CERBEYRA

Cyber Threat Intelligence Platform

SERVIZI AVANZATI DI CYBER SECURITY

La piattaforma cloud di

CYBER THREAT INTELLIGENCE

« FUNZIONALITÀ E CASI D'USO »

Francesco Arruzzoli
Resp. R&D e Centro Studi Cyber Defense Cerbeyra

Vola S.p.A | Gruppo Vianova S.p.A.

Webinar | aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

"Le piattaforme di Cyber Threat Intelligence: l'attuale stato dell'arte ed il loro uso nella gestione della sicurezza digitale"

CERBEYRA

“Un ‘anima digitale dal cuore italiano”

vianova VOLA Winitalia CYBER SECURITY

Cerbeyra è una piattaforma di Cyber Threat Intelligence progettata e realizzata interamente nel **polo italiano della Cyber Security di Vola Spa del Gruppo Vianova. Vianova è il quarto operatore nazionale in area business** di servizi avanzati ed integrati di telecomunicazioni (voce e dati) per le imprese su rete fissa e mobile , presente su tutto il territorio grazie ad una rete di partner selezionati.

109 aziende

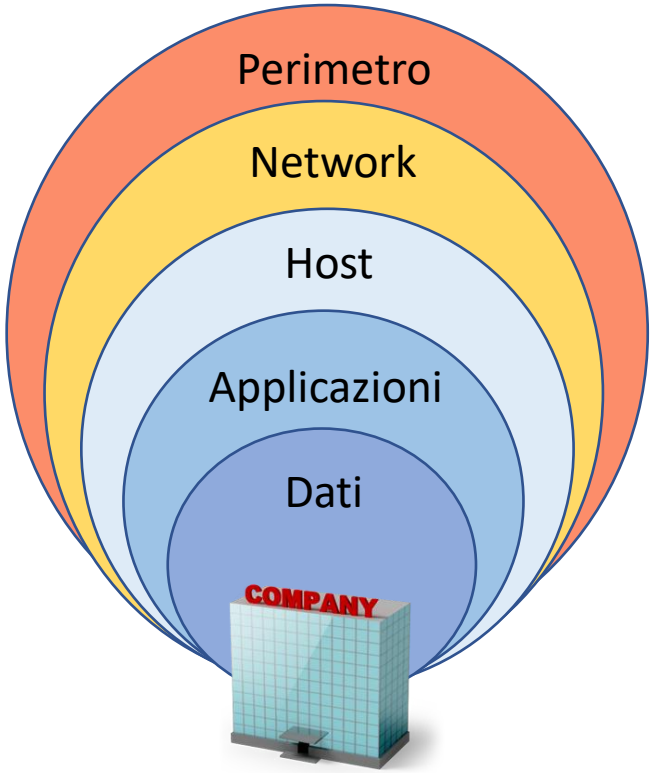
1.266 persone

235 imprenditori

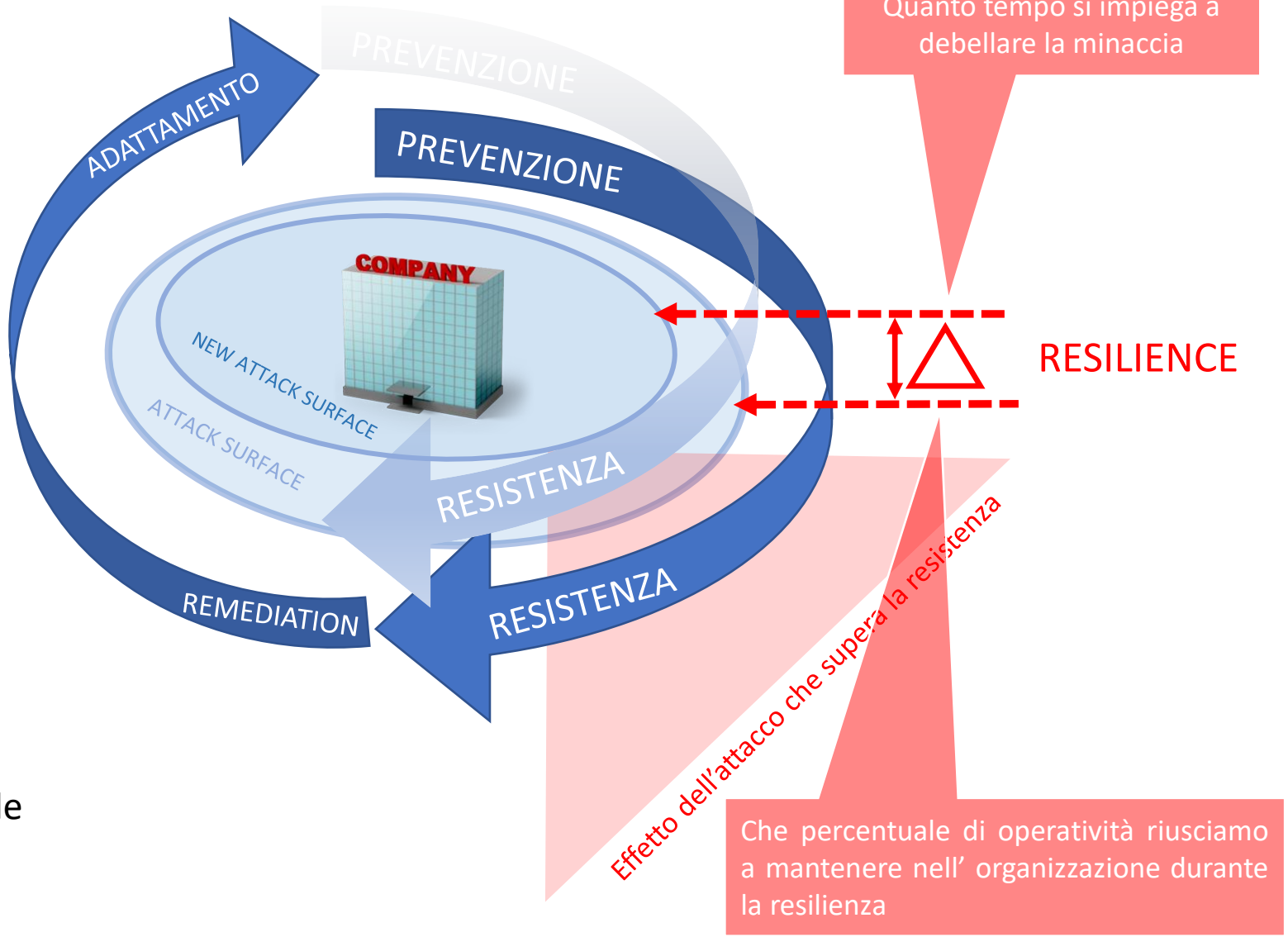
Il Gruppo Vianova, 11 milioni di capitale sociale e **9,4 milioni di investimenti in TLC** è composto da una Rete di imprese specializzate in settori strategici per la crescita di aziende e organizzazioni, come le telecomunicazioni integrate, i servizi in hosting e in cloud. **Il Gruppo impiega 235 persone e ha un fatturato complessivo nel 2021 di 67 milioni di euro.**

AGID Cloud Marketplace

LA CYBER RESILIENCE DELLE AZIENDE VIENE CONTINUAMENTE MESSA ALLA PROVA



Persone, informazioni,Procedure, Regole

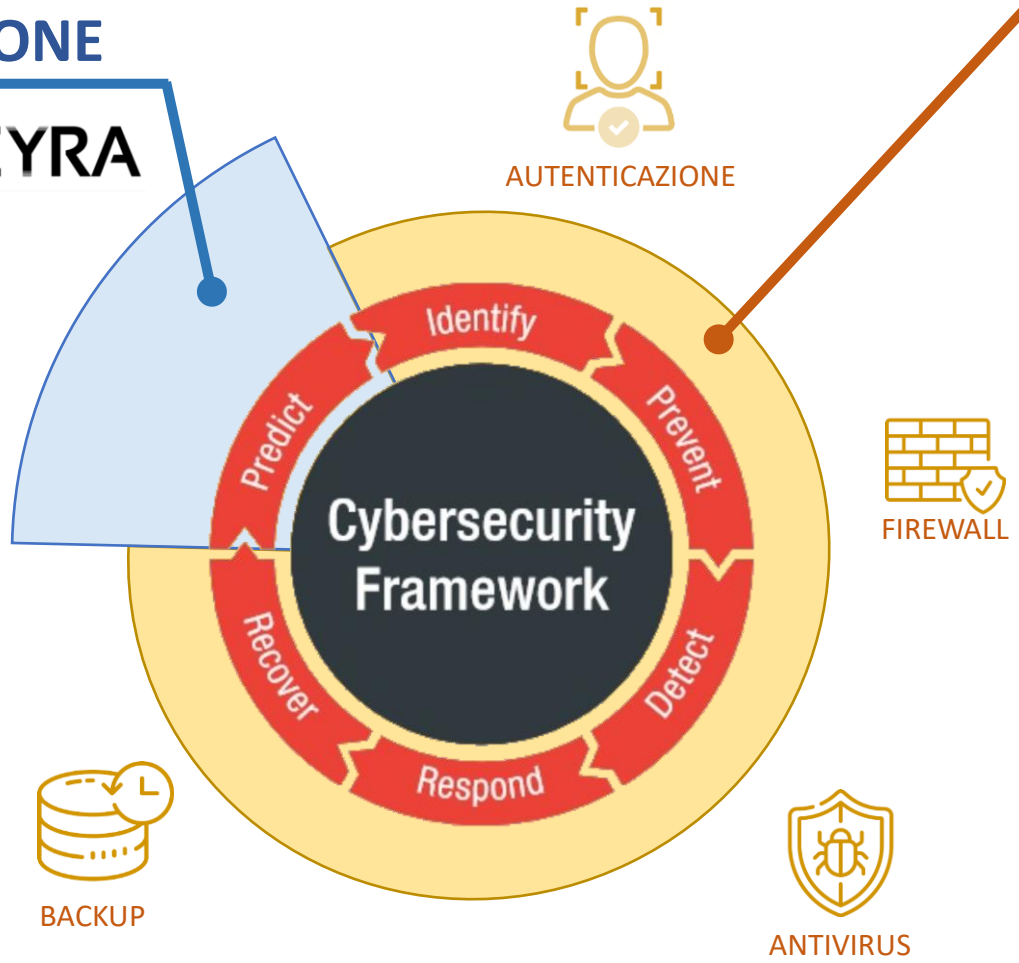


Cybersecurity framework

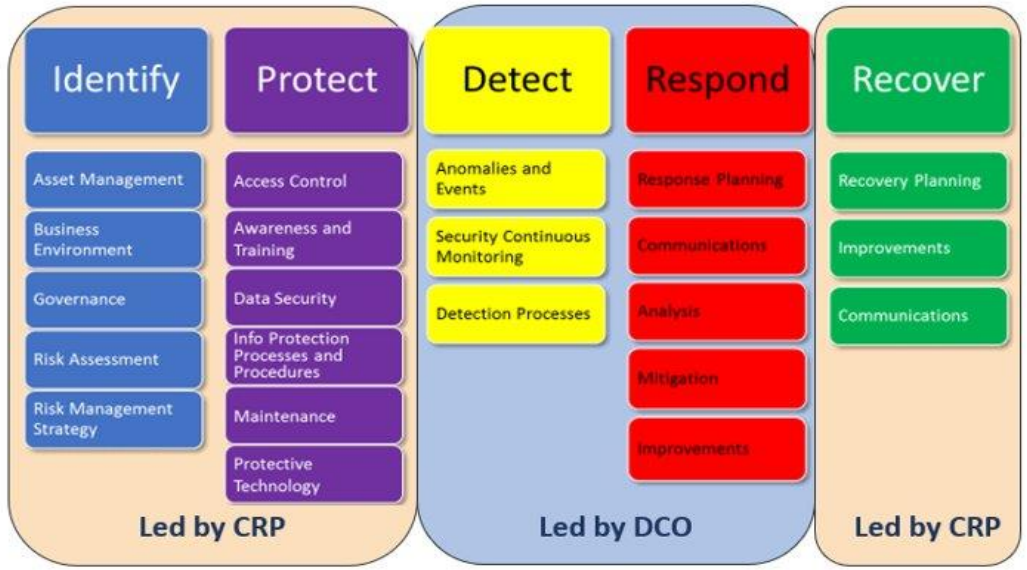
PREDIZIONE

CERBEYRA

PREVENZIONE E CONTRASTO



National Institute of Standards and Technology (NIST) Cyber Security Framework



The Defensive Cyber Programmes are:

- Defensive Cyber Operations (DCO) Programme
- Cyber Resilience Programme (CRP)

PREDIZIONE.. COSA VUOL DIRE ? **VUOL DIRE FARE** **INTELLIGENCE**

Cos'è l'intelligence ? **L'intelligence è un metodo di trattazione dell'informazione.**

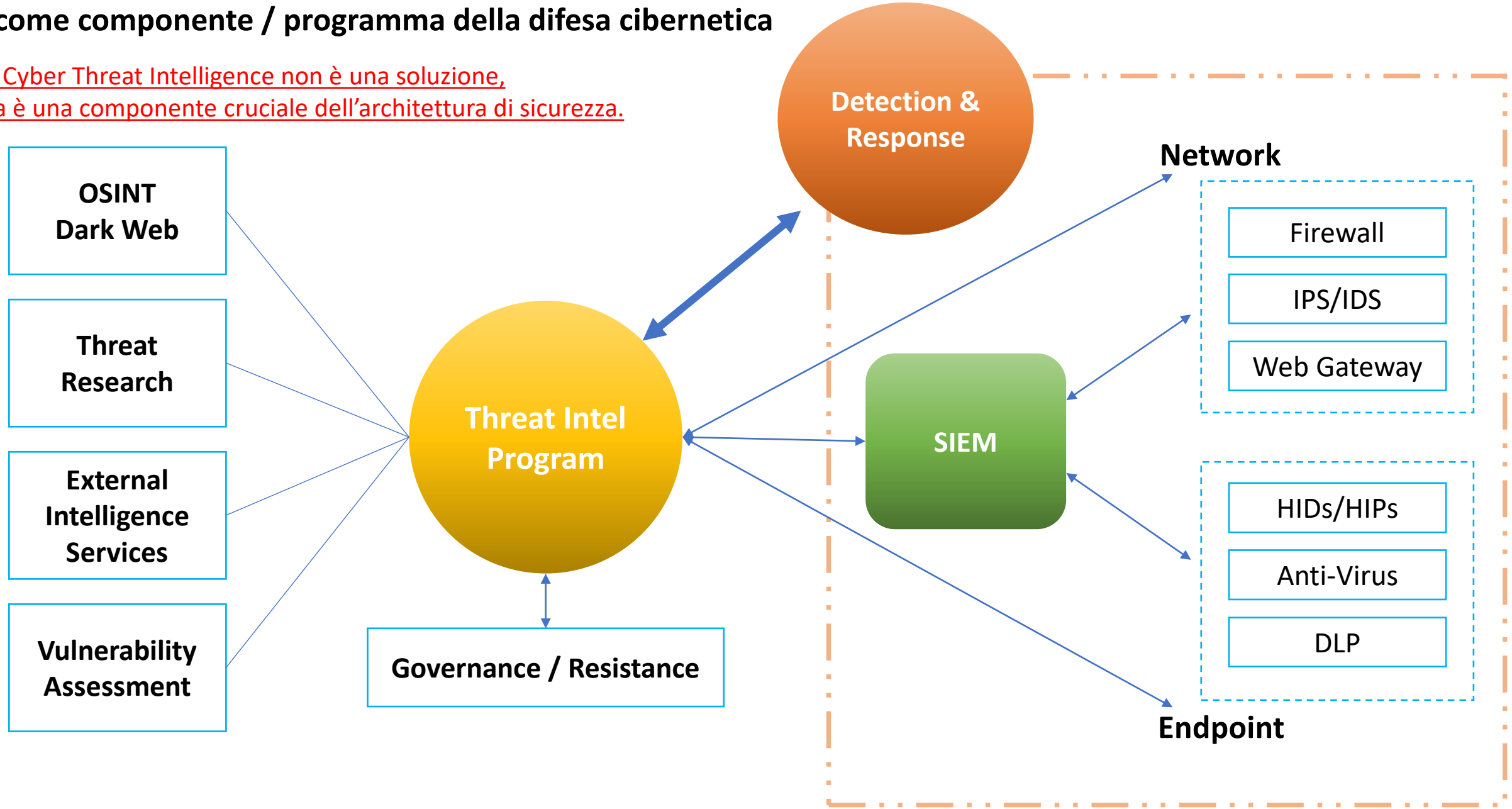
Cos'è la Cyber Threat Intelligence (CTI) ? **Servizi di informazione strategica sulle cyber minacce**

LA CTI TRASFORMA LE INFORMAZIONI RELATIVE AD UNA CYBER MINACCIA IN INFORMAZIONI DI INTELLIGENCE SU UNA CYBER MINACCIA CIOE' **CONTESTUALIZZA LA MINACCIA**, GENERA CONSAPEVOLEZZA DELLA SITUAZIONE (**SITUATIONAL AWARENESS**).

QUESTO PERMETTE COSÌ DI **CONCENTRARSI SUBITO SUGLI ASSET PIÙ VULNERABILI**, CON PIÙ ALTA PROBABILITÀ DI ACCADIMENTO ED IMPATTO, **OTTIMIZZANDO COSTI, RISORSE E GUADAGNANDO TEMPO** PER GESTIRE I PROCESSI DI MESSA IN SICUREZZA DI TUTTI GLI **ASSET POTENZIALMENTE VULNERABILI**; PERMETTE DI **VALUTARE MEGLIO IL RISCHIO RESIDUO**.

CTI come componente / programma della difesa cibernetica

La Cyber Threat Intelligence non è una soluzione,
ma è una componente cruciale dell'architettura di sicurezza.



GLI OBIETTIVI DI CERBEYRA

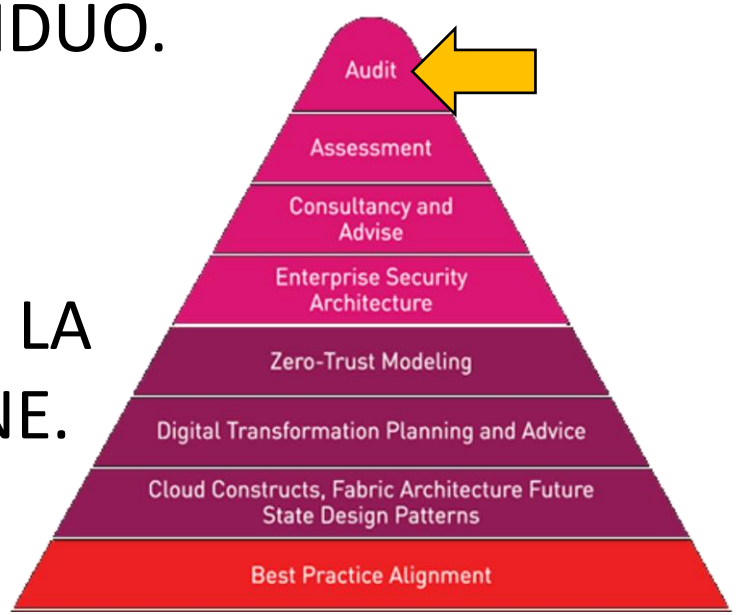
PREVEDERE LE CYBER MINACCE DI DOMANI
ANALIZZANDO IL PRESENTE ED IL PASSATO.

Janus «a memoria in futurum»

"Se conosci il nemico e conosci te stesso, non devi temere il risultato di cento battaglie. Se conosci te stesso, ma non il nemico, per ogni vittoria guadagnata soffrirai anche una sconfitta.
Se non conosci né il nemico né te stesso, tu perderai in ogni battaglia ."

Sun Tzu, L'arte della guerra

PREVEDERE LA CONCLUSIONE DI CYBER ATTACCHI
E VALUTARE IL RISCHIO RESIDUO.



DIVENTARE «LO» STRUMENTO DI AUDIT STRATEGICO PER LA SICUREZZA DELLE INFORMAZIONI DI UNA ORGANIZZAZIONE.

CERBEYRA

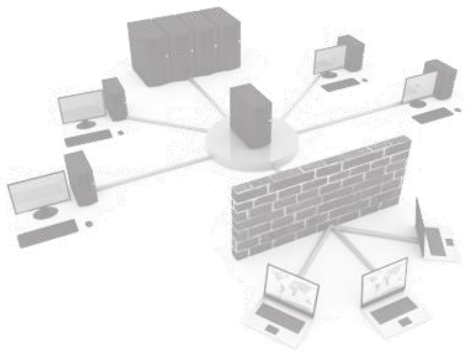
Servizio cloud Software as a Service (SaaS)

Non utilizza le risorse ICT del cliente

Attivazione rapida (entro le 8 ore lavorative)

Installazione e Configurazione e Gestione «ZERO EFFORT»

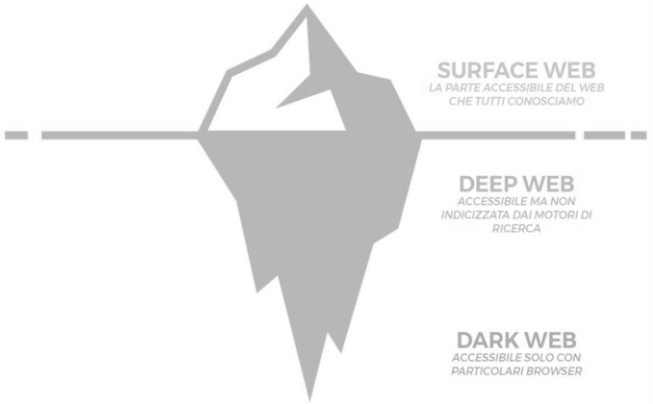
VULNERABILITY ASSESSMENT



CERBEYRA

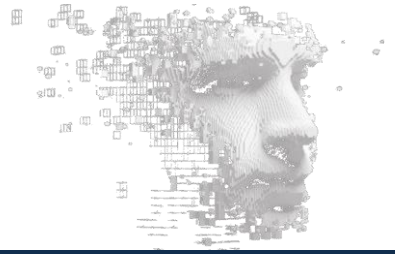
ASSET MANAGEMENT

CYBER THREAT INTELLIGENCE



CYBER SURVEY

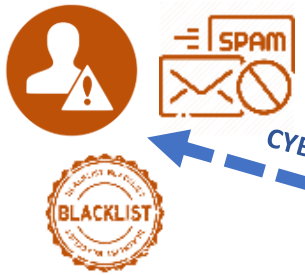
CYBER FEED / CYBER REPUTATION



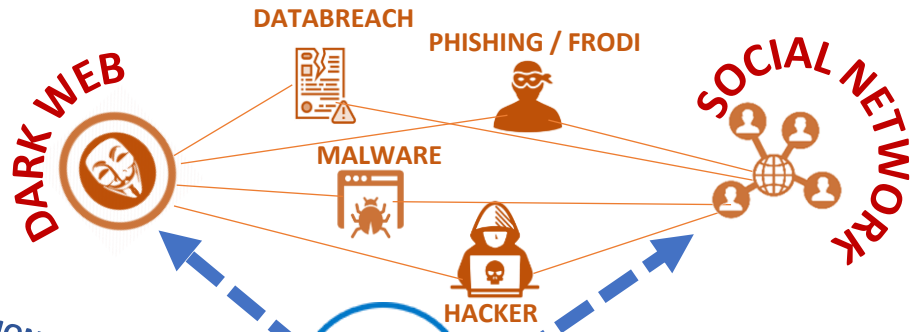
COGNITIVE SECURITY

- **CONTINUOUS SCANNING**
- **CONTINUOUS ASSESSMENT**
- **24h su 24h per 365gg**

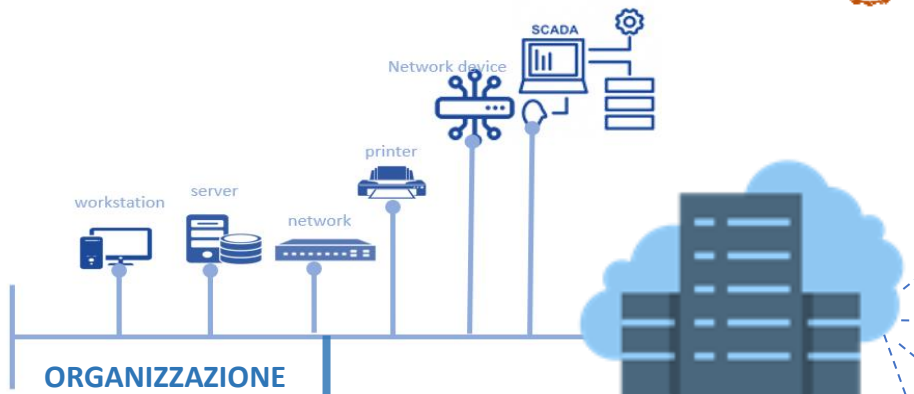
CERBEYRA



CYBER FEED / CYBER REPUTATION



THREAT INTELLIGENCE



ORGANIZZAZIONE

INTERNET

VULNERABILITY ASSESSMENT

Sensori Ambientali IoT

ASSET MANAGEMENT
- HW & SW INVENTORY
- HOST MONITORING
- IOT SENSORS

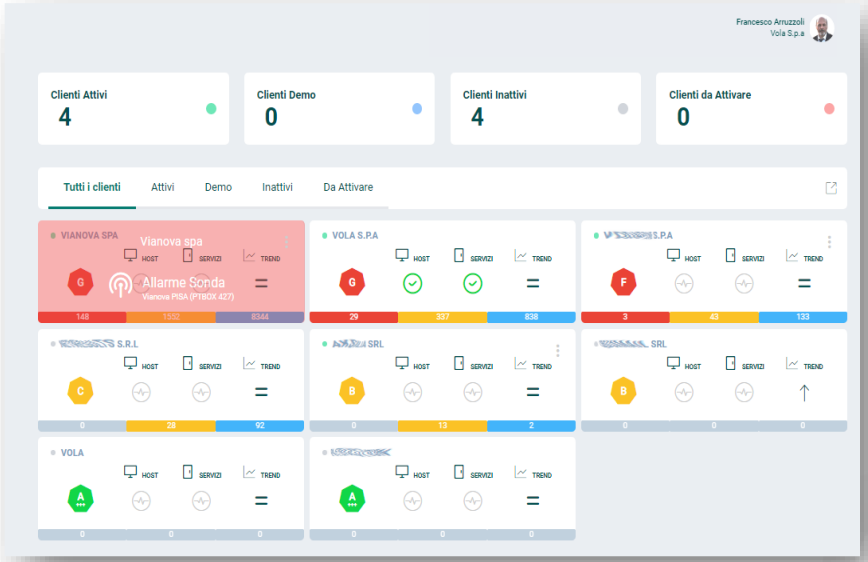
CYBER SURVEY
- KRI - Key Risk Indicator
- ASSET PROFILE

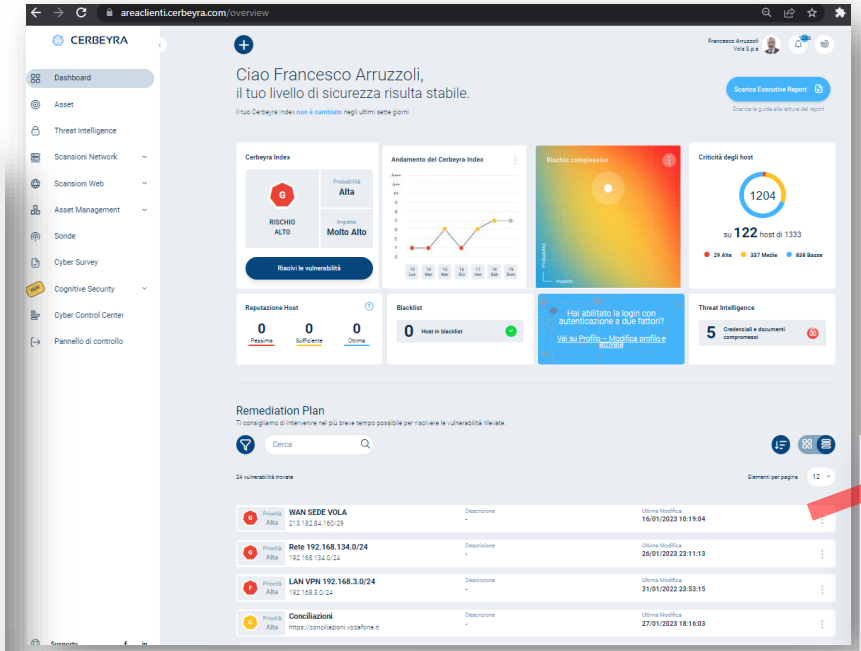
COGNITIVE SECURITY
- Phishing Simulator
- Cyber Marker
- Cyber Deception

CERBEYRA

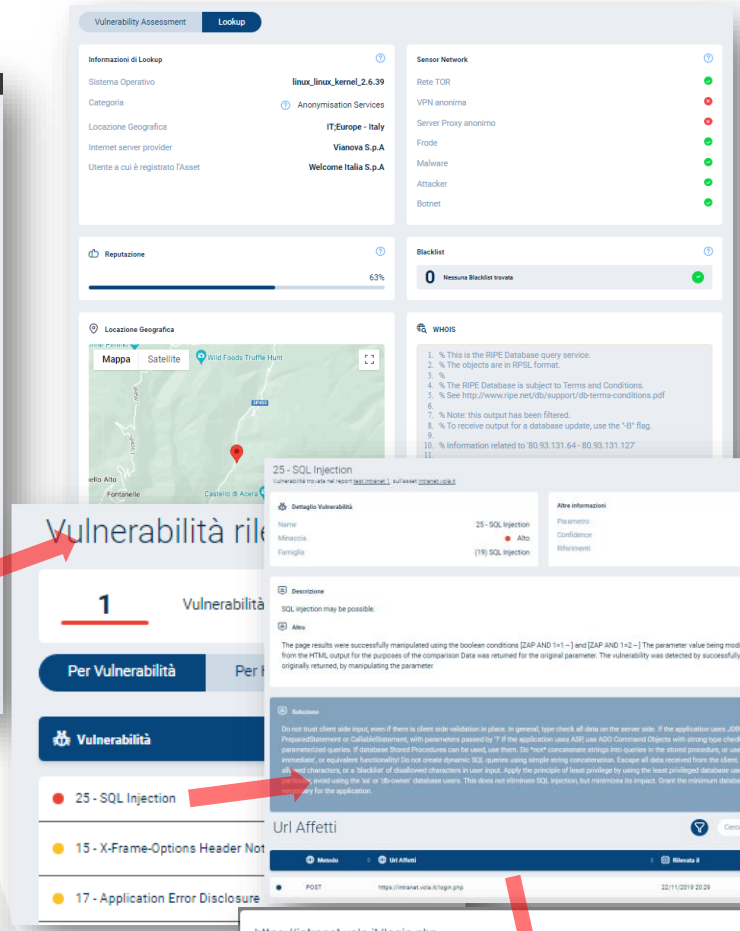
Dashboard Executive e Tecnica

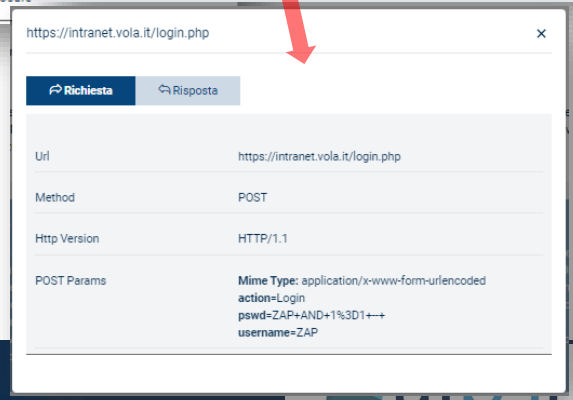
MSSP : **Zero Effort** per SOC





Onclick drilldown





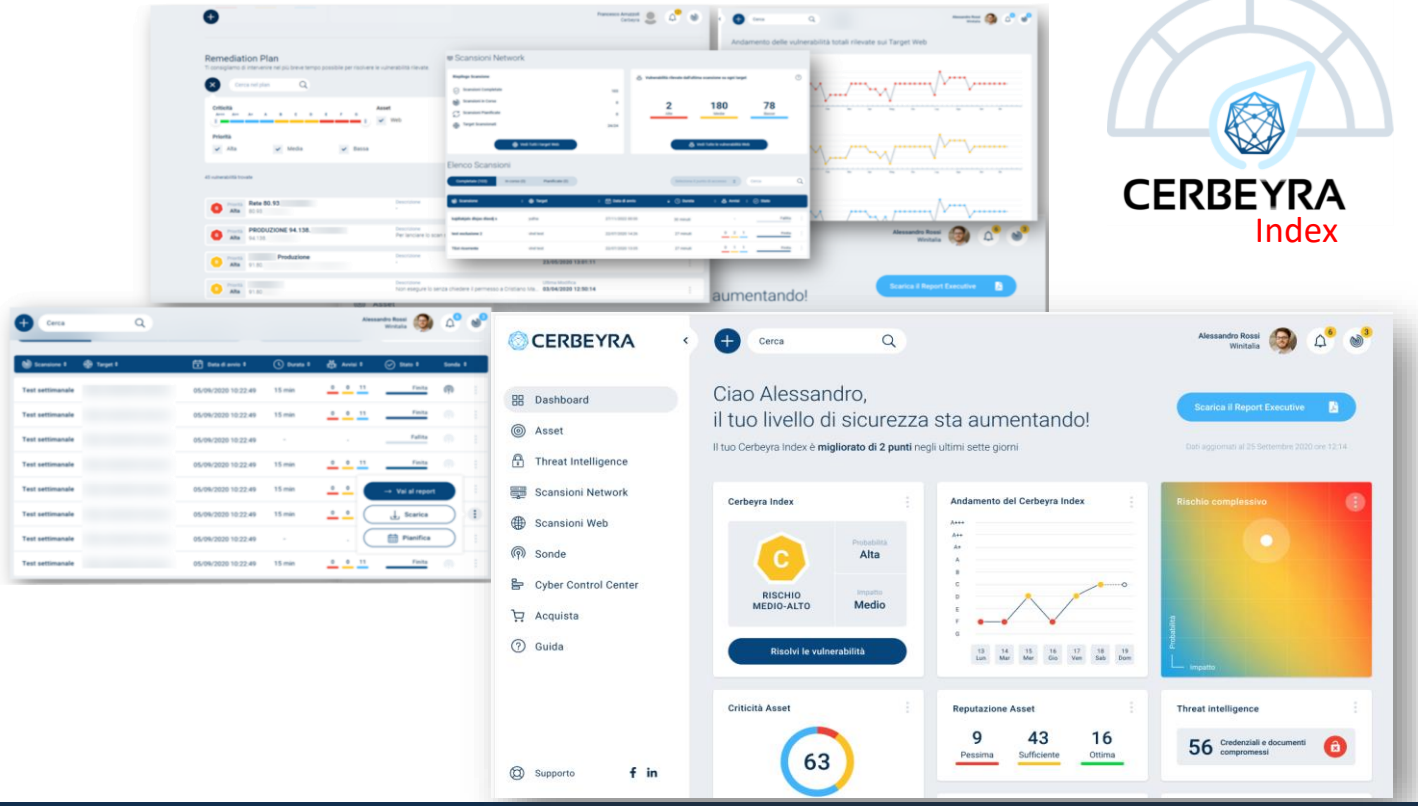
API

Application Programming Interface

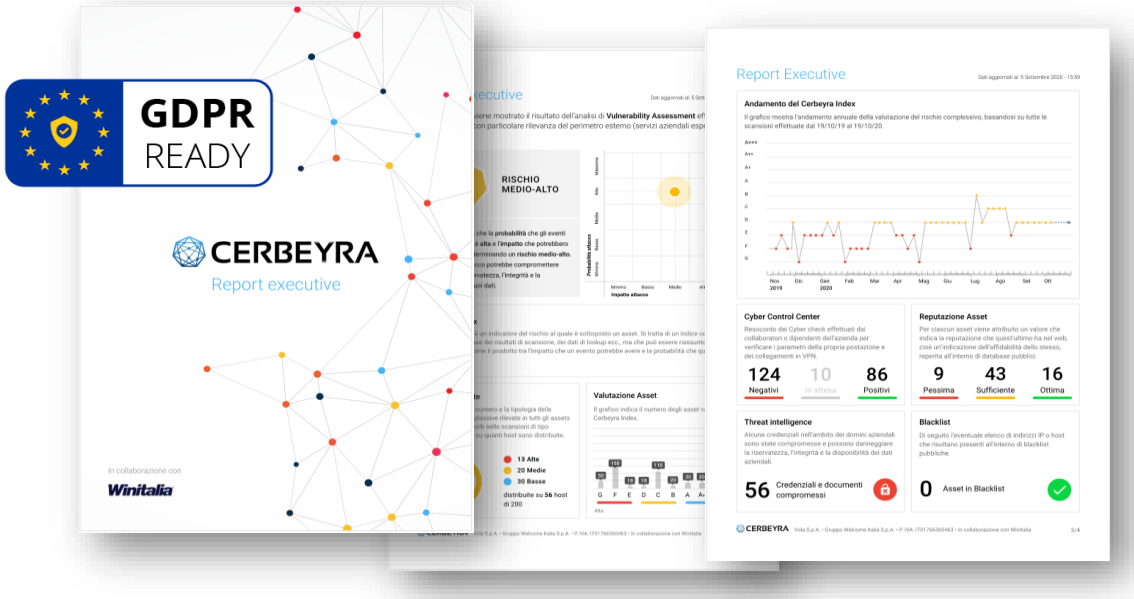
Integrazione chiamate Rest API per applicazioni di terze parti .

CERBEYRA

Interfaccia Web responsive «EASY TO USE», progettata per analizzare e comprendere le informazioni sulle minacce cyber e permettere ala management di mettere in campo le azioni correttive e preventive.



CERBEYRA
Index



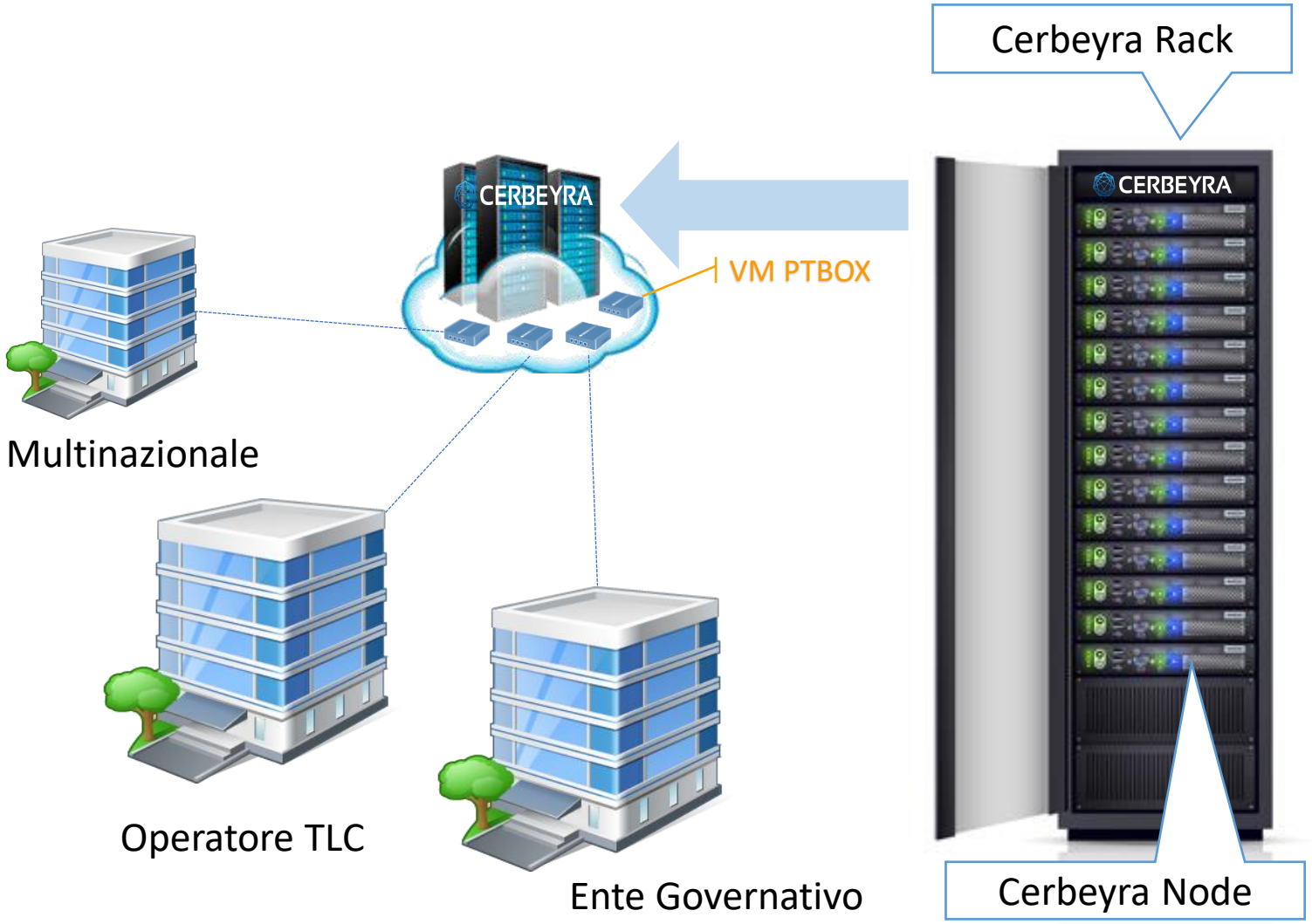
Produzione di report executive e tecnici dettagliati in tempo reale, compliance con la normativa vigente sulla sicurezza dei dati personali, inoltre la piattaforma stessa soddisfa i criteri richiesti all' art.32 comma 1d del GDPR.

Cerbeyra «Corporate»

E’ la versione on premise di Cerbeyra pensata e progettata per realtà multinazionali, operatori TLC ed organizzazioni governative di grandi dimensioni o che hanno la necessità di utilizzare l’intero ecosistema Cerbeyra all’interno della propria organizzazione.

L’intera piattaforma Cerbeyra viene fornita in modalità stand-alone con hardware dedicato.

La configurazione della soluzione è modulare e facilmente scalabile in base alle esigenze.



CERBEYRA

Cyber threat intelligence platform

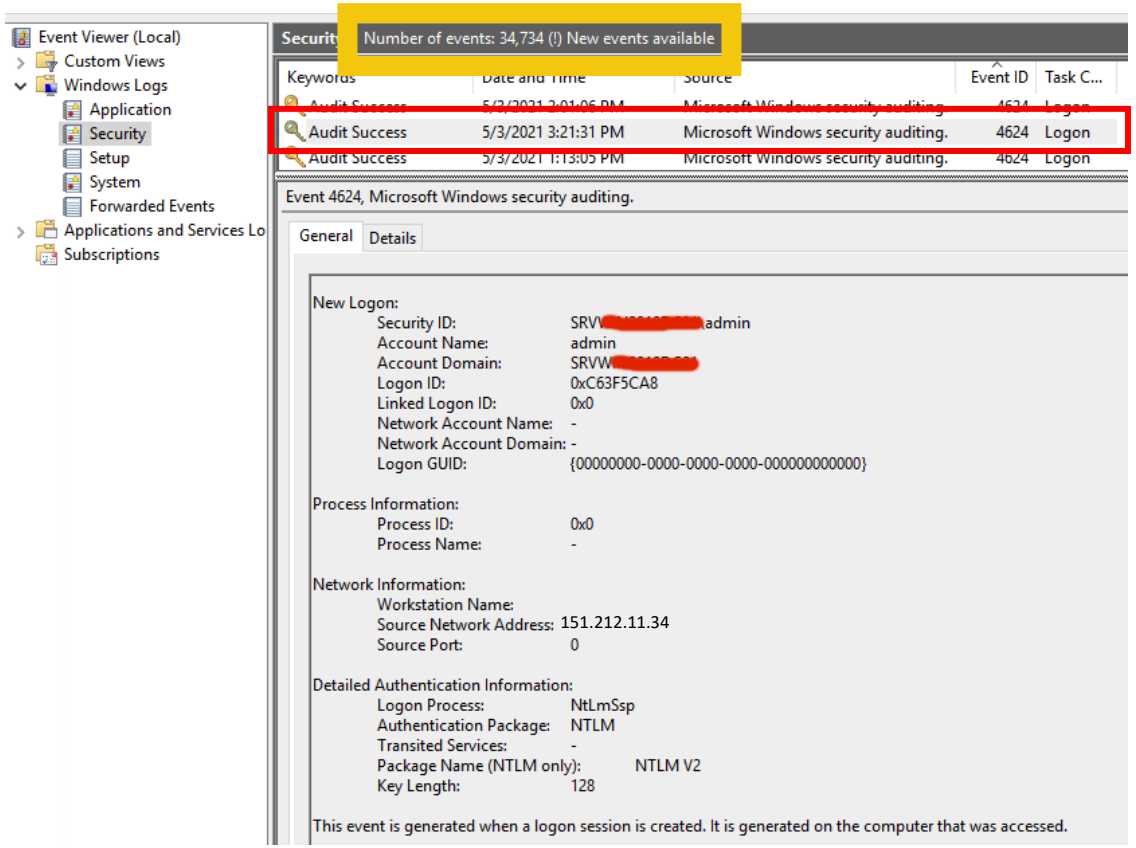
DEMO PIATTAFORMA

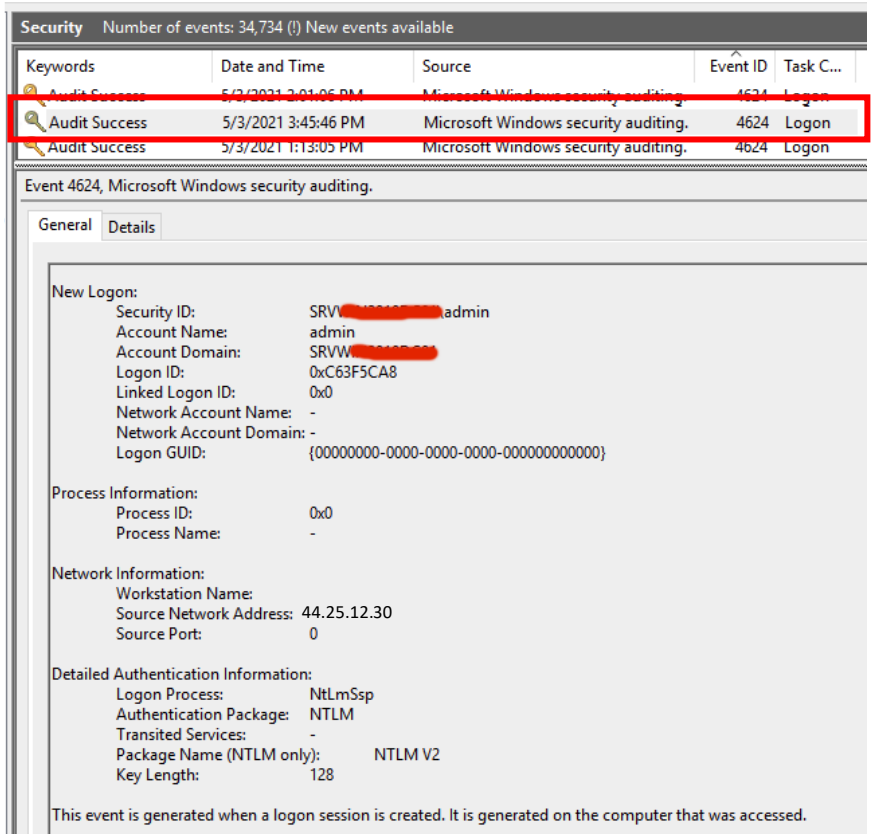
Grazie per l’attenzione

francesco.arruzzoli@cerbeyra.com

Esempio di analisi CTI sui log di un sistema ICT

L'utente **Mario Rossi** ha l'account personale **admin** con il quale si collega da remoto ad un server aziendale, esegue correttamente il login due volte a distanza di 24 minuti… trova l'anomalia.





LOG MANAGEMENT

Nei classici sistemi di log management possiamo archiviare ed analizzare statisticamente i dati in un unico repository risolvendo il problema della retention. La possibilità di correlazione tra log diversi rimane complicato come inserire degli alert sui log registrati è molto limitato; ad es. si possono impostare regole che generano un allarme se un utente fallisce per più di tre volte un login, ma niente di particolarmente più complicato.

NESSUNA ANOMALIA

SIEM

Il SIEM (Security Information and Event Management) è lo strumento che si occupa di raccogliere log prodotti da diverse fonti, interpretarli, normalizzarli e correlarli tra di loro, specificatamente in ambito security. Anche il SIEM risolve il problema della retention archiviando i dati in un unico repository.

Il SIEM oltre a correlare dispone di algoritmi più sofisticati di analisi come ad es. :

- Monitoraggio di ripetuti login falliti
- Riconoscimento di attacchi di forza bruta
- Tentativi ripetuti di login provenienti da una singola sorgente
- Tentativi ripetuti di login rivolti ad un singolo account
- Quante volte al giorno si collega normalmente ?

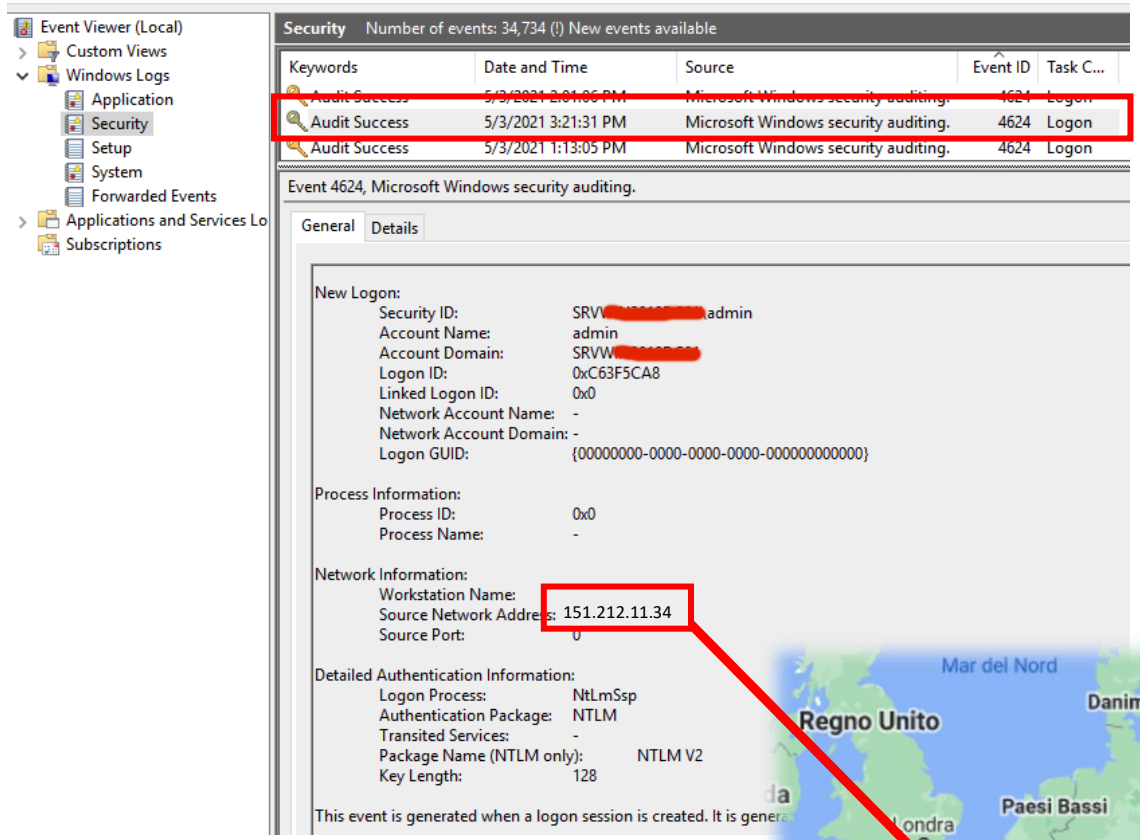
NESSUNA ANOMALIA

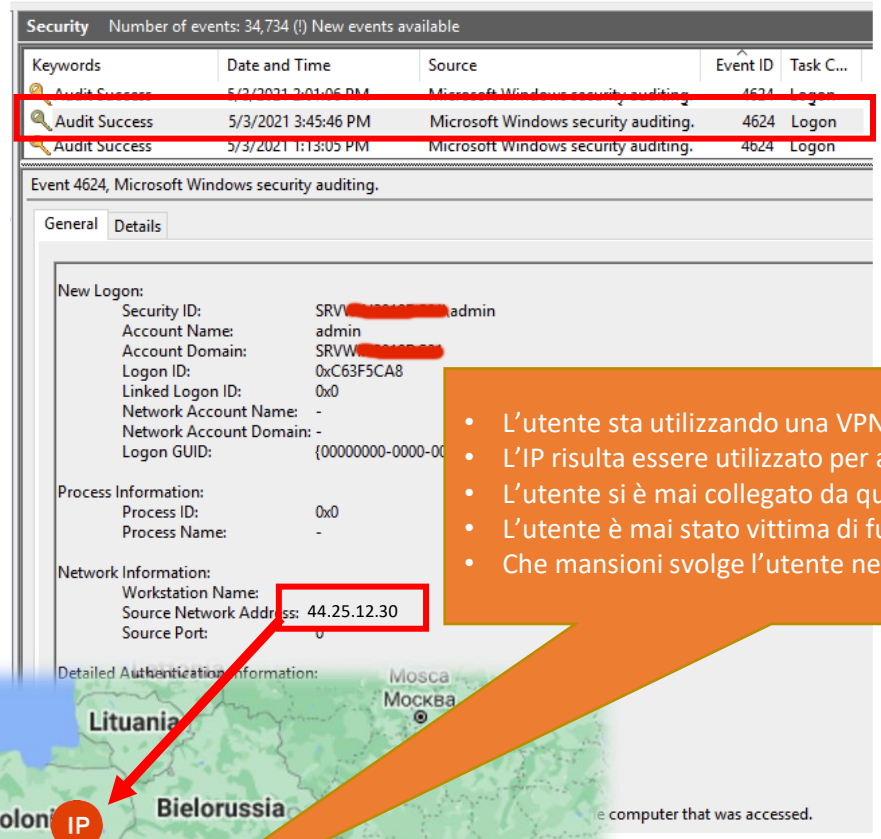
CYBER THREAT INTELLIGENCE PLATFORM

Le piattaforme CTI effettuano un'analisi più estesa cercando di «magnificare» le informazioni esistenti per trasformarle in nuove informazioni. Lo scopo è quello di comprendere le informazioni attraverso le quali comprendere la realtà. I precedenti strumenti elaborano le informazioni esistenti e dispongono di metodologie di analisi pensate per specifico evento: il login (riuscito / non riuscito).
Le piattaforme CTI prendono tutte le informazioni contenute nell'evento, identificano le entità e valutano il contesto in cui l'evento si è verificato in modo tale da comprendere anche altri fattori esterni che possono aggiungere valore all'analisi.

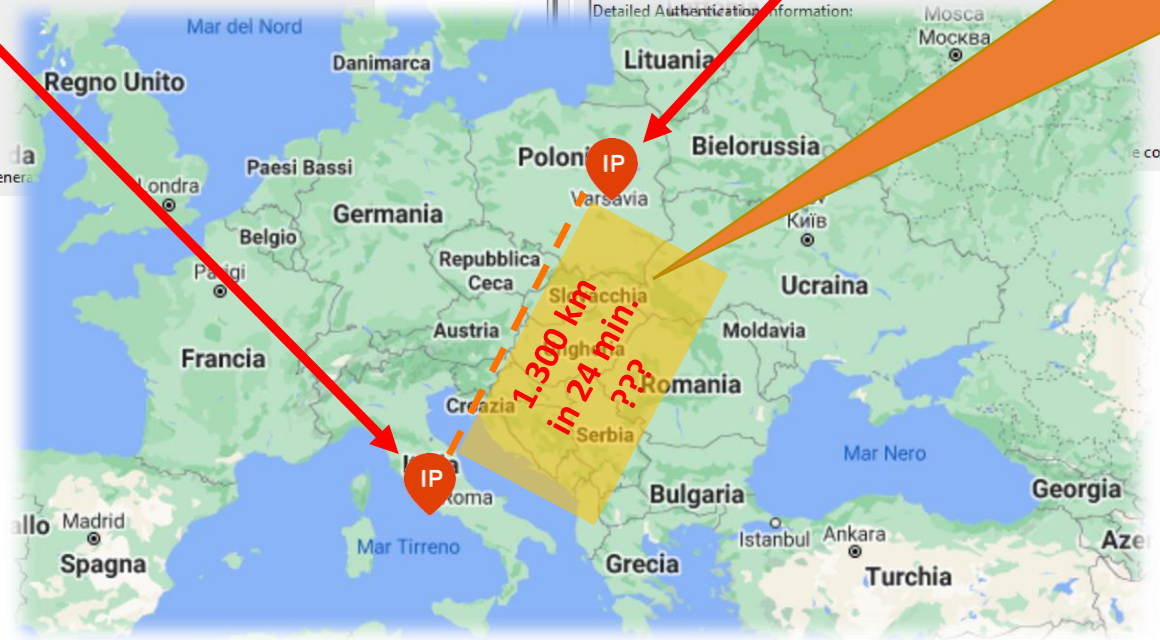
RISCONTRATA ANOMALIA

Esempio analisi CTI sui log di un sistema ICT





- L'utente sta utilizzando una VPN tracciabile o anonima ?
- L'IP risulta essere utilizzato per attività ostili ?
- L'utente si è mai collegato da quelle aree geografiche ?
- L'utente è mai stato vittima di furti / phishing conosciuti ?
- Che mansioni svolge l'utente nell'organizzazione ?



Se si toglie il contesto dall'analisi le informazioni tornano ad essere semplici dati