LIDATA

THE POWER OF PIONEERS

THE OLI ONE

THE OLI ONE

Le aziende richiedono una piattaforma di sicurezza intelligente e collaborativa per contrastare minacce cyber sempre più sofisticate: è nata **THE OLI ONE,** la soluzione definitiva **contro il cybercrime!**

THE OLI ONE offre una piattaforma all'avanguardia che unisce la condivisione proattiva delle informazioni con una potente **Cyber AI** per l'analisi in tempo reale degli eventi di sicurezza. Essa traccia indirizzi IP, assegna punteggi di affidabilità e risponde automaticamente alle minacce, **garantendo una protezione tempestiva e precisa**.

THE OLI ONE è una soluzione **100% italiana**, sviluppata e mantenuta senza dipendenze estere, garantendo la **completa sovranità sui dati** e sulla **tecnologia utilizzata**.

THE OLI ONE

Grazie all'esperienza consolidata di Olidata nell'analisi dei **Big Data** e nello sviluppo di sistemi avanzati di **Intelligenza Artificiale**, basati sulla tecnologia proprietaria "**Safe Mind**", **THE OLI ONE** si pone come un sistema di **Threat Intelligence completo e indispensabile**.

La piattaforma non solo raccoglie dati, ma **mappa attivamente l'intera rete IPv4**, monitorando costantemente gran parte del **traffico Internet pubblico** attraverso l'osservazione di attori pubblici chiave, garantendo una **sorveglianza globale** delle minacce.

OLIDATA
THE POWER OF PIONEERS

Principi funzionali di Olidata THE OLI ONE

01 Rilevamento delle intrusioni

Analisi costante del traffico di rete per identificare in tempo reale potenziali minacce provenienti da fonti conosciute e sconosciute, o le più sofisticate che spesso sfuggono ai controlli tradizionali.

02 Analisi AI

L'intelligenza artificiale assegna un **punteggio di affidabilità a ogni indirizzo IP**, basandosi su un'analisi approfondita di fattori comportamentali, storici e contestuali per anticipare tattiche di attacco non ancora emerse.

03 Prevenzione delle intrusioni

Le regole di prevenzione vengono aggiornate automaticamente in tempo reale grazie all'analisi continua dei dati raccolti da fonti globali e canali alternativi, garantendo una protezione proattiva e adattandosi dinamicamente alle tattiche di attacco.

04 Coordinamento delle Operazioni di Soccorso

I dati sono inviati in tempo reale alla centrale operativa, dove vengono visualizzati su mappe **GIS**. Ciò consente ai coordinatori di emergenza di identificare i punti critici e ottimizzare l'intervento delle squadre di soccorso, riducendo i tempi di risposta.

LIDATA
THE POWER OF PIONEERS

I Numeri che Contano Contro il Cybercrime

280 MLN Sorgenti Maligne

THE OLI ONE monitora costantemente **280 milioni di sorgenti malevole** in tempo reale, garantendo una copertura globale contro le **minacce informatiche** più avanzate e diversificate.

Plugin Sviluppati

THE OLI ONE offre una vasta gamma di **plugin sviluppati** che dialogano nativamente con i maggiori produttori mondiali di firewall, IDS e IPS e sistemi Server, consentendo una **gestione centralizzata** dei sistemi di sicurezza, raccogliendo i log in tempo reale e inviando automaticamente le policy di blocco per neutralizzare gli attacchi.

Risposta in 30 Secondi

L'efficienza di **THE OLI ONE** si traduce in una velocità di reazione straordinaria: solo **30 secondi** dal rilevamento di una minaccia alla sua neutralizzazione, garantendo una risposta immediata ed efficace e mantenendo l'infrastruttura sicura anche contro le minacce più dinamiche.

LIDATA
THE POWER OF PIONEERS

I Moduli Chiave

Rilevamento Intrusioni Intelligente

Il modulo di rilevamento delle intrusioni utilizza **machine learning** e **analisi comportamentale**. Questo sistema non solo riconosce pattern di attacco già noti, ma è anche in grado di rilevare nuove minacce emergenti grazie alla sua capacità di apprendimento, anticipando e neutralizzando potenziali rischi prima che compromettano l'infrastruttura.

Valutazione del Rischio Dinamica

Il sistema di Cyber AI assegna un **valore di affidabilità** a ogni **indirizzo IP** monitorato, basandosi su analisi di fattori critici quali il comportamento storico dell'indirizzo, le sue associazioni con attività maligne e il contesto in cui opera.
Il risultato è una **protezione** mirata che combina accuratezza e velocità per fronteggiare il cybercrime su larga scala.

Retriever di Minacce di Rete

Questo modulo raccoglie dati su potenziali minacce da fonti come feed di intelligence, honeypot e dark web.
Il sistema è potenziato da moduli di NLP (Natural Language Processing) che monitorano oltre **50.000 canali** OSINT e CLOSINT (Telegram, blog nella rete Onion, mercati di hacker).
I dati raccolti vengono integrati nel sistema Cyber AI, migliorando il rilevamento e la prevenzione delle minacce, consentendo azioni rapide e mirate per **aumentare la sicurezza** e **ridurre i tempi di risposta**.

Architettura Logica di THE OLI ONE

01 Raccolta Dati

L'architettura di **THE OLI ONE** si basa sulla raccolta di dati da diverse fonti, come intelligence proprietarie, feed di minacce esterne e log di sistema. Questo processo consente di **mappare in tempo reale** le minacce cyber globali, utilizzando un sistema scalabile che gestisce grandi volumi di dati in modo efficiente.

02 Elaborazione e Arricchimento

I dati raccolti vengono elaborati con intelligenza artificiale, che analizza informazioni, comportamenti e pattern anomali. Il sistema esegue analisi semantiche per migliorare la precisione delle segnalazioni e ridurre i falsi positivi. Integra feed di intelligence da fonti tradizionali e non, come il dark web e canali OSINT/CLOSINT, arricchendo continuamente la conoscenza delle minacce emergenti.

03 Distribuzione e Azione

I dati elaborati vengono trasformati in **azioni concrete** grazie agli appliance **THE OLI ONE**, che inviano in tempo reale configurazioni specifiche a dispositivi di sicurezza come firewall e router. Questo garantisce difese sempre aggiornate contro le minacce.
Le informazioni sono accessibili tramite dashboard intuitive e report personalizzati, migliorando la visibilità delle minacce e la capacità di risposta dell'infrastruttura aziendale.

Valore Aggiunto di THE OLI ONE

Report Personalizzati

THE OLI ONE offre report personalizzabili con analisi dettagliata del traffico di rete, distinguendo attività legittime da attacchi. I report includono metriche su misura, trend delle minacce e raccomandazioni per migliorare le decisioni del team di sicurezza.

Protezione Senza Compromessi

THE OLI ONE rileva e neutralizza minacce complesse con precisione avanzata. Il sistema Cyber AI identifica oltre il **15%** del traffico come potenzialmente maligno, concentrandosi su minacce critiche e ad alto rischio, riducendo i rischi per l'infrastruttura aziendale.

Integrazione STIX 2.0

THE OLI ONE utilizza lo **standard STIX 2.0** per condividere informazioni sulle minacce, migliorando l'integrazione con piattaforme esterne e la collaborazione tra attori della sicurezza. Ciò potenzia la difesa contro attacchi informatici a livello globale e accelera l'efficacia delle contromisure.

API Avanzate

Le API avanzate di **THE OLI ONE** offrono integrazione fluida con sistemi di terze parti, potenziando la sicurezza e permettendo automazione e integrazioni su misura. Questo garantisce flessibilità alle organizzazioni nell'ampliare e ottimizzare le funzionalità di sicurezza.

OLIDATA
THE POWER OF PIONEERS

Il Futuro della Cybersecurity con THE OLI ONE

Innovazione Continua

Olidata è leader nella **cybersecurity**, impegnata in un'innovazione continua che integra ricerca e sviluppo con tecnologie emergenti. L'obiettivo è **anticipare le minacce**, mantenendo THE OLI ONE sempre un passo avanti rispetto agli attacchi, prevedendoli e neutralizzandoli prima che si verifichino.

Collaborazione e Condivisione

Il futuro della cybersecurity si fonda sulla collaborazione e condivisione di informazioni critiche. Olidata THE OLI ONE funge da catalizzatore, sviluppando una **rete di intelligence collettiva contro il cybercrime** e, attraverso standard come **STIX 2.0**, facilita la condivisione sicura delle minacce, migliorando la risposta agli attacchi su larga scala.

Espansione Globale

Olidata, con THE OLI ONE, sta mappando l'**Internet IPv4** per ampliare la propria copertura globale e creare una rete di difesa resiliente. La piattaforma analizza minacce in tempo reale, offrendo **protezione proattiva contro il cybercrime**, e diventando essenziale per la sicurezza delle infrastrutture critiche e delle reti globali.

Intelligenza Artificiale Avanzata

THE OLI ONE integra **tecnologie avanzate di intelligenza artificiale**, offrendo capacità predittive per identificare e neutralizzare minacce in anticipo. La sua AI apprende continuamente dai dati, migliorando la precisione e adattandosi a nuovi attacchi, garantendo così una protezione proattiva e intelligente.

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

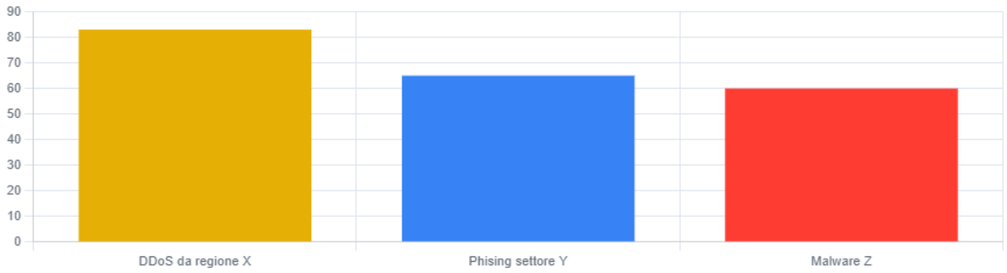
Dispositivi Aggiornati
150

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

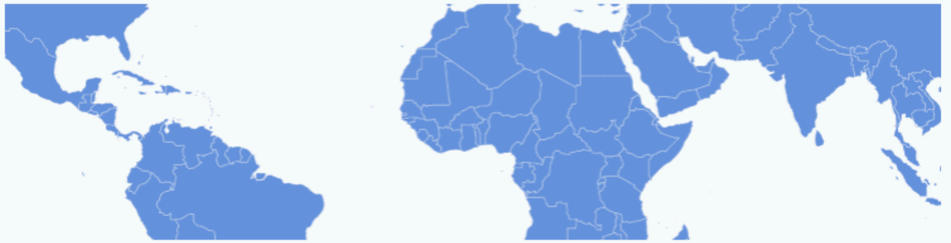
SFERADEFENCE

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

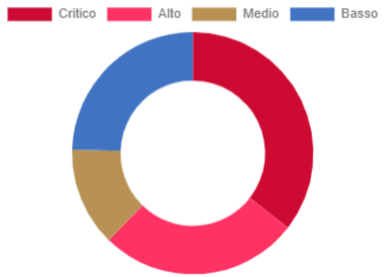
CONNESSIONI TOTALI
183.939
100,00%

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

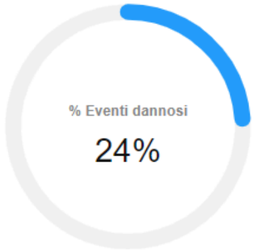
14136
Attori unici

17530
Rischio Basso e Medio

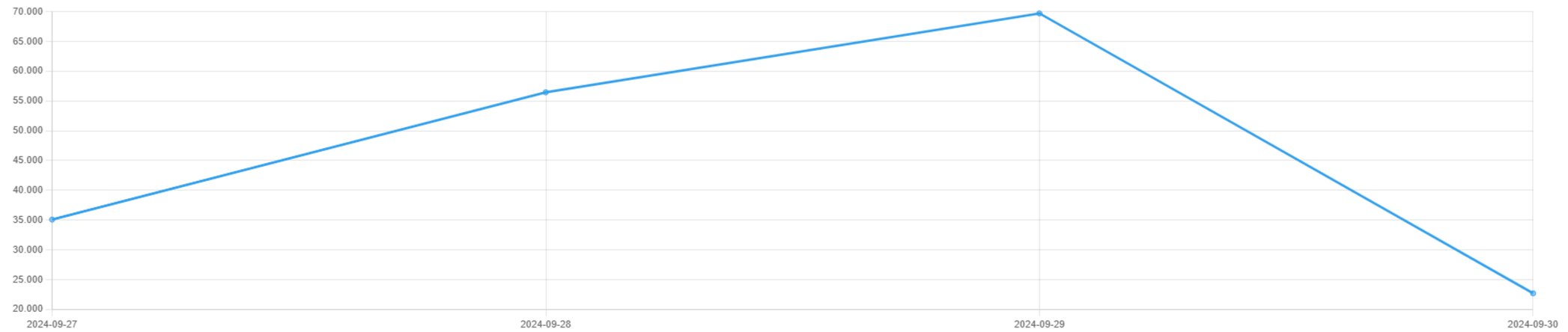
28913
Rischio Elevato e Critico

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