LIDATA

THE POWER OF PIONEERS

THE OLI ONE

LIDATA
THE POWER OF PIONEERS

THE OLI ONE

Businesses require an intelligent and collaborative security platform to counter increasingly sophisticated cyber threats - **THE OLI ONE**, the ultimate solution **against cybercrime**, is born!

THE OLI ONE offers a cutting-edge platform that combines proactive information sharing with powerful **Cyber AI** for real-time analysis of security events. It tracks IP addresses, assigns reliability scores, and automatically responds to threats, **ensuring timely and accurate protection**.

THE OLI ONE is a **100% Italian** solution, developed and maintained without foreign dependencies, ensuring **complete sovereignty over the data** and **technology used**.

OLIDATA
THE POWER OF PIONEERS

THE OLI ONE

Thanks to Olidata's established experience in **Big Data analysis** and the development of advanced **Artificial Intelligence systems** based on its proprietary "**Safe Mind**" technology, **THE OLI ONE** stands as a comprehensive and indispensable **Threat Intelligence system**.

The platform not only collects data, but actively **maps the entire IPv4 network**, constantly monitoring much of the **public Internet traffic** through observation of key public actors, ensuring comprehensive **threat surveillance**.

OLIDATA
THE POWER OF PIONEERS

Functional principles of Olidata THE OLI ONE

01 Intrusion detection

Constant analysis of network traffic to identify in real time potential threats from known and unknown sources, or the more sophisticated ones that often escape traditional controls.

02 AI Analysis

Artificial intelligence assigns a **reliability score to each IP address**, relying on an in-depth analysis of behavioral, historical, and contextual factors to anticipate attack tactics that have not yet emerged.

03 Intrusion prevention

Prevention rules are automatically updated in real time through continuous analysis of data collected from global sources and alternative channels, ensuring proactive protection and dynamically adapting to attack tactics.

04 Coordination of Rescue Operations

Data are sent in real time to the operations center, where they are displayed on **GIS** maps. This enables emergency coordinators to identify trouble spots and optimize the deployment of rescue teams, reducing response times.

LIDATA
THE POWER OF PIONEERS

The Numbers That Matter Against Cybercrime.

280 MLN Malignant Sources

THE OLI ONE constantly monitors **280 million malicious sources** in real time, providing comprehensive coverage against the most advanced and diverse **malware threats**.

Developed Plugins

THE OLI ONE offers a wide range of **developed plugins** that natively dialogue with the world's leading manufacturers of firewalls, IDS and IPS, and Server systems, enabling **centralized management** of security systems, collecting logs in real time and automatically sending blocking policies to neutralize attacks.

Response in 30 Seconds

THE OLI ONE's efficiency translates into extraordinary speed of response: only **30 seconds** from detection of a threat to its neutralization, ensuring an immediate and effective response and keeping the infrastructure secure against even the most dynamic threats.

LIDATA
THE POWER OF PIONEERS

The Key Modules

Intelligent Intrusion Detection

The intrusion detection module uses **machine learning** and **behavioral analysis**. This system not only recognizes already known attack patterns, but is also able to detect new emerging threats through its learning capability, anticipating and neutralizing potential risks before they compromise the infrastructure.

Dynamic Risk Assessment

The Cyber AI system assigns a **reliability value** to each monitored **IP address**, based on analysis of critical factors such as the address's historical behavior, its associations with **malicious activity**, and the context in which it operates.
The result is **targeted protection** that combines accuracy and speed to confront large-scale cybercrime.

Retriever of Threats of Network

This module collects data on potential threats from sources such as intelligence feeds, honeypots, and the dark web.
The system is enhanced by NLP (Natural Language Processing) modules that monitor more than **50,000 OSINT** and **CLOSINT** channels (Telegram, blogs in the Onion network, hacker markets).
The collected data is integrated into the Cyber AI system, improving threat detection and prevention, enabling rapid and targeted actions to **increase security** and **reduce response time**.

LIDATA
THE POWER OF PIONEERS

Logical Architecture of THE OLI ONE

01 Data Collection

THE OLI ONE's architecture is based on collecting data from a variety of sources, such as proprietary intelligence, external threat feeds, and system logs. This process enables **real-time mapping** of global cyber threats using a scalable system that handles large volumes of data efficiently.

02 Processing and Enrichment

The collected data is processed with artificial intelligence, which analyzes anomalous information, behaviors, and patterns. The system performs semantic analysis to improve the accuracy of reports and reduce false positives. It integrates intelligence feeds from traditional and non-traditional sources, such as the dark web and OSINT/CLOSINT channels, continuously enriching knowledge of emerging threats.

03 Distribution and Action

Processed data is turned into action with **THE OLI ONE** appliances, which send specific configurations in real time to security devices such as firewalls and routers. This ensures up-to-date defenses against threats.
Information is accessible through intuitive dashboards and customized reports, improving threat visibility and responsiveness of the enterprise infrastructure.

Added Value of THE OLI ONE

Customised Reports

THE OLI ONE offers customisable reports with detailed analysis of network traffic, distinguishing legitimate activity from attacks. Reports include tailored metrics, threat trends and recommendations to improve security team decisions.

Protection Without Compromises

THE OLI ONE detects and neutralises complex threats with advanced accuracy. The Cyber AI system identifies more than **15 per cent** of traffic as potentially malicious, focusing on critical and high-risk threats, reducing risks to the corporate infrastructure.

STIX 2.0 integration

THE OLI ONE uses the **STIX 2.0** standard to share threat information, improving integration with external platforms and collaboration between security actors. This enhances the defence against cyber attacks globally and accelerates the effectiveness of countermeasures.

Advanced API

THE OLI ONE's advanced APIs offer seamless integration with third-party systems, enhancing security and enabling automation and customised integrations. This provides flexibility for organisations to extend and optimise security functionality.

OLIDATA
THE POWER OF PIONEERS

The Future of Cybersecurity with THE OLI ONE

Continuous Innovation

Olidata is a leader in **cybersecurity**, committed to continuous innovation that integrates research and development with emerging technologies. The goal is to **anticipate threats**, keeping THE OLI ONE one step ahead of attacks, predicting and neutralising them before they occur.

Global Expansion

Olidata, with THE OLI ONE, is mapping the IPv4 Internet to expand its global coverage and create a resilient defence network. The platform analyses threats in real time, **offering proactive protection against cybercrime**, and becoming essential to the security of critical infrastructure and global networks.

Collaboration and Sharing

The future of cybersecurity relies on collaboration and sharing of critical information. Olidata THE OLI ONE acts as a catalyst, developing a **collective intelligence network against cybercrime** and, through standards such as STIX 2.0, facilitates secure threat sharing, improving the response to large-scale attacks.

Advanced Artificial Intelligence

THE OLI ONE integrates advanced **artificial intelligence technologies**, offering predictive capabilities to identify and neutralise threats in advance. Its AI continuously learns from data, improving accuracy and adapting to new attacks, thus ensuring proactive and intelligent protection.

LIDATA
THE POWER OF PIONEERS

THE OLI ONE

OLIDATA
THE POWER OF PIONEERS

OLI-ONE

Dashboard | Perimetro | Intelligence | Alleanza | Impostazioni | Lucky

Attacchi Mitigati Oggi
325

Configurazioni Inviate
52

Fonti Attive nell'alliance
1450

Nuove Minacce Rilevate
8

Minacce Attive
3

Distribuzione Rapida delle Regole

Regole Generate
120

Tempo Medio di Distribuzione
45s

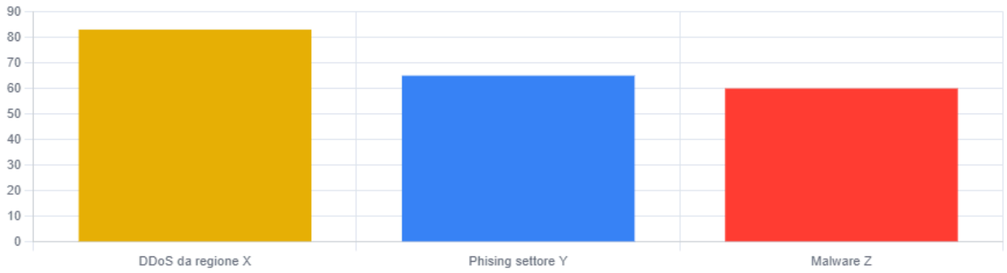
Dispositivi Aggiornati
150

Fonti di Intelligence
25

Tipi di Minacce Rilevate

Attacchi Mitigati nelle Ultime 24 Ore

Analisi Machine Learning - Previsioni Proattive



LIDATA
THE POWER OF PIONEERS

OLI-ONE

Dashboard | Perimetro | Intelligence | Alleanza | Impostazioni | Lucky

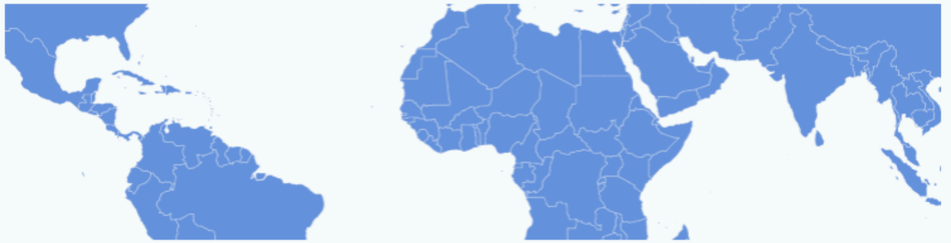
SFERADEFENCE

Sfera Defence Srl

sferadefence.com

Livello di Esposizione

Dominio Radice	sferadefence.com
Sito Istituzionale	https://www.sferadefence.com
Indirizzo IP	34.89.127.226
Fornitore di Cloud	Google



1000
Domini Relativi

373
Sottodomini

72
Indirizzi IP

76
Prodotti e Tecnologie

208
Vulnerabilità

139
Porte Aperte

Dispositivi Connessi

Cerca

Nome Dispositivo	Tipo	Stato	Ultimo Aggiornamento	Azioni
Cerca per nome	Cerca per tipo	Seleziona		
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli
Firewall-Branch-01	Firewall	Aggiornato	04/10/24, 16:04	Dettagli

« ‹ 1 › » 10

Logs di Sistema

Cerca

Timestamp	Fonte	Indirizzo IP	Tipo di Minaccia	Azione Intrapresa	Azioni
	Cerca per fonte	Cerca per IP	Cerca per tipo di minaccia	Seleziona	
04/10/24, 16:11	Server-Web 01	192.0.2.10	SQL Injection	Bloccato	Visualizza
04/10/24, 16:11	Server-Web 01	192.0.2.10	SQL Injection	Bloccato	Visualizza
04/10/24, 16:11	Server-Web 01	192.0.2.10	SQL Injection	Bloccato	Visualizza
04/10/24, 16:11	Server-Web 01	192.0.2.10	SQL Injection	Bloccato	Visualizza
04/10/24, 16:11	Server-Web 01	192.0.2.10	SQL Injection	Bloccato	Visualizza

« ‹ 1 › » 10

Configurazioni Inviate

Cerca

ID Configurazione	Dispositivo	Tipo	Stato	Data	Azioni
Cerca per ID	Cerca per dispositivo	Cerca per tipo	Seleziona		
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli

Configurazioni Inviate

Cerca

ID Configurazione	Dispositivo	Tipo	Stato	Data	Azioni
Cerca per ID	Cerca per dispositivo	Cerca per tipo	Seleziona		
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli
CFG-20231010-001	Firewall-Branch-02	Aggiornamento Regole	Completato	04/10/24, 16:11	Dettagli

« ‹ 1 › » 10

Intelligence Web Canali Hacker - Minacce Recenti

- 16:11 - Vulnerabilità zero-dat per Apache Server rilevata
- 16:11 - Vulnerabilità zero-dat per Apache Server rilevata
- 16:11 - Vulnerabilità zero-dat per Apache Server rilevata
- 16:11 - Vulnerabilità zero-dat per Apache Server rilevata
- 16:11 - Vulnerabilità zero-dat per Apache Server rilevata

Notifiche Recenti

- 16:11 - Configurazione aggiornata inviata al Firewall FW-01
- 16:11 - Configurazione aggiornata inviata al Firewall FW-01
- 16:11 - Configurazione aggiornata inviata al Firewall FW-01
- 16:11 - Configurazione aggiornata inviata al Firewall FW-01
- 16:11 - Configurazione aggiornata inviata al Firewall FW-01

Intelligence Web Canali Hacker

- **16:11** - Vulnerabilità zero-day per Apache Server rilevata
- **16:11** - Vulnerabilità zero-day per Apache Server rilevata
- **16:11** - Vulnerabilità zero-day per Apache Server rilevata
- **16:11** - Vulnerabilità zero-day per Apache Server rilevata

LIDATA
THE POWER OF PIONEERS

OLI-ONE

Dashboard | Perimetro | Intelligence | Alleanza | Impostazioni | Lucky

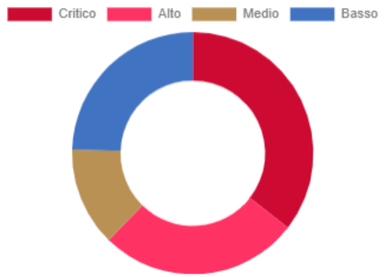
CONNESSIONI TOTALI
183.939
100,00%

CONNESSIONI LEGITTIME
137.496
74,75%

POTENZIALMENTE DANNOSE
29.944
16,28%

DANNOSE
16.499
8,97%

TRAFFICO DANNOSO PER PUNTEGGIO DI CRIMINALITÀ



183939
Traffico consentito

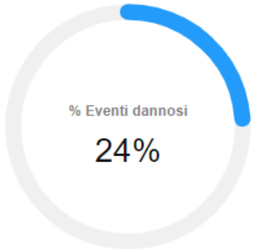
14136
Attori unici

17530
Rischio Basso e Medio

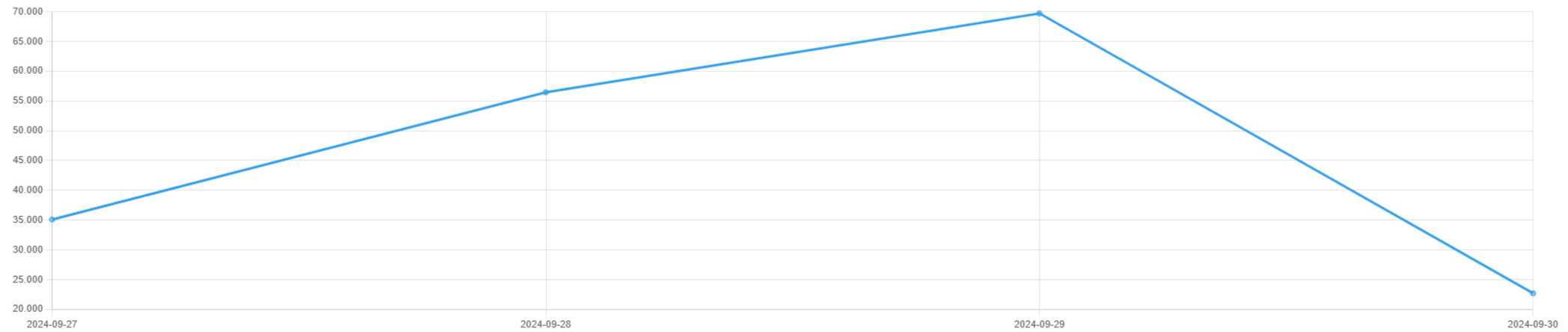
28913
Rischio Elevato e Critico

402
Attachi ogni ora

PERCENTUALE TRAFFICO DANNOSO



ANALISI TEMPORALE DELL'ATTIVITÀ DI RETE



PRINCIPALI EVENTI DANNOSI

Cerca

Attore	Data	Dispositivo	Direzione	Punteggio in tempo reale	Servizio	Paese
Cerca		Cerca	Cerca	Cerca	Cerca	Cerca
93.113.63.8	27/09/24, 23:03	Checkpoint	inbound	440	SMTP	Turkey
93.113.63.8	28/09/24, 11:03	Checkpoint	inbound	437	ssh	Turkey
93.113.63.8	28/09/24, 14:04	Fortigate	outbound	437	ssh	Turkey
93.113.63.8	29/09/24, 15:04	Checkpoint	inbound	433	RDP	Turkey
93.113.63.8	29/09/24, 16:03	Fortigate	inbound	432	SMTP	Turkey
93.113.63.8	29/09/24, 20:04	CISCO	inbound	424	SMTP	Turkey

OLIDATA

THE POWER OF PIONEERS

www.olidata.com

info@olidata.com

+39 06 9432 0183

Via Giulio Vincenzo Bona, 120A,
00156 - RM