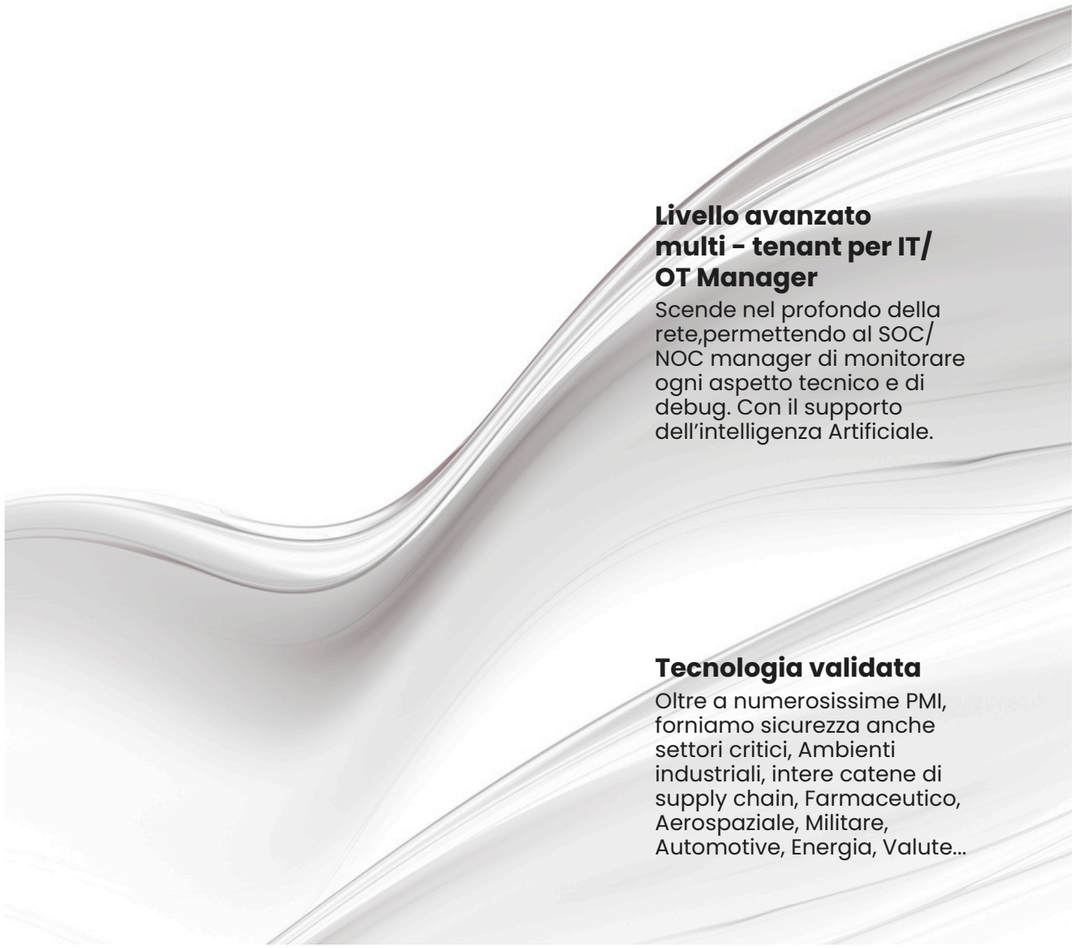
LECS NON È DIRETTAMENTE ATTACCABILE

A DIFFERENZA DI ALTRI SISTEMI CONFIGURABILI CHE SPESSO ESPONGONO PPS, COME FIREWALL O ALTRI ECOSISTEMI.

NOTIFICHE MULTILIVELLO

Visualizzazione semplificata con chat

Evidenzia in automatico gli eventi salienti. Usa un'interfaccia a linguaggio naturale, prima al Mondo per questo campo.



Livello avanzato multi - tenant per IT/ OT Manager

Scende nel profondo della rete,permettendo al SOC/ NOC manager di monitorare ogni aspetto tecnico e di debug. Con il supporto dell'intelligenza Artificiale.

Tecnologia validata

Oltre a numerosissime PMI, forniamo sicurezza anche settori critici, Ambienti industriali, intere catene di supply chain, Farmaceutico, Aerospaziale, Militare, Automotive, Energia, Valute...

NOTIFICHE IN TEMPO REALE

Lecs usa attuatore cyber-fisici per:

HMI

Locale acustico

- Allarmi sonori (dB personalizzabili)
- Integrazione con device interni

Locale visivo

- Allarmi visivi
- Integrazione HMI
- ISO 27001

Remoto

- Allarmi via rete
- Integrazione SIEM
- Customizzazioni di ogni genere

+ SIEM INTEGRATION

Le notifiche sono istantantee in caso di potenziali pericoli avvenuti. Vengono inviate per email e classificate in base alla gravità.

TECNOLOGIA LECS: LA NUOVA ERA DELLA CYBER SECURITY

LECS è il primo sistema di interfacciamento in linguaggio naturale al mondo.
Ha una Dashboard intuitiva, adatta sia per il debugging che per una rapida visione dello stato globale della rete.

Architettura zero-knowledge

LECS ha un'architettura **zero-knowledge** e non ha bisogno di manutenzione. Collegato al router o allo switch di rete, il dispositivo di sicurezza informatica LECS analizza il traffico, i movimenti interni ed esterni alla rete e una volta rilevata un'anomalia, la classifica ed agisce in base al grado di gravità con una risposta modulata all' attacco. **LECS è il partner ideale per il rilevamento di movimenti laterali, ransomware e data-exfiltration.**

Sinergia di Algoritmi: La Tripla Difesa della Rete

La tecnologia di LECS si basa su **3 engine** che fanno da cardine per tutto l'ecosistema. Specto, Raises e Tiresia sono gli algoritmi di machine learning che lavorano sinergicamente e parallelamente per **proteggere** un intero segmento di rete, eseguendo detection e classificazione delle anomalie sul traffico della rete, agendo con contromisure e risposte mirate nei casi di minacce critiche ed **effettuando una previsione intelligente** che fornisce un feedback di aggiornamento basato sulle ultime statistiche rilevate.

Agisce dove il firewall non può

LECS **copre l'intera superficie della rete**, non solo il perimetro, fornendo una protezione completa, anche nelle aree più "oscure" e nascoste dove le minacce proliferano maggiormente.

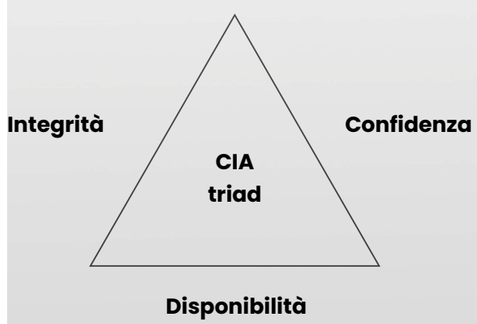
INTRODUZIONE ALLA BLOCKCHAIN

Logs sono ad **elevata resilienza**, in quanto sono scritti ed **encoded** in aree di memoria dedicate. Grazie ad algoritmi unici di DLT, assicura con **certezza metematica** che il contenuto di **LOG è invariato.**

PERCHÉ?

Compliance e Sicurezza che supporta aspetti legali, assicurativi e bancari.
Es. 62443, GDPR EU, ISO and many more.

BLOCKCHAIN E CIA T.



Lo scopo del task di notarizzazione è quello di sfruttare le caratteristiche della blockchain per rendere immutabili i record relativi agli attacchi più critici, cioè quelli a maggiore impatto per l'organizzazione.
La notarizzazione di un documento in blockchain consiste nel garantire l'immodificabilità dello stesso ad una certa data.
Infatti una volta stabilita una data di notarizzazione, si avrà la certezza assoluta che, in quella determinata data, quel documento sia immodificabile e integro.

BLOCKCHAIN NOTARIZATION

Il log notarizzato risulta integro in quanto **è sempre possibile verificarne la validità**; grazie all'utilizzo delle funzioni di hash le quali permettono di associare ad ogni documento una stringa univoca di 256 bit.
Nel caso in cui il documento cambi anche di un solo carattere il risultato della funzione di hash sarà diverso rispetto al valore di hash del documento notarizzato.
Pertanto, quando si notarizza un documento sulla blockchain, in realtà **non si invia il documento fisico**, ma un suo riferimento, unico al mondo, che si esprimerà in una formula a 256 bit.

BLOCKCHAIN SUMMIT

Sicurezza e ridondanza

Questa tecnologia rappresenta una **soluzione innovativa** rispetto ai metodi tradizionali, con enormi potenzialità per applicazioni in Cyber Security:

- Integrazione completa con i log di LECS;
- Elimina la necessità di eventuali firme digitali esterne;
- Riduce i rischi di frode assicurando trasparenza e tracciabilità rispetto alle soluzioni attuali:
- ogni modifica è registrata sulla blockchain, fornendo una traccia completa e verificabile. Garantisce sicurezza grazie alla crittografia e all'immutabilità della blockchain che protegge i documenti notarizzati da alterazioni e falsificazioni

L'unicità

Non solo il perimetro. **LECS** permette di raccogliere dati di movimenti nascosti e annidati nelle reti interne ad oggi sconosciuti.

L' implementazione di **LECS** in diversi punti, crea una GRID che permette di avere il controllo della superficie e congiuntamente ad EDR e Firewall, completa la gestione della sicurezza di un'AREA.

LECS è complementare a tutte le soluzioni e completa attivamente firewall, antivirus ed EDR nella gestione e nella detection.

Perché è così unico

Caratteristiche	Competitor	Tecnologia LECS
Tempo di attuazione	Da molte ore a intere giornate lavorative	10 minuti
Plug & Play	NO	SI
EDR Network Protection	Protegge solo i dispositivi con sistema operativo	Completa e protegge tutti i tipi di dispositivi anche senza OS
Air-Gap di ispirazione militare	NO	SI
Manutenzione e implementazione	Ecosistemi costosi	Scalabile per qualsiasi tipologia e grandezza di infrastruttura
Gestione del LOG	Solo cloud	Alta resilienza, locale, LAN interna e/o Cloud a seconda del modello
Caratteristiche aggiuntive	NO	Si, sistema di debug e controllo della sicurezza
Scalabilità e modularità	Molto difficile	Da Embedded a Dispositivo HW
Difficoltà di implementazione	Richiede una progettazione e studio per integrazione	Installabile in parallelo senza causare alcun blocco produttivo

I PIÙ ALTI STANDARD DI SICUREZZA

PRODOTTI

Ogni azienda ha esigenze diverse di sicurezza informatica in funzione della propria infrastruttura tecnologica e dell'ambito in cui opera.

LECS BUSINESS

Device base Plug&Play di detection e response, che protegge qualsiasi rete LAN dagli attacchi informatici più pericolosi con sistema brevettato di contromisura. Ottima per piccole aziende con pochi nodi di rete. Contromisura procedurale software. Design compatto con corpo in alluminio anodizzato.

LECS ENTERPRISE 2.0

Simile al modello Lecs +. Ha l'utilità di essere inserito all'interno del proprio armadio Rack, supportando più dispositivi. Ideale per aziende medio grandi. Supporta un numero host e banda di traffico superiore al Plus. Design per rack 1 U e mezza. Supporta protocolli industriali. Contromisura procedurale ed hardware con prese Shucko IEC13-14 220v

UNICA VERSIONE CON LA CONTROMISURA ENERGETICA

LECS CORE

Detection più potente grazie alle prestazioni di questo device. Perfetto per Corporate ed Enterprise. Ha un potente hardware che permette un'ispezione approfondita e il debug della rete. Grazie alle molteplici porte può fare detection e risposta multiplo con una sola Appliance.

LECS EMBEDDED/ SaaS

Versione personalizzata. Virtuale o hardware completamente integrabile nei macchinari.

LECS CUSTOM

Versione personalizzata. Perfetta per ambienti critici e implementazioni particolari virtualizzate.

LECS version	LECS Business	LECS Enterprise 2.0	LECS Core	LECS Core SFP
HW Features	ARM64 - DC	ARM64 - QC	x64 - 3.1Ghz	x64 - 3.7 Ghz
Phy Log Archiviation	32Gb	64Gb	128Gb	512Gb
RAM	2Gb	4Gb	8Gb	16Gb
Network Ports	1x Gigabit	1x Gigabit + Giga USB3 Adapt	4x Port 2.5Gb (3x Detection, 1x Data)	6x Port 1Gb (5x Detection, 1x Data) 2x SFP
Supported Unique Host	max 30 host	max 180 host	from 30 to 1000 host	>1000
Raccomanded Detection Bandwidth	<= 30 MB/s	<= 100 MB/s	400MB/s - **STD** 600MB/s - **PLUS** <750MB/s - **PRO**	<800MB/s - SFP
DETECTION				
DLT Cert Critical LOG	**YES**	**YES**	**YES**	**YES**
Full Tiresia AI Engine	BASIC	**YES**	**YES**	**YES**
Web Application & Dark Web	NO	**YES**	**YES**	**YES**
Specific Industry Procotols	NO	**YES**	**YES**	**YES**
Advanced Low Level Detection	NO	NO	**YES**	**YES**
Multi Network Correlation	NO	NO	**YES**	**YES**
REPONSE				
Automatic Freezing Injection Energetic AIR-GAP	**YES**	**YES**	**YES**	**YES**
Parallalel Network Freezing	NO	**YES**	-	-
LOG & NOTIFY Dashboard	NO	NO	**YES**	**YES**
Natural Language Chat				
	YES	**YES**	**YES**	**YES**
	YES	**YES**	**YES**	**YES**
SOC/SIEM Integration*	NO	NO	**YES**	**YES**
EMAIL	**YES**	**YES**	**YES**	**YES**
Weekly Report	**YES**	**YES**	**YES**	**YES**
Log Retention	**15 days**	**30 days**	**36 days (moroe days can be purchased)**	**36 days (moroe days can be purchased)**

LECS BUSINESS FEATURES TIRES-IA 1.0

Hybrid and balanced engine between server and appliance.

LECS ENTERPRISE 2.0 FEATURES TIRES-IA 2.0

More powerful multi-layered and more optimized engine.

LECS CORE FEATURES TIRES-IA 3.0

The most advanced and complex AI network in the range ,multi-source and multi-paradigm approach, with unique learning.

LECS CORE SFP FEATURES TIRES-IA 4.0

Top-of-the-line implementation of the engines, direct evolution of 3.0 , due to more available computational power, optimized for large trades.

LECS EMBEDDED

Algoritmi di Cyber-Protezione specifici per Industria ed IoT.
È possibile integrare LECS ad altri sistemi.

+ Multi-HW
arm32
arm64
x86 x64...

+ Multi-SW Edge
Container
Virtualizzazione Locale
e molto altro

+ Backend

Integrazione
server e/o servizi
digitali già presenti

Machinery & IoT
Protocolli IT ed OT
Semplifica la gestione della Cyber Security
Protezione device senza OS
Protezione sistemi SCADA

Compliance Normativo
Supporto:
IEC 62443 sugli IACS
NIS
NIST

Full-Integration
Integrabile con diversi approcci SW
Punto di vista stealth ed interno
Protegge dove firewall ed EDR non possono

Complementare
Piena integrabilità e compatbilità in ogni tipo di ambiente d' implementazione.
Sistema parallelo

CERTIFICAZIONI E BREVETTI.

Tecnologia Brevettata e Eccellenza Certificata LECS

Tecnologia Brevettata Certificazione ISO-27100 Certificazione NIST Framework 1.1 Certificazione NIST Framework SP800 Certificazione NIS-Directive hostravendem publisse teriumur ales condam

Tecnologia brevettata

Sistema di protezione della rete informatica e relativa procedura di sicurezza con estensione internazionale PCT. Di seguito la differenza tra **LECS** e le altre soluzioni.
LECS è complementare ad altre soluzioni di sicurezza.

Caratteristiche	LECS	Antivirus	Firewall	IPS
Plug & Play	✓	✗	✗	✗
Contromisure energetiche uniche	✓	✗	✗	✗
Proteggere attivamente i disp, IoT e Ind. IoT	✓	✗	✓	✓
Approccio completamente furtivo	✓	✗	✗	✓
Archiviazione fisica del LOG	✓		✗	✗
Protezione interna e innovativa di tipo POV	✓		✓	✓
Installazione in parallelo, senza passaggi	✓		✗	✓
Zero conoscenze tech per manutenzione	✓	✓	✗	✗
Approccio Blackbox	✓		✗	✗
Dashboard intuitiva	✓		✗	✗

I più alti standard di sicurezza.

It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.

— Stephane Nappo.