CYBER Pro

SOC

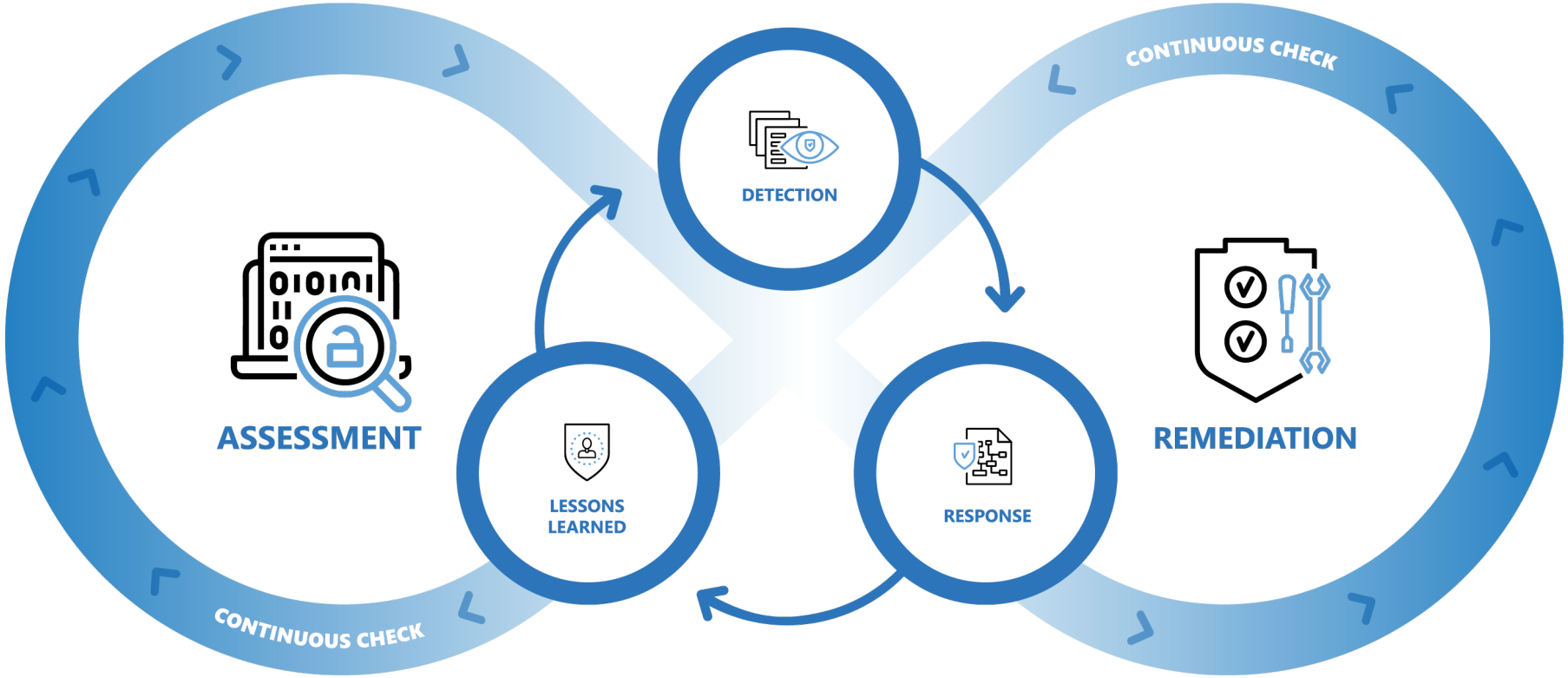
Security Operation Center

© 2023 PCS Group

Powered by PCS Group

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**.

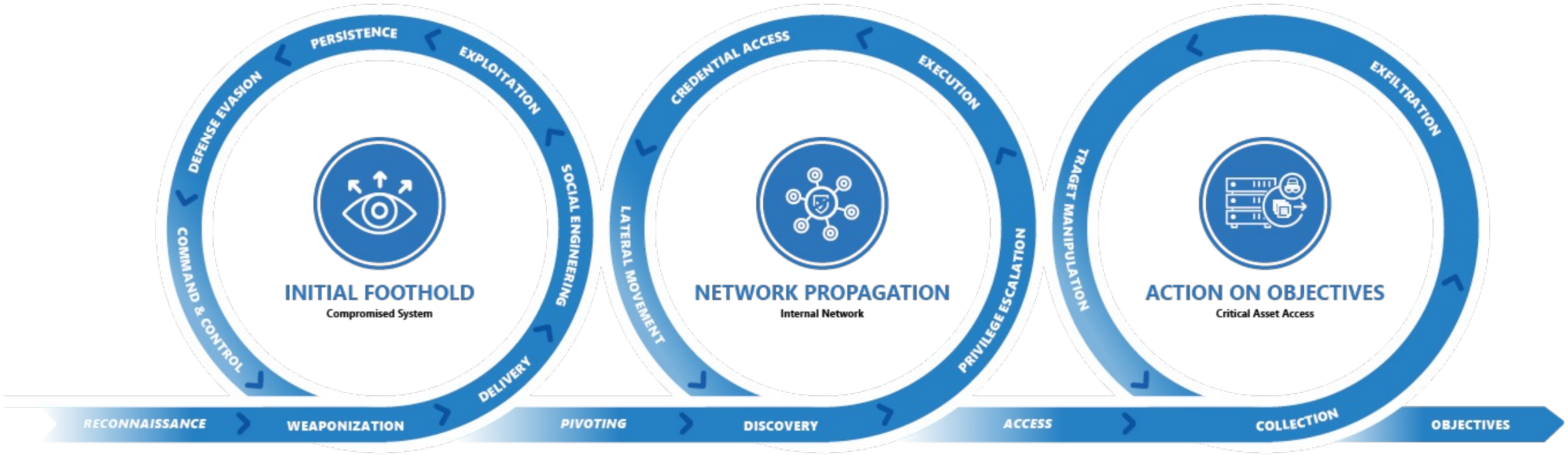


Difendersi nel modo corretto salva i dati!

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»

Powered by PCS Group

Rilevazione delle minacce cyber

Certificazioni associate ai servizi

ISO 27018 · ISO 9001 · ISO 27701 · ISAE 3402 TYPE II CERTIFIED · ANSI TIA 942 RATED 4 · CYBERSECURITY MADE IN EUROPE

ISO 14001 · ISO 27001 · ISO 20000 · SSAE 18 CERTIFIED AICPA · AGID Agenzia per l'Italia Digitale · Clusit

ISO 27017 · ISO 22301 · STAR LEVEL ONE · gaia-x · CISPE DECLARED

Powered by PCS Group

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

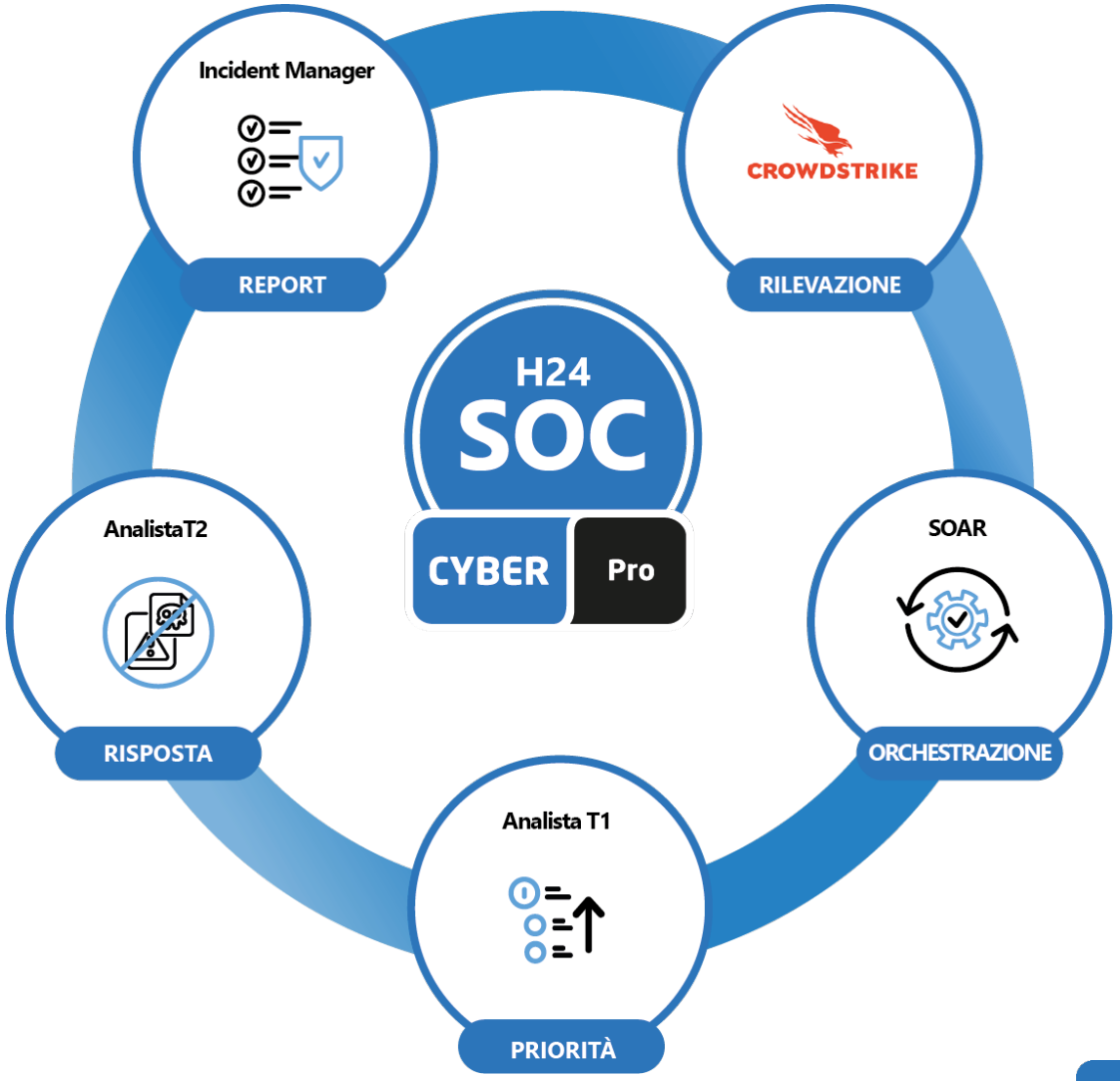
CYBER Pro

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

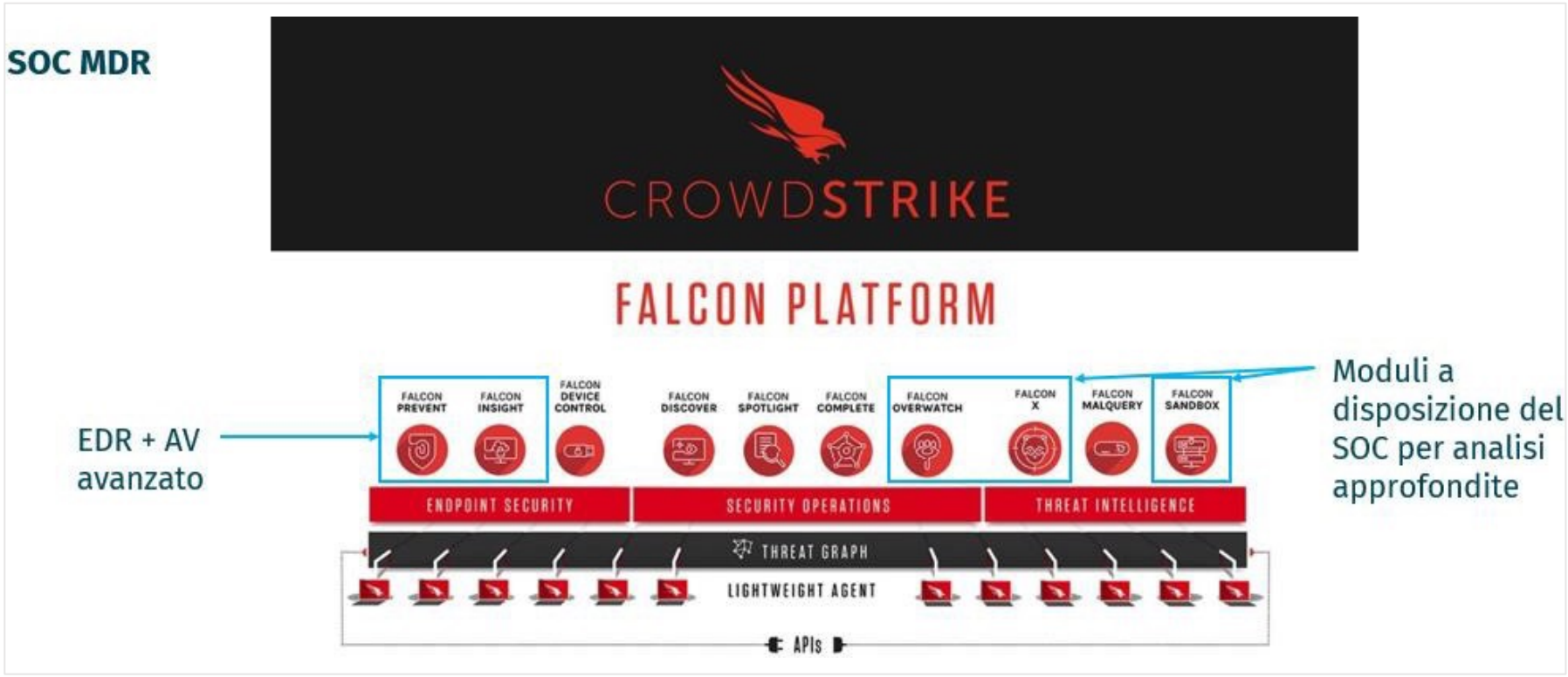
Gravità	Livello	SLA (presa in carico+mitigation+analisi+segnalazione)
P4	basso	8 ore
P3	medio	4 ore
P2	alto	2 ore
P1	critico	1 ora

SOC - MDR

MDR – protezione client e server

Obiettivo del servizio:

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

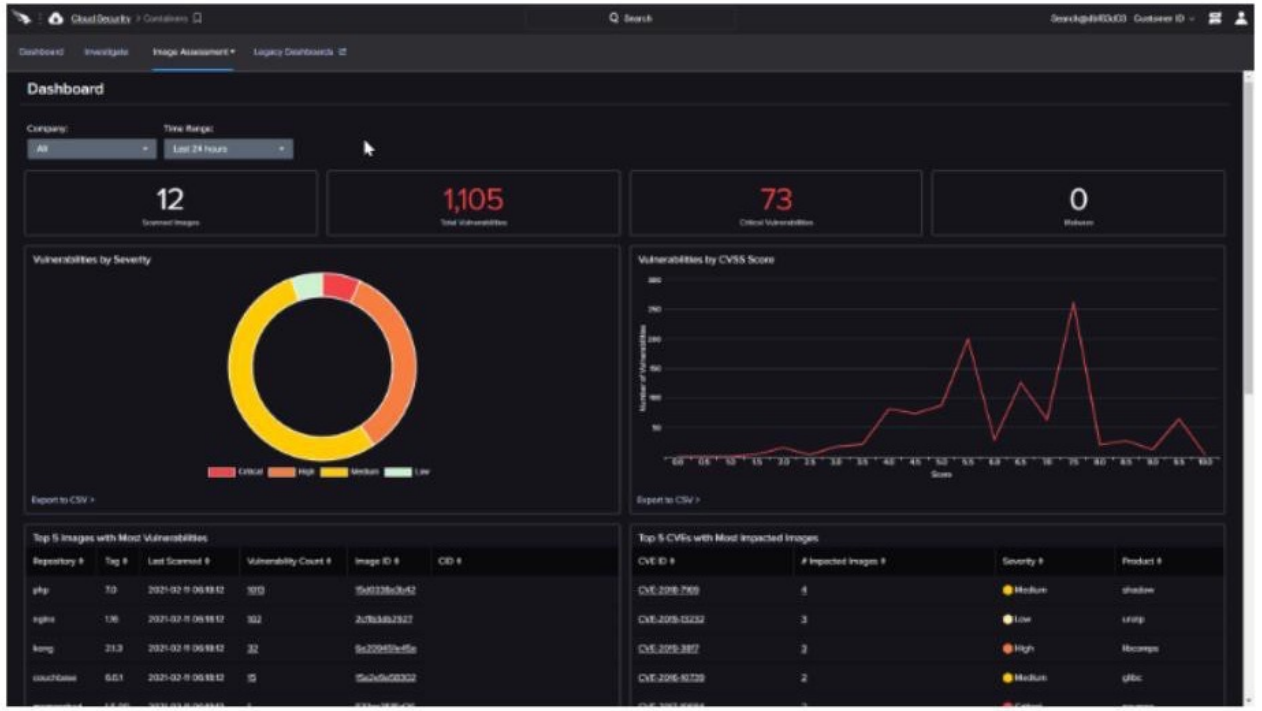


SOC - MDR

MDR – protezione dei container

Obiettivo del servizio:

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

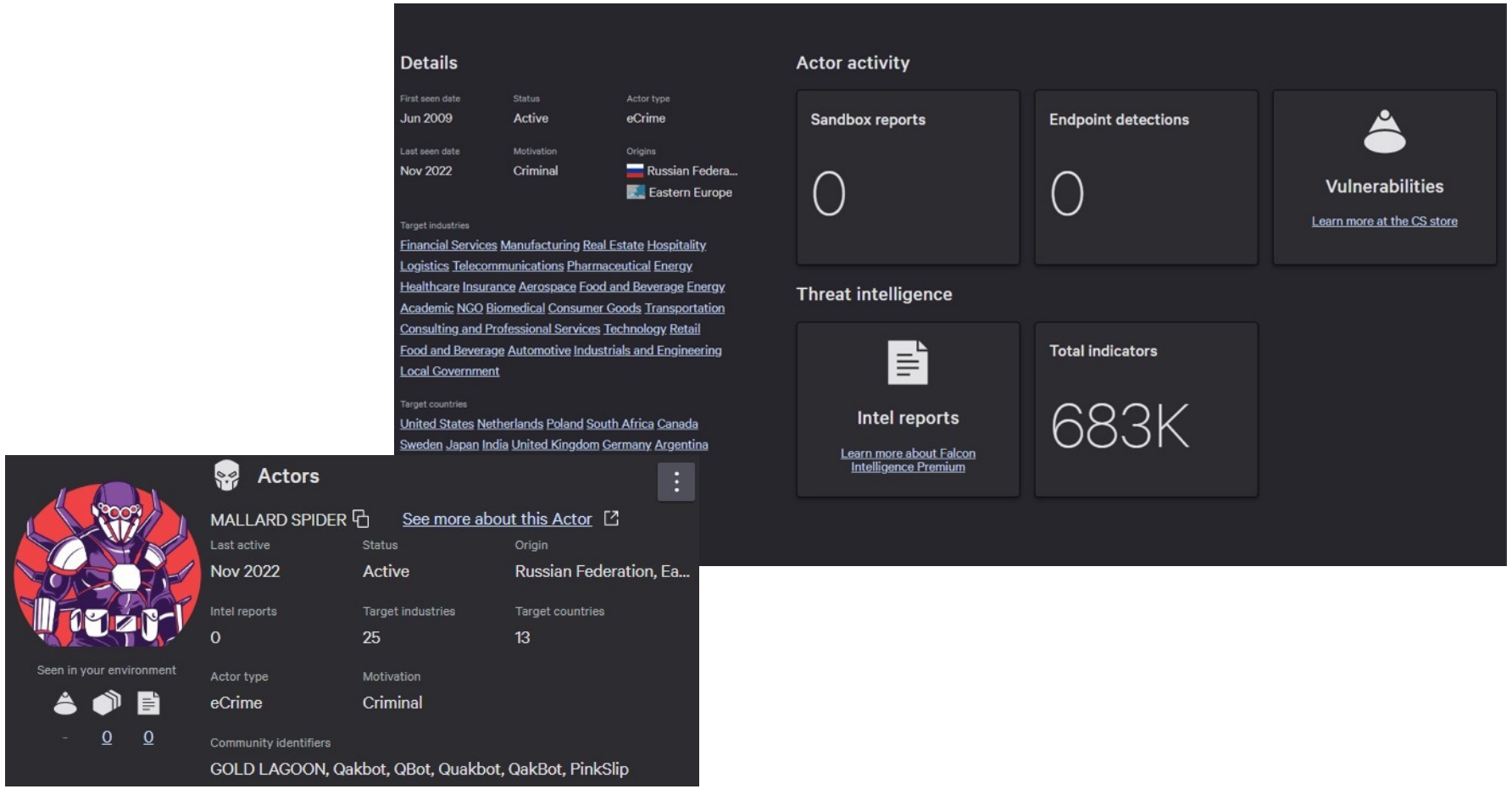


SOC - MDR

MDR – Cyber Threat Intelligence

Obiettivo del servizio:

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

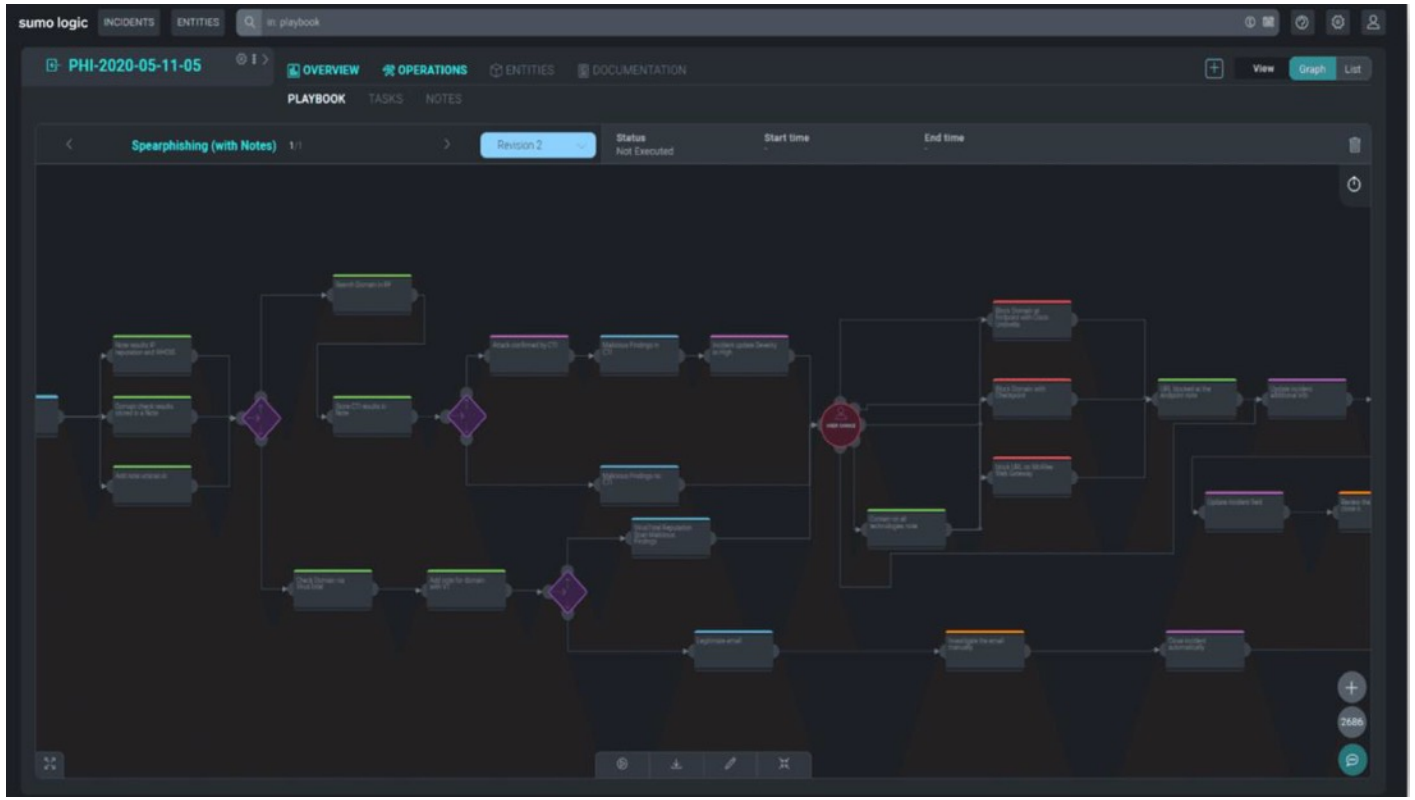


SOC - SOAR

SOAR-Sumo Logic Orchestrazione

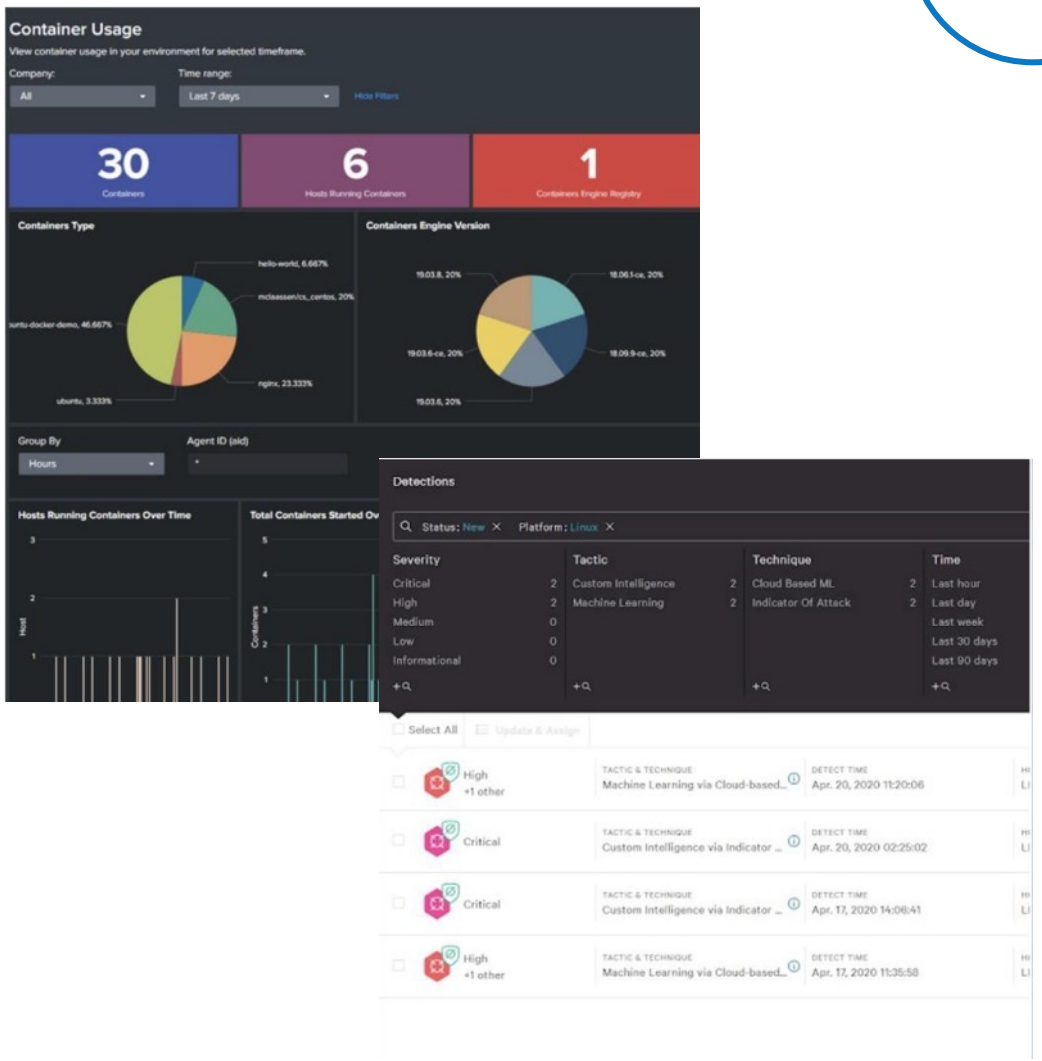
Obiettivo del servizio:

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



SOC - RISPOSTA AUTONOMA

MDR – Response

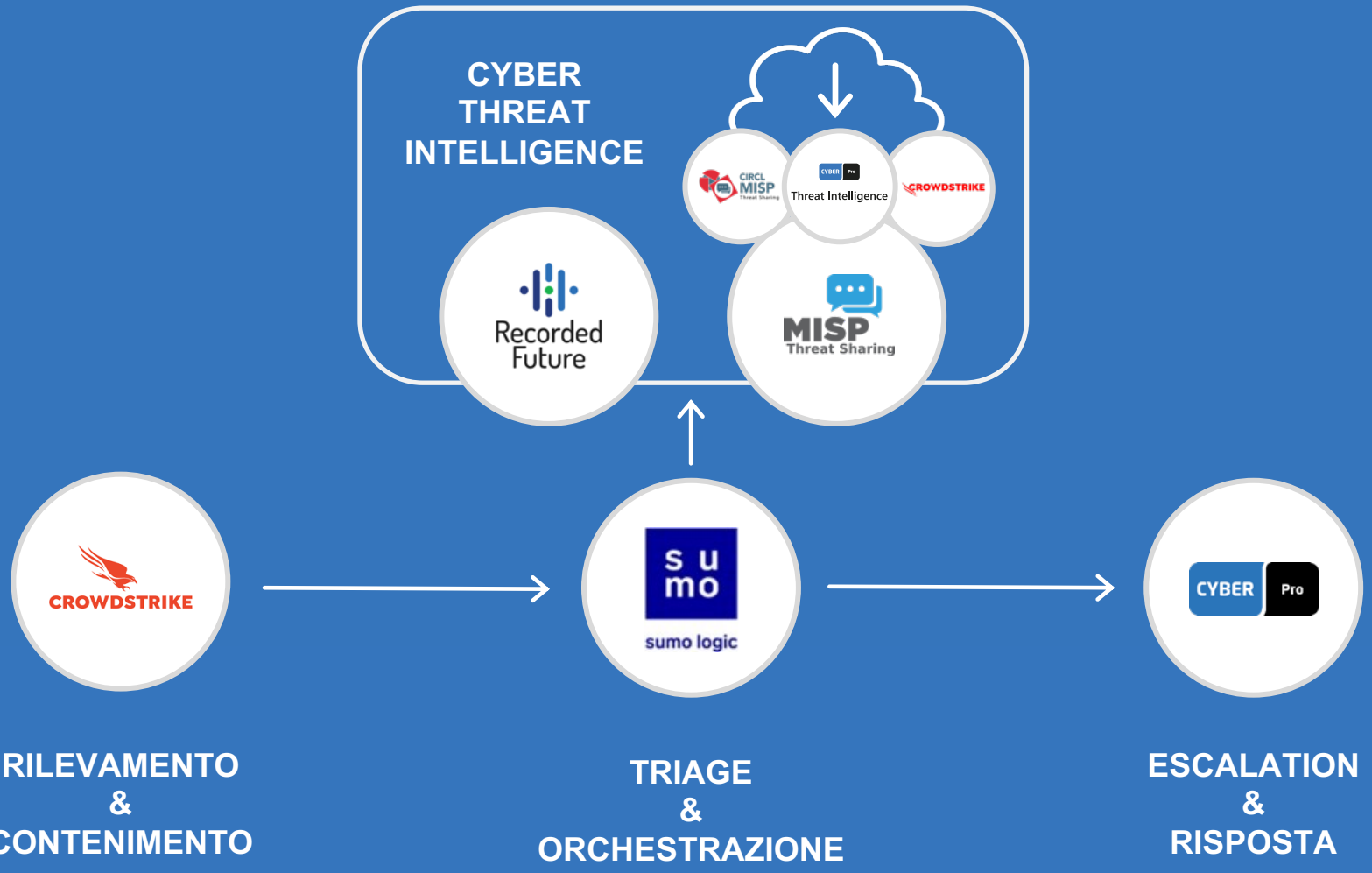


CROWDSTRIKE MDR

- ✓ **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:

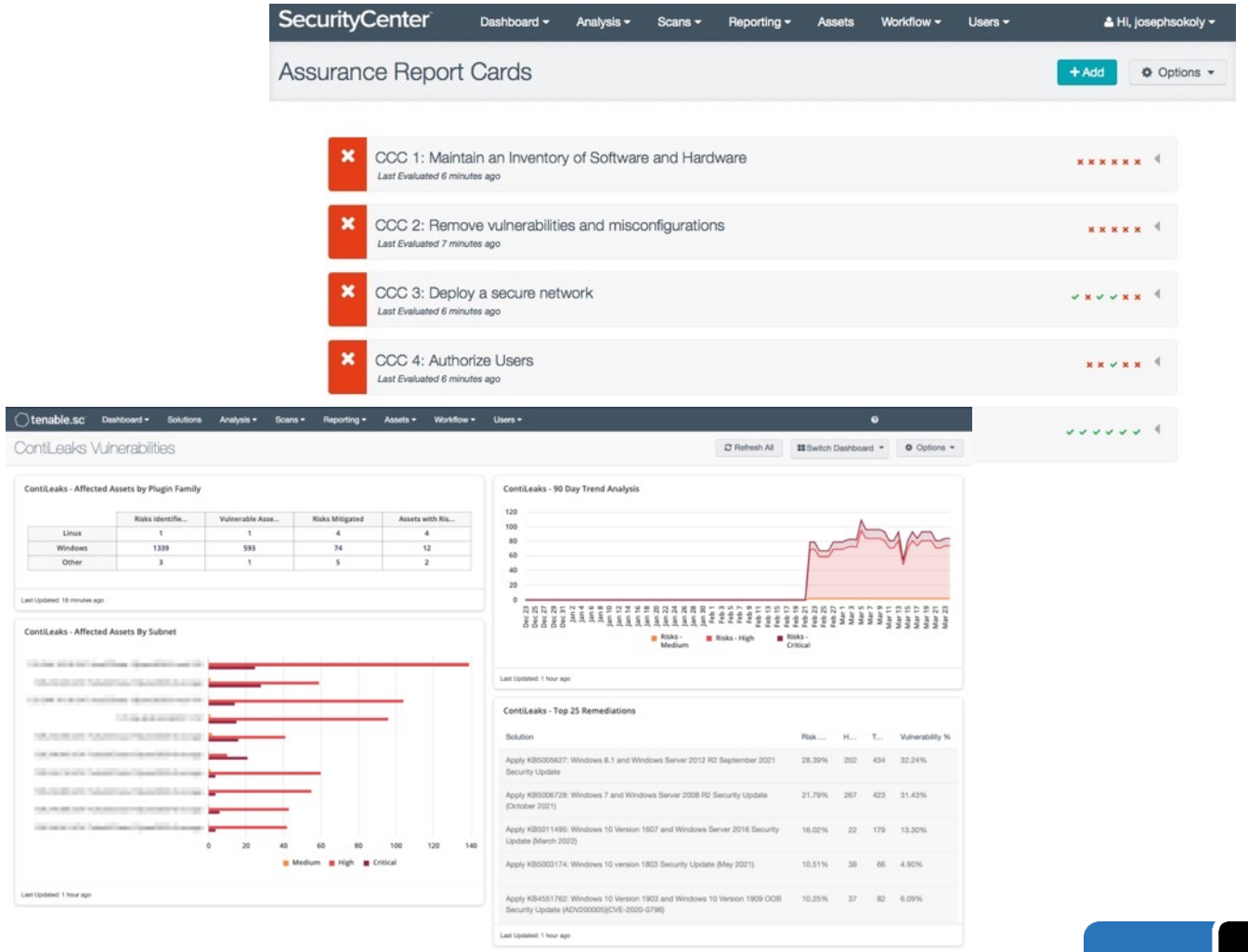
- ✓ Compliance e Vulnerability Assessment continuativo di
- ✓ infrastrutture IT
- ✓ Compliance e Web Application Security Assessment continuativo di applicazioni Web
- ✓ Audit di ambienti Cloud e SAAS
  - ✓ Microsoft 365
  - ✓ Azure, Azure Active directory
  - ✓ AWS
  - ✓ Google

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



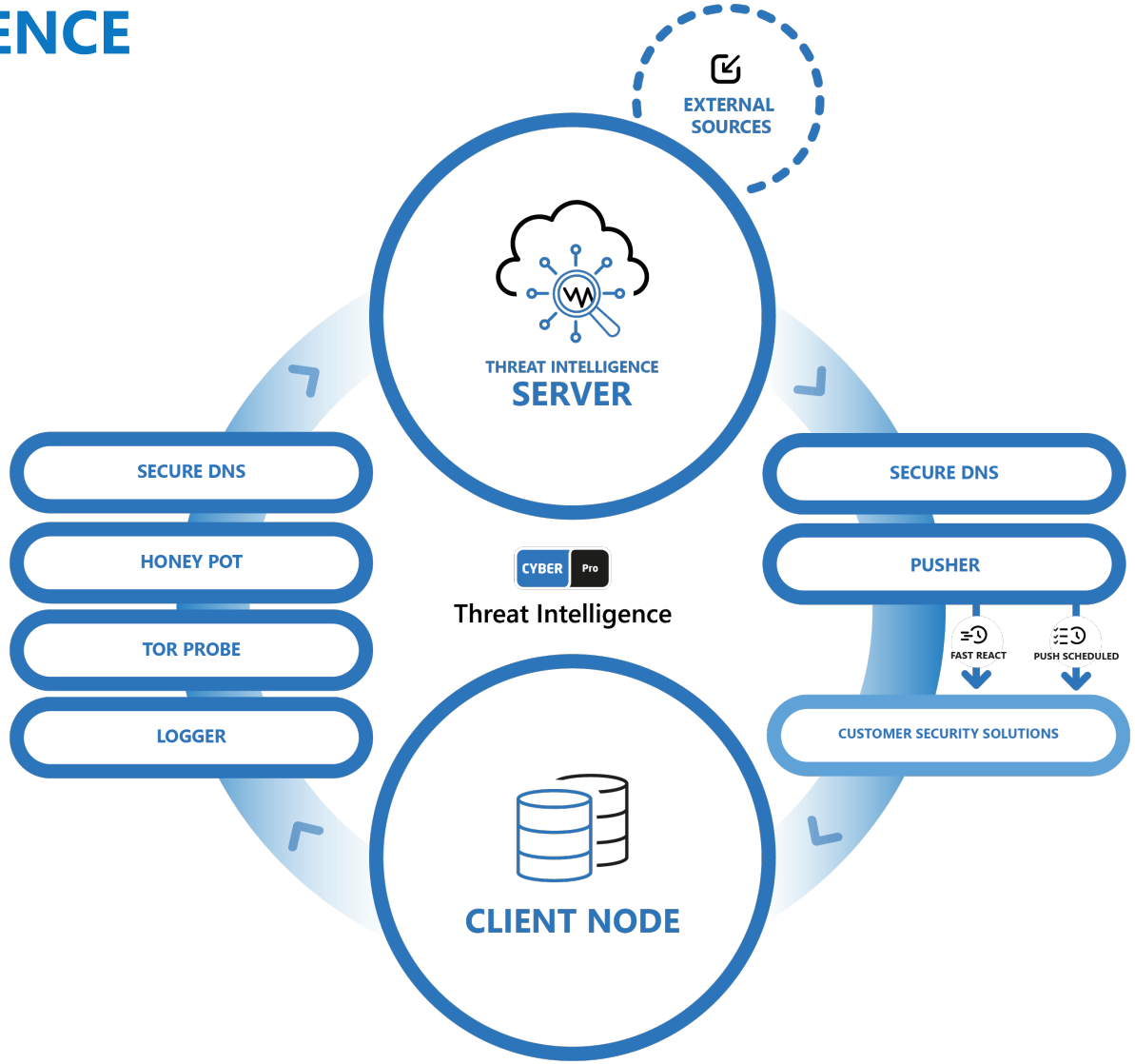
SOC - CYBER PRO THREAT INTELLIGENCE

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:

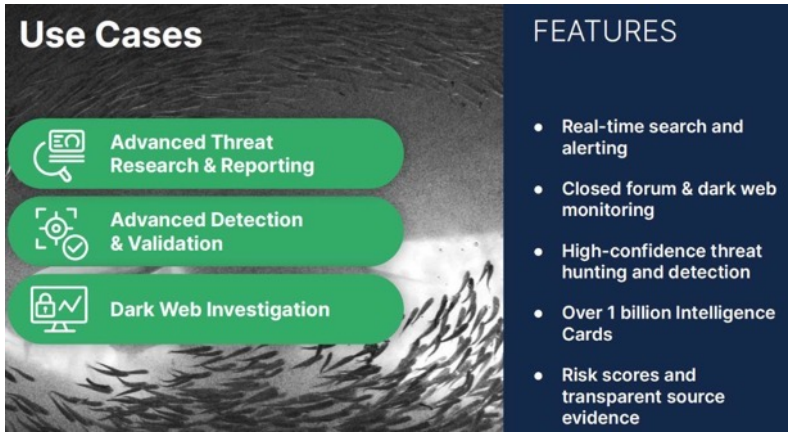
- ✓ DASHBOARD
- ✓ IOCS
- ✓ HONEYPOT
- ✓ BLACK LIST/WHITE LIST
- ✓ SECURE DOCUMENT
- ✓ PUSHER
- ✓ LOGGER
- ✓ THREAT ANALYSIS
- ✓ NODE
- ✓ PHISHING DOMAINS
- ✓ FAST REACT
- ✓ DARK WEB & BOTNET MONITORING
- ✓ CLOUD SANDBOX
- ✓ ADVANCED SUPPORT
- ✓ SECURE DNS
- ✓ EXTERNAL PERIMETER ASSESSMENT



SOC - BRAND & IDENTITY PROTECION

Servizi opzionabili

- ✓ **BRAND REPUTATION**: Soluzione Recorded Future per l'analisi della superfice 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 superfice d'attacco esposta dalle terze parti su Clear/Dark/Deep Web



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

t +39 075 5005589

e info@cyber-pro.it