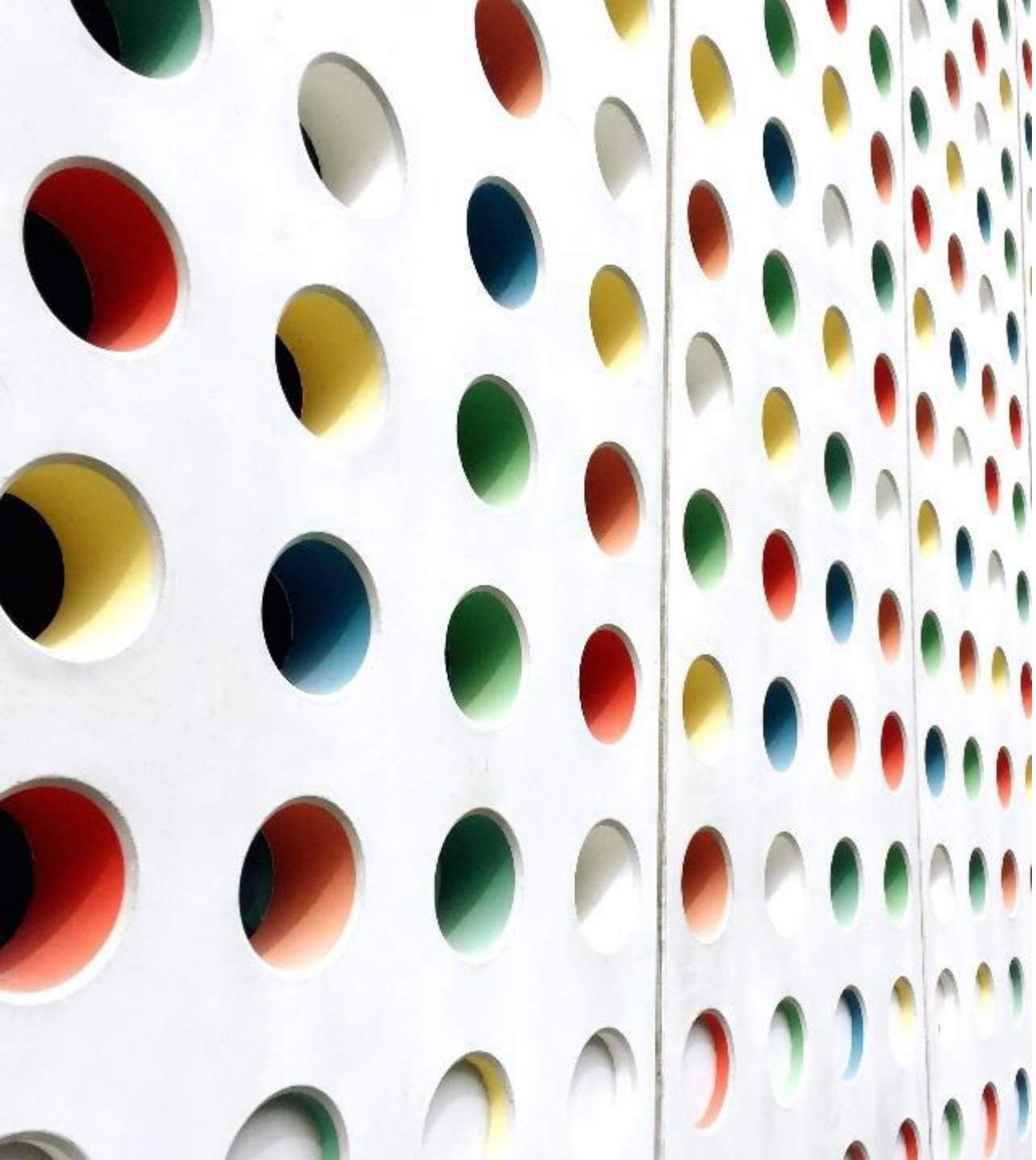


Tecnologie per la Sicurezza Informatica

Incident Management

Anno Accademico 2024/2025

VINCENZO CALABRÒ

Università degli Studi
Mediterranea
di Reggio Calabria

Agenda

1. Introduzione ai principali Framework per la Cybersecurity
2. Ciclo di vita della cybersecurity
   - **Governare**: definizione e monitoraggio continuo della strategia
   - **Identificare**: comprensione del contesto, degli asset critici e dei rischi associati
   - **Proteggere**: implementazione delle misure di protezione dei processi
   - **Rilevare**: definizione e attuazione delle attività di identificazione degli incidenti
   - **Rispondere**: definizione e attuazione delle attività di intervento in caso di incidente
   - **Ripristinare**: definizione e attuazione delle attività di ripristino dei processi
3. Tecnologie per la sicurezza informatica
4. Compliance normativa e regolatoria

Processo di Gestione della Sicurezza

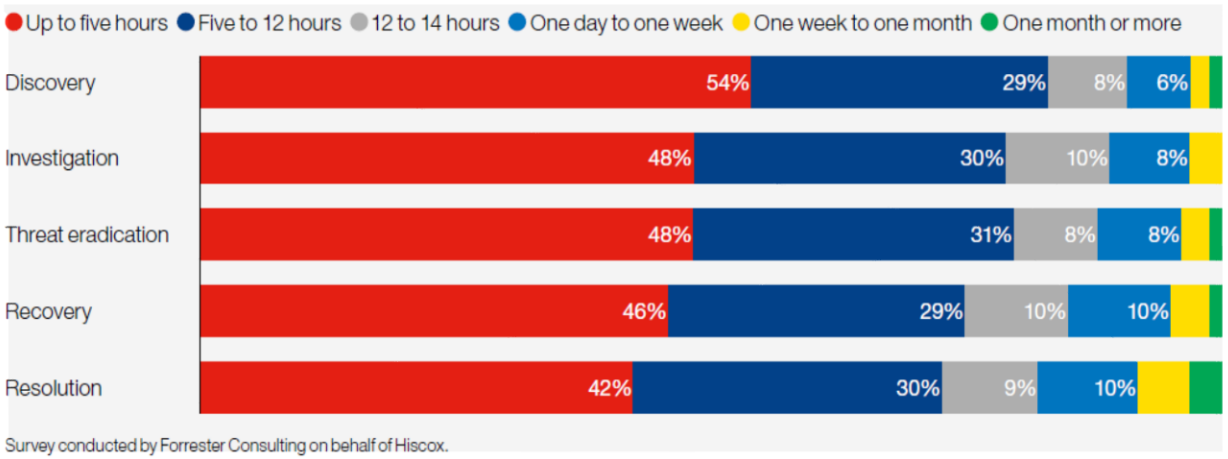
	Function	Obiettivo
Gestione del rischio	IDENTIFY	La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.
	PROTECT	La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
Gestione dell'incidente	DETECT	La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
	RESPOND	La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
	RECOVER	La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.

Gestione dell'Incident Response

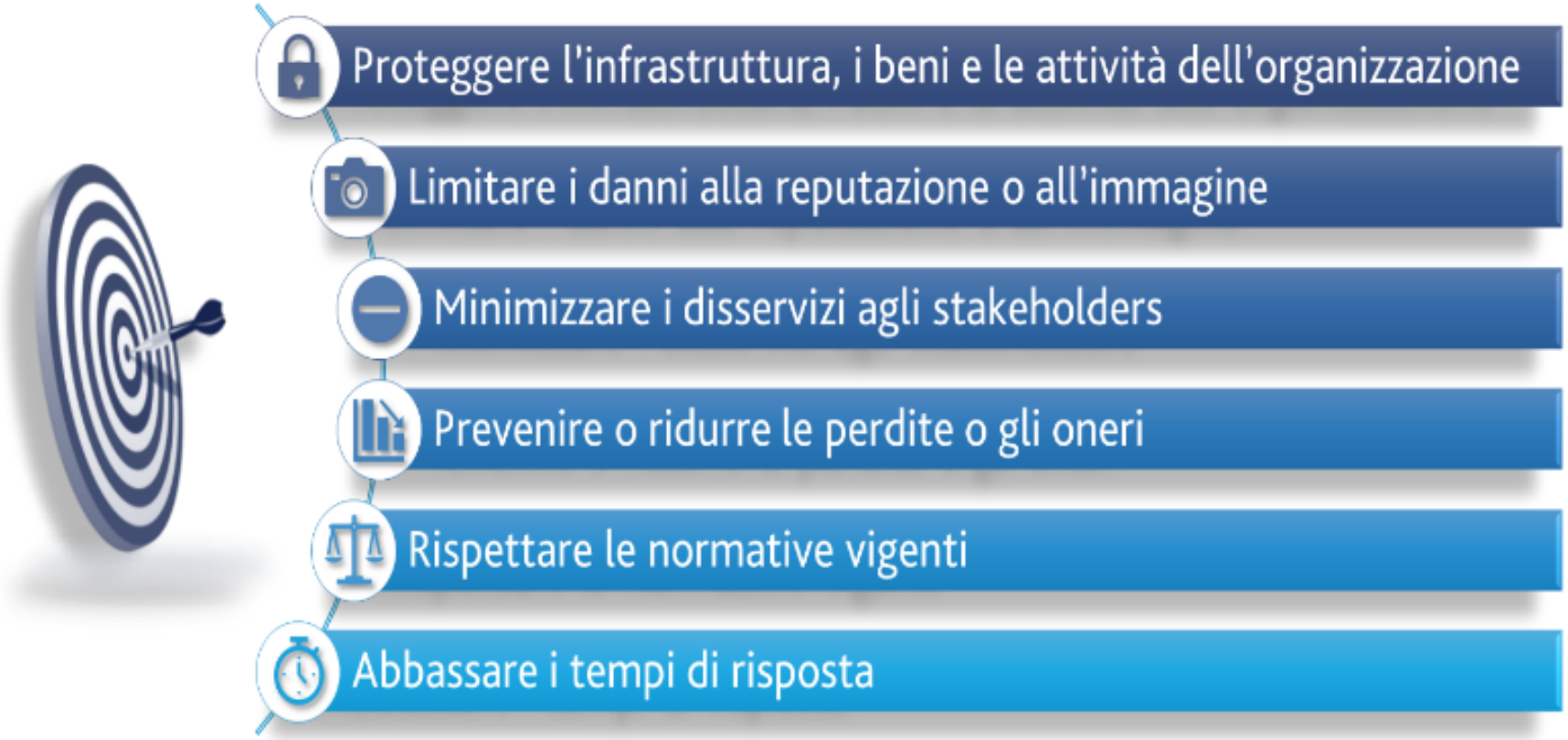
- processo coordinato per reagire alle conseguenze di un incidente finalizzato al ripristino dell'operatività
- normalmente articolato in una sequenza di fasi:

Quanto tempo è stato speso per risolvere un **«security incident»?**

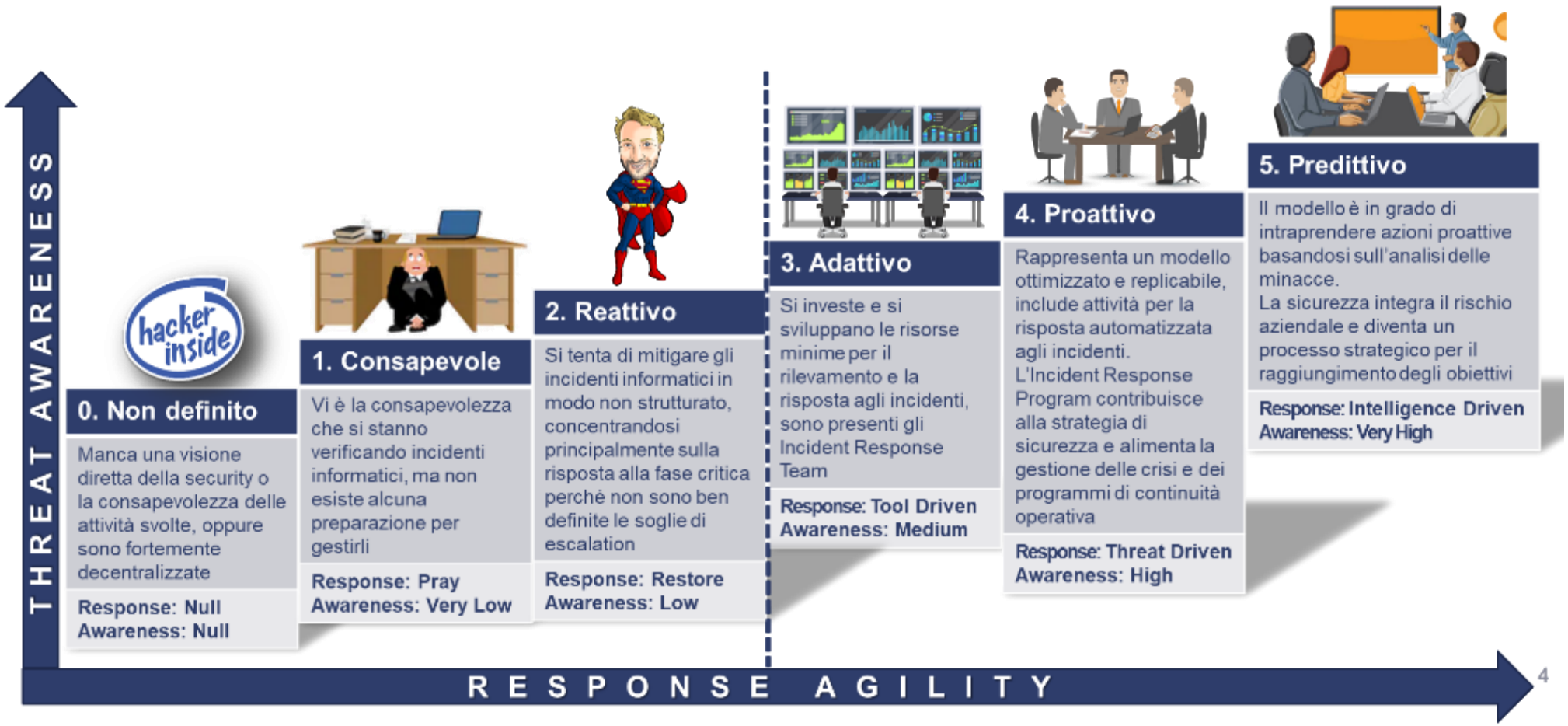
Il tempo è prezioso



Obiettivi dell'Incident Response



Incident Response Maturity Model



Esempio di Incident Response Life Cycle

Prima: PREPARE

- PEOPLE: INCIDENT RESPONSE TEAM
- PROCESS: INCIDENT RESPONSE PLAN
- TECH: INCIDENT RESPONSE PLATFORM
- IMPROVEMENT PROGRAM

Durante: DETECT & RESPOND

- IDENTIFICAZIONE DELL'EVENTO
- CONTENIMENTO DEGLI EFFETTI
- RIMOZIONE DELLA MINACCIA
- RIPRISTINO DELL'OPERATIVITÀ

Dopo: FOLLOW UP

- DIGITAL FORENSICS
- ANALISI DELL'EVENTO
- LEZIONE DI APPRENDIMENTO
- CONDIVISIONE DEL CASO

Cosa fare prima: People Incident Response Team

QUAL È L'OBIETTIVO DELL'I.R.TEAM?

- L'obiettivo principale consiste nel coordinare e valutare le risorse principali e i membri del team durante un incidente di sicurezza informatica per ridurre al minimo l'impatto e ripristinare l'operatività il più rapidamente possibile

CHE COSA FA UN I.R.TEAM?

- Analizza le informazioni raccolte (regola 5 W)
- Risponde agli incidenti informatici
- Gestisce le comunicazioni interne ed esterne
- È responsabile della notifica dell'incidente alle agenzie governative
- Verifica periodicamente le procedure dell'IR

QUALI COMPETENZE SONO NECESSARIE?

- Cercare denominatori ed eccezioni comuni
- Fare affermazioni e non ipotesi
- Eliminare l'impossibile
- Cercare sempre la spiegazione più semplice
- Ragionare come un hacker

Cosa fare prima: Process Incident Response Plan

QUAL È L'OBIETTIVO DELL'I.R.PLAN?

- Formalizzare i ruoli e le responsabilità
- Gestire una serie completa di risposte agli incidenti informatici pertinenti all'organizzazione per cui è stato elaborato

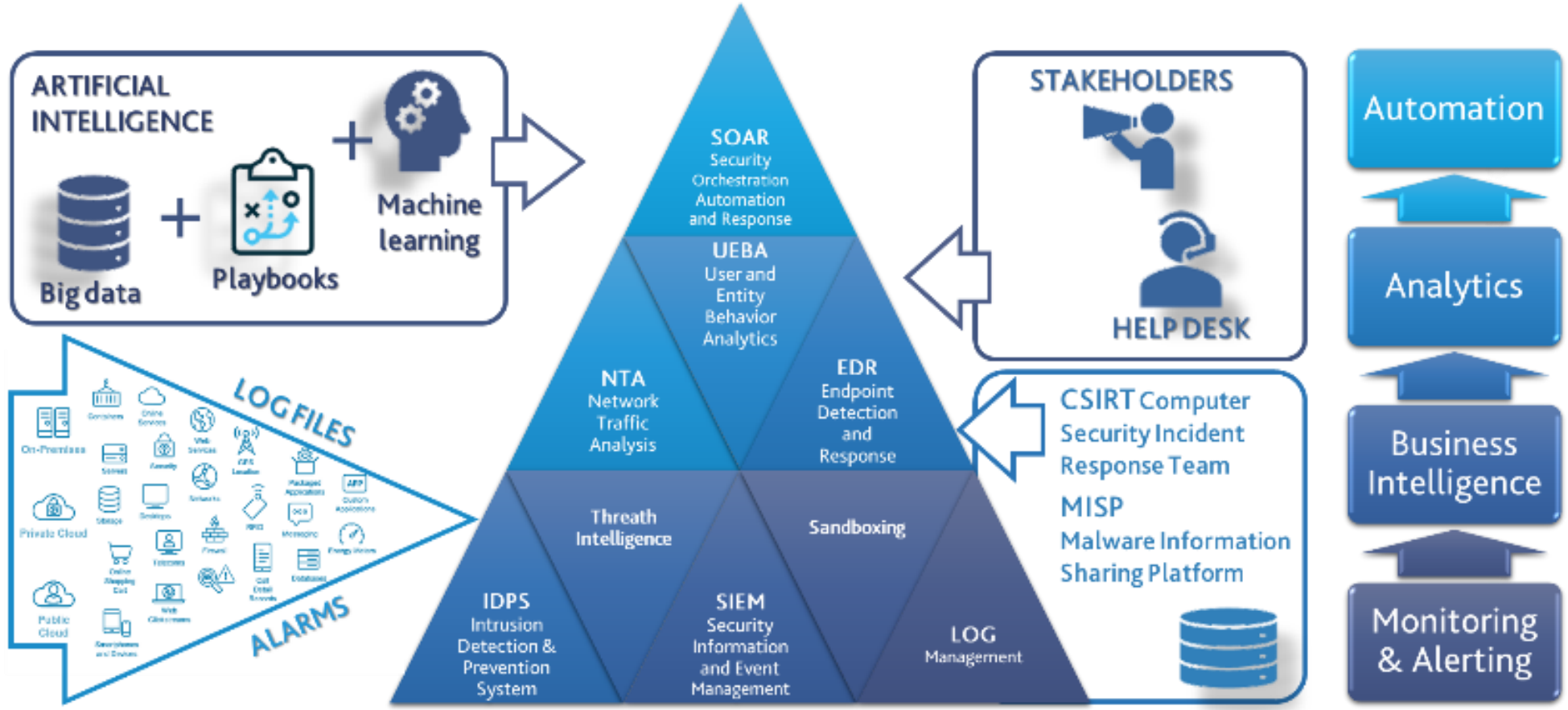
COME SI SVILUPPA UN I.R.PLAN?

- Effettuare una valutazione delle criticità
- Eseguire un'analisi realistica delle minacce
- Considerare le implicazioni sulle persone, sui processi, sulle tecnologie e sulle informazioni
- Creare modelli di risposta appropriati (Playbook)
- Rivedere periodicamente la capacità di risposta

QUALI SONO LE CRITICITÀ DI UN I.R.PLAN?

- Obsolescenza per carenza di aggiornamenti
- Complessità delle procedure da adottare
- Scarsa condivisione con gli stakeholders

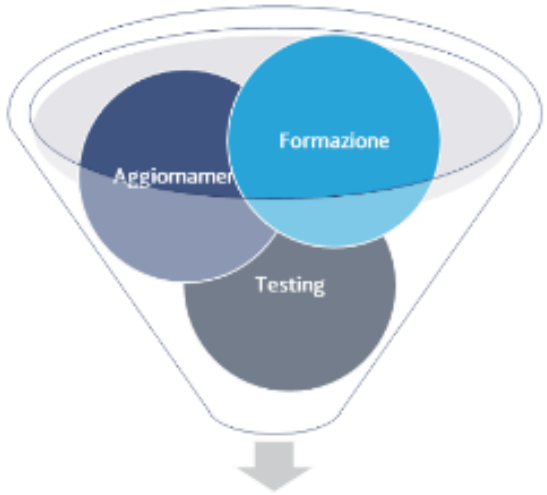
Cosa fare prima: Tech
Incident Response Platform



Cosa fare prima: Improvement Program

Rivedere periodicamente il proprio stato di preparazione all'incident response

Attività	Formazione	Aggiornamento	Testing
People	✓		✓
Plan		✓	✓
Platform		✓	✓



Detect / Rilevare (DE)

Definizione e attuazione delle attività per identificare tempestivamente incidenti di sicurezza informatica

Monitoraggio continuo (DE.CM)

Obiettivo:

Monitorare tutte le risorse IT per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente negativi

Attività
Monitorare le reti e i servizi di rete per individuare eventi potenzialmente negativi
Monitorare l'ambiente fisico per individuare eventi potenzialmente avversi
Monitorare l'attività del personale e l'uso della tecnologia per individuare eventi potenzialmente avversi
Monitorare le attività e i servizi dei fornitori di servizi esterni per individuare eventi potenzialmente avversi
Monitorare l'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati per individuare eventi potenzialmente avversi

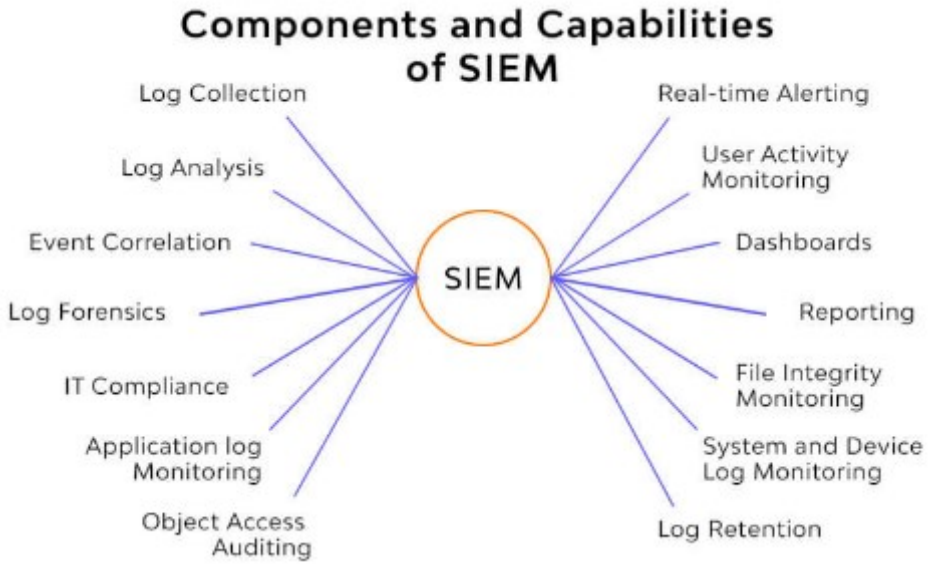
In questa fase è fondamentale la condivisione delle informazioni di sicurezza tra organizzazione dello stesso settore (p.e. minacce, incidenti e indicatori di compromissione) per aumentare l'efficacia di detection

Implementare un sistema di monitoraggio

Il **monitoraggio continuo** è la chiave di volta su cui regge l'attuale paradigma di cybersecurity.

Per implementarlo occorre:

1. Identificare gli asset critici
2. Distribuire i sensori e individuare le fonti di dati
3. Centralizzare la raccolta dei dati (SIEM o piattaforme simili)
4. Implementare monitoraggi a più livelli
5. Garantire la ridondanza
6. Separare la gestione del monitoraggio dal resto dell'IT
7. Proteggere i sistemi di monitoraggio
8. Stabilire la priorità degli alert
9. Implementare la correlazione eventi
10. Implementare la contestualizzazione con ambiente e altri asset



Analisi degli eventi avversi (DE.AE)

Obiettivo:

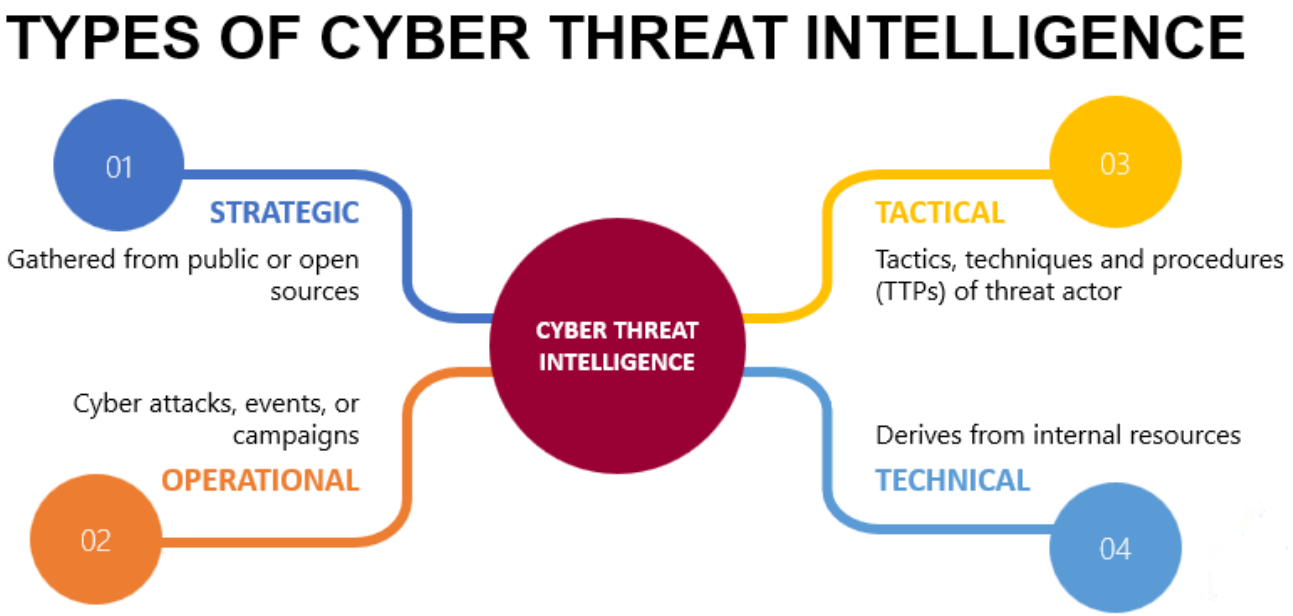
Analizzare le anomalie, gli indicatori di compromissione e gli altri eventi potenzialmente avversi per caratterizzare gli eventi per essere in grado di rilevare gli incidenti di cybersecurity

Attività
Analizzare gli eventi potenzialmente avversi per comprendere meglio le attività associate
Correlare le informazioni provenienti da più fonti
Comprendere l'impatto stimato e la portata degli eventi avversi
Fornire le informazioni sugli eventi avversi al personale e agli strumenti autorizzati
Integrare l'analisi con le informazioni sulle minacce informatiche e le altre informazioni contestuali
Dichiarare gli incidenti nel momento in cui gli eventi avversi soddisfano i criteri definiti per gli incidenti

Implementazione di un sistema di analisi

L'analisi delle attività malevole necessita di un sistema di threat intelligence, eventualmente provvisto di intelligenza artificiale, alimentato da fonti di minacce:

- CVE (Common Vulnerabilities and Exposures)
- TTPs (Tattiche, Tecniche e Procedure)
- IOC (Indicatore di compromissione)
- IOA (Indicatore di attacco)
- Payload / Exploit / Malware
- Threat Actors



I sistemi di cyber threat intelligence sfruttano l'AI per migliorare le capacità di detection e analisi

XDR

wazuh.

The Open Source Security Platform

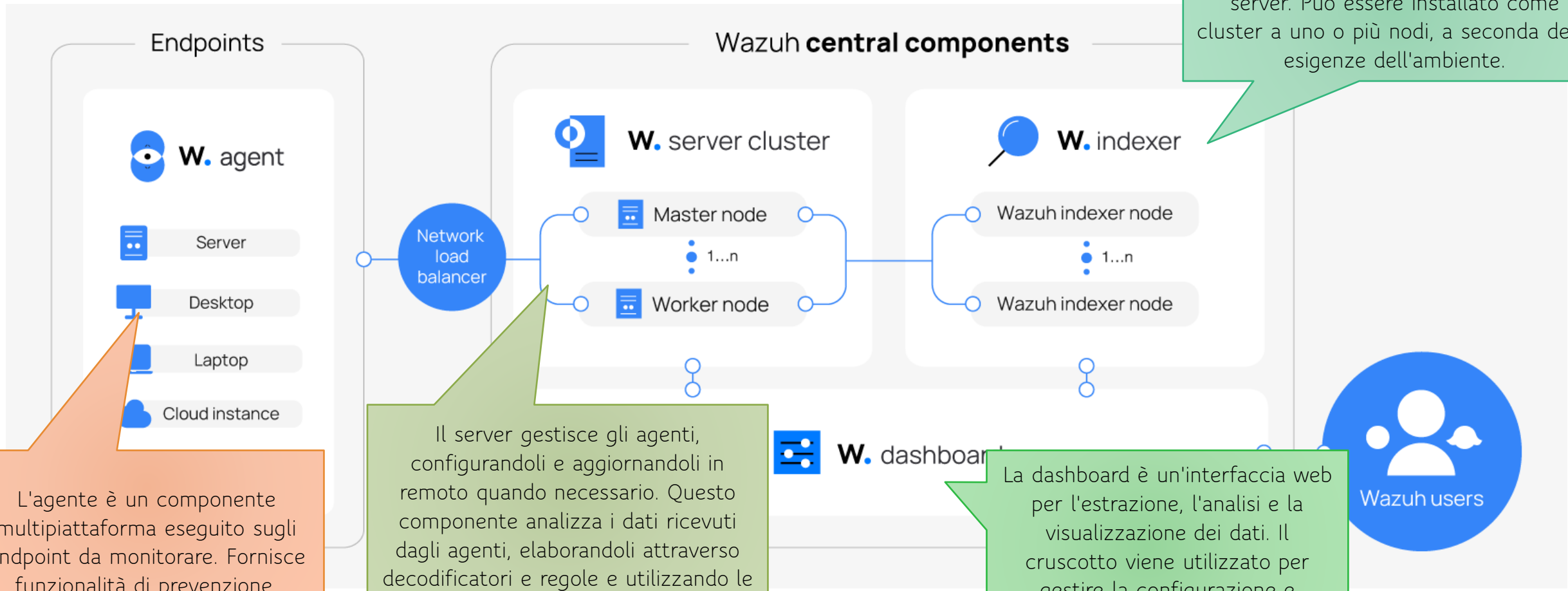
SIEM

Esempio di implementazione

XDR - Extended Detection and Response

SIEM - Security Information and Event Management

Componenti del SIEM/XDR



L'agente è un componente multipiattaforma eseguito sugli endpoint da monitorare. Fornisce funzionalità di prevenzione, rilevamento e risposta.

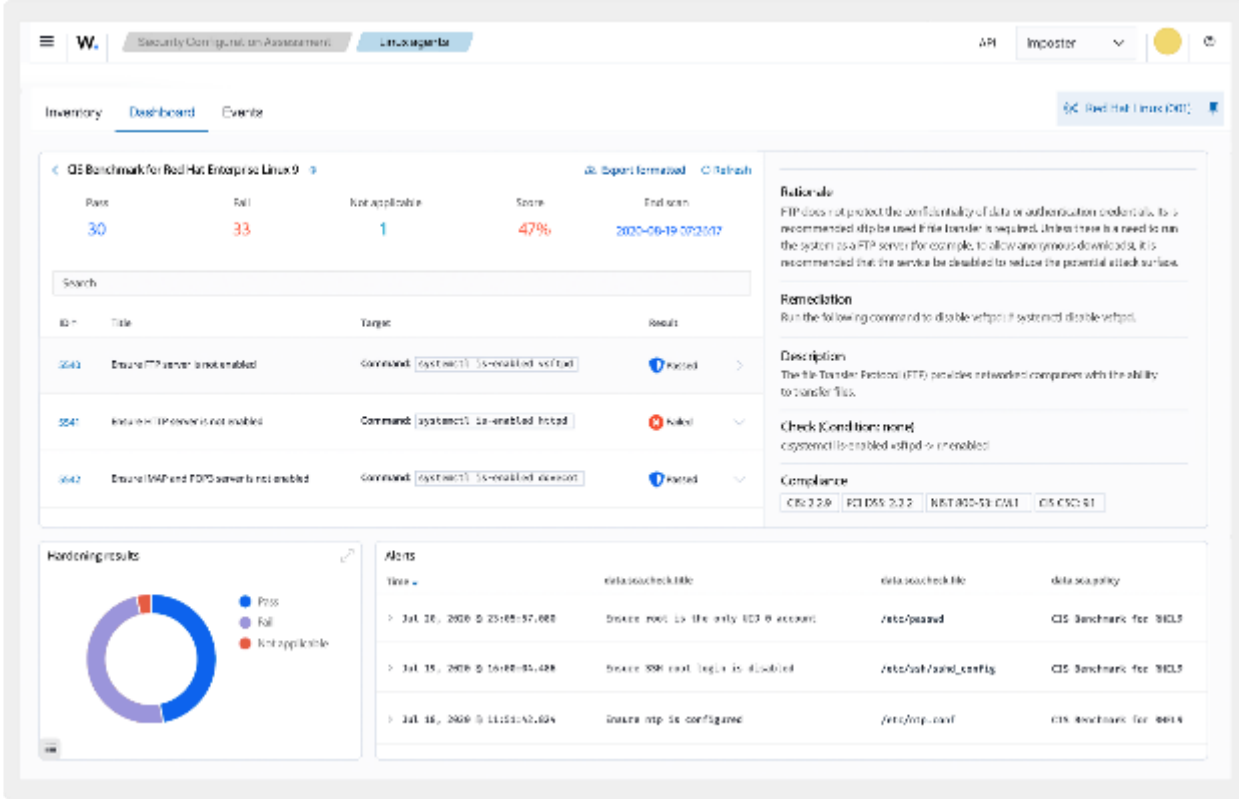
Il server gestisce gli agenti, configurandoli e aggiornandoli in remoto quando necessario. Questo componente analizza i dati ricevuti dagli agenti, elaborandoli attraverso decodificatori e regole e utilizzando le informazioni sulle minacce per cercare indicatori di compromissione.

L'indexer è un motore di ricerca e analisi full-text altamente scalabile. È responsabile dell'indicizzazione e dell'archiviazione degli avvisi generati dal server. Può essere installato come cluster a uno o più nodi, a seconda delle esigenze dell'ambiente.

La dashboard è un'interfaccia web per l'estrazione, l'analisi e la visualizzazione dei dati. Il cruscotto viene utilizzato per gestire la configurazione e monitorarne lo stato.

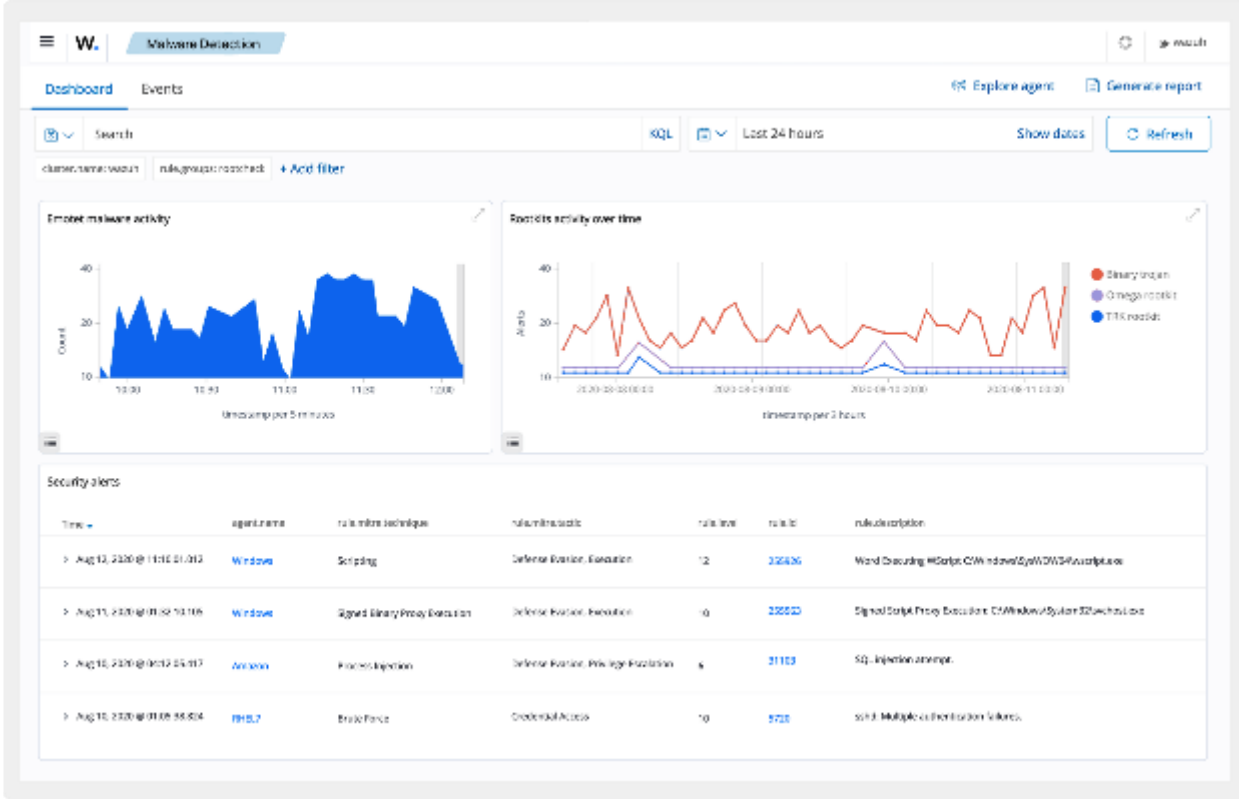
Configuration Assessment

Monitora le impostazioni di configurazione del sistema e delle applicazioni per garantire che siano conformi ai criteri di sicurezza, agli standard e/o alle guide di hardening.
Gli agenti eseguono scansioni periodiche per rilevare configurazioni errate o lacune di sicurezza negli endpoint che possono essere sfruttate dagli attori delle minacce. Inoltre, è possibile personalizzare questi controlli di configurazione, in modo da allinearli correttamente alle esigenze dell'organizzazione. Gli avvisi di sicurezza includono raccomandazioni per una migliore configurazione, riferimenti e mappatura con la conformità normativa.



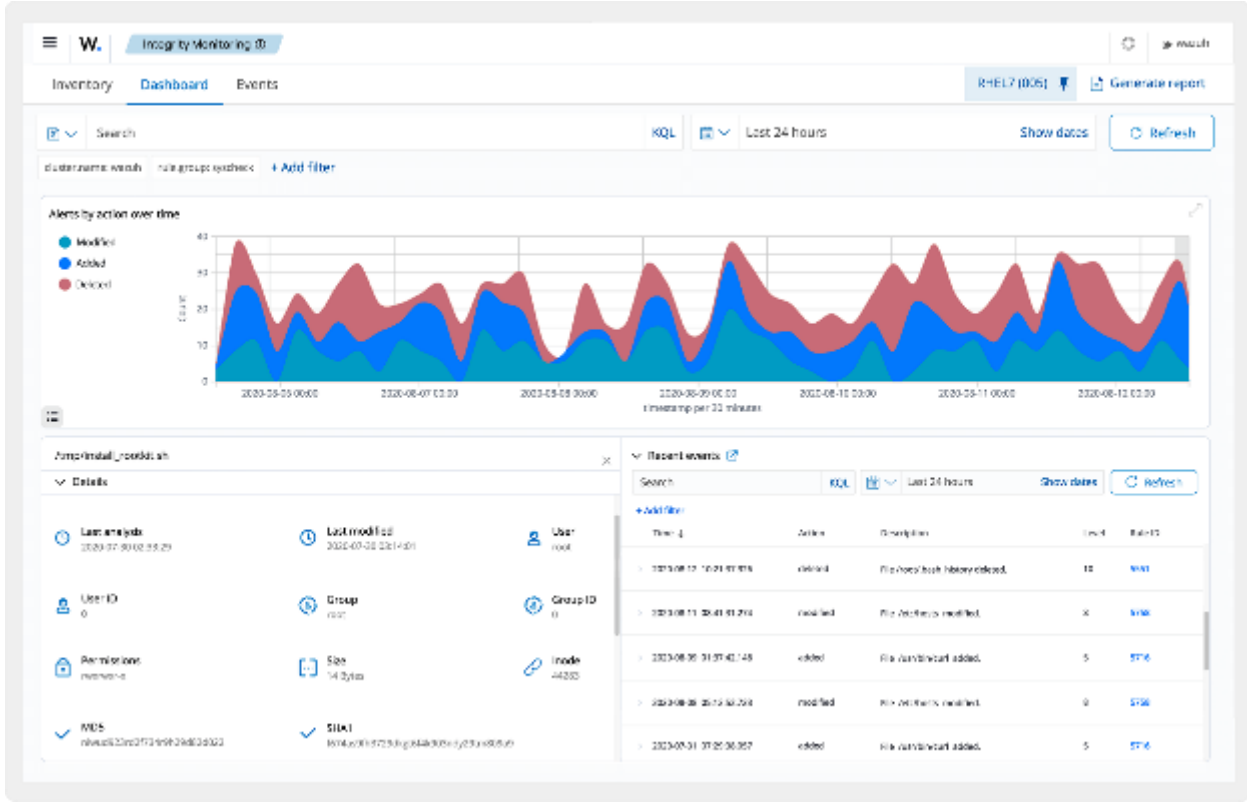
Malware Detection

Rileva le attività dannose e gli indicatori di compromissione che si verificano sugli endpoint a seguito di un'infezione da malware o di un attacco informatico.
Il set di regole out-of-the-box e le funzionalità come Security Configuration Assessment (SCA), Rootcheck e File Integrity Monitoring (FIM) contribuiscono a rilevare le attività e le anomalie dannose.
È possibile configurare e personalizzare queste funzionalità in base alle esigenze della propria organizzazione.



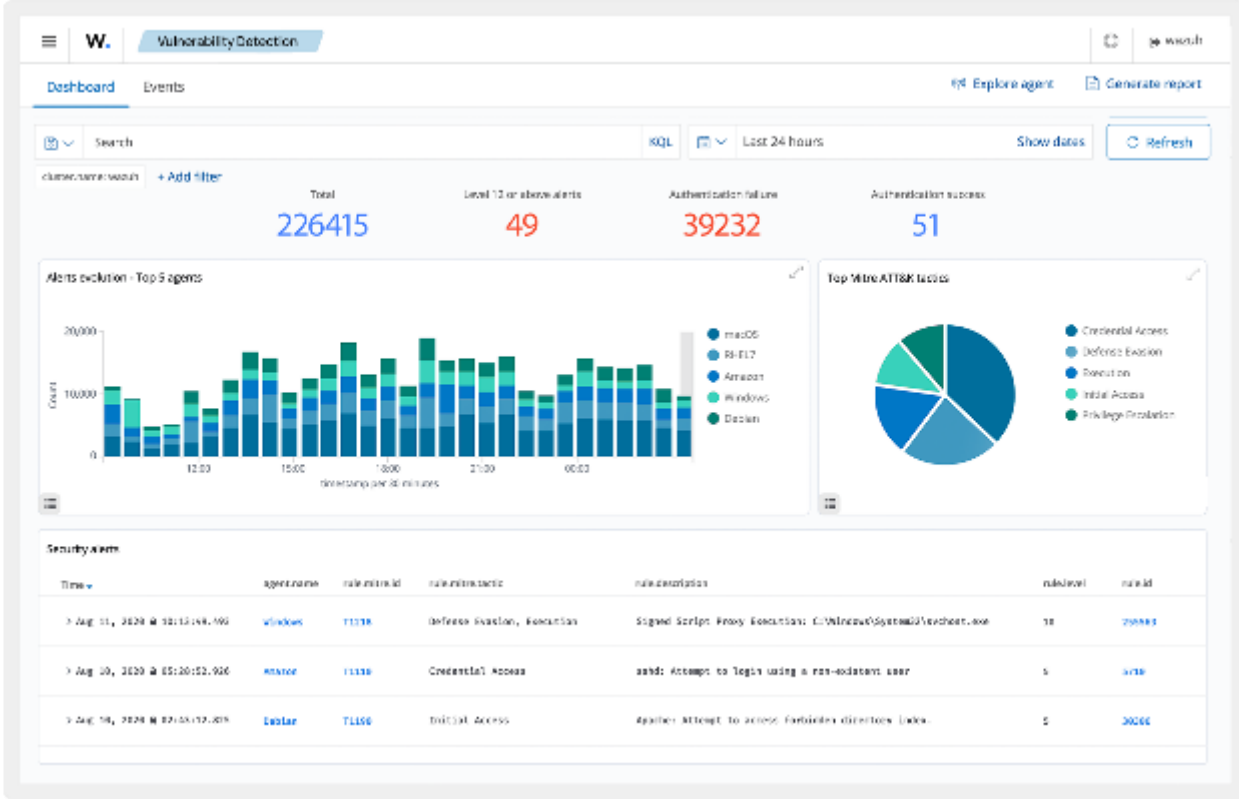
File Integrity Monitoring

Monitora il file system, identificando le modifiche di contenuto, permessi, proprietà e attributi dei file di cui è necessario tenere traccia. Inoltre, identifica in modo nativo gli utenti e le applicazioni utilizzate per creare o modificare i file. È possibile utilizzare la funzionalità di monitoraggio dell'integrità dei file in combinazione con le informazioni sulle minacce per identificare le minacce o gli endpoint compromessi. Inoltre, FIM aiuta a soddisfare diversi standard di conformità normativa, come PCI DSS, NIST e altri.



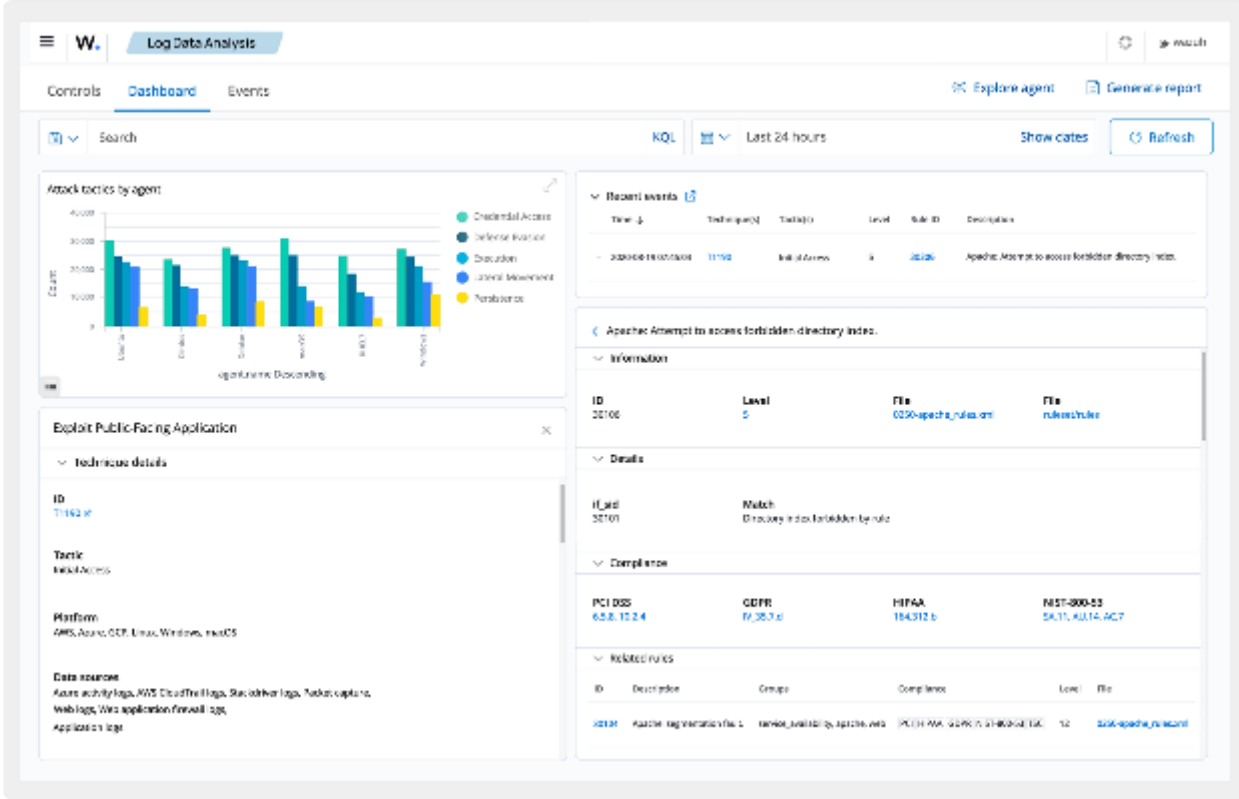
Threat Hunting

Offre una visibilità completa degli endpoint e dell'infrastruttura monitorati. Fornisce funzionalità di conservazione, indicizzazione e interrogazione dei log che aiutano a indagare sulle minacce che potrebbero aver aggirato i controlli di sicurezza iniziali. Le regole di rilevamento delle minacce sono mappate rispetto al framework MITRE ATT&CK per facilitare l'indagine e il riferimento a tattiche, tecniche e procedure comunemente utilizzate dagli aggressori. Si integra anche con feed e piattaforme di threat intelligence di terze parti per migliorare la ricerca delle minacce.



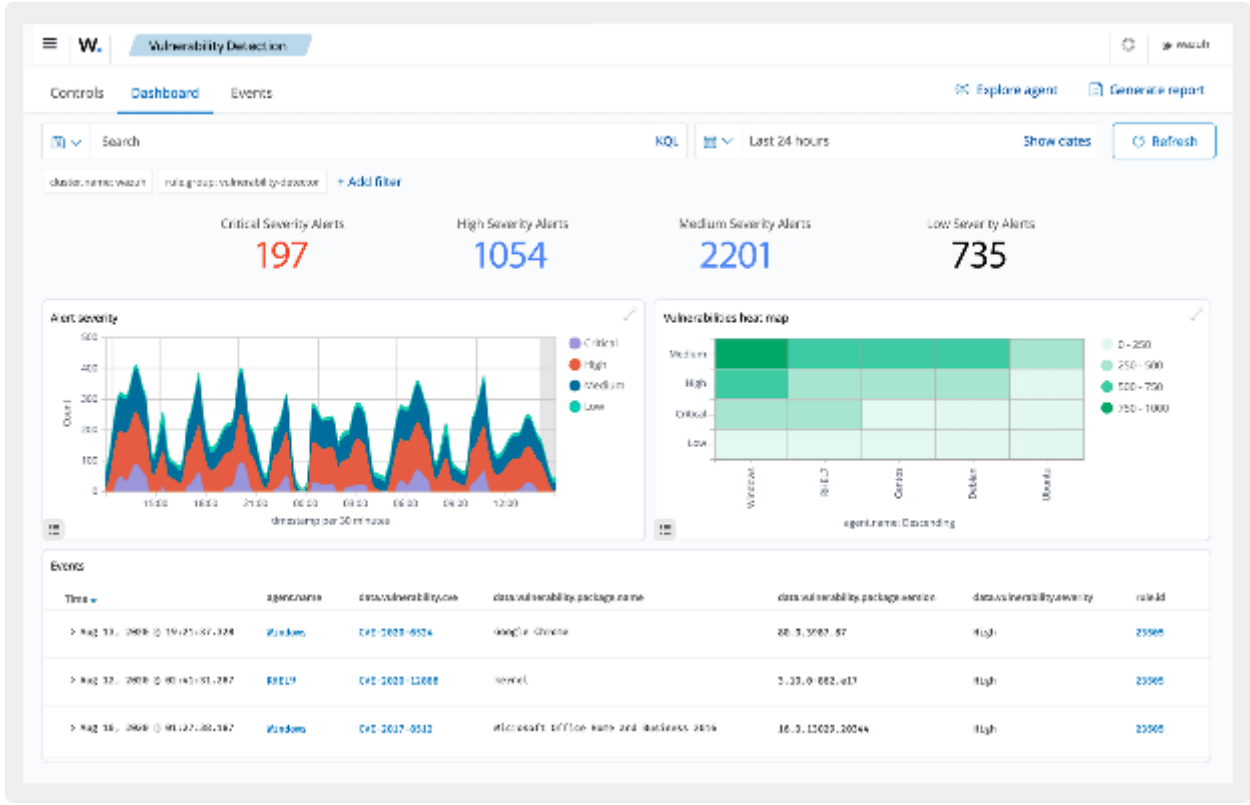
Log Data Analysis

Gli agenti raccolgono i registri del sistema operativo e delle applicazioni e li inoltrano in modo sicuro al server per l'analisi e l'archiviazione basata su regole. Le regole rilevano errori di applicazione o di sistema, configurazioni errate, attività dannose, violazioni di policy e vari altri problemi di sicurezza e operativi.



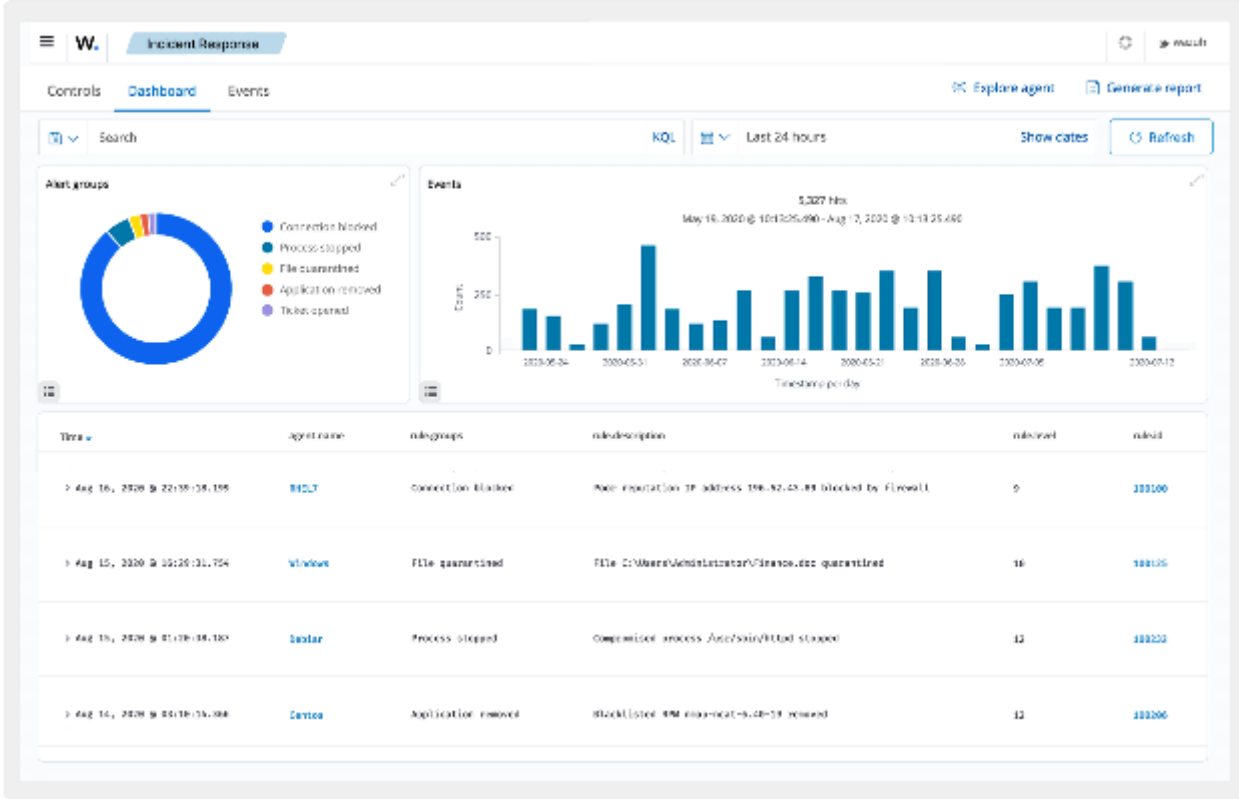
Vulnerability Detection

Gli agenti raccolgono i dati dell'inventario software e li inviano al server. I dati dell'inventario raccolti vengono poi correlati con i database CVE (Common Vulnerabilities and Exposure) costantemente aggiornati, per identificare i software vulnerabili noti. Il rilevamento automatico delle vulnerabilità vi aiuta a trovare le falle nelle vostre risorse critiche e a intraprendere azioni correttive prima che gli aggressori le sfruttino per scopi dannosi.



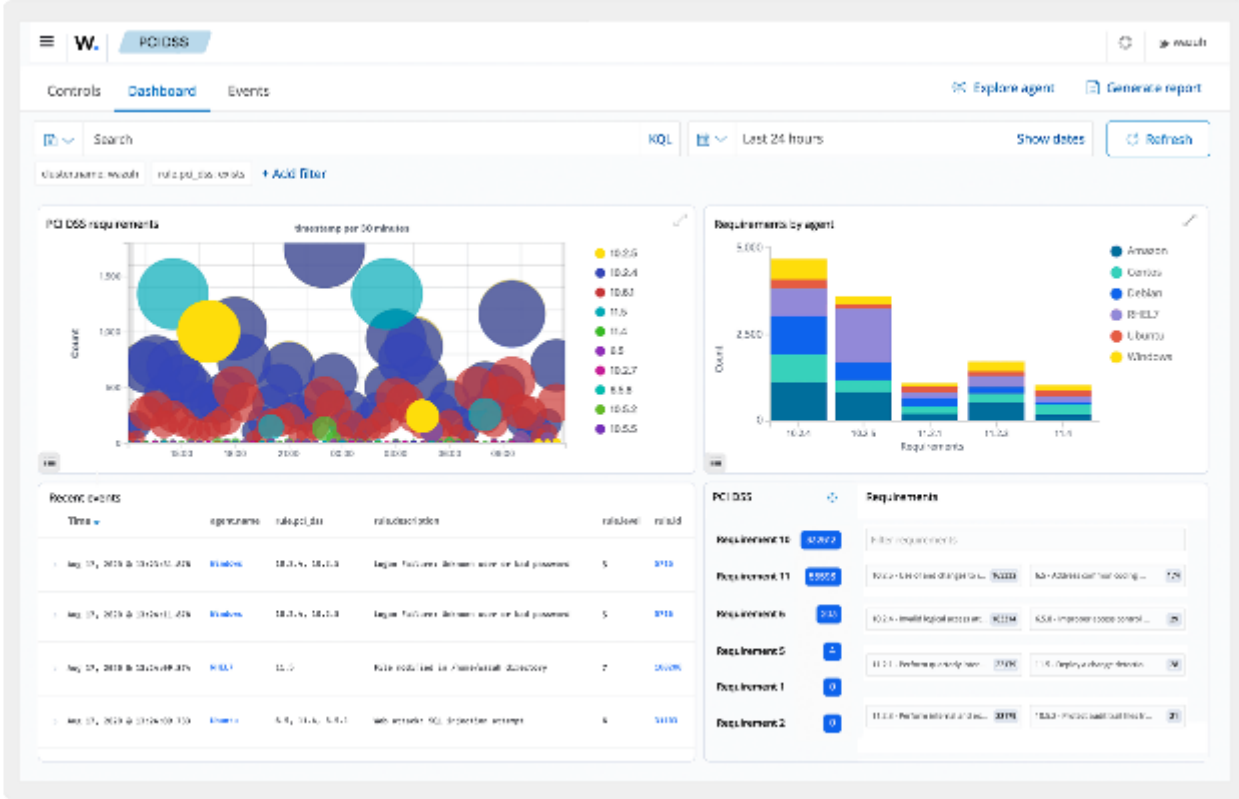
Incident Response

Fornisce risposte attive pronte all'uso per eseguire varie contromisure contro le minacce in corso. Queste risposte vengono attivate quando sono soddisfatti determinati criteri e comprendono azioni come il blocco dell'accesso alla rete a un endpoint dalla fonte della minaccia e altre ancora. Inoltre, può essere utilizzato per eseguire in remoto comandi o query di sistema, identificare indicatori di compromissione (IOC) e contribuire all'esecuzione di attività di risposta agli incidenti.



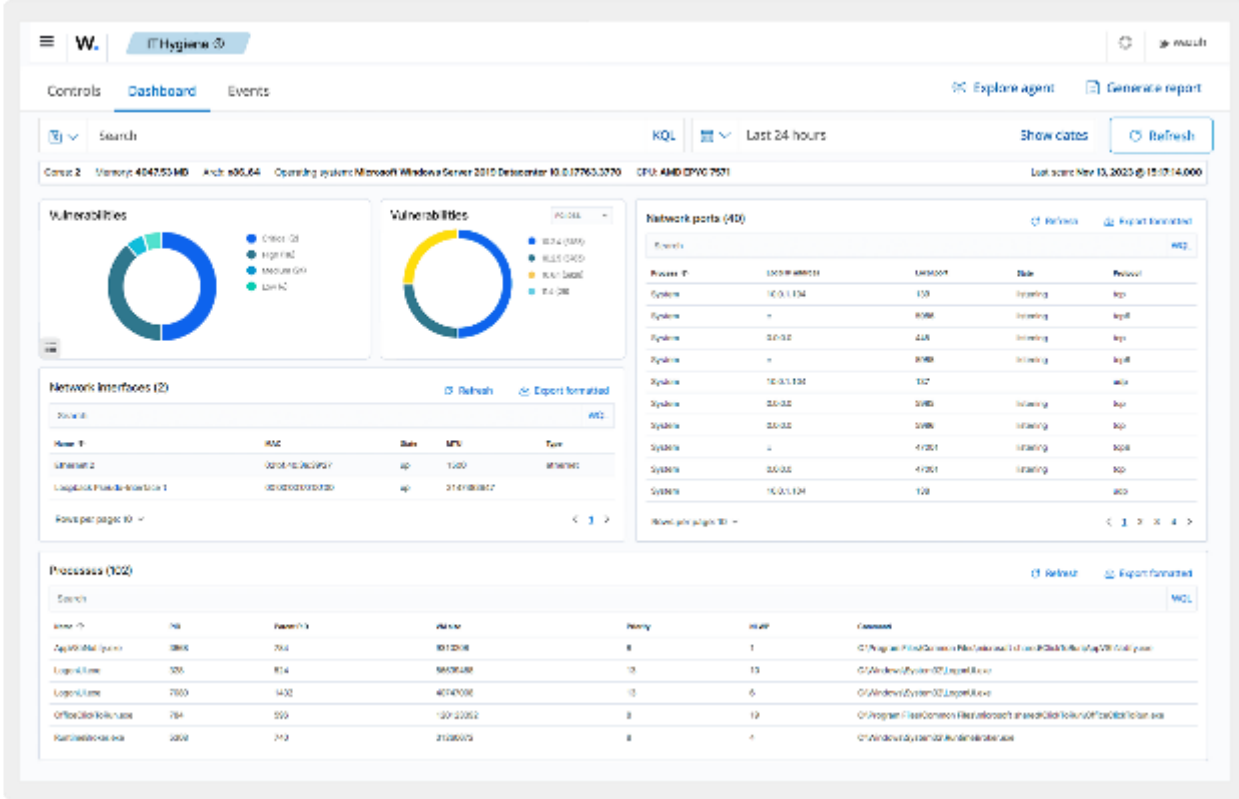
Regulatory Compliance

Fornisce alcuni dei controlli di sicurezza necessari per diventare conformi agli standard e alle normative del settore. Alcuni di questi controlli di sicurezza includono il monitoraggio dell'integrità dei file (FIM), la valutazione della configurazione di sicurezza (SCA), il rilevamento delle vulnerabilità, l'inventario dei sistemi e altro ancora. Queste funzionalità, unite alla scalabilità e al supporto multipiattaforma, aiutano le organizzazioni a soddisfare i requisiti di conformità tecnica. Fornisce report e dashboard per normative quali PCI DSS, NIST, TSC e HIPAA.



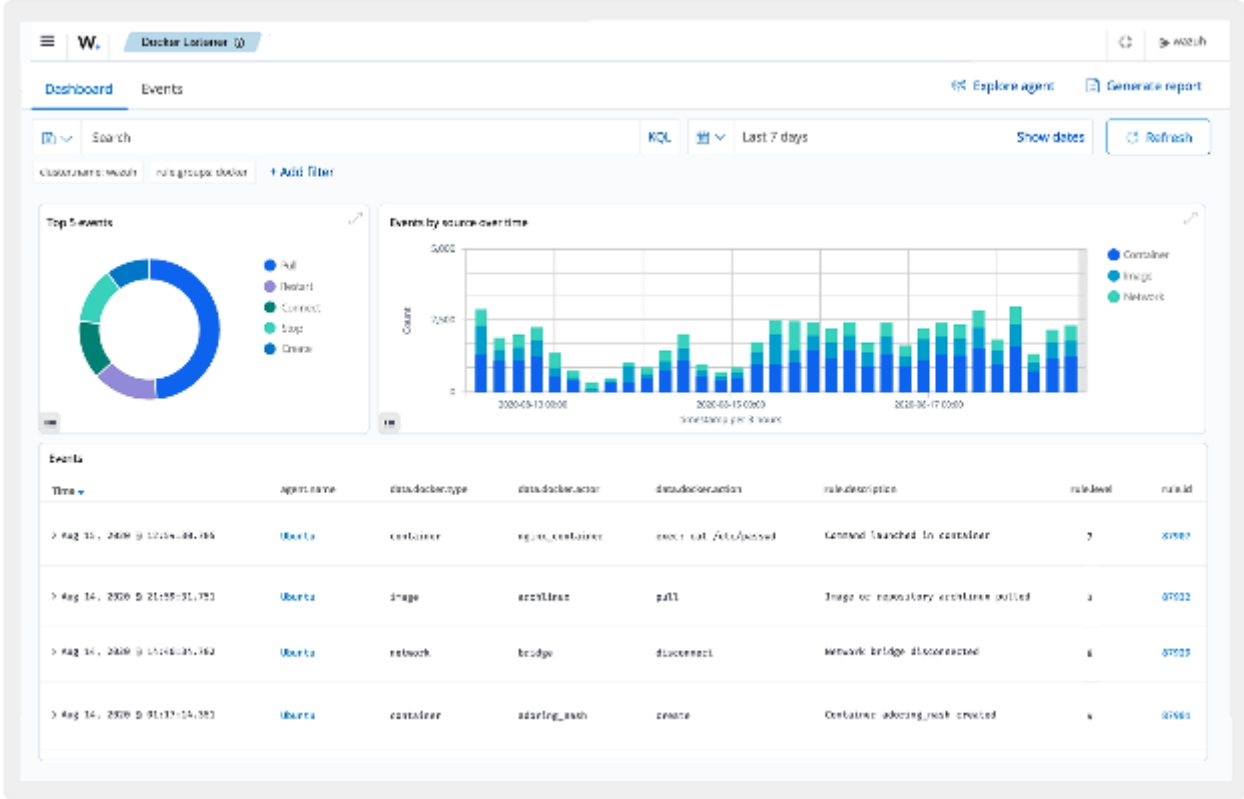
IT Hygiene

Crea un inventario di sistema aggiornato di tutti gli endpoint monitorati. Questo inventario di sistema contiene dati come le applicazioni installate, i processi in esecuzione, le porte aperte, le informazioni sull'hardware e sul sistema operativo e altri ancora. La raccolta di queste informazioni aiuta le organizzazioni a ottimizzare la visibilità degli asset e a mantenere una buona igiene IT. Molte altre funzionalità come il rilevamento delle vulnerabilità, la valutazione della configurazione di sicurezza e il rilevamento del malware, aiutano a proteggere gli endpoint monitorati e a migliorare l'igiene IT.



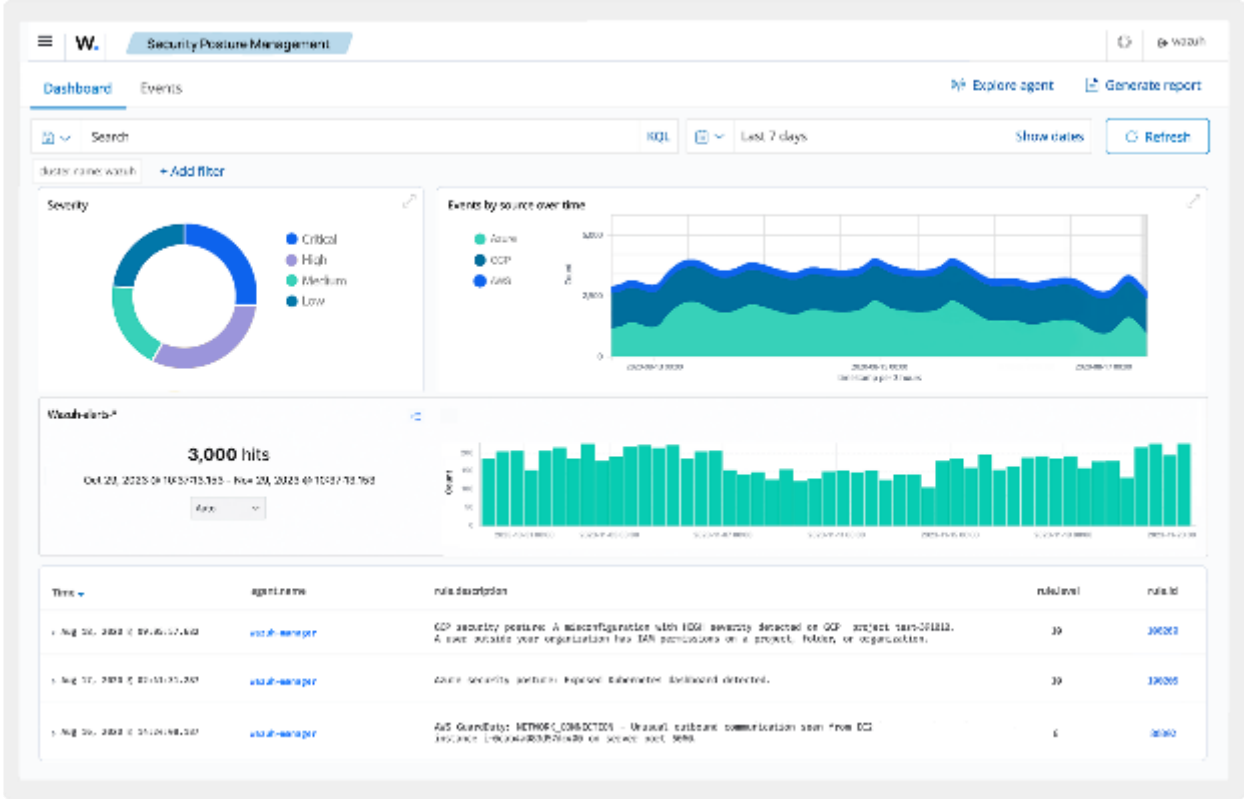
Containers Security

Fornisce visibilità sulla sicurezza degli host e dei container Docker, monitorandone il comportamento e rilevando minacce, vulnerabilità e anomalie. L'agente si integra in modo nativo con il motore Docker, consentendo agli utenti di monitorare immagini, volumi, impostazioni di rete e container in esecuzione.
Raccoglie e analizza continuamente informazioni dettagliate sul tempo di esecuzione. Ad esempio, avvisa in caso di container in esecuzione in modalità privilegiata, applicazioni vulnerabili, una shell in esecuzione in un container, modifiche a volumi o immagini persistenti e altre possibili minacce.



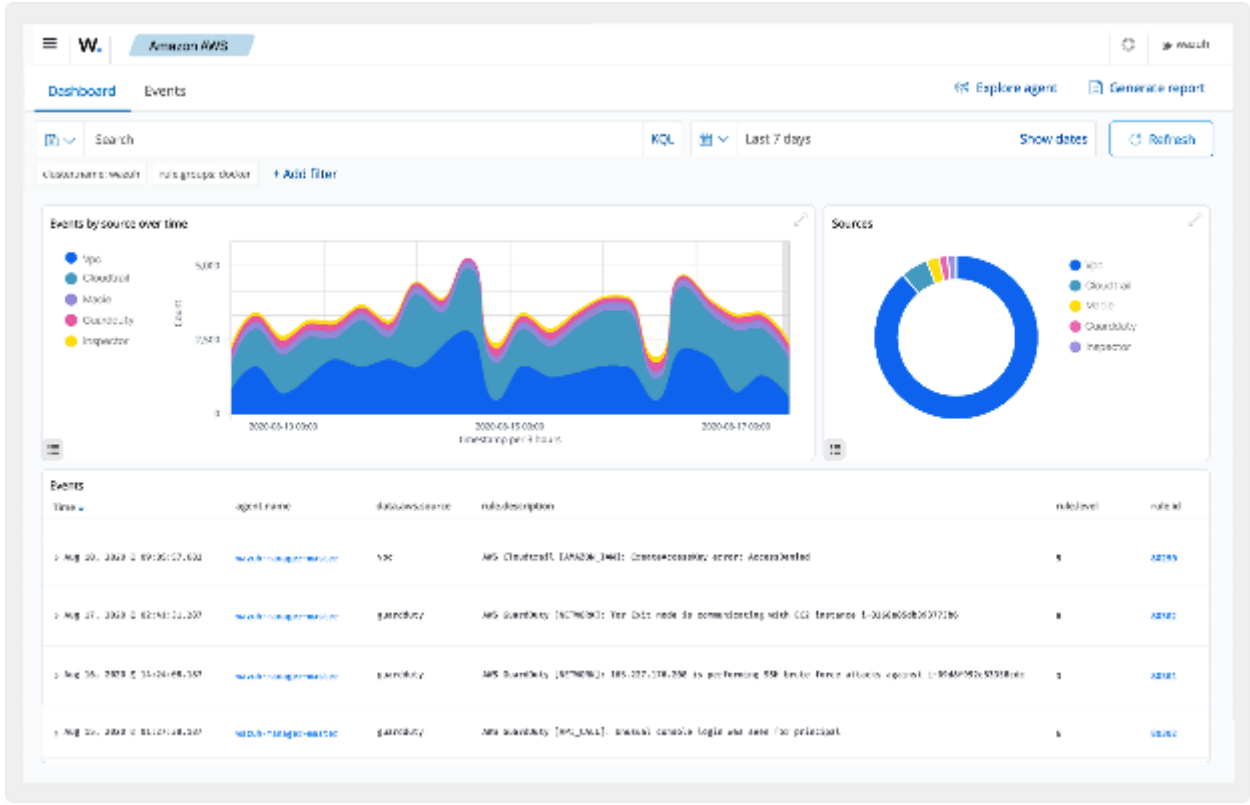
Posture Management

Si integra con le piattaforme cloud, raccogliendo e aggregando i dati sulla sicurezza. Avverte dei rischi di sicurezza e delle vulnerabilità scoperte per garantire la sicurezza e la conformità agli standard normativi.



Workload Protection

Monitora e protegge i carichi di lavoro in ambienti cloud e on-premise. È possibile integrarlo con piattaforme cloud come AWS, Microsoft Azure, GCP, Microsoft 365 e GitHub per monitorare servizi, macchine virtuali e attività che si svolgono su queste piattaforme. La gestione centralizzata dei log aiuta le organizzazioni che utilizzano queste piattaforme cloud a rispettare i requisiti normativi.



Esercitazione Wazuh

- Importare la VM Wazuh
- Configurare una scheda rete NAT
- Configurare scheda video VMSVGA
- Eseguire la VM
- Eseguire una seconda VM (p.e. kali)
- Collegarsi tramite web ip_wazuh
- Credenziali console user: wazuh-user password: wazuh
- Credenziali web user: admin password: admin

Per un'installazione completa visitare il sito: https://wazuh.com/install/

Riepilogo

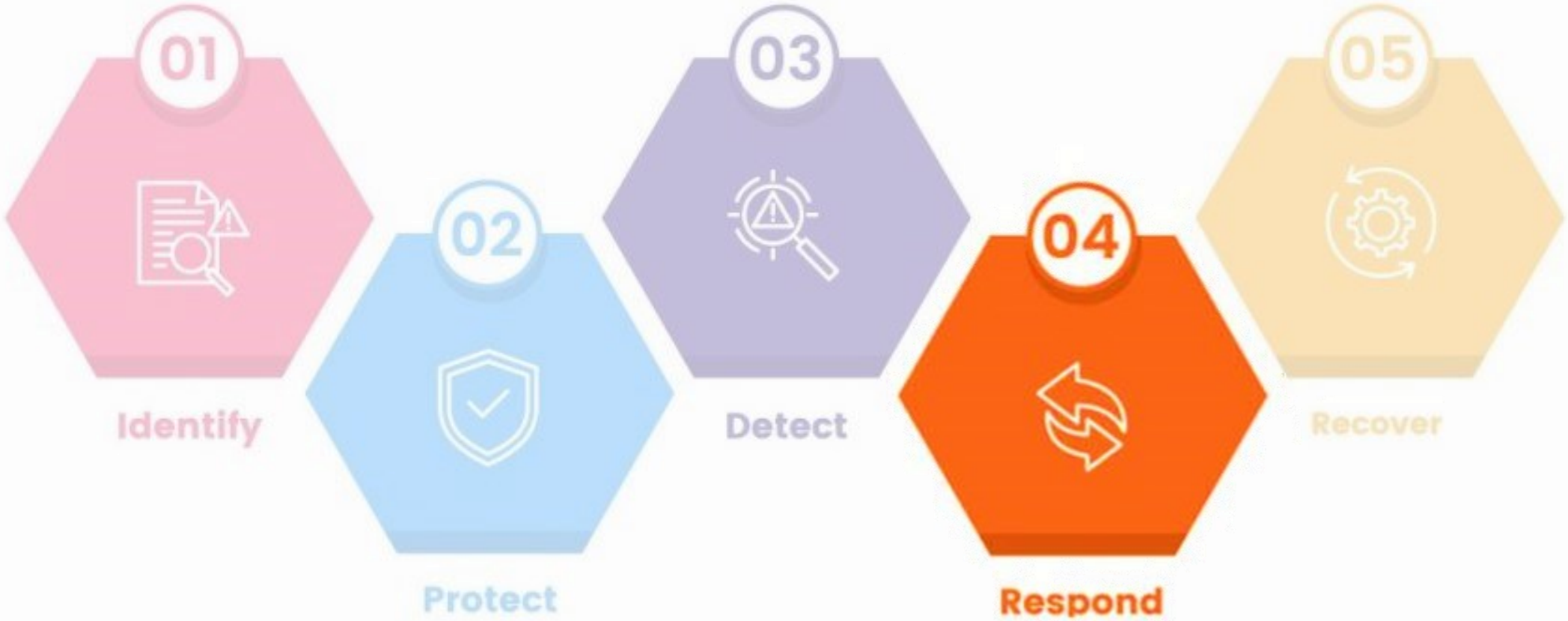
Il monitoraggio rappresenta un fattore abilitante per garantire la sicurezza dei sistemi in ambienti complessi, eterogenei, variabili e indefiniti.

Le informazioni da analizzare sono quantitativamente e qualitativamente ampie, pertanto è necessario automatizzare il processo.

L'intelligenza artificiale può supportare questa attività perché consente di:

- Ridurre il rumore dei dati
- Rilevare anomalie
- Avvisare dei rischi sui dati
- Simulare attacchi

Use case di applicazioni di AI per potenziare la cybersecurity



Responde / Rispondere (RS)

Definizione e attuazione delle attività di intervento quando è rilevato un incidente di sicurezza informatica

Gestione degli incidenti (RS.MA)

Obiettivo:

Gestire le risposte agli incidenti di cybersicurezza rilevati

Attività
Una volta dichiarato un incidente eseguire il piano di risposta agli incidenti in coordinamento con le terze parti interessate
Gestire e convalidare i report sugli incidenti
Classificare gli incidenti
Gli incidenti vengono intensificati o elevati a seconda delle necessità
Applicare i criteri per l'avvio del recupero dagli incidenti

Analisi degli incidenti (RS.AN)

Obiettivo:

Condurre indagini per garantire una risposta efficace e supportare le attività forensi e di recupero

Attività
Eseguire l'analisi per stabilire cosa è accaduto durante un incidente e la causa principale dell'incidente
Registrare le azioni eseguite durante un'indagine e preservare l'integrità e la provenienza delle registrazioni
Raccogliere i dati e i metadati relativi agli incidenti e preservare la loro integrità e provenienza
Stimare e convalidare la magnitudo di un incidente

Spesso gli incidenti violano delle norme penali per cui è necessario acquisire le evidenze e analizzarle per l'identificazione dell'autore del reato (digital forensics)

L'analisi e la condivisione dei risultati è un ottimo sistema di difesa preventiva, perché alimenta la conoscenza dei sistemi di detection

Segnalazione e comunicazione della risposta agli incidenti (RS.CO)

Obiettivo:

Coordinare le attività di risposta con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche

Attività
Informare gli stakeholder interni ed esterni degli incidenti in corso
Condividere le informazioni con gli stakeholder interni ed esterni designati

Valutare se l'organizzazione o il tipo di incidente deve essere comunicato alle autorità competenti

È molto utile redigere un piano di comunicazione per non improvvisare o, peggio ancora, non comunicare

Mitigazione degli incidenti (RS.MI)

Obiettivo:

Svolgere le attività propedeutiche a prevenire l'espansione di un evento e mitigarne gli effetti

Attività
Contenere gli effetti degli incidenti
Eliminare gli effetti degli incidenti

Anche in questo caso è utile avere predisposto dei playbook di supporto alle attività ed effettuare il testing

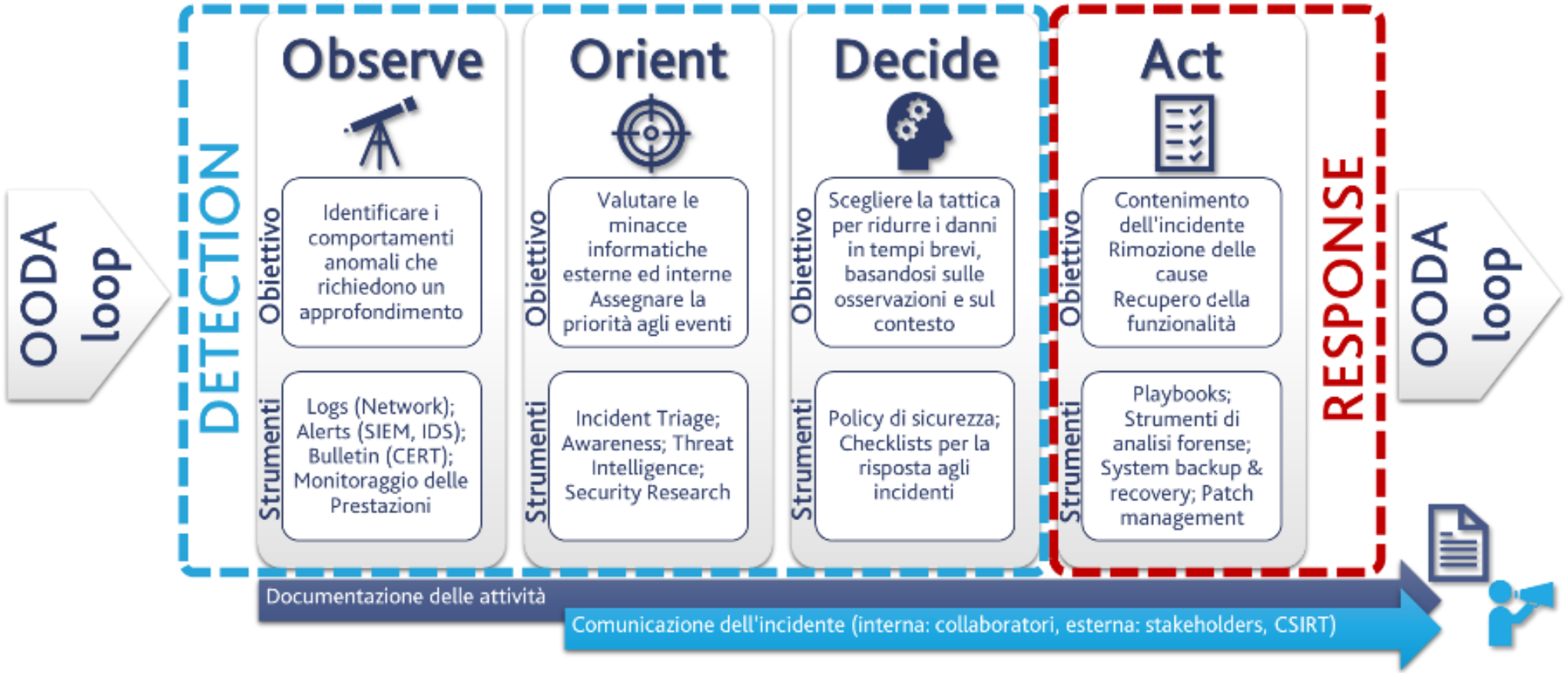
OODA loop applicato all'Incident Response

L'importanza dell'OODA loop nell'Incident Response:

- **Velocità e Agilità**: In un contesto di incidente, il tempo è fondamentale. L'OODA loop enfatizza la necessità di muoversi rapidamente attraverso le fasi per rispondere efficacemente alla minaccia in evoluzione.
- **Adattabilità**: La capacità di osservare i risultati delle proprie azioni e di riorientare la strategia di conseguenza è cruciale per affrontare incidenti complessi e dinamici.
- **Miglioramento Continuo**: Ogni ciclo dell'OODA loop fornisce nuove informazioni e feedback che possono essere utilizzati per migliorare i processi di Incident Response futuri.

In sintesi, l'OODA loop applicato all'Incident Response è un modello concettuale che aiuta i team a strutturare il loro processo decisionale e operativo durante la gestione di un incidente di sicurezza. Permette di affrontare le minacce in modo metodico, adattabile e veloce, massimizzando le possibilità di una risoluzione efficace.

Esempio di Detection & Response



Incident response gestito attraverso OODA loop

Dopo l'azione, il ciclo si ripete. Il team Osserva l'effetto delle proprie azioni: la minaccia è stata contenuta? I sistemi sono tornati online? Ci sono ancora segnali di attività malevola? Questa nuova osservazione porta a una nuova fase di Orientamento, Decisione e Azione, e il ciclo continua fino a quando l'incidente non è completamente risolto e i sistemi sono tornati a uno stato sicuro.

- **Osserva**: Quando si verifica un incidente di sicurezza (un attacco malware, una violazione di dati, un malfunzionamento del sistema), il team di Incident Response inizia a raccogliere tutte le informazioni possibili. Questo include l'analisi dei log di sistema, degli avvisi di sicurezza, del traffico di rete, delle segnalazioni degli utenti, ecc.
- **Orienta**: Il team analizza le informazioni raccolte per capire la natura dell'incidente. Che tipo di attacco è? Quali sistemi sono stati compromessi? Qual è l'impatto potenziale sull'azienda? Quali sono le priorità (contenere la minaccia, ripristinare i servizi, proteggere i dati)? Questa fase richiede competenze tecniche, conoscenza dei sistemi e delle minacce, e capacità di analisi.
- **Decidi**: Sulla base della comprensione dell'incidente, il team decide il piano d'azione. Questo può includere l'isolamento dei sistemi infetti, la rimozione del malware, il ripristino dei backup, la notifica alle parti interessate, ecc. La decisione deve essere presa rapidamente ma anche in modo informato.
- **Agisci**: Il team implementa il piano d'azione. Questo può comportare l'esecuzione di comandi tecnici, la comunicazione con altri team, l'applicazione di patch di sicurezza, ecc.

Triage di un incidente informatico

È un processo cruciale per rispondere in modo efficace ed efficiente a una potenziale minaccia o interruzione. L'obiettivo principale del triage è valutare rapidamente la situazione, comprendere la portata e la gravità dell'incidente, e stabilire le priorità per le azioni di risposta. Ecco i passaggi chiave su come si effettua il triage di un incidente informatico:

1. Ricezione e Identificazione dell'Incidente:

- **Raccolta delle informazioni iniziali**: L'incidente può essere segnalato da diverse fonti: sistemi di monitoraggio (SIEM, IDS/IPS), segnalazioni degli utenti, avvisi di sicurezza, log di sistema, ecc.
- **Identificazione preliminare**: In base alle informazioni iniziali, cerca di ottenere una comprensione di base di cosa è successo. Qual è il tipo di evento? Quando è iniziato? Quali sistemi o utenti sembrano essere coinvolti?

2. Valutazione Iniziale e Raccolta Dati:

- **Verifica dell'incidente**: Determina se l'evento segnalato è effettivamente un incidente di sicurezza o un falso positivo. Analizza i dati iniziali per confermare la validità della segnalazione.
- **Raccolta di dati di base**: Raccogli ulteriori informazioni pertinenti all'incidente.
- **Documentazione:** Inizia a documentare l'incidente, registrando l'ora di ricezione, la fonte della segnalazione, le informazioni iniziali raccolte e le azioni intraprese durante il triage.

3. Analisi e Classificazione:

- **Analisi dei dati**: Esamina attentamente i dati raccolti per comprendere la natura, la causa potenziale e la portata dell'incidente. Cerca pattern, anomalie e indicatori di compromissione (IOC).
- **Determinazione del tipo di incidente**: Classifica l'incidente in base alla sua natura (es. attacco malware, tentativo di intrusione, denial-of-service, violazione di dati, attività interna malevola).
- **Valutazione dell'impatto potenziale**: Stima le possibili conseguenze dell'incidente sull'organizzazione.

4. Prioritizzazione:

Assegnazione della priorità: In base alla gravità dell'impatto potenziale e alla probabilità che l'incidente si espanda o causi ulteriori danni, assegna una priorità all'incidente.

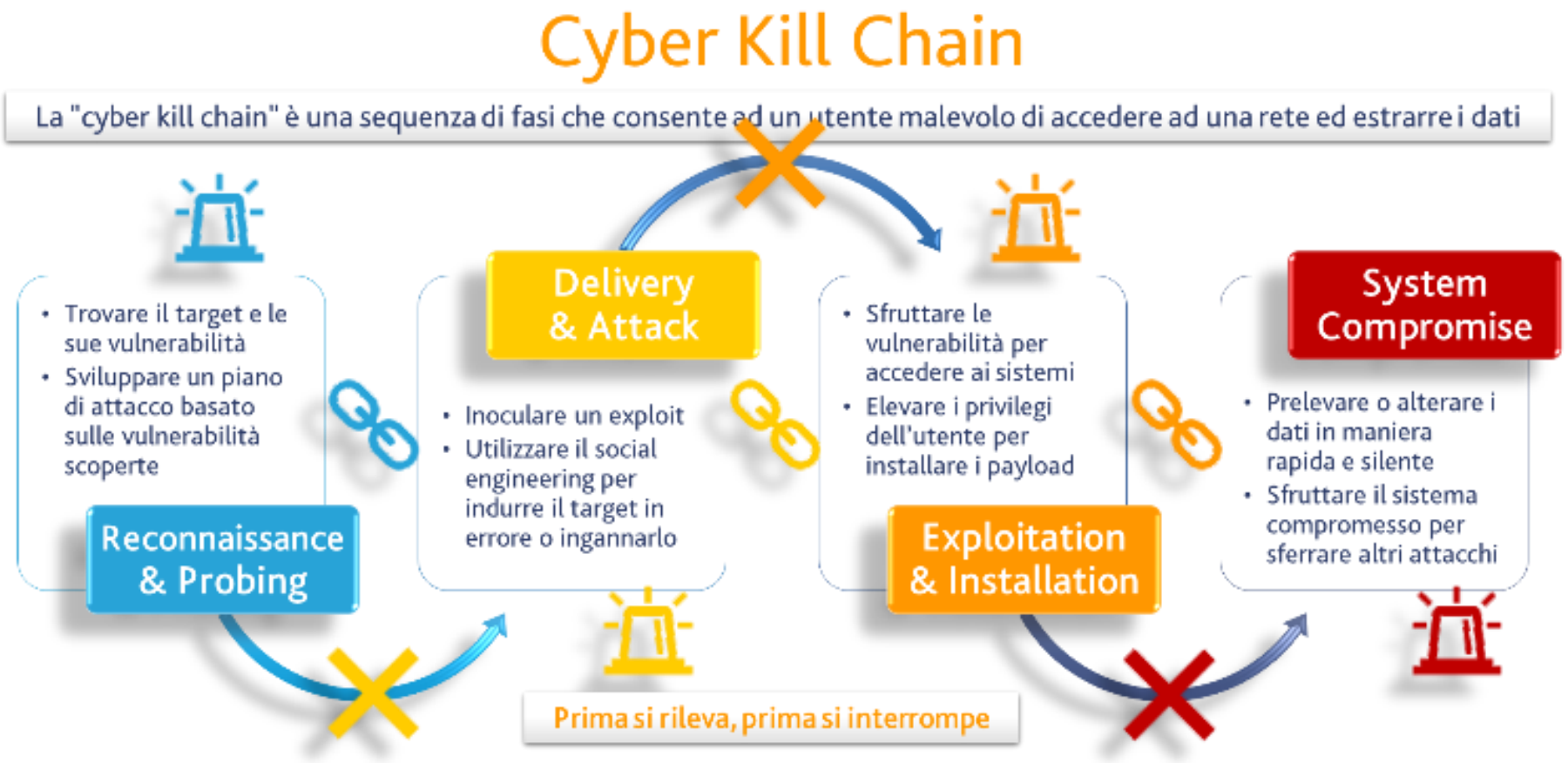
5. Assegnazione e Escalation (se necessario):

- **Assegnazione del responsabile**: Individua il team o la persona responsabile della gestione dell'incidente in base alla sua natura e priorità.
- **Escalation**: Se l'incidente supera le capacità o l'autorità del team di triage, o se la sua gravità aumenta, esegui l'escalation al team o al livello di gestione appropriato.

6. Documentazione Continua:

- **Aggiornamento della documentazione**: Continua a registrare tutte le azioni intraprese, le scoperte fatte durante l'analisi e le decisioni prese durante il processo di triage. Questo è fondamentale per la tracciabilità e per le fasi successive della gestione dell'incidente.

Criticità: Incident Triage



Alcuni esempi di Incident Triage

Evento	Kill Chain Stage	Priorità	Azione Consigliata
Port-scannig activity	Reconnaissance & Probing	Low	Ignorare la maggior parte di questi eventi tranne se l'IP di origine non abbia una cattiva reputazione o ci siano più eventi dallo stesso IP in un breve lasso di tempo
Malware Infection	Delivery & Attack	High	Correggere le eventuali infezioni da malware il più rapidamente possibile prima che progrediscano. Analizzare il resto della rete per individuare eventuali apparati compromessi
Distribuited Denial of Service	Exploitation & Installation	High	Configurare i server Web per la protezione dalle richieste di HTTP e SYN FLOOD. Filtrare le richieste durante un attacco per bloccare gli IP di origine
Distribuited Denial of Service (diversivo)	Exploitation & Installation	High	A volte un DDOS viene utilizzato per distogliere l'attenzione da un altro tentativo di attacco più serio. Aumentare il monitoraggio e indagare su tutte le attività correlate
Unauthorized access	Exploitation & Installation	Medium	Abilitare il monitoraggio sui tentativi di accesso non autorizzati, con priorità su quelli critici e / o contenenti dati sensibili

Alcuni esempi di Incident Triage

Incidente	Kill Chain Stage	Priorità	Azione consigliata
Insider Breach	System Compromise	High	Identificare gli account utente privilegiati per tutti i domini, server, app e dispositivi critici. Assicurarsi che il monitoraggio sia abilitato per tutti i sistemi e per tutti gli eventi di sistema e assicurarsi che stiano alimentando la tua infrastruttura di logs
Unauthorized Privilege Exclalaion	Exploitation and Installation	High	Configurare i sistemi critici per registrare tutti gli eventi di escalation dei privilegi e impostare gli allarmi per i tentativi di escalation dei privilegi non autorizzati
Destructive attack (data, system, etc)	System Compromise	High	Eseguire il backup di tutti i dati e i sistemi critici. Testare, documentare e aggiornare le procedure di ripristino del sistema. Durante una compromissione: acquisire le prove con attenzione e documentare tutte le fasi e tutti i dati probatori raccolti
Advanced Persistent Threat (APT) or Multistage Attack	All Stages	High	Considerare ciascun evento in un contesto più ampio, che includa le informazioni sulle minacce più recenti
False Allarms	All Stages	Low	Configurare la piattaforma di Incident Response per ottenere la giusta quantità di segnale-rumore

Follow up


Indagare sull'incidente in maniera approfondita
Segnalare l'incidente agli stakeholder e alle agenzie governative
Realizzare una revisione del piano di incident response
Condividere e approfondire la lezione appresa

OSSIM
(Open Source Security Information Management)

OSSIM è un sistema SIEM (Security Information and Event Management) open source
Il suo scopo principale è fornire una visione completa della sicurezza IT di un'organizzazione, aggregando e analizzando dati di sicurezza provenienti da diverse fonti
In termini più semplici, OSSIM raccoglie "registri" (log) e avvisi di sicurezza da vari dispositivi e applicazioni all'interno della rete (firewall, intrusion detection systems, server, applicazioni web, ecc.), li normalizza (li rende in un formato comprensibile), li correla (trova connessioni tra eventi apparentemente isolati) e li presenta in un'unica interfaccia per l'analisi e la risposta agli incidenti di sicurezza

AlienVault OSSIM di AT&T

Principali funzionalità:

1. Asset Discover & Inventory
   - Identificazione e Prioritizzazione degli asset
   - Rilevamento di asset non autorizzati
2. Vulnerability Assessment
   - Identificazione delle vulnerabilità degli asset, tramite utilizzo di database sulle vulnerabilità note
   - Valutazione più efficace delle risorse sfruttando una modalità di autenticazione dell'asset (ad esempio tramite SSH)
3. Intrusion Detection
   - Monitoraggio del traffico, dei messaggi di registro di sistema e delle attività dell'utente
   - Un host-based intrusion detection (HIDS) con funzioni aggiuntive di monitoraggio dell'integrità di file e controllo dei file di sistema
   - Un network-based intrusion detection (NIDS) che tramite un monitoraggio passivo della rete in cerca di potenziali attività dannose
4. Behavioral Monitoring
   - Un monitoraggio comportamentale fornisce dei modelli di traffico e dei flussi di dati NetFlow, utilizzati per rilevare anomalie che le semplici statistiche di rete non evidenziano
   - Monitoraggio continuo delle funzionalità e delle attività degli asset
5. SIEM Event Correlation
   - Aggregazione e analisi di log raccolti dalla rete e dagli asset

AlienVault OSSIM di AT&T

I componenti dell'Architettura di suddividono in:

1. SERVER: analizza e correla le informazioni ricevute dai sensori, agent e logger, e fornisce un'interfaccia web gestire la piattaforma
2. SENSORE (1..n): svolge, principalmente, due funzioni:
   - Raccolta e normalizzazione delle informazioni grezze dalla rete
   - Invio dei dati al server

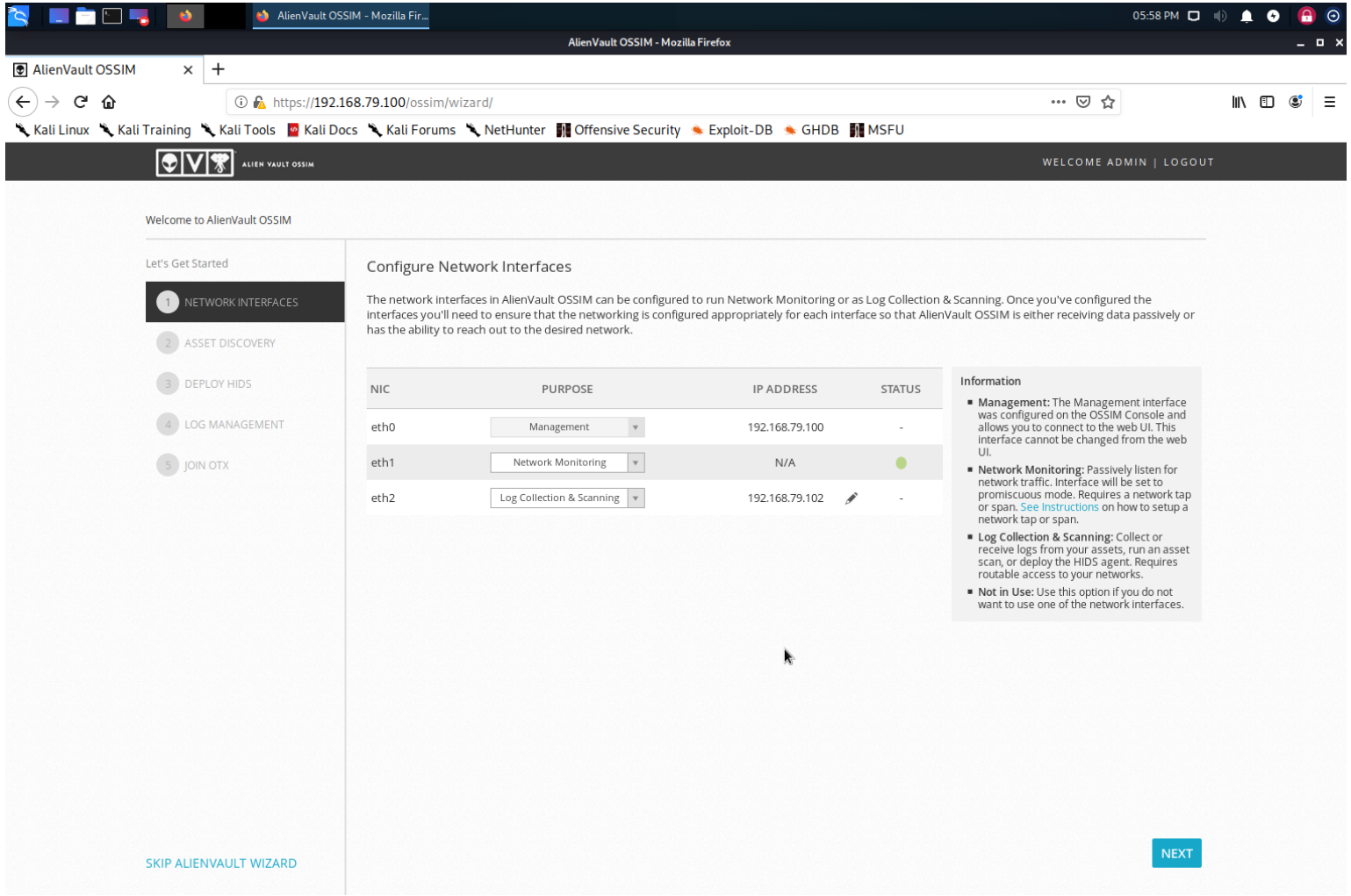
   La raccolta delle informazioni avviene in due modi:
   - Monitoraggio passivo del traffico di rete, attraverso l'uso di un NIDS
   - Monitoraggio delle attività di un host della rete attraverso un agent HIDS
3. AGENT (1..n): la comunicazione tra un sensore e un host della rete avviene tramite un meccanismo client-server, ed in particolare fa uso di un agent installato sugli host.
   Il software integrato con la piattaforma è OSSEC HIDS che esegue:
   - analisi dei log
   - intrusion detection (HIDS)
   - controllo di integrità dei file
   - monitoraggio dei file di sistema
   - rilevamento di rootkit
4. LOGGER (1..n): archivia in modo sicuro i dati di ogni singolo evento, sia per conformità normative sia per successive analisi forensi (è presente nella versione a pagamento)

Esercitazione OSSIM

- Installare OSSIM e gli Agent HDIS su Windows e Linux
- Configurare tre schede di rete
- Provare gli attacchi di Penetration Testing sulle macchine Windows e Linux
- Analizzare i risultati ottenuti su OSSIM
- Implementare le regole di incident response

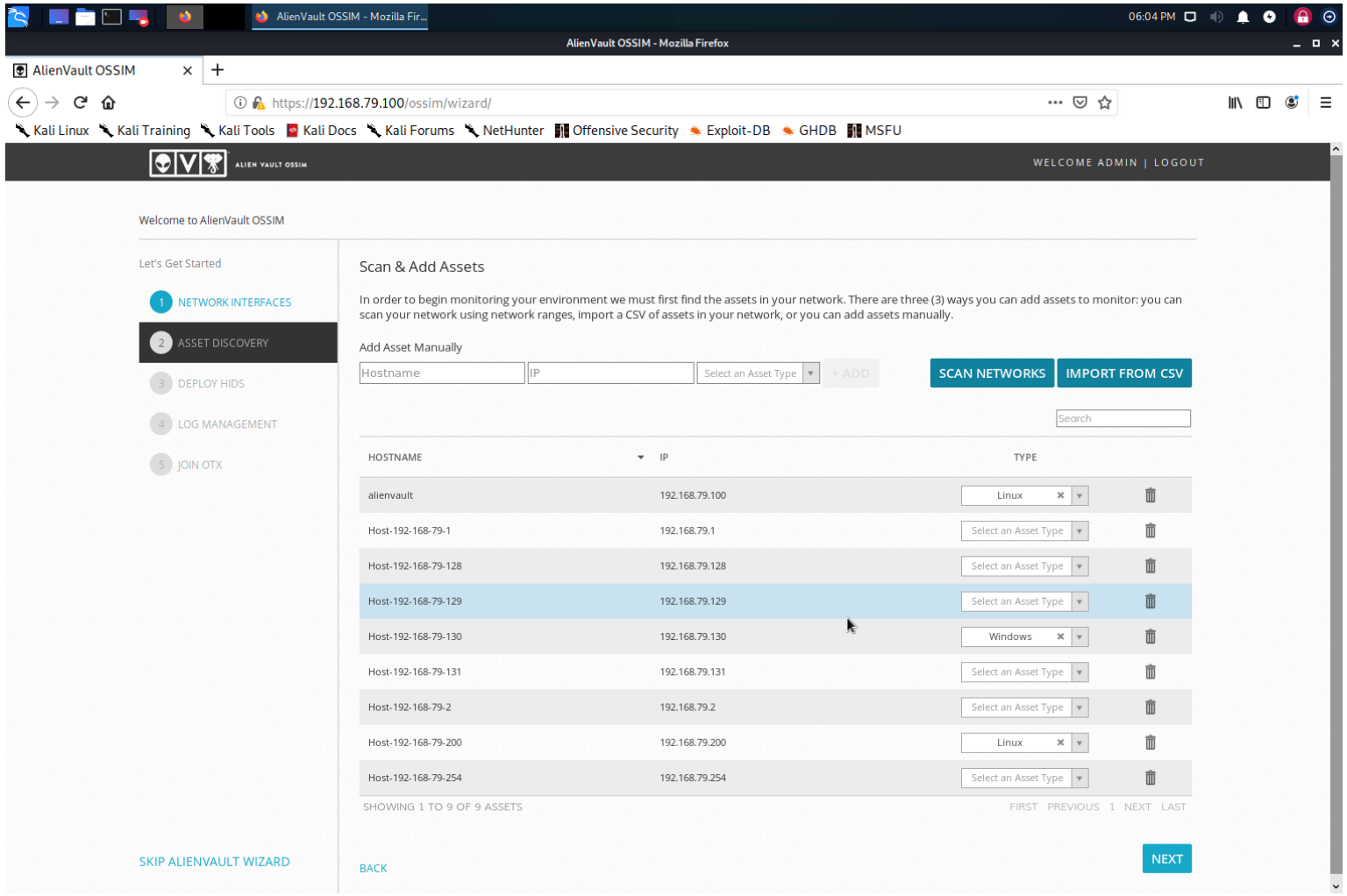
Configurazione delle interfacce

1. Management
2. Network Monitoring
3. Logging collection & scanning



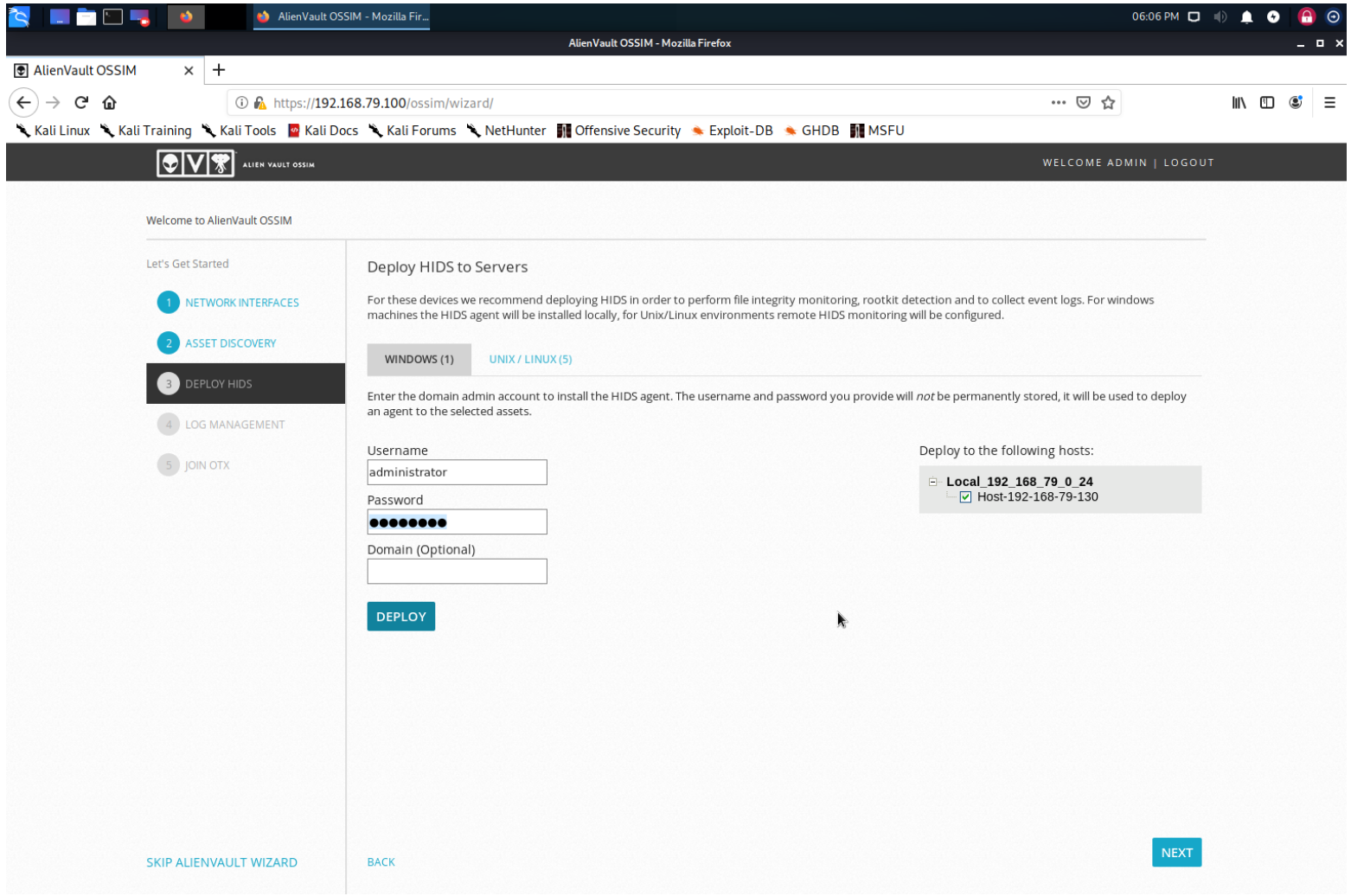
Asset discovery

Scanning network

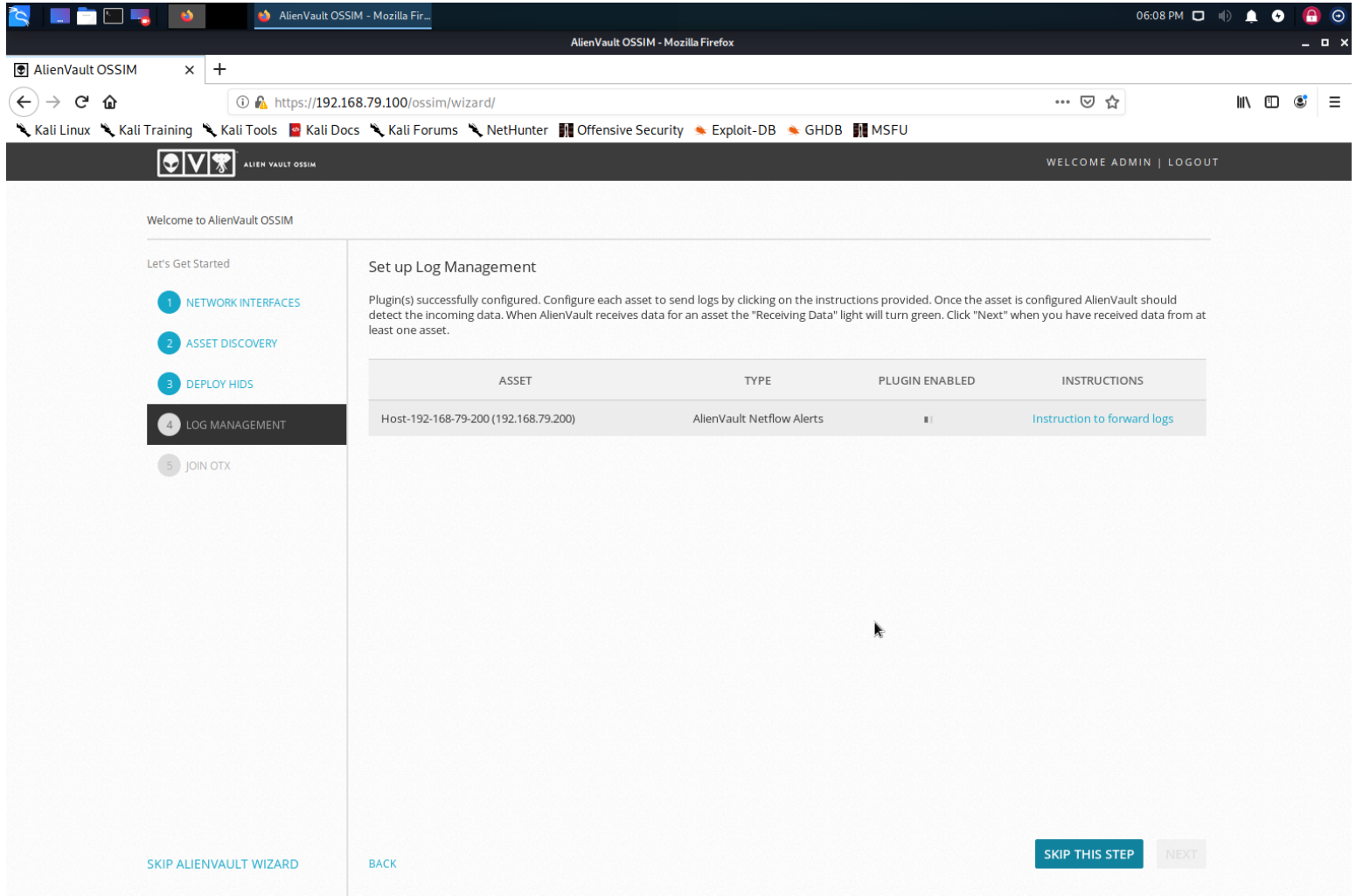


Agent deployment

Installazione dell'agent

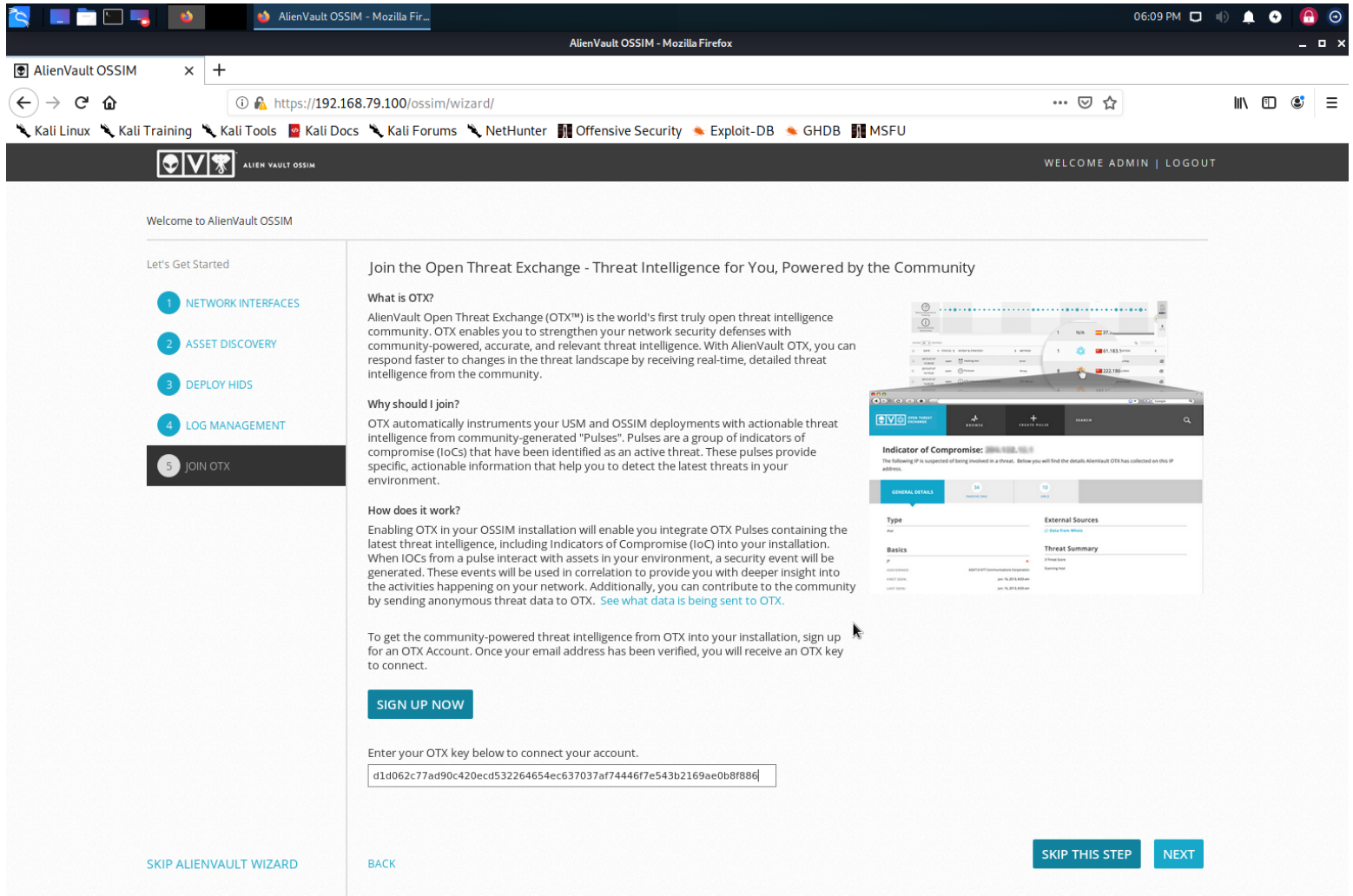


Log management

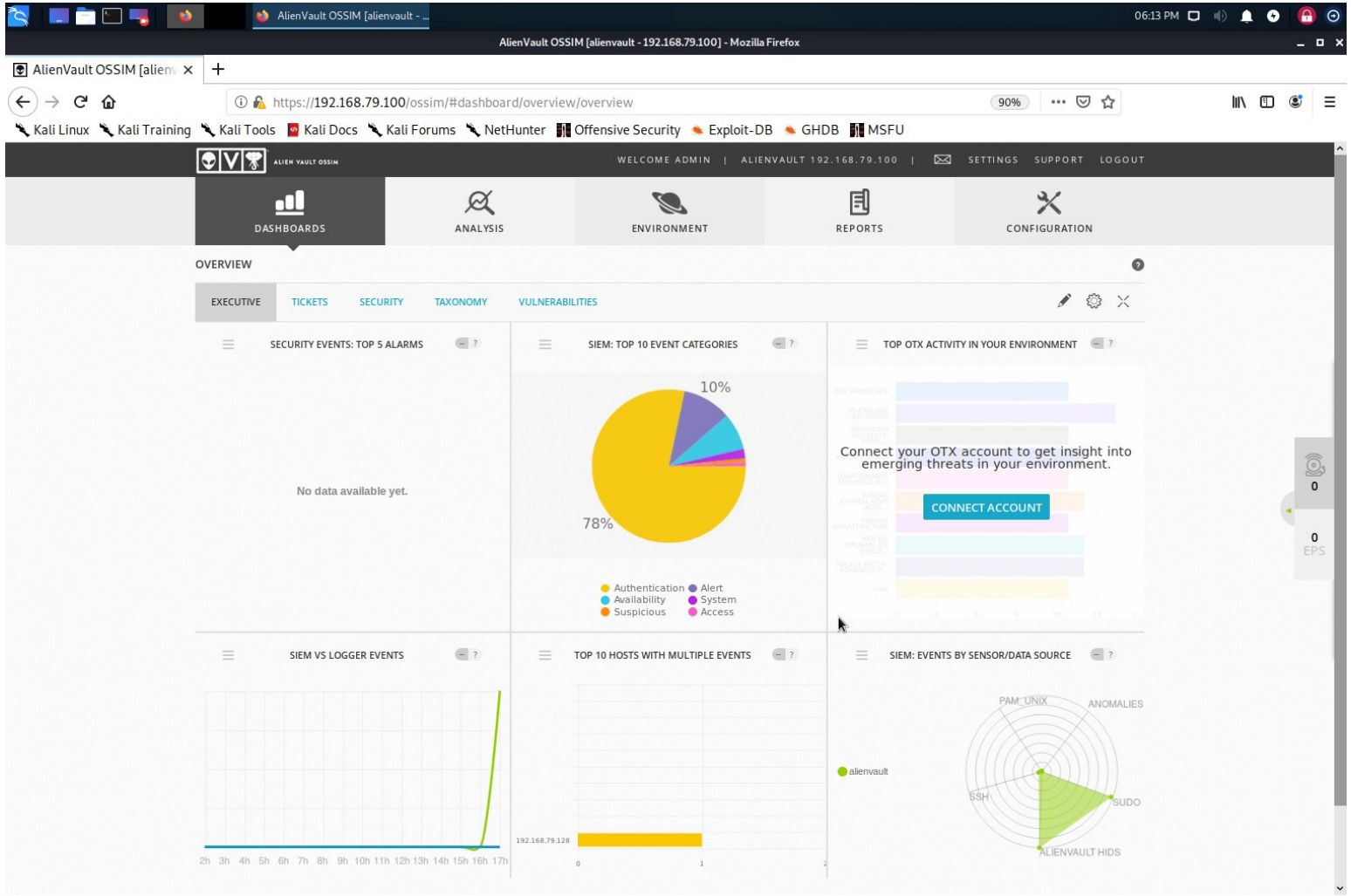


Threat Intelligence

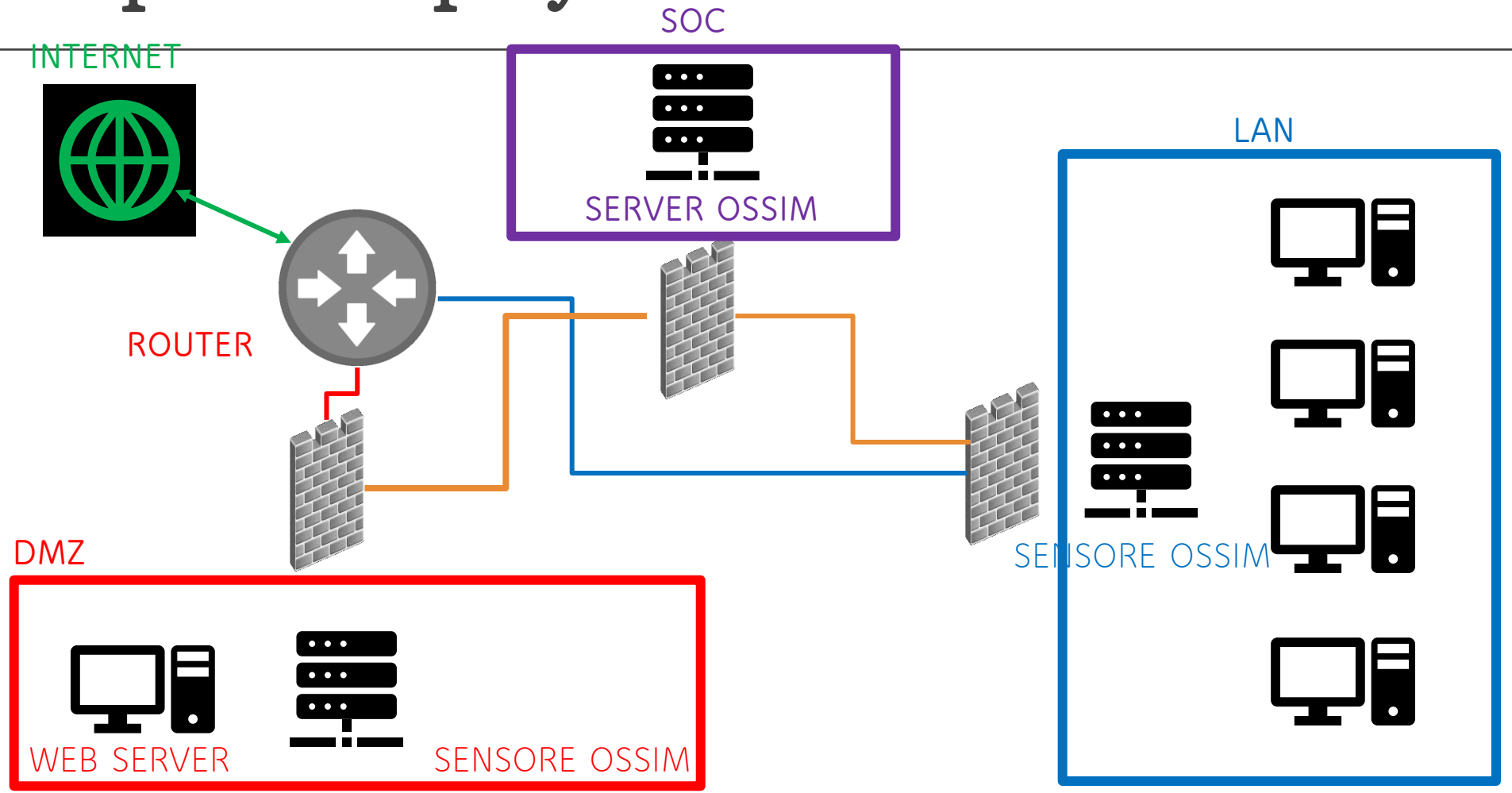
Connessione con OTX



Cruscotto


AlienVault OSSIM [alienvault - 192.168.79.100] - Mozilla Firefox
https://192.168.79.100/ossim/#dashboard/overview/overview
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
WELCOME ADMIN | ALIENVAULT 192.168.79.100 | SETTINGS SUPPORT LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
SECURITY EVENTS: TOP 5 ALARMS
No data available yet.
SIEM: TOP 10 EVENT CATEGORIES
10%
78%
Authentication
Alert
Availability
System
Suspicious
Access
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
Connect your OTX account to get insight into emerging threats in your environment.
CONNECT ACCOUNT
SIEM VS LOGGER EVENTS
TOP 10 HOSTS WITH MULTIPLE EVENTS
SIEM: EVENTS BY SENSOR/DATA SOURCE
PAM_UNIX
ANOMALIES
alienvault
SSH
SUDO
ALIENVAULT HIDS

Esempio di deployment



SOAR

SOAR è un acronimo che sta per Security Orchestration, Automation and Response e si riferisce ad una categoria di tecnologie per la sicurezza che aiutano le organizzazioni a:

- **Orchestrare**: Integrare diversi strumenti e tecnologie di sicurezza in un flusso di lavoro unificato
- **Automatizzare**: Eseguire attività di sicurezza ripetitive e prevedibili senza intervento umano
- **Rispondere**: Gestire e rispondere agli incidenti di sicurezza in modo più efficiente e coerente

In termini più semplici, un sistema SOAR agisce come un "direttore d'orchestra" per i tuoi strumenti di sicurezza. Invece di dover gestire manualmente allarmi e rispondere a minacce utilizzando diverse console e processi, SOAR centralizza queste attività e automatizza le azioni quando possibile, sfruttando il machine learning per apprendere le reazioni più corrette

SOAR

Ecco i componenti chiave di una piattaforma SOAR:

- **Orchestration Engine**: Il cuore del sistema SOAR. Permette di creare flussi di lavoro (spesso chiamati "playbook") che definiscono le sequenze di azioni da intraprendere in risposta a specifici eventi o allarmi di sicurezza. Questi playbook possono coinvolgere diversi strumenti di sicurezza, come firewall, sistemi di rilevamento delle intrusioni (IDS/IPS), soluzioni EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), strumenti di gestione delle vulnerabilità e altro ancora.

- **Automation Engine**: Consente di automatizzare le attività definite nei playbook. Questo può includere l'arricchimento degli allarmi con informazioni contestuali (ad esempio, interrogando database di threat intelligence), l'isolamento di endpoint compromessi, il blocco di indirizzi IP malevoli, l'invio di notifiche e l'apertura di ticket nei sistemi di gestione degli incidenti.

- **Case Management**: Fornisce un sistema per gestire e tracciare gli incidenti di sicurezza dall'inizio alla risoluzione. Permette agli analisti di collaborare, documentare le azioni intraprese e tenere traccia delle metriche di risposta.

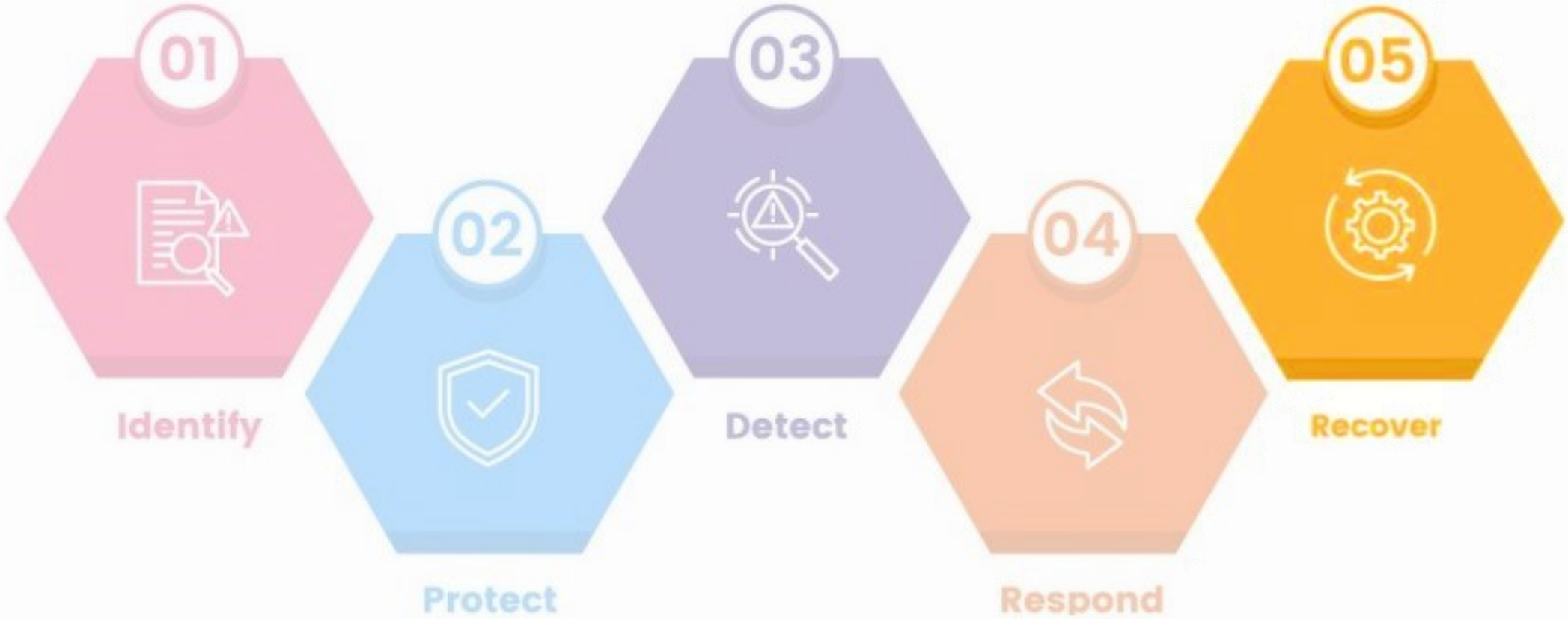
- **Threat Intelligence Platform (TIP) Integration**: Molte piattaforme SOAR si integrano con TIP per automatizzare la raccolta, l'analisi e la distribuzione di informazioni sulle minacce, arricchendo il contesto degli allarmi e migliorando la capacità di rilevamento e risposta.

Riepilogo

La capacità di risposta agli incidenti si basa sulla preparazione anticipata.
Chi si prepara a rilevare e rispondere agli incidenti ha buone probabilità di resistere.

Pertanto, è fondamentale:

- Predisporre un sistema di detection
- Formare il personale
- Preparare i playbook di risposta
- Testare le procedure di detection e response
- Condividere l'esperienza con gli altri attori
- Non dormire sugli allori (il nemico è sempre un passo più avanti)
- Non trascurare l'aspetto della comunicazione (può causare danni peggiori dell'incidente)



Recover / Ripristinare (RC)

Definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente

Esecuzione del piano di ripristino degli incidenti (RC.RP)

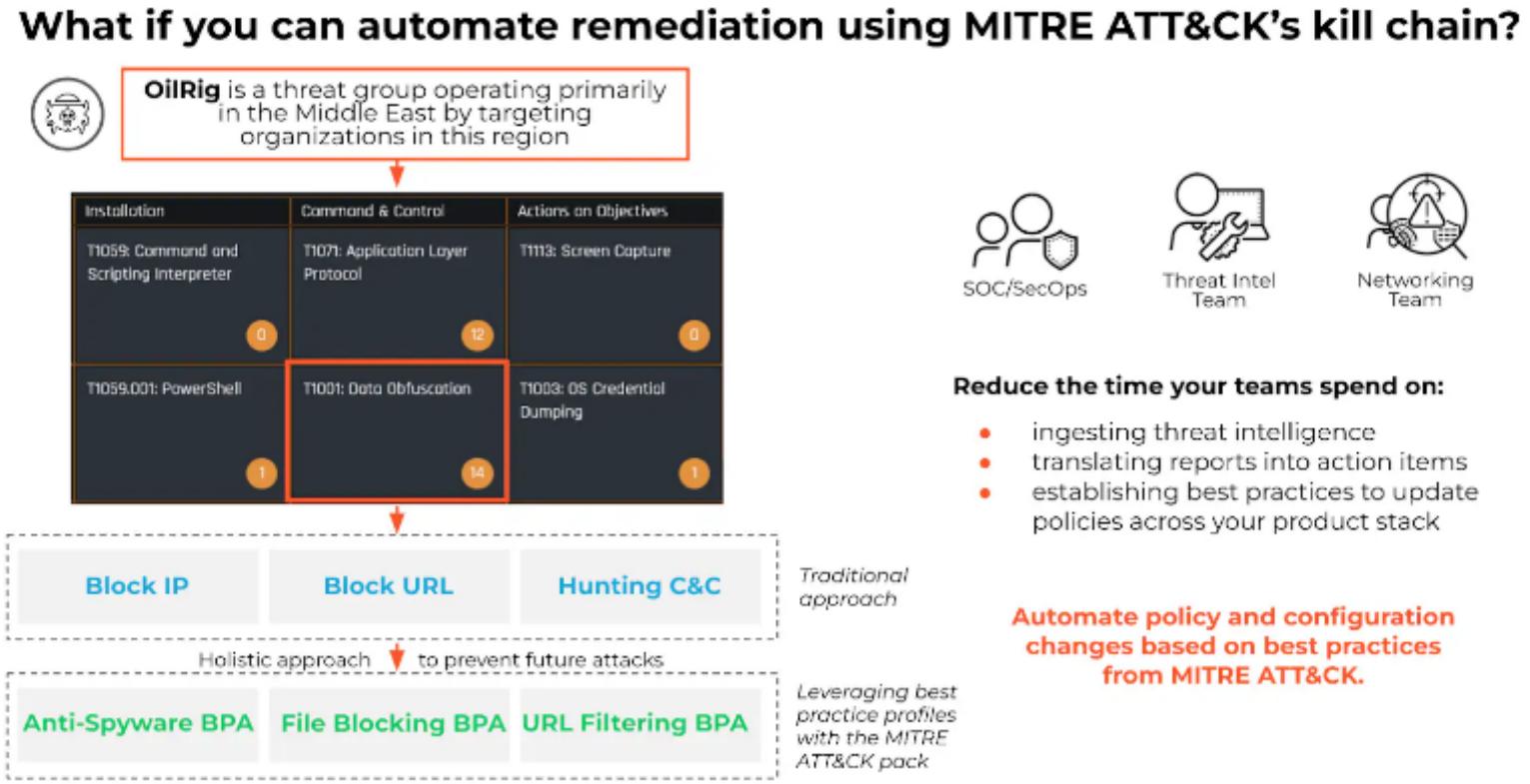
Obiettivo:

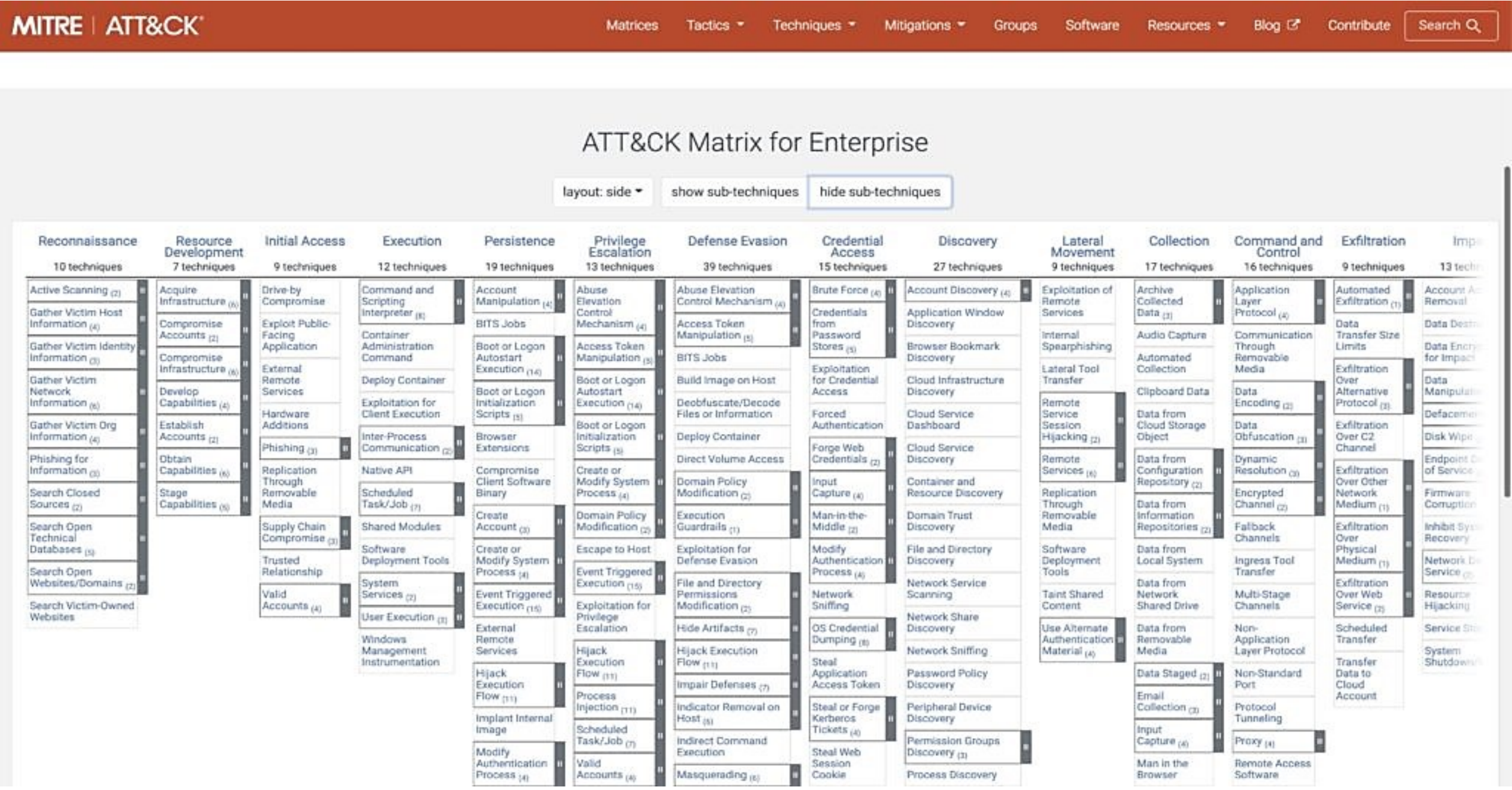
Eseguire le attività di ripristino per garantire la disponibilità operativa dei sistemi e dei servizi colpiti da incidenti di cybersecurity

Attività
Dopo avere avviato il processo di risposta agli incidenti, eseguire la parte di recupero del piano di risposta agli incidenti
Selezionare, definire, valutare ed eseguire le azioni di ripristino
Verificare l'integrità dei backup e delle altre risorse di ripristino prima di utilizzarle per il ripristino
Valutare le funzioni critiche e la gestione del rischio di cybersecurity per stabilire le norme operative post-incidente
Verificare l'integrità degli asset ripristinati, dei sistemi e dei servizi e confermare lo stato operativo
Dichiarare la fine del ripristino dell'incidente e completare la documentazione concernente l'incidente

Esempi di Remediation

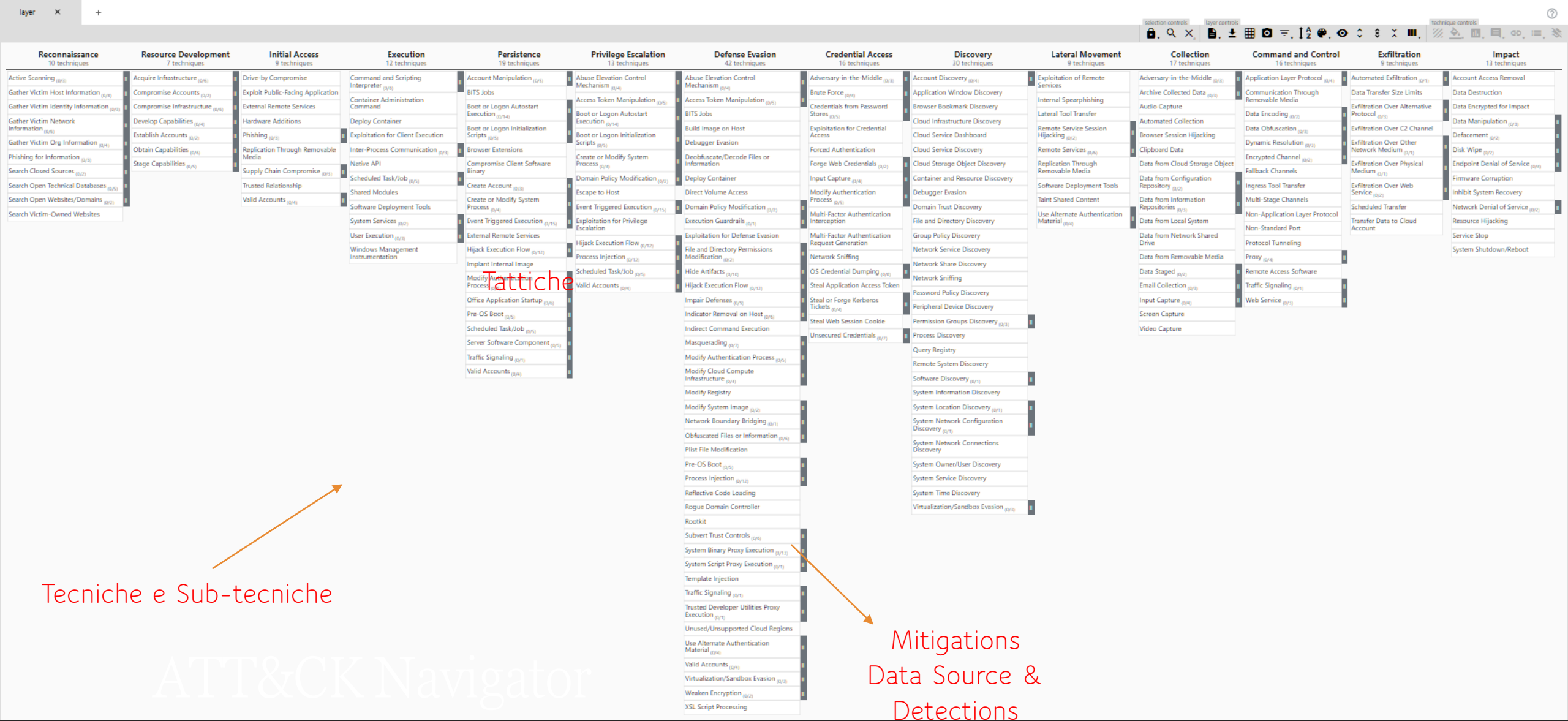
Il Framework MITRE ATT@CK offre un'efficace banca dati di procedure di remediation e può essere utilizzato sia per fare testing, sia come guida in caso di incidente




MITRE | ATT&CK
Matrices
Tactics
Techniques
Mitigations
Groups
Software
Resources
Blog
Contribute
Search
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (2)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
7 techniques
Acquire Infrastructure (6)
Compromise Accounts (2)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Obtain Capabilities (6)
Stage Capabilities (5)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
12 techniques
Command and Scripting Interpreter (8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (7)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Internal Image
Modify Authentication Process (4)
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (7)
Valid Accounts (4)
Defense Evasion
39 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (7)
Hijack Execution Flow (11)
Impair Defenses (7)
Indicator Removal on Host (5)
Indirect Command Execution
Masquerading (6)
Credential Access
15 techniques
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Man-in-the-Middle (2)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Discovery
27 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (3)
Scheduled Transfer
Transfer Data to Cloud Account

ATT&CK Matrices

- MITRE ATT&CK può essere usato come simulatore di scenari di rischio per valutare la risposta dell'organizzazione, ma anche come checklist di cose da fare è cioè in senso proattivo.
- MITRE v.16.1 mette a disposizione 3 matrici:
  - Enterprise (PRE, Windows, macOS, Linux, Cloud, Network, Containers)
  - Mobile (android, ios)
  - ICS (industrial control systems)



ATT&CK Navigator

ATT&CK Tactics

- Una **Tattica** è una descrizione di alto livello del comportamento di un attaccante
- È l'obiettivo intermedio dell'avversario durante un attacco
- Spiega il «*perché*» di ogni azione dell'attaccante
- Ogni tecnologia ha una lista di tattiche
- Ad ogni tattica è assegnato un ID univoco e può prevedere più specifiche tecniche

Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

ATT&CK Technique

- Una **Tecnica** rappresenta una descrizione dettagliata di una determinata Tattica
- Si suddividono in **tecniche** e **sub-tecniche**
- Identificano «***come***» l'avversario effettuerà ogni azione con diversi livelli di dettaglio
- Ogni tecnologia ha una lista di tecniche
- Oltre ad indicare la tecnica o il codice utilizzato, possono altre informazioni quali:
  - Informazioni
  - Azioni per Mitigare l'attacco
  - Azioni per Rilevare l'attacco
  - Reference

ATT&CK Mitigations

- Identificano le configurazione, gli strumenti o i processi che possono «prevenire» una tecnica di attacco
- Suggeriscono le attività cambiare una regola di sicurezza o lo sviluppo di un tool
- Sono raccomandati per prevenire l'esecuzione di specifici attività degli avversari
- Le azioni di mitigation sono mappate per ogni specifica tecnica e sono visualizzate nella stessa pagina

ATT&CK data sources & detections

- Identificano come vengono utilizzati i dati e la detection per ogni specifica tecnica di attacco
- I dati sono le informazioni raccolte dai sensori o dai logs
- I dati sono fondamentali per identificare le attività dell'attacante
- La detection può rappresentare un processo di alto livello, un sensore, i dati e le strategie di detection
- L'interpretazione dei dati aiuta ad identificare la tecnica utilizzata dall'avversario

ATT&CK Groups and Software

- Identificano i gruppi e i tools che hanno utilizzato per prima la tattica di attacco
- Le tecniche di attacco si modificano nel tempo per cui il framework deve essere aggiornato frequentemente ed è in continua evoluzione
- Chiunque può contribuire allo sviluppo o correzione

Esempio di remediation usando il MITRE

Scenario: *Un sistema endpoint all'interno della tua organizzazione è stato infettato da un ransomware. L'EDR (Endpoint Detection and Response) ha rilevato attività sospette e ha generato un allarme.*

FASE 1: RILEVAMENTO (MITRE ATT&CK TACTIC: DETECTION)

- **Tecnica Rilevata:** C1486 - Crittografia dei Dati per Impatto
- **Descrizione:** L'EDR ha identificato un processo sconosciuto che stava scrivendo un gran numero di file con estensioni insolite e modificando i file esistenti in modo anomalo. Sono stati rilevati anche tentativi di eliminare shadow copy di volume (T1490).
- **Allarme EDR:** "Rilevata attività di crittografia anomala sul sistema HOST-01."

Esempio di remediation usando il MITRE

FASE 2: ANALISI E CONTENIMENTO (MITRE ATT&CK TACTICS: ANALYSIS, CONTAINMENT)

- **Analisi**: L'analista della sicurezza esamina l'allarme EDR e i dati contestuali forniti:
  - **Processo Incriminato**: evil_encryptor.exe con un hash sconosciuto.
  - **Percorso del Processo**: C:\Users\utente\AppData\Local\Temp\
  - **Comunicazioni di Rete**: Tentativi di connessione a indirizzi IP esterni sospetti (possibili server C2 - Command and Control, T1071).
  - **Persistenza**: Sono state rilevate chiavi di registro create per l'esecuzione automatica all'avvio (T1547).
  - **Utente Compromesso**: utente con privilegi standard.
- **Contenimento**: L'obiettivo immediato è impedire un'ulteriore diffusione dell'infezione e proteggere altri sistemi:
  - **Isolamento dell'Endpoint (T1039)**: Utilizzando la funzionalità di isolamento della rete fornita dall'EDR, l'endpoint HOST-01 viene immediatamente isolato dalla rete aziendale per impedire la comunicazione con altri sistemi e potenziali server C2.
  - **Terminazione del Processo Malevolo (T1489)**: L'EDR viene utilizzato per terminare forzatamente il processo evil_encryptor.exe in esecuzione sull'endpoint compromesso.
  - **Quarantena dei File Sospetti (T1031)**: I file identificati come crittografati e l'eseguibile malevolo vengono messi in quarantena dall'EDR per impedirne l'ulteriore esecuzione o modifica.

Esempio di remediation usando il MITRE

FASE 3: ERADICAZIONE (MITRE ATT&CK TACTIC: ERADICATION)

- Rimozione della Minaccia:
  - **Analisi Forense Approfondita**: Viene eseguita un'analisi forense più dettagliata sull'endpoint isolato per identificare tutti i file, le chiavi di registro, i servizi e gli altri artefatti creati o modificati dal ransomware.
  - **Rimozione degli Artefatti Malevoli**: Utilizzando gli strumenti di risposta dell'EDR o altri strumenti di rimozione malware, tutti i componenti dannosi identificati vengono eliminati dal sistema, inclusi l'eseguibile del ransomware, le chiavi di registro di persistenza e qualsiasi altro file correlato.
  - **Ripristino (T1485)**: Se disponibili backup affidabili e non compromessi, i file crittografati sull'endpoint vengono ripristinati all'ultima versione pulita.
  - **Rimozione degli Account Compromessi (se applicabile)**: Se l'analisi indica che un account utente è stato compromesso e utilizzato per diffondere l'attacco, l'account viene disabilitato o reimpostato.

Esempio di remediation usando il MITRE

FASE 4: RECOVERY (MITRE ATT&CK TACTIC: RECOVERY)

- Ripristino Operativo:
  - **Verifica dell'Integrità**: Dopo il ripristino, l'endpoint viene accuratamente verificato per assicurarsi che tutti i file siano stati ripristinati correttamente e che non siano rimasti artefatti malevoli.
  - **Ripristino della Connettività**: Una volta verificata la pulizia dell'endpoint, viene gradualmente reintegrato nella rete aziendale, monitorando attentamente eventuali attività sospette.
  - **Monitoraggio Post-Incidente**: Viene implementato un monitoraggio più stretto sull'endpoint ripristinato per un periodo di tempo per rilevare eventuali segni di persistenza o attività residue dell'attaccante.

Esempio di remediation usando il MITRE

FASE 5: LEZIONI APPRESE E MIGLIORAMENTO

- **Analisi Post-Incidente**: Viene condotta un'analisi approfondita dell'incidente per comprendere come l'attacco è penetrato, quali vulnerabilità sono state sfruttate e quali controlli di sicurezza non hanno funzionato come previsto
- **Aggiornamento delle Difese**: In base alle lezioni apprese, vengono apportate modifiche alle policy di sicurezza, alle configurazioni degli strumenti di sicurezza (inclusi gli aggiornamenti delle regole dell'EDR), alla formazione degli utenti e ai processi di gestione delle patch per prevenire incidenti simili in futuro. Ad esempio, potrebbero essere implementate regole EDR più stringenti per rilevare comportamenti simili o bloccare l'esecuzione di file da percorsi temporanei

Comunicazione sul ripristino dell'incidente (RC.CO)

Obiettivo:

Coordinare le attività di ripristino con le parti interne ed esterne

Attività
Comunicare le attività di recupero e i progressi nel ripristino delle capacità operative alle parti interessate interne ed esterne designate
Condividere gli aggiornamenti sul recupero dell'incidente utilizzando metodi e messaggistica approvati

Anche in questo caso risulta utile redigere preliminarmente un piano di comunicazione

Riepilogo

Anche la capacità di ripristino dagli incidenti si basa sulla preparazione.
Chi si prepara in anticipo ha buone probabilità di ripartire velocemente.

Pertanto, è fondamentale:

- Predisporre un sistema di backup sicuro
- Formare il personale
- Preparare i playbook di ripristino
- Testare le procedure di recovery
- Non trascurare l'aspetto della comunicazione (può causare danni peggiori dell'incidente)

Govern / Governare (GV)

Definire e monitorare la strategia di cybersecurity dell'organizzazione

Contesto organizzativo (GV.OC)

Obiettivo:

Comprende tutte le variabili di contesto che possono influire sulle decisioni di gestione dei rischi di cybersecurity

Attività
Conoscere la mission dell'organizzazione e la gestione dei rischi di cybersecurity
Conoscere gli stakeholder interni ed esterni, le loro esigenze e aspettative relative alla gestione dei rischi di cybersecurity
Conoscere e gestire i requisiti legali, normativi e contrattuali relativi alla cybersecurity, compresi gli obblighi in materia di privacy
Conoscere e comunicare gli obiettivi, le capacità e i servizi critici da cui dipendono gli stakeholder esterni o che si aspettano dall'organizzazione
Conoscere e comunicare i risultati, le capacità e i servizi da cui dipende l'organizzazione

Strategia di gestione del rischio (GV.RM)

Obiettivo:

Stabilire, comunicare e utilizzare le priorità, i vincoli, le soglie di tolleranza, la propensione al rischio e le ipotesi in cui l'organizzazione può supportare le decisioni sul rischio operativo

Attività
Gli stakeholder dell'organizzazione stabiliscono e approvano gli obiettivi di gestione del rischio
Stabilire, comunicare e gestire le asserzioni sulla propensione e sulla tolleranza al rischio
Includere le attività e i risultati di gestione del rischio cyber nei processi gestionali di rischio
Stabilire e comunicare la direzione strategica che descrive le opzioni di risposta al rischio
Stabilire i canali di comunicazione all'interno dell'organizzazione per i rischi di cybersecurity, compresi i rischi provenienti da fornitori e altre terze parti
Stabilire e comunicare il metodo per calcolare, documentare, classificare i rischi di cybersecurity
Inserire le opportunità strategiche (cioè i rischi positivi) nelle valutazioni dei rischi cybersecurity

Ruoli, responsabilità e autorità (GV.RR)

Obiettivo:

Stabilire e comunicare i ruoli, le responsabilità e le autorità in materia di cybersecurity per promuovere la responsabilità, la valutazione delle prestazioni e il miglioramento continuo

Attività
La leadership dell'organizzazione è responsabile del rischio di cybersecurity e promuove una cultura consapevole del rischio, etica e in continuo miglioramento
Stabilire, comunicare, comprendere e applicare i ruoli, le responsabilità e le autorità relative alla gestione del rischio di cybersecurity
Assegnare risorse adeguate e commisurate alla strategia di rischio di cybersecurity, ai ruoli, alle responsabilità e alle politiche.
Includere la cybersecurity nella gestione delle risorse umane

Policy (GV.PO)

Obiettivo:

Stabilire, comunicare e applicare la policy di cybersecurity dell'organizzazione

Attività
Stabilire una policy per la gestione dei rischi di cybersecurity in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità
Rivedere, aggiornare, comunicare e applicare la policy di gestione dei rischi di cybersecurity per riflettere i cambiamenti dei requisiti, delle minacce, della tecnologia e della mission organizzativa

Oversight/Supervisione (GV.OV)

Obiettivo:

Utilizzare i risultati delle attività di gestione del rischio di cybersecurity a livello di organizzazione per informare, migliorare e adeguare la strategia di gestione del rischio

Attività
Rivedere i risultati della strategia di gestione del rischio di cybersecurity per informare e adeguare la strategia e la direzione
Rivedere e adattare la strategia di gestione del rischio di cybersecurity per garantire la copertura dei requisiti e dei rischi organizzativi
Valutare e rivedere le performance della gestione del rischio di cybersecurity dell'organizzazione per gli aggiustamenti necessari

Gestione del rischio della catena di fornitura per la sicurezza informatica (GV.SC)

Obiettivo:

Identificare, stabilire, gestire, monitorare e migliorare i processi di gestione del rischio della catena di approvvigionamento informatico degli stakeholder dell'organizzazione

Attività
Stabilire e approvare un programma di gestione del rischio della supply chain per la cybersecurity, la strategia, gli obiettivi, le politiche e i processi
Stabilire, comunicare e coordinare i ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner
Integrare la gestione del rischio della supply chain per la cybersecurity nei processi di gestione, valutazione e miglioramento del rischio della cybersecurity e dell'impresa
Classificare i fornitori per grado di criticità
Stabilire i requisiti per affrontare i rischi di cybersecurity nelle catene di fornitura e integrarli nei contratti e in altri tipi di accordi con i fornitori e le altre terze parti
Eseguire la due diligence per ridurre i rischi prima di iniziare i rapporti formali con i fornitori o con altre terze parti
Conoscere, registrare, classificare, valutare e monitorare i rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti nel corso della relazione
Coinvolgere i fornitori e le altre terze parti nelle attività di pianificazione, risposta e recupero degli incidenti
Integrare le pratiche di sicurezza della supply chain nei programmi di cybersecurity e di gestione del rischio aziendale
Includere disposizioni per le attività che si verificano dopo la conclusione di un accordo di partnership o di servizio nei piani di gestione del rischio della catena di fornitura

CIS Critical Security Controls

I CIS Critical Security Controls (CIS Controls) possono essere utilizzati per verificare le misure di sicurezza applicate e rafforzare la postura di sicurezza informatica dell'organizzazione

https://www.cisecurity.org/

Compliance normativa e regolatoria

Obblighi normativi e compliance regolatoria

Compliance normativa

L'organizzazione deve sottostare a normative riguardanti la sicurezza dei dati e la resilienza dei servizi:

- D.lgs. n. 138/2024
  Codice in materia di protezione dei dati personali
- D.l. n. 105/2019
  Perimetro di Sicurezza Nazionale Cibernetica
- L. n. 90/2024
  Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici
- D.lgs. n. 138/2024
  Recepimento della Direttiva UE 2022/2555 NIS relativa a misure per un livello comune elevato di cibersicurezza
- Regolamenti europei: CS Act, NIS, eIDAS, GDPR, PSD2, AI Act, DORA, CER

Hanno il vantaggio che adottano tutte metodologie risk based

Compliance regolatoria

L’organizzazione deve sottostare a obblighi regolamentari o standard internazionali

Molti di questi standard prevedono sistemi gestionali e sono anch’essi risk based, pertanto, è fortemente consigliato adottare un unico modello gestionale che li integri tutti insieme, in modo tale che le attività sovrapponibili siano eseguite una sola volta e l’aggiornamento risulti facilitato

Framework Nazionale per la Cyber Security e la Data Protection - www.cybersecurityframework.it

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1

Conclusioni

La best practice generale per costruire qualsiasi soluzione di sicurezza deve necessariamente adottare una metodologia risk-based, che parta dall'analisi delle minacce, prosegue con l'analisi dell'esposizione ai rischi e la definizione di un livello di sicurezza adeguato e accettabile per il business aziendale e, infine, si conclude con l'implementazione delle contromisure e il monitoraggio e miglioramento continuo

La sicurezza informatica non è un procedura tecnico-informatica, ma è un processo organizzativo che investe le persone, i flussi informativi, i regolamenti e le norme, e le soluzioni tecnologiche

Inoltre, la sicurezza informatica è anche un opportunità, perché consente all'azienda di sopravvivere in un contesto digitale e tecnologico in continua evoluzione