



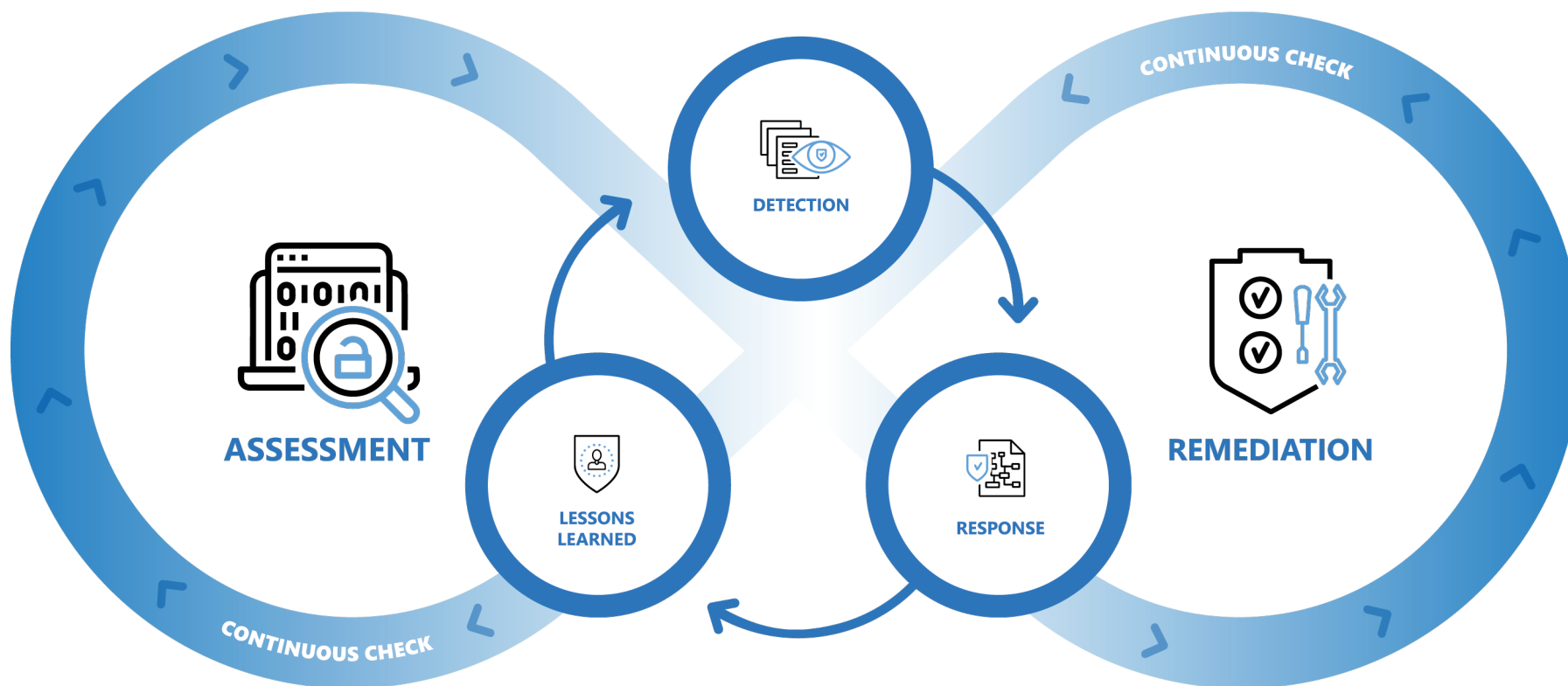
# SOC

Security Operation Center



# Cyber Pro

Cyber Pro ha l'obiettivo di contribuire a creare una **cultura diffusa della sicurezza informatica**.  
Puntiamo a ridefinire il concetto di **Cyber Security** attraverso lo **sviluppo di soluzioni e servizi innovativi** in grado di agire efficacemente non solo sul **fattore tecnologico**, ma anche sul **fattore umano**.

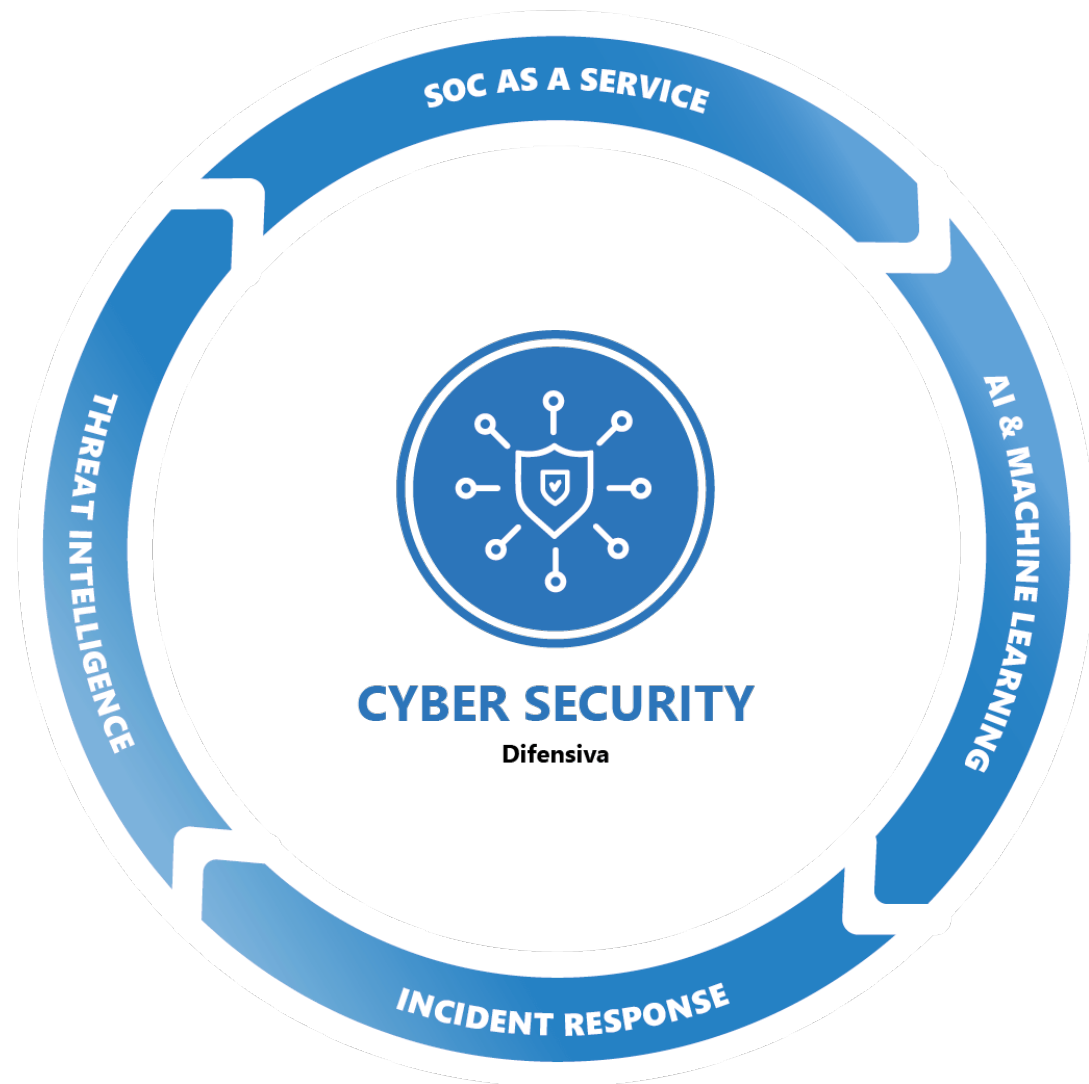


## Difendersi nel modo corretto salva i dati!

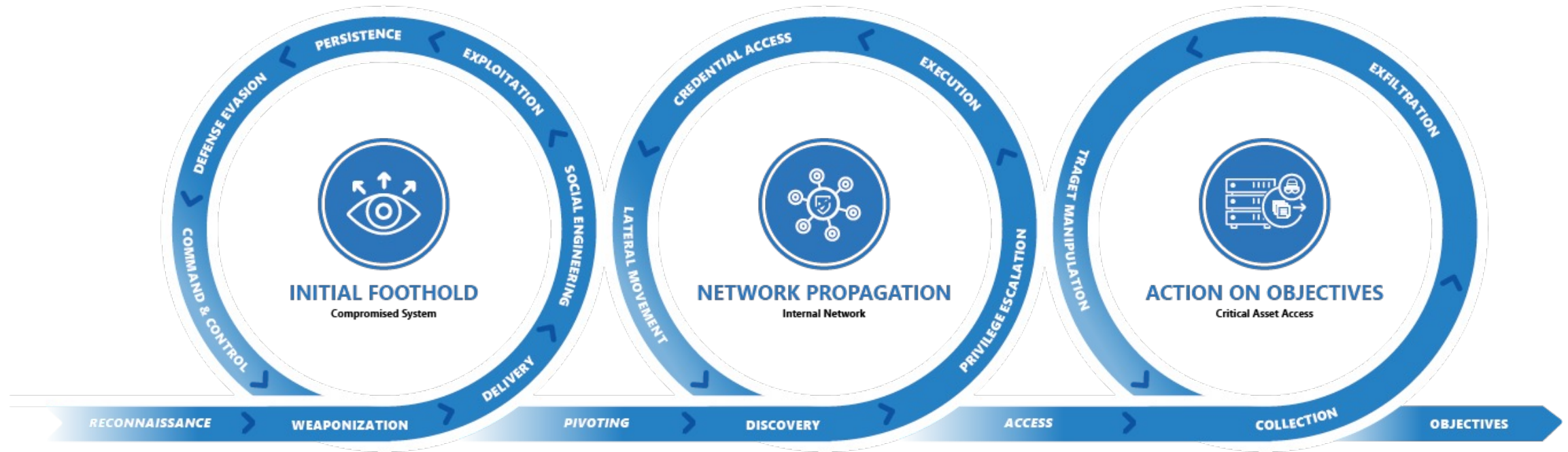
### Security Operation Center (SOC)

ha l'obiettivo di identificare le attività malevole che coinvolgono i sistemi IT aziendali.

Tramite l'adozione di tecnologie che garantiscono visibilità sugli eventi di sicurezza **gli analisti del SOC del team di Cyber Pro possono identificare e gestire gli attacchi informatici in modo da evitare che questi si propaghino sulla rete**, con lo scopo di compromettere il funzionamento dei servizi aziendali fondamentali per garantire l'operatività e la produttività dell'organizzazione.



# Come si muove un attaccante



In seguito alla rilevazione di un'anomalia potranno essere attivate delle prime misure di contenimento e allertato prontamente il cliente in modo da poter procedere con le successive attività necessarie al ripristino del livello di sicurezza dei sistemi coinvolti.



# Rilevazione delle minacce cyber

## Cyber Security Operation Center

### CARATTERISTICHE

- ✓ Servizio erogato dalla struttura SOC
- ✓ Supporto h24
- ✓ Servizio certificato ISO27001

### FUNZIONALITÀ

- ✓ Analisi degli eventi di sicurezza e dei flussi di rete
- ✓ Identificazione di comportamenti anomali o compromissioni
- ✓ Interfacciamento con le sorgenti di Cyber Intelligence
- ✓ Utilizzo di una o più «sonde»



# Rilevazione delle minacce cyber

Certificazioni associate ai servizi

ISO 27018



ISO 9001



ISO 27701



ANSI TIA 942



ISO 14001



ISO 27001



ISO 20000



AGID Agenzia per l'Italia Digitale



ISO 27017



ISO 22301



# Attività di Incident Response

Cyber Pro adotta il modello **NIST di Incident Response**



# Risposta alle minacce Cyber

Servizio SOC- Stack Tecnologico

MDR

SIEM

NDR



## VISIBILITÀ

Raccolta, correlazione e interrogazione delle informazioni relative all'incident

SOAR



## ORCHESTRAZIONE

Gestione delle comunicazioni verso tutti gli stakeholders, automazione di analisi e attività di risposta all'incident

MDR

NDR



## RISPOSTA

Isolamento dei sistemi compromessi in modo da contenere l'attacco

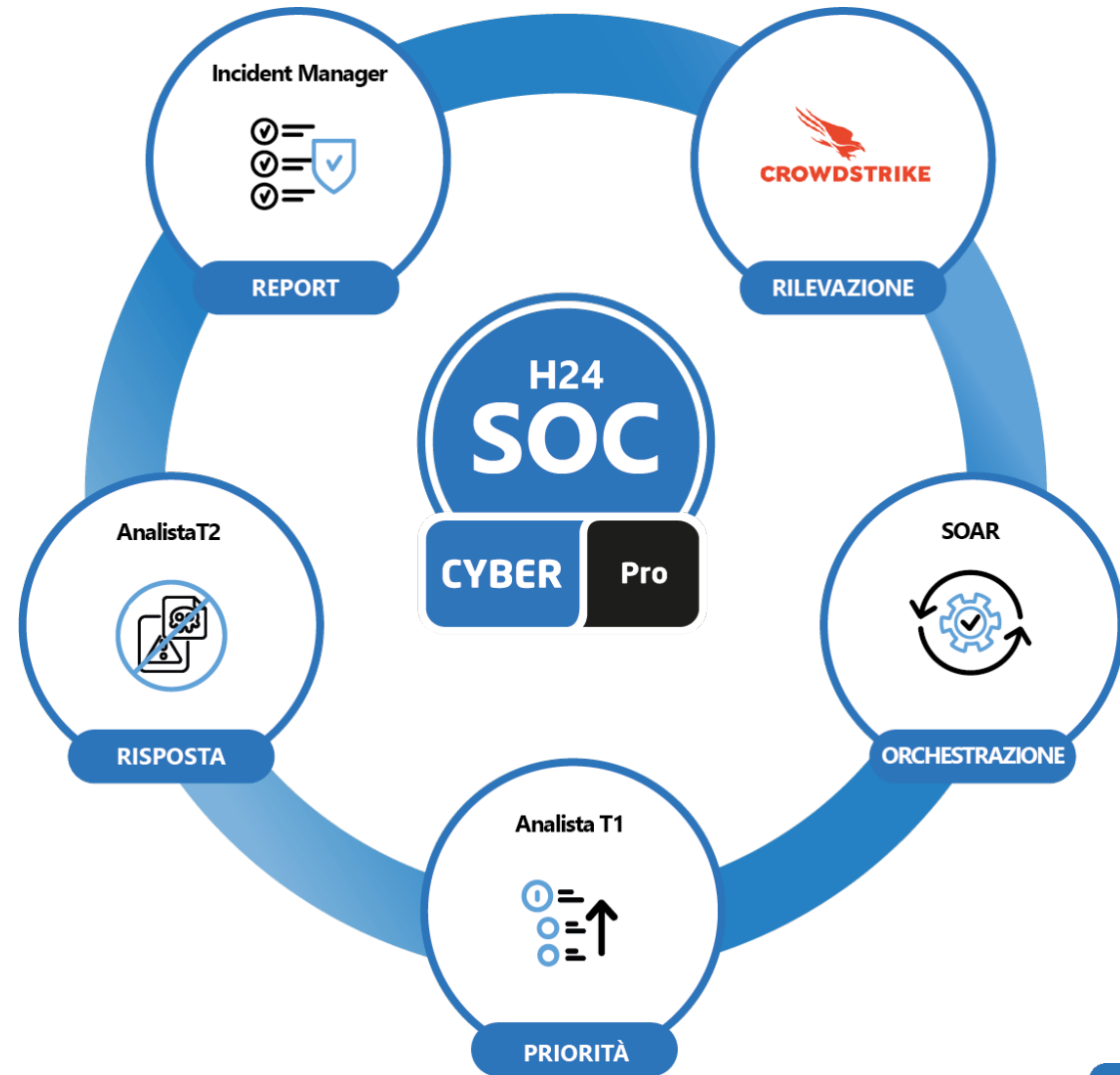


# Rilevazione delle minacce Cyber

Cyber SOC - Processo di Incident Response

Le tecnologie sono integrate in un processo unificato di gestione degli Incidenti di Sicurezza.

Questo modello permette di rilevare e rispondere in tempo reale al verificarsi di un'anomalia.



# Rilevazione delle minacce Cyber

Cyber SOC-SLA di servizio

L'attività di **Incident Management** comprende una prima fase di contenimento automatica applicata dai sistemi EDR e supervisionata dal SOC di Cyber Pro

Gravità	Livello	SLA (presa in carico+mitigazione+analisi+segnalazione)
 P4	basso	8 ore
 P3	medio	4 ore
 P2	alto	2 ore
 P1	critico	1 ora

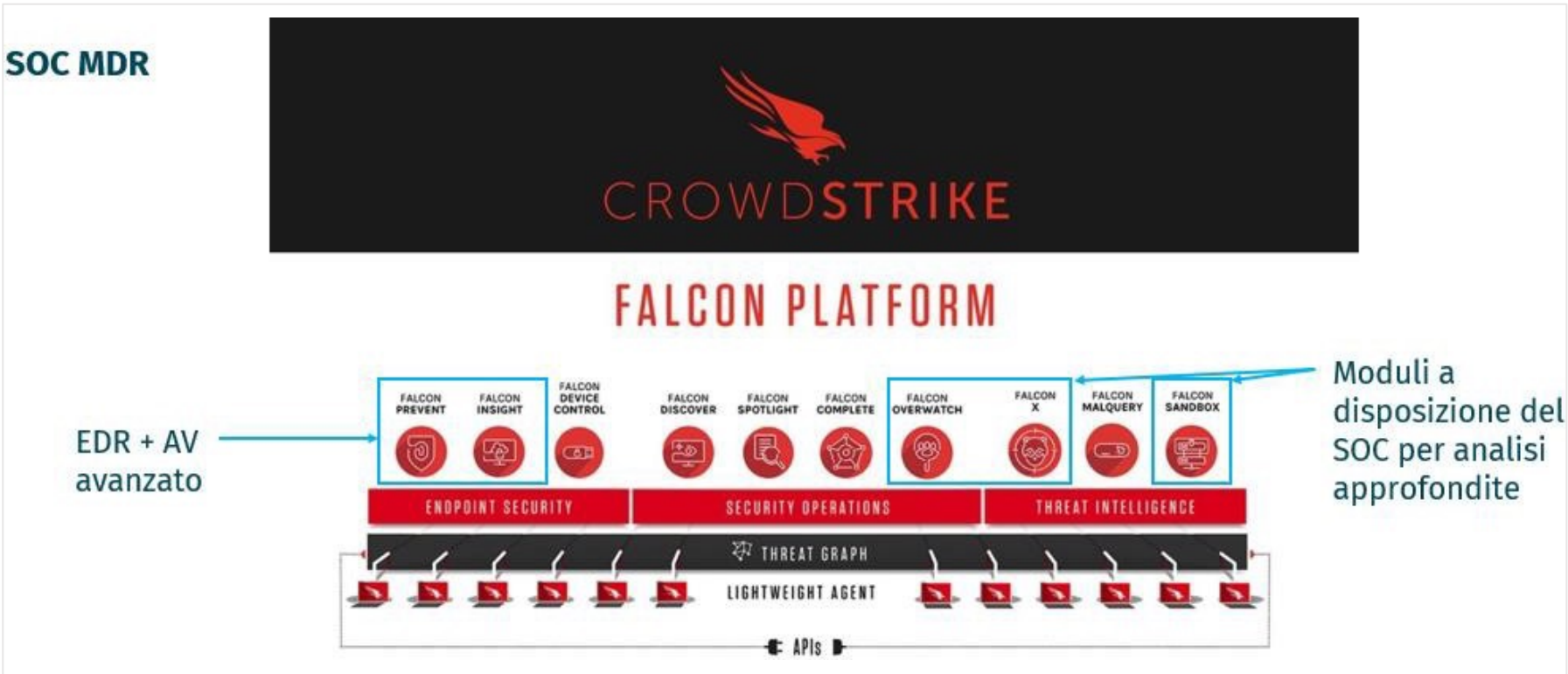


# SOC - MDR

MDR – protezione client e server

## Obiettivo del servizio:

Protezione dei sistemi client e server con focus sulle minacce malware.



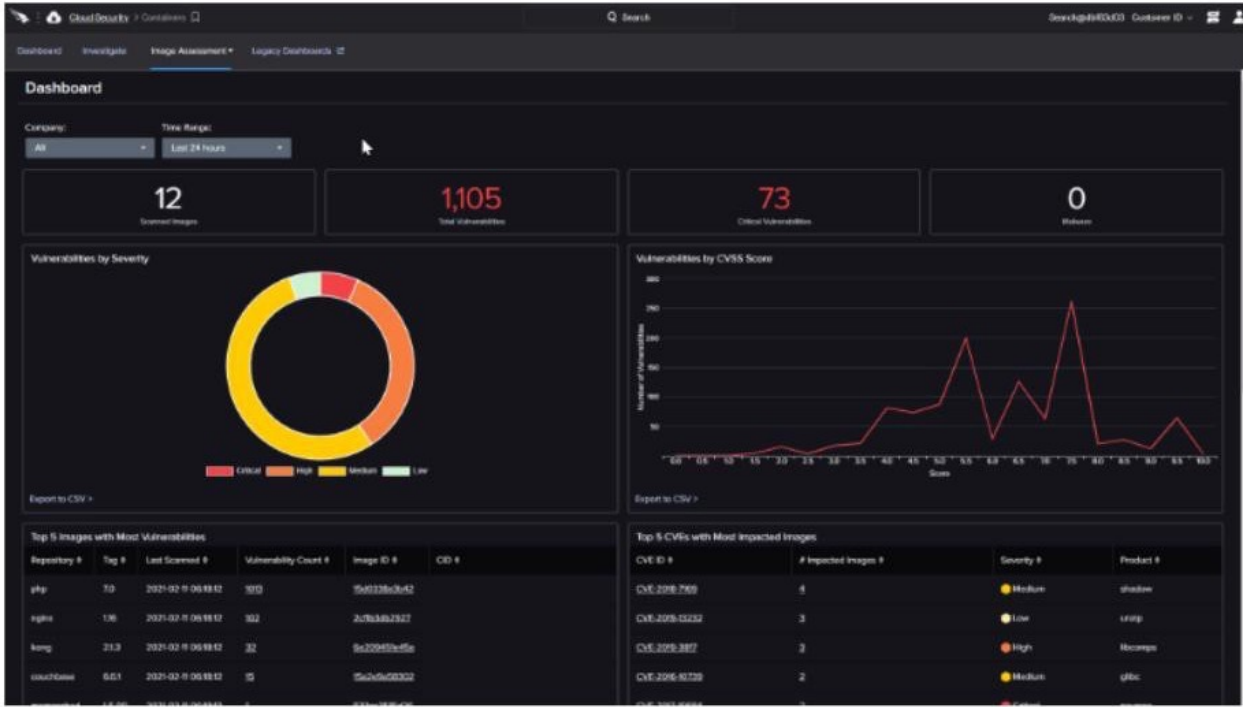


# SOC - MDR

MDR – protezione dei container

## Obiettivo del servizio:

Protezione dell'infrastruttura AWS con focus sulla sicurezza dei pod in termini di immagini e di runtime.



Hosts / Groups / Default Pod Namespace Group

Back to Default Pod Namespace Group Details

Choose filter values for "Default Pod Namespace Group". Matching hosts are automatically assigned to this group.

Host	Exclude	Grouping	Domain	OS Version	OU	Site	Platform	Pod ID	Pod Labels	Pod Name	Pod Namespace	Pod Service Account	Type	Status									
WIN-NJA	N/A	54	N/A	68	Windows...	N/A	68	N/A	68	Windows...	43	N/A	54	apponem...	N/A	54	Namespace	Account	Workst...	41	Normal	67	
SE-4	N/A	36	N/A	68	Linux	N/A	68	Linux	22	2a5c771c...	1	apponem...	5	mariaadb...	1	N/A	54	Pod	19	Contain...	1		
SE-4	N/A	15	N/A	68	Windows...	N/A	68	Windows...	5	43a9d40...	1	pod term...	5	mariaadb...	1	default	13	N/A	54	Server	8		
SE-4	N/A	3	N/A	68	Big Sur C...	N/A	68	Big Sur C...	1	0714023...	1	apponem...	3	mariaadb...	1	lumen sp...	1	default	14				
SE-4	N/A	3	N/A	68	Catalina	N/A	68	Catalina	1	5b2c96e...	1	pod term...	3	mariaadb...	1								



# SOC - MDR

MDR – Cyber Threat Intelligence

## Obiettivo del servizio:

Acquisire informazioni riguardo i threat actors e le tecniche/tattiche d'attacco sfruttate

**Details**

First seen date	Status	Actor type
Jun 2009	Active	eCrime
Last seen date	Motivation	Origins
Nov 2022	Criminal	Russian Federa... Eastern Europe

Target industries  
[Financial Services](#) [Manufacturing](#) [Real Estate](#) [Hospitality](#)  
[Logistics](#) [Telecommunications](#) [Pharmaceutical](#) [Energy](#)  
[Healthcare](#) [Insurance](#) [Aerospace](#) [Food and Beverage](#) [Energy](#)  
[Academic](#) [NGO](#) [Biomedical](#) [Consumer Goods](#) [Transportation](#)  
[Consulting and Professional Services](#) [Technology](#) [Retail](#)  
[Food and Beverage](#) [Automotive](#) [Industrials and Engineering](#)  
[Local Government](#)

Target countries  
[United States](#) [Netherlands](#) [Poland](#) [South Africa](#) [Canada](#)  
[Sweden](#) [Japan](#) [India](#) [United Kingdom](#) [Germany](#) [Argentina](#)

**Actor activity**

Sandbox reports	Endpoint detections	Vulnerabilities
0	0	Learn more at the CS store

**Threat intelligence**

Intel reports	Total indicators
Learn more about Falcon Intelligence Premium	683K

**Actors**

**MALLARD SPIDER** [See more about this Actor](#)

Last active	Status	Origin
Nov 2022	Active	Russian Federation, Ea...
Intel reports	Target industries	Target countries
0	25	13
Actor type	Motivation	
eCrime	Criminal	

Community identifiers  
 GOLD LAGOON, Qakbot, QBot, Quakbot, QakBot, PinkSlip

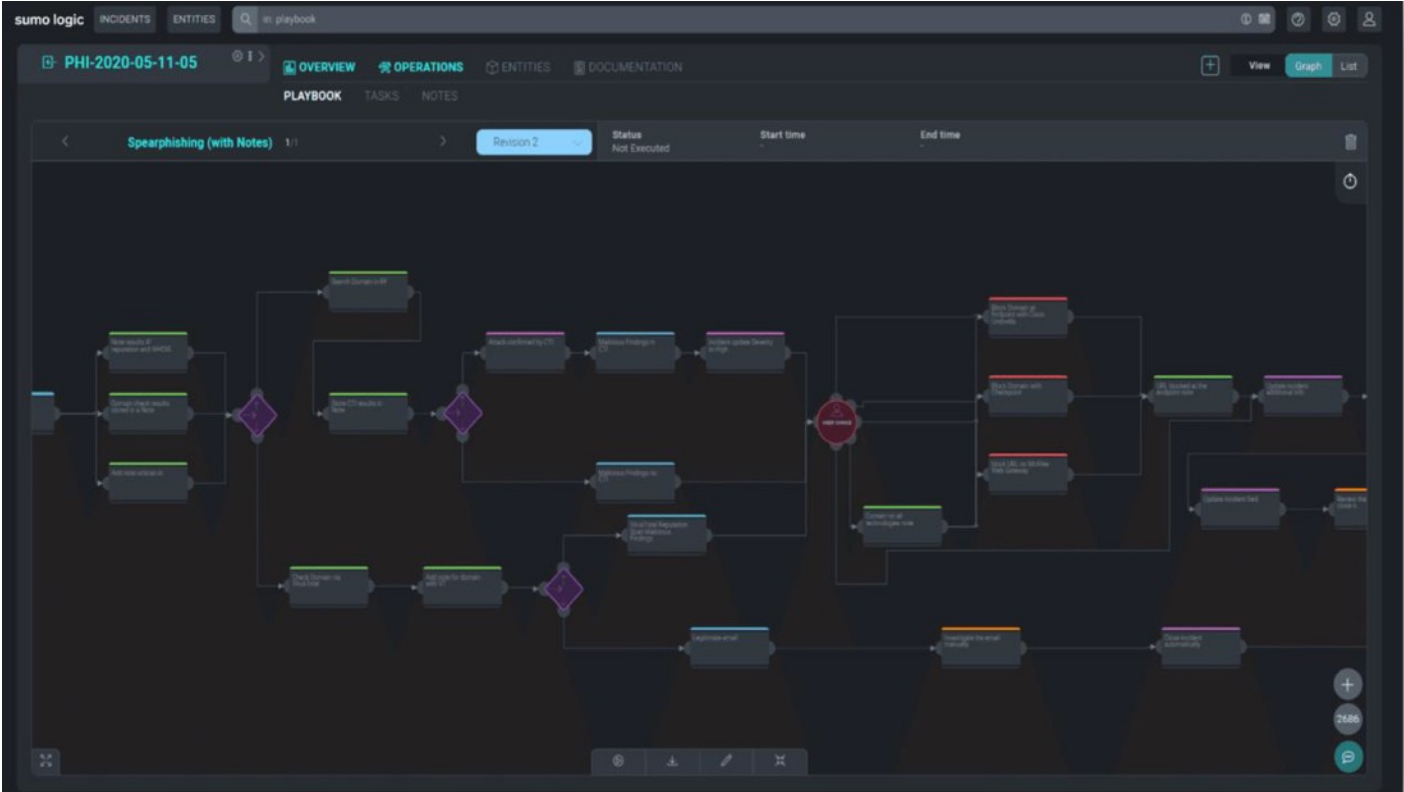


# SOC - SOAR

SOAR-Sumo Logic Orchestrazione

### Obiettivo del servizio:

Gestione, Rilevazione e Orchestrazione degli Incidenti di Sicurezza. I workflow vengono definiti sulla base delle esigenze di servizio



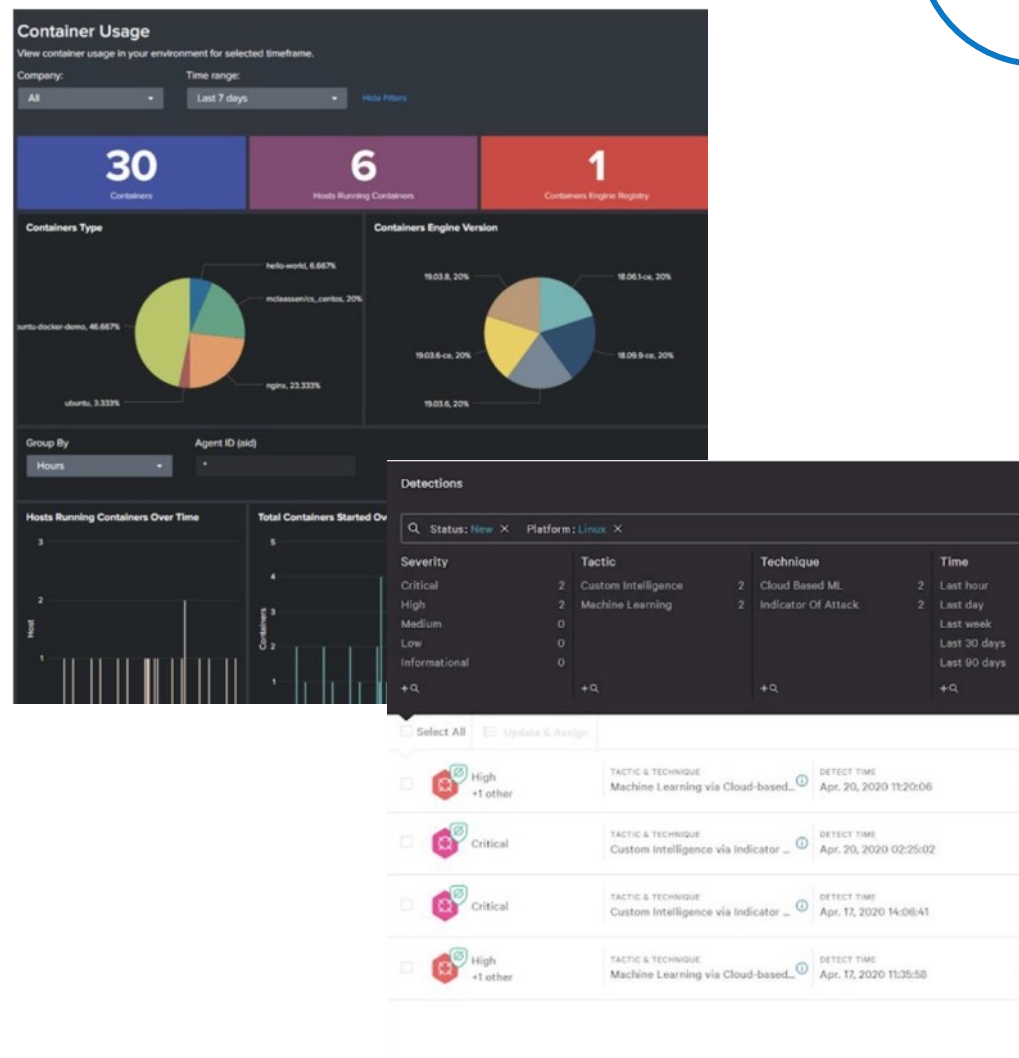


# SOC - RISPOSTA AUTONOMA

MDR – Response

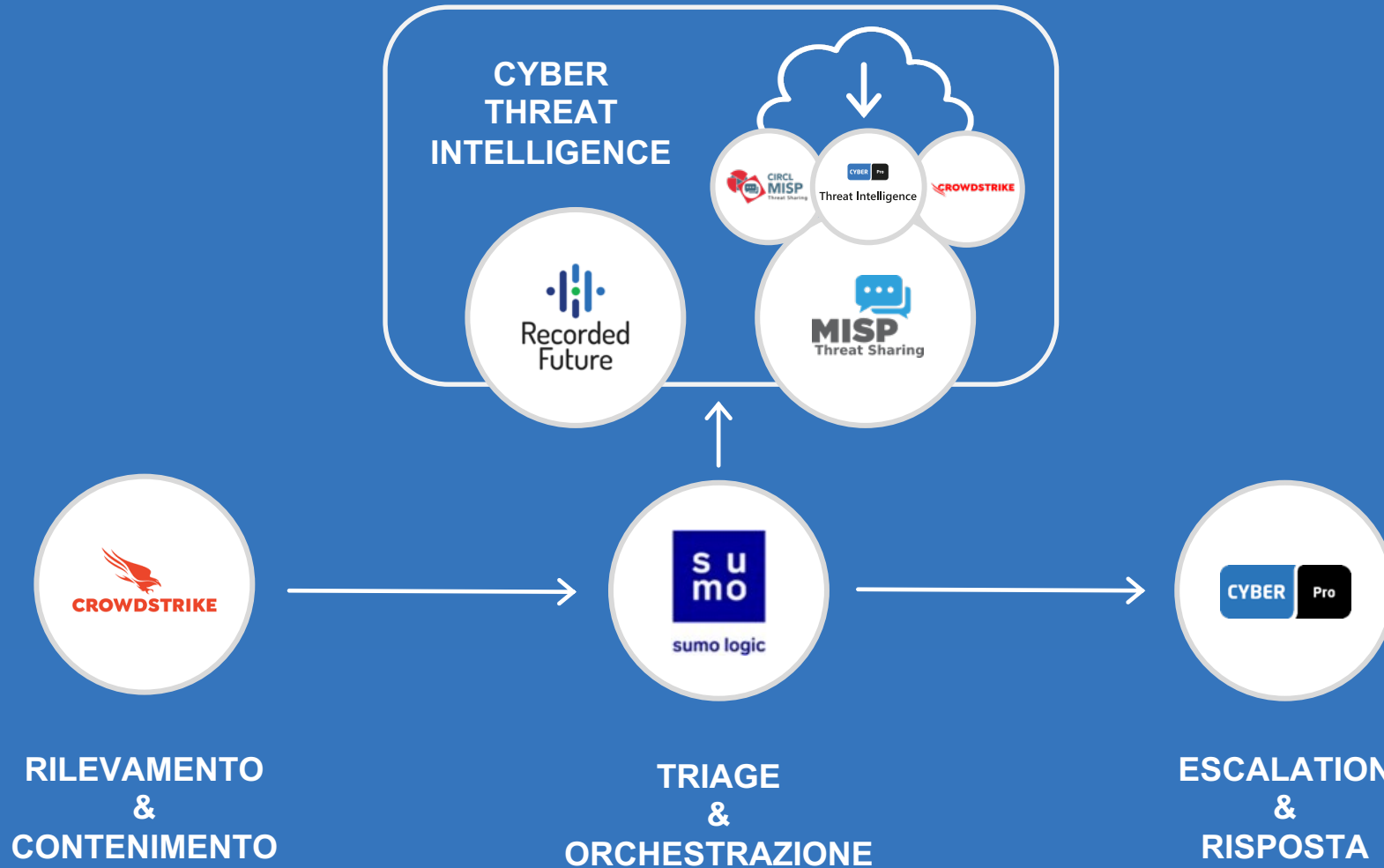
## CROWDSTRIKE MDR

- ✓ **Interruzione autonoma** e chirurgica degli attacchi per un rapido intervento
- ✓ **Contenimento delle minacce** in pochi secondi
- ✓ Ideale per **combattere gli attacchi zero day**
- ✓ **Supervisione completa del team SOC H24 e azione**
- ✓ Combina precisione e flessibilità delle competenze umane con velocità e portata dell'AI



# SOC Threat Intelligence

## Threat Information Sharing



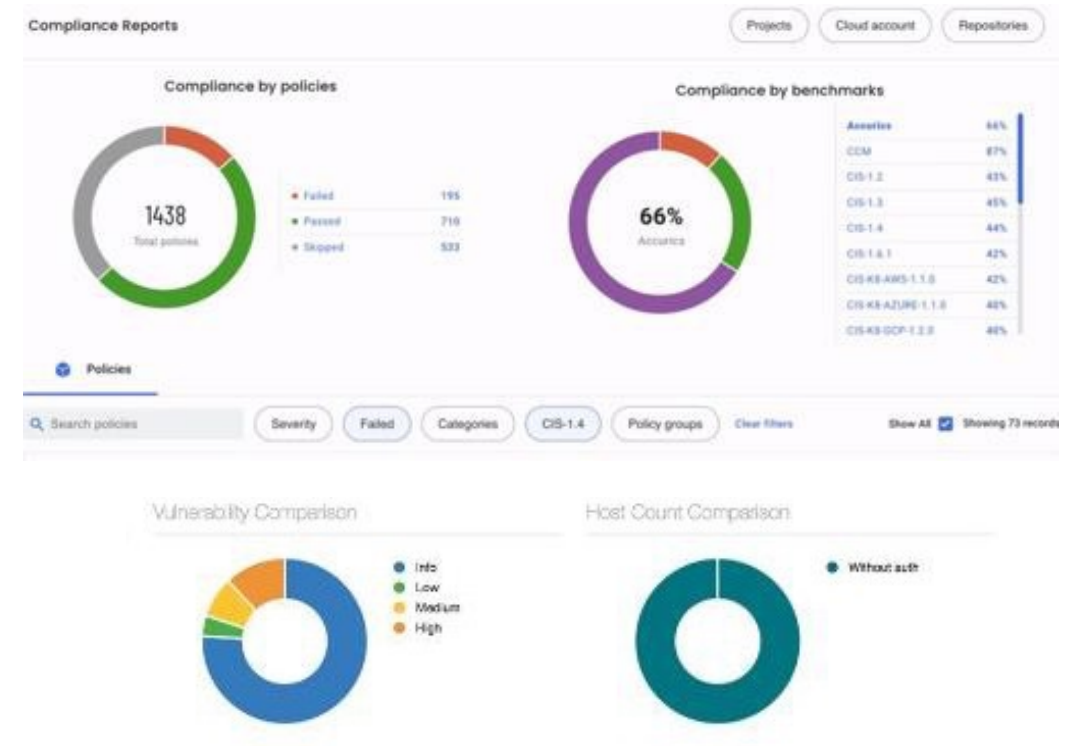


# SOC - VULNEABILITY MANAGEMENT

Servizi opzionabili

Il SOC di Cyber Pro può fornire il servizio di **Vulnerability Management as-a-service**.  
**La soluzione di Vulnerability Management è Tenable e prevede diversi ambiti di assessment:**

- ✓ Compliance e Vulnerability Assessment continuativo di infrastrutture IT
- ✓ Compliance e Web Application Security Assessment continuativo di applicazioni Web
- ✓ Audit di ambienti Cloud e SAAS
  - ✓ Microsoft 365
  - ✓ Azure, Azure Active directory
  - ✓ AWS
  - ✓ Google

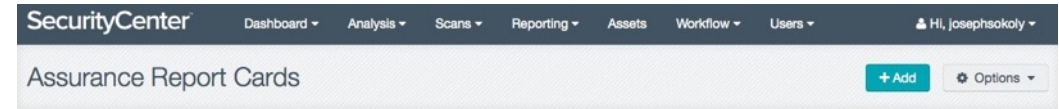


# SOC - VULNEABILITY MANAGEMENT

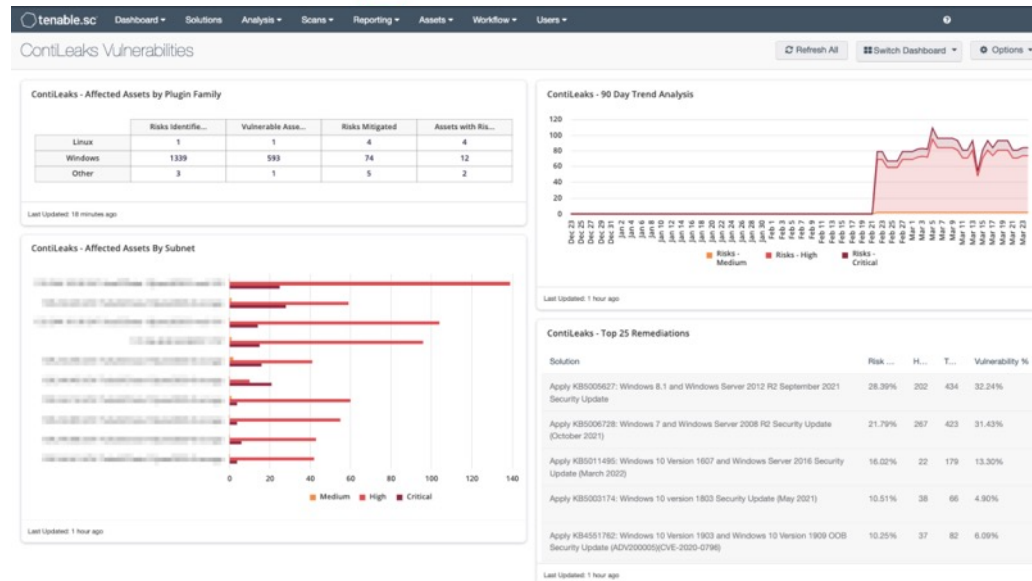
Servizi opzionabili

## Cosa comprende il servizio:

- ✓ Scansioni su IP pubblici
- ✓ Scansioni su IP privati
- ✓ Scansioni aggiuntive
- ✓ Remediation report con cadenza mensile
- ✓ Executive report con cadenza trimestrale



- CCC 1: Maintain an Inventory of Software and Hardware  
Last Evaluated 6 minutes ago
- CCC 2: Remove vulnerabilities and misconfigurations  
Last Evaluated 7 minutes ago
- CCC 3: Deploy a secure network  
Last Evaluated 6 minutes ago
- CCC 4: Authorize Users  
Last Evaluated 6 minutes ago



**ContiLeaks - Affected Assets by Plugin Family**

	Risks Identified	Vulnerable Assets	Risks Mitigated	Assets with Risks
Linux	1	1	4	4
Windows	1339	593	74	12
Other	3	1	5	2

**ContiLeaks - 90 Day Trend Analysis**

**ContiLeaks - Affected Assets By Subnet**

**ContiLeaks - Top 25 Remediations**

Solution	Risk ...	H...	T...	Vulnerability %
Apply KB5005627: Windows 8.1 and Windows Server 2012 R2 September 2021 Security Update	28.36%	202	434	32.24%
Apply KB5006728: Windows 7 and Windows Server 2008 R2 Security Update (October 2021)	21.79%	267	423	31.43%
Apply KB5011486: Windows 10 Version 1807 and Windows Server 2016 Security Update (March 2022)	16.02%	22	179	13.30%
Apply KB5001174: Windows 10 version 1803 Security Update (May 2021)	10.51%	38	66	4.90%
Apply KB4551782: Windows 10 Version 1903 and Windows 10 Version 1909 OOB Security Update (ADV2000005)(CVE-2020-0798)	10.25%	37	82	6.09%

# SOC - CYBER PRO THREAT INTELLIGENCE

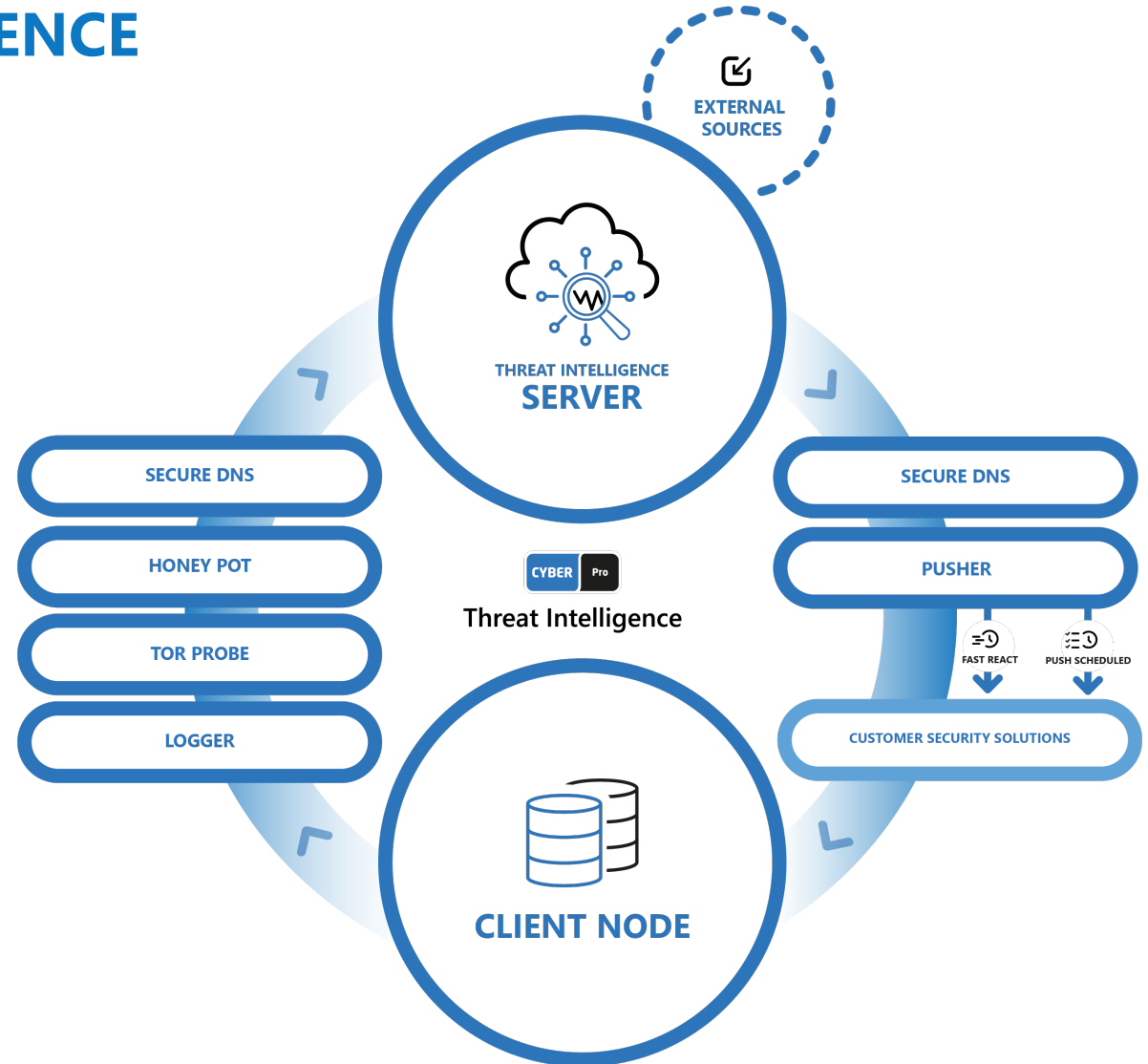
Servizi opzionabili

Cyber Pro Threat Intelligence è la soluzione sviluppata per la difesa preventiva, analitica e proattiva da minacce informatiche di molteplici tipologie.

**Nasce con l'obiettivo di difendere e rendere più resiliente il core business di un'organizzazione.**

## FEATURES:


- ✓ DASHBOARD
- ✓ IOCS
- ✓ HONEYPOT
- ✓ BLACK LIST/WHITE LIST
- ✓ SECURE DOCUMENT
- ✓ PUSHER
- ✓ LOGGER
- ✓ THREAT ANALYSIS
- ✓ NODE
- ✓ PHISHING DOMAINS
- ✓ FAST REACT
- ✓ DARK WEB & BOTNET MONITORING
- ✓ CLOUD SANDBOX
- ✓ ADVANCED SUPPORT
- ✓ SECURE DNS
- ✓ EXTERNAL PERIMETER ASSESSMENT



# SOC - BRAND & IDENTITY PROTECCION

Servizi opzionabili

- ✓ **BRAND REPUTATION:** Soluzione Recorded Future per l'analisi della superficie d'attacco esposta dall'azienda e la rilevazione di eventuali dati pubblicati su Clear/Dark/Deep Web o domini fraudolenti (typosquatting)
- ✓ **IDENTITY PROTECTION:** Soluzione Recorded Future per la rilevazione di credenziali compromesse su Clear/Dark/Deep Web
- ✓ **THIRD PARTY MONITORING:** Soluzione Recorded Future per l'analisi della superficie d'attacco esposta dalle terze parti su Clear/Dark/Deep Web




**Use Cases**

- Alert Triage
- Threat Detection
- Threat Prevention

**FEATURES**

- Broadest source coverage
- Real-time risk scores and context
- Block-grade indicators
- 10+ SIEM and SOAR integrations



**Use Cases**

- Advanced Threat Research & Reporting
- Advanced Detection & Validation
- Dark Web Investigation

**FEATURES**

- Real-time search and alerting
- Closed forum & dark web monitoring
- High-confidence threat hunting and detection
- Over 1 billion Intelligence Cards
- Risk scores and transparent source evidence

# INCIDENT RESPONSE AS-A-SERVICE

Servizi opzionabili

## Tutti siamo a rischio attacchi

La domanda da farsi non è se saremo attaccati, ma quando.

È quindi opportuno arrivare preparati all'evento per ridurre i disservizi e tornare rapidamente alla normalità.

## Supporto Post Incident

Supportiamo il cliente nelle attività successive all'incidente.

Il nostro Team oltre a produrre un report esaustivo dell'evento, collaborerà al miglioramento dei processi interni all'azienda.

## Copertura 24/7

La velocità di analisi e risposta è fondamentale per contenere un incidente e limitare i danni. Attivo 24 ore su 24, 7 giorni su 7, il servizio assicura alla tua azienda un team di esperti che agisce in modo mirato e tempestivo.





# Contatti

[www.cyber-pro.it](http://www.cyber-pro.it)

t +39 075 5005589

e [info@cyber-pro.it](mailto:info@cyber-pro.it)