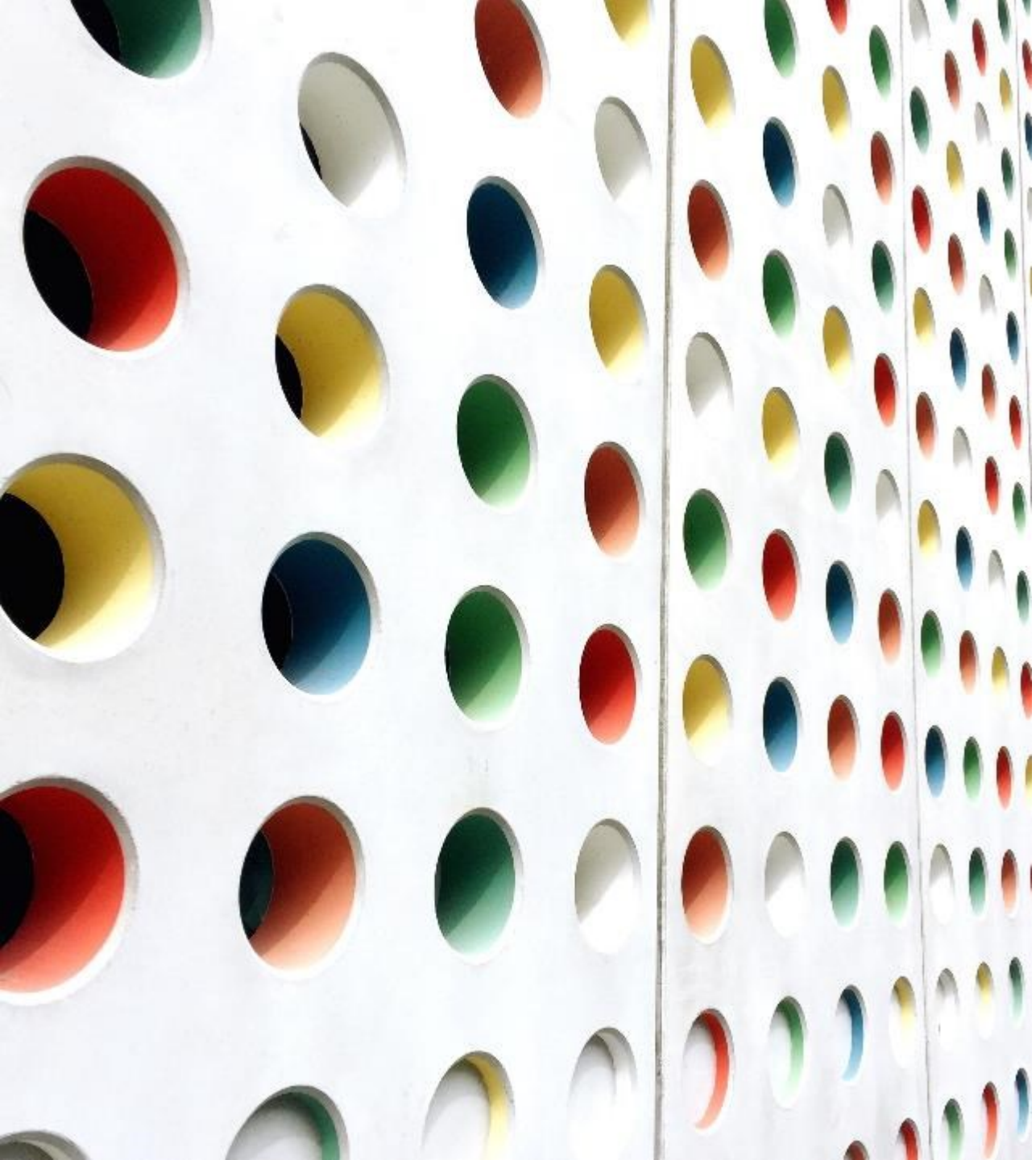


Politecnico di Bari

Best practices per la sicurezza delle reti

VINCENZO CALABRÒ

15 MARZO 2025

Agenda

1. Introduzione ai principali Framework per la Cybersecurity
2. Ciclo di vita della cybersecurity
   - **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
   - **Governare**: definizione e monitoraggio continuo della strategia
3. Best practices per la sicurezza delle reti
4. Compliance normativa e regolatoria

Premesse

- La maggior parte delle attività economiche, produttive e sociali vengono svolte attraverso l'uso delle tecnologie dell'informazione e della comunicazione
  - Alcune rivestono carattere di riservatezza e/o segretezza
  - Altre sono determinanti per il benessere delle persone o il progresso delle organizzazioni
- Nasce la necessità di proteggere le persone e le organizzazioni, attraverso la difesa delle loro rappresentazioni digitali in termini di dati, asset, proprietà, processi, prodotti, servizi, ecc.
- Corollario 1: la sicurezza completa non è raggiungibile
- Corollario 2: la sicurezza è un processo iterativo-evolutivo

Contesto

	In passato	Attuale
Utenti e Dispositivi	Noti e Omogenei	Non noti ed Eterogenei
Sistemi informativi	On-premise o Silos	Cloud o Distribuiti
Perimetro delle reti	Delimitato	Illimitato
Processi	Codificati e Stabili	Iterativi e Flessibili
Minacce	Notevoli e Persistenti	Evolute e Sofisticate
Sicurezza	Perimetrale	Adattiva

ON-PREMISE

CLOUD

La sicurezza completa non è raggiungibile

Fattori come il perimetro indefinito, l'aumento della superfice di attacco, la sofisticazione delle minacce **non consentono di individuare e applicare** misure di contenimento delle minacce definitive e stabili.

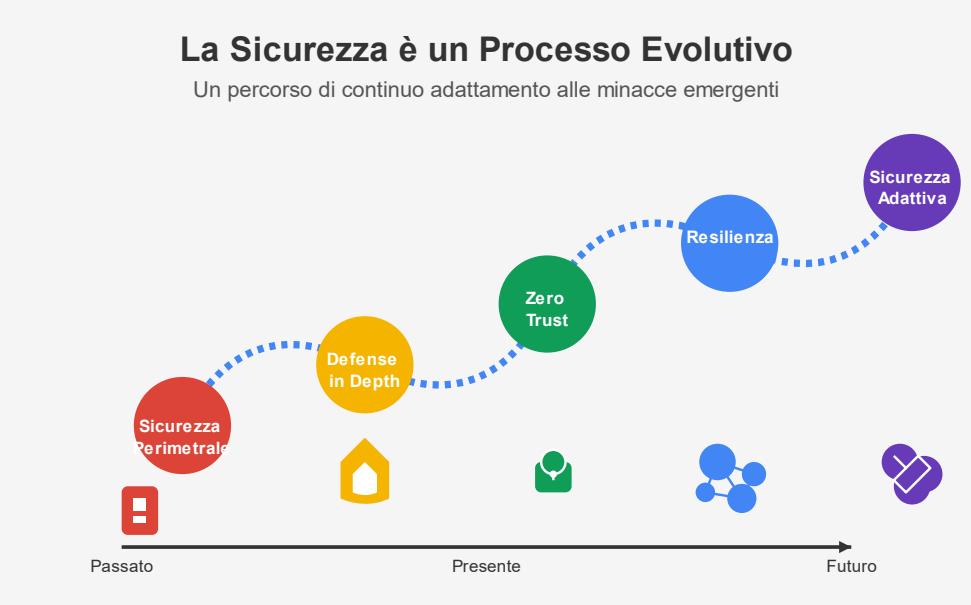
Inoltre, i costi di implementazione e gestione per una sicurezza generalizzata potrebbe risultare economicamente **svantaggiosi**.

Occorre, pertanto, adottare un nuovo paradigma: **la sicurezza risk based.**

La sicurezza è un processo iterativo-evolutivo

Il contesto ambientale, le organizzazioni, i processi, gli stakeholders, le variabili tecniche e economiche e le minacce rendono i **fattori di rischio mutevoli**.

Un approccio risk-based, pertanto, deve periodicamente rimodulare le proprie strategie e azioni per non diminuire la capacità di resilienza, ovvero l'abilità di continuare a operare efficacemente e a fornire i propri servizi nonostante gli eventi avversi come attacchi informatici, guasti tecnici o disastri naturali.



I principali framework per la gestione del rischio cyber

NIST Cybersecurity Framework	Il framework più utilizzato e completo. È strutturato in cinque funzioni core: Identificare, Proteggere, Rilevare, Rispondere e Recuperare
ISO/IEC 27001	Standard che specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni (ISMS)
ISO/IEC 27005	Standard specifico per la gestione del rischio della sicurezza delle informazioni, fornisce linee guida dettagliate per il processo di valutazione e trattamento dei rischi
FAIR: Factor Analysis of Information Risk	Framework con un approccio quantitativo all'analisi del rischio cyber, aiuta le organizzazioni a monetizzare, gestire e comunicare i rischi in termini finanziari
CIS Controls	Set di best practice per la protezione contro le minacce informatiche più comuni, organizzato in 18 controlli di sicurezza
COBIT: Control Objectives for Information and Related Technologies	Framework per la governance e la gestione dell'IT che include componenti specifiche per la gestione del rischio cyber
ISF Standard of Good Practice	Standard che fornisce una serie completa di pratiche di sicurezza per gestire tutti gli aspetti della sicurezza delle informazioni
MITRE ATT&CK	Framework che cataloga tattiche, tecniche e procedure (TTP) utilizzate dagli attaccanti, utile per identificare i rischi basati su scenari reali
ENISA Risk Management Framework	Framework Europeo, basato sulla ISO/IEC 27005:2018, offre linee guida specifiche per organizzazioni europee e conforme a: CS Act, NIS, eIDAS, GDPR, PSD2, AI Act
Framework Nazionale per la Cyber Security e la Data Protection	Framework Italiano, basato sul NIST Cybersecurity framework, integra controlli per la privacy

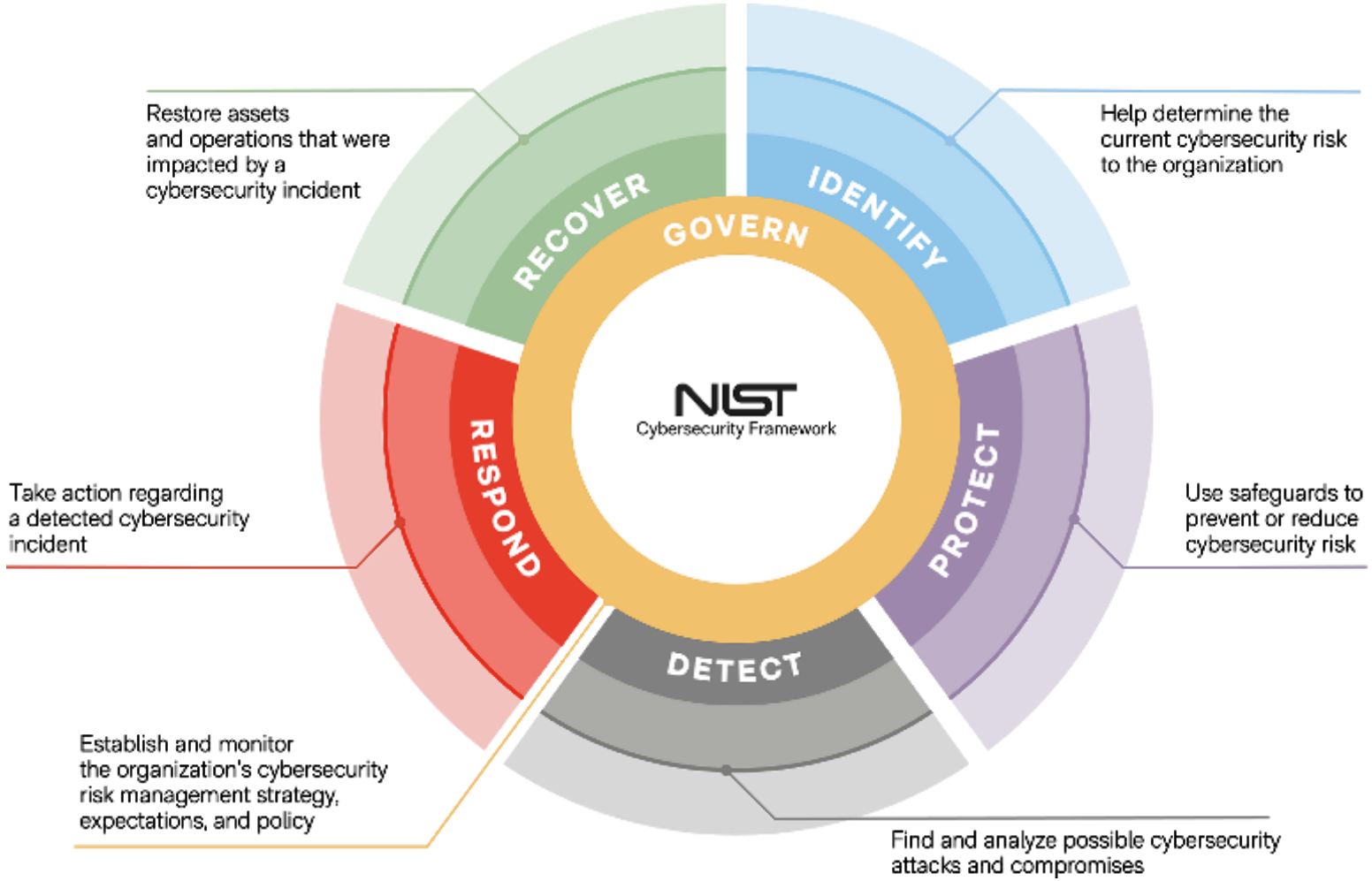
NIST Cybersecurity Framework

L'obiettivo è fornire alle organizzazioni uno strumento di supporto al processo di gestione e trattamento del rischio cyber.

Le Funzioni core:

1. Identify (Identificare)
2. Protect (Proteggere)
3. Detect (Rilevare)
4. Respond (Rispondere)
5. Recover (Recuperare)

Il framework prevede una sesta sezione dedicata alla Governance (Governo), per la gestione del framework (iterativo) e il miglioramento continuo (evolutivo).



CIS Critical Security Controls

I CIS Critical Security Controls (CIS Controls) è una check-list di best practice raggruppate in **18 categorie** che può essere utilizzato per:

1. Implementare le misure di sicurezza
2. Verificare le misure di sicurezza applicate e rafforzare la postura di sicurezza informatica dell'organizzazione

https://www.cisecurity.org/

Esempio di CIS Control – Gruppo 1

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3
1				Inventory and Control of Enterprise Assets	Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.			
1	1,1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x
1	1,2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	x	x	x
1	1,3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		x	x
1	1,4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		x	x
1	1,5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			x

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.

Risk management: livelli di implementazione

Livello 1 Parziale

Non tiene conto in modo sistematico del rischio cyber o delle minacce ambientali.
Il rischio è gestito con processi ad hoc e spesso in modo reattivo.
Il livello di consapevolezza del rischio a livello organizzativo è limitato.
Non esistono processi di condivisione delle informazioni con entità esterne.

Livello 2 Informato

L'organizzazione ha processi interni che tengono conto del rischio cyber, ma non sono estesi a tutta l'organizzazione.
Il livello di consapevolezza del rischio cyber è sufficientemente esteso, ma non è accompagnato da processi di gestione pervasivi che coinvolgano tutti i livelli dell'organizzazione.
L'organizzazione comprende il suo ruolo nell'ecosistema di riferimento, ma lo scambio informativo relativo agli eventi di cybersecurity è limitato e passivo.

Livello 3 Ripetibile

Il rischio è formalmente definito ed approvato e l'organizzazione aggiorna regolarmente le proprie pratiche di cybersecurity basandosi sull'output del processo di risk management.
La gestione del rischio cyber è pervasiva a tutti i livelli organizzativi e il personale è formato per gestire i ruoli che gli vengono assegnati.
L'organizzazione scambia regolarmente informazione inerenti alla cybersecurity con altri attori operanti nello stesso ecosistema

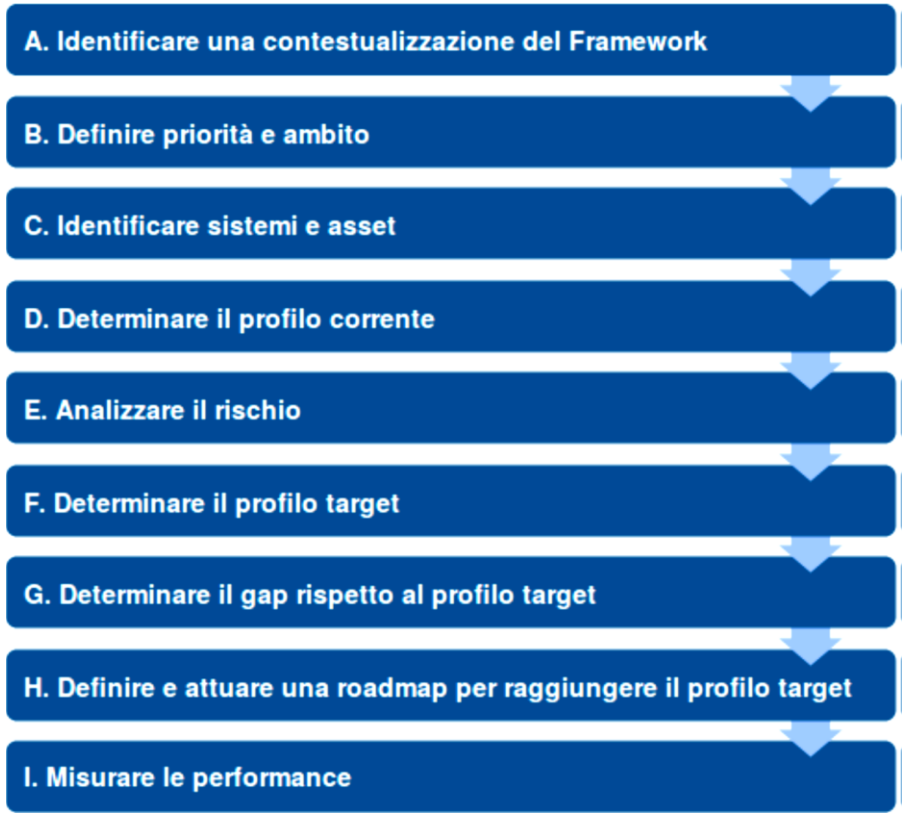
Livello 4 Adattivo

L'organizzazione adatta le sue procedure di cybersecurity regolarmente attraverso l'utilizzo delle esperienze passate e degli indicatori di rischio.
Attraverso un processo adattivo l'organizzazione si adegua in modo continuo a minacce in continua evoluzione ed è capace di rispondere efficacemente ad attacchi sofisticati.
Lo scambio informativo con altri attori operanti nello stesso ecosistema è continuo ed avviene in tempo reale.

Applicazione del Framework

L'obiettivo principale è fornire uno strumento di supporto del processo di gestione e trattamento del rischio cyber al fine di:

- Migliorare o definire un programma di cybersecurity in maniera strutturata e integrata
- Determinare il profilo di cyber maturità corrente e target
- Agevolare la comunicazione con il top management



https://www.nist.gov/cyberframework/profiles

Obblighi normativi

+

Misure tecniche e organizzative per ridurre il rischio

→

Sicurezza Informatica e Protezione dei Dati

- Confidenzialità
- Integrità
- Disponibilità
- Resilienza

→

Security is a process, not a product → Continuous Improvement Process

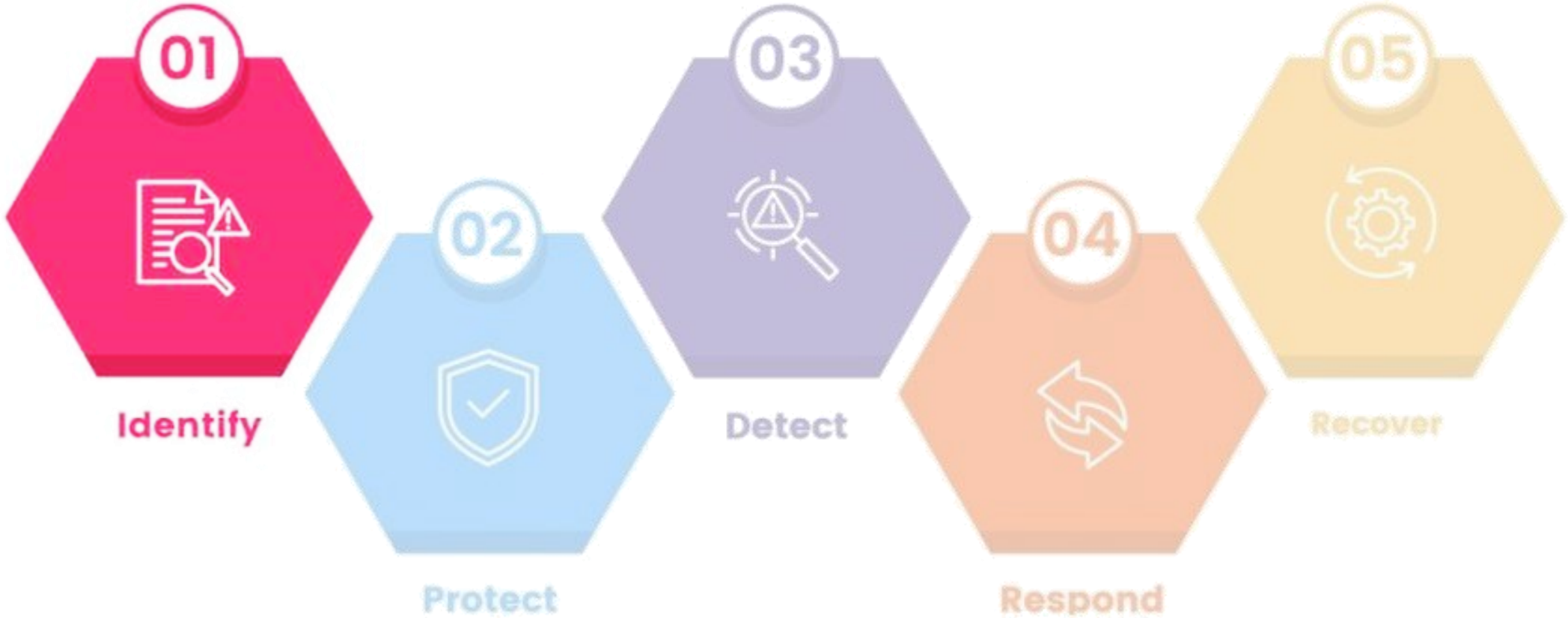
Riepilogo

Le best pratices in materia di cybersecurity **non riguardano più solo le tecnologie di protezione**, ma **sono incentrati sulla gestione di tutte le variabili connesse alla sicurezza degli asset digitali** (dati, persone, sistemi, device, funzioni, procedure, regolamenti, normative, luoghi fisici).

Perché:

- gli asset non hanno tutti lo stesso livello di criticità
- le minacce e i threat actor sono in continua evoluzione
- i perimetri aziendali e la superfice di attacco sono indistinti
- le risorse economiche utili a contrastarle sono limitate

Si predilige l'approccio **risk based** perché consente di determinare gli asset, assegnare le priorità, individuare le vulnerabilità e le azioni di contrasto e, infine, prevede un **miglioramento continuo**.



Identify / Identificare (ID)

Comprensione del contesto, degli asset che supportano i processi critici di business e dei rischi associati

Asset Management (ID.AM)

Obiettivo:

Identificare i dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione

Attività
Censire i sistemi e gli apparati hardware in uso
Censire le piattaforme, i servizi e le applicazioni software in uso
Identificare i flussi di dati e le comunicazioni utilizzati
Catalogare i sistemi informativi o i servizi forniti dai fornitori
Prioritizzare le risorse (hardware, dispositivi, dati, allocazione temporale, personale e software) in base alla classificazione (confidenzialità, integrità, disponibilità), criticità, impatto e valore per il business
Catalogare i dati e i metadati corrispondenti ai tipi di dati designati
Gestire i sistemi, l'hardware, i software, i servizi e i dati durante il ciclo di vita
Definire e rendere noti i ruoli e le responsabilità per la cybersecurity a tutto il personale e alle eventuali terze parti rilevanti (fornitori, clienti, partner)

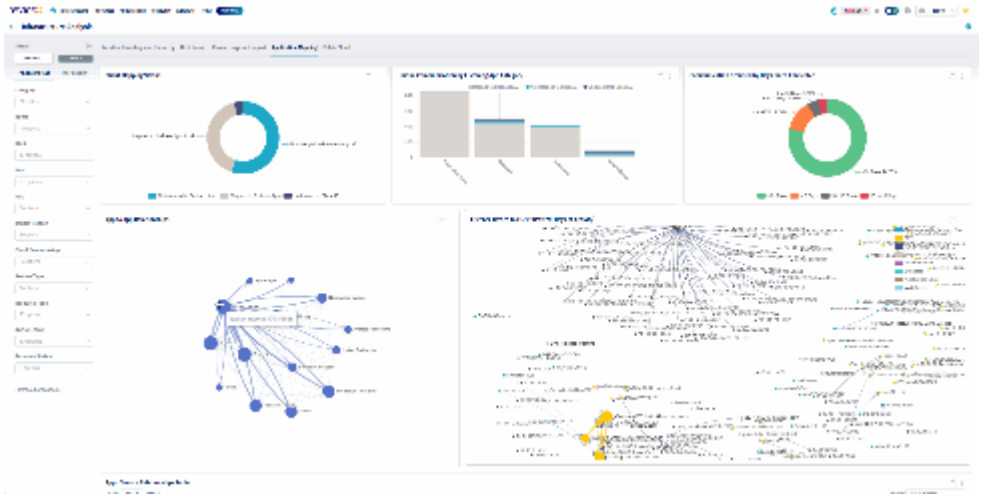
Tool di Asset Management

E' fondamentale indicare:

- **Tipologia** (IT, OT, Servizio, Componente)
- **Scopo/Finalità**
- **Fornitore** (Interno, Esterno, Ibrido)
- **Classifica** (Critical, High, Medium, Low)

Esempi:

- Asset Management System Microsoft
- Spiceworks
- Device4 2



L'identificazione e la classificazione degli asset
è un attività utile anche in altri processi
(privacy, business continuity, risk management)

Risk Assessment (ID.RA)

Obiettivo:

Comprendere il grado di rischio di cybersecurity per l'organizzazione, gli asset e le persone

Attività
Identificare, convalidare e registrare le vulnerabilità degli asset
Ricevere le informazioni sulle minacce da fonti esterne
Identificare e registrare le minacce interne ed esterne all'organizzazione
Identificare e registrare gli impatti potenziali e le probabilità con cui le minacce potrebbero sfruttare le vulnerabilità
Utilizzare le minacce, le vulnerabilità, le probabilità e gli impatti per comprendere il rischio intrinseco e la prioritizzazione della risposta al rischi
Selezionare, prioritizzare, pianificare, monitorare e comunicare le risposte ai rischi
Gestire, valutare per l'impatto sul rischio, registrare e tracciare le modifiche e le eccezioni
Stabilire i processi per la ricezione, l'analisi e la risposta alle segnalazioni di vulnerabilità
Valutare l'autenticità e l'integrità di hardware e software prima dell'acquisizione e dell'uso
Valutare i fornitori critici prima dell'acquisizione dei loro prodotti o servizi

Macro-modello di calcolo del rischio

Il rischio cyber è definito come una funzione che combina diverse componenti: **Rischio = f(Minaccia, Vulnerabilità, Probabilità, Impatto)**

- **Minaccia**: Un potenziale evento avverso causato da un attore malintenzionato, un errore umano o un evento naturale. Le minacce vengono caratterizzate in base alla loro fonte, capacità, intento e obiettivi.
- **Vulnerabilità**: Debolezza in un sistema, applicazione o controllo che potrebbe essere sfruttata da una minaccia. Le vulnerabilità sono valutate in base alla loro gravità e facilità di sfruttamento.
- **Probabilità**: La possibilità che una minaccia riesca a sfruttare una vulnerabilità. La valutazione tiene conto di quanto sia motivato l'attore della minaccia e delle sue capacità, dell'efficacia dei controlli di sicurezza esistenti e della presenza di fattori predisponenti
- **Impatto**: Le conseguenze negative che deriverebbero se una minaccia sfruttasse con successo una vulnerabilità, valutate in termini di: danno alla confidenzialità, integrità e disponibilità dei dati, conseguenze finanziarie, danno reputazionale, impatti operativi e sulla missione dell'organizzazione

Si raccomanda un processo di valutazione del rischio strutturato in quattro fasi:

1. Preparazione della valutazione
2. Conduzione della valutazione
3. Comunicazione dei risultati
4. Mantenimento della valutazione

Questo approccio permette alle organizzazioni di identificare, prioritizzare e affrontare i rischi cyber in modo sistematico e coerente.

Esempio di calcolo del rischio

1. Identificare e classificare gli asset
2. Identificare le minacce
3. Identificare le vulnerabilità
   (cosa potrebbe accadere):
   - Interruzione del sistema o dell'applicazione
   - Perdita di dati
   - Conseguenze legali
   - Sanzioni per la conformità
   - Danni alla reputazione aziendale e alla fuga dei clienti
   - Danni fisici a dispositivi e proprietà
4. Stimare la probabilità di accadimento
5. Calcolare l'indice d'impatto
   (quanto incide la vulnerabilità)

MALEVOLI:

- Accesso non autorizzato da parte di attori esterni a causa di malware, negligenza dei dipendenti, ransomware, phishing, ecc.
- Attacchi insider causati da insider privilegiati, insider negligenti, venditori terzi, spionaggio aziendale, Stati nazionali
- Perdite di dati causate dalla divulgazione di Personally Identifiable Information (PII), dati sensibili o da problemi di configurazione errata
- Perdita di dati a causa di una replica o di un backup inadeguati
- Perdita di fatturato e di reputazione dovuta a tempi di inattività che causano l'interruzione del servizio

NON MALEVOLI:

- Disastri naturali come inondazioni, terremoti, incendi e altri disastri che possono distruggere hardware e software
- Guasti all'hardware o al sistema che possono causare la perdita o la corruzione dei dati
- Minacce basate sull'errore umano relative alla perdita, al danneggiamento o alla perdita di dati sensibili. Potrebbe essere causata da una truffa di phishing, dall'esecuzione accidentale di malware tramite supporti rimovibili o da altri modi

MITRE ATT&CK

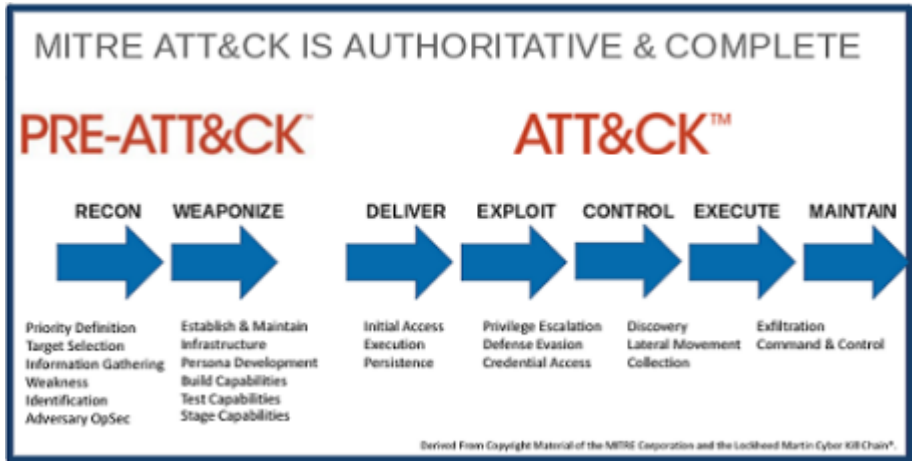
MITRE ATT&CK (*Adversarial Tactics, Techniques and Common Knowledge*) è una risorsa di conoscenze di tattiche e tecniche di attacco basate su osservazioni del mondo reale

- la Tattica è una descrizione di alto livello del comportamento di un attaccante
- la Tecnica rappresenta una descrizione dettagliata di una determinata Tattica
- la Procedura è il metodo per attuare una determinata Tecnica

Le informazioni contenute nel D.B. ATT&CK vengono utilizzate come base per lo sviluppo di modelli e metodologie di minacce specifici nel settore privato, nel governo e nella comunità di prodotti e servizi della sicurezza informatica

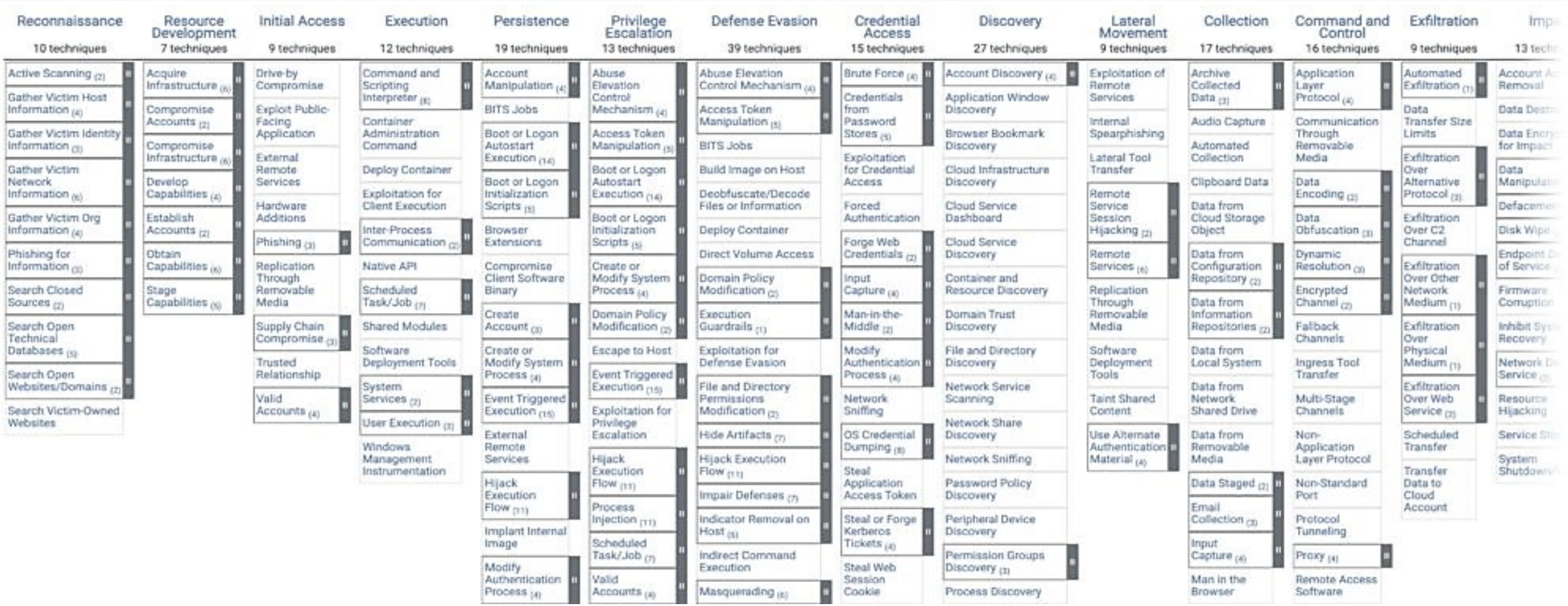
- È free, open e accessibile a livello globale
- Chiunque può contribuire allo suo sviluppo

https://attack.mitre.org/



ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques



Individuare le vulnerabilità

Ecco alcuni metodi principali per individuare le vulnerabilità cyber:

- **Vulnerability scanning**: Utilizzo di strumenti automatizzati per scansionare sistemi, reti e applicazioni e individuare vulnerabilità note (CVE)
- **Penetration testing** (Pen testing): Simulazione di attacchi reali per identificare debolezze che potrebbero essere sfruttate da malintenzionati
- **Code review**: Analisi manuale o automatizzata del codice sorgente per identificare problemi di sicurezza
- **Threat modeling**: Processo strutturato per identificare potenziali minacce e vulnerabilità durante la fase di progettazione
- **Bug bounty programs**: Programmi che incentivano ricercatori di sicurezza esterni a trovare e segnalare vulnerabilità
- **Social engineering assessment**: Valutazione della suscettibilità del personale a tecniche di manipolazione psicologica
- **Configuration review**: Controllo delle impostazioni di sistemi e delle applicazioni per identificare configurazioni non sicure
- **Network analysis**: Monitoraggio e analisi del traffico di rete per identificare comportamenti anomali
- **Red teaming**: Attività di un team dedicato a simulare attacchi avanzati contro l'organizzazione
- **Security audit**: Valutazione completa dell'infrastruttura IT rispetto agli standard di sicurezza

Esempio di implementazione

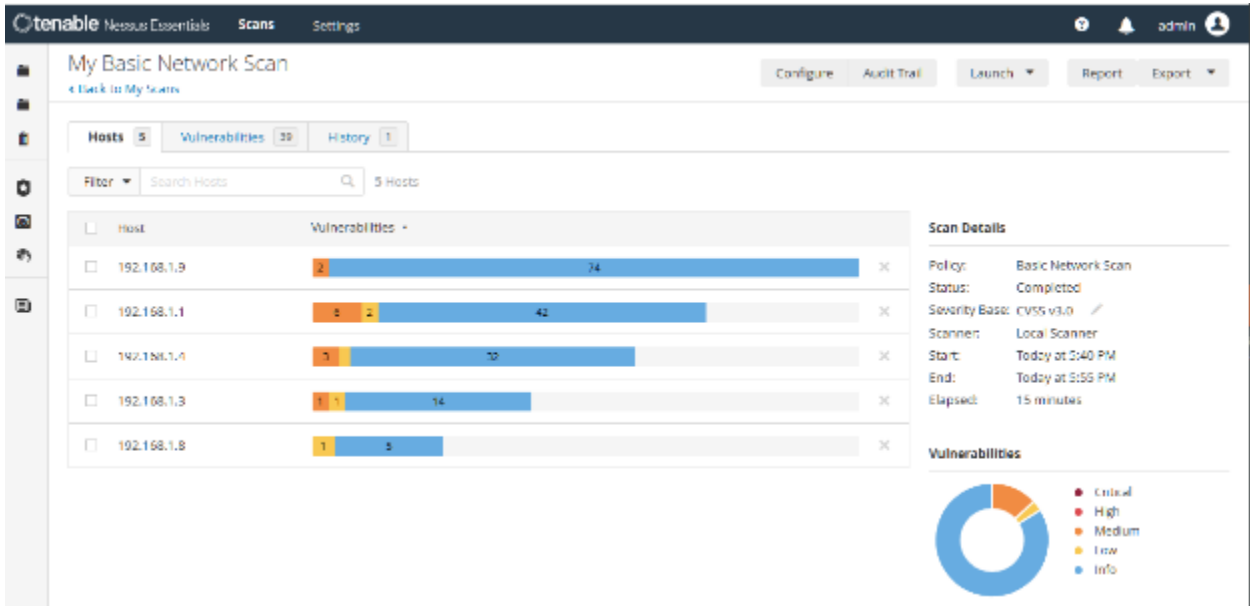
Vulnerability Assessment

Platform for Vulnerability Assessment

Scoprire le vulnerabilità: effettua una valutazione puntuale per identificare le falle del software, le patch mancanti, i malware e le configurazioni errate

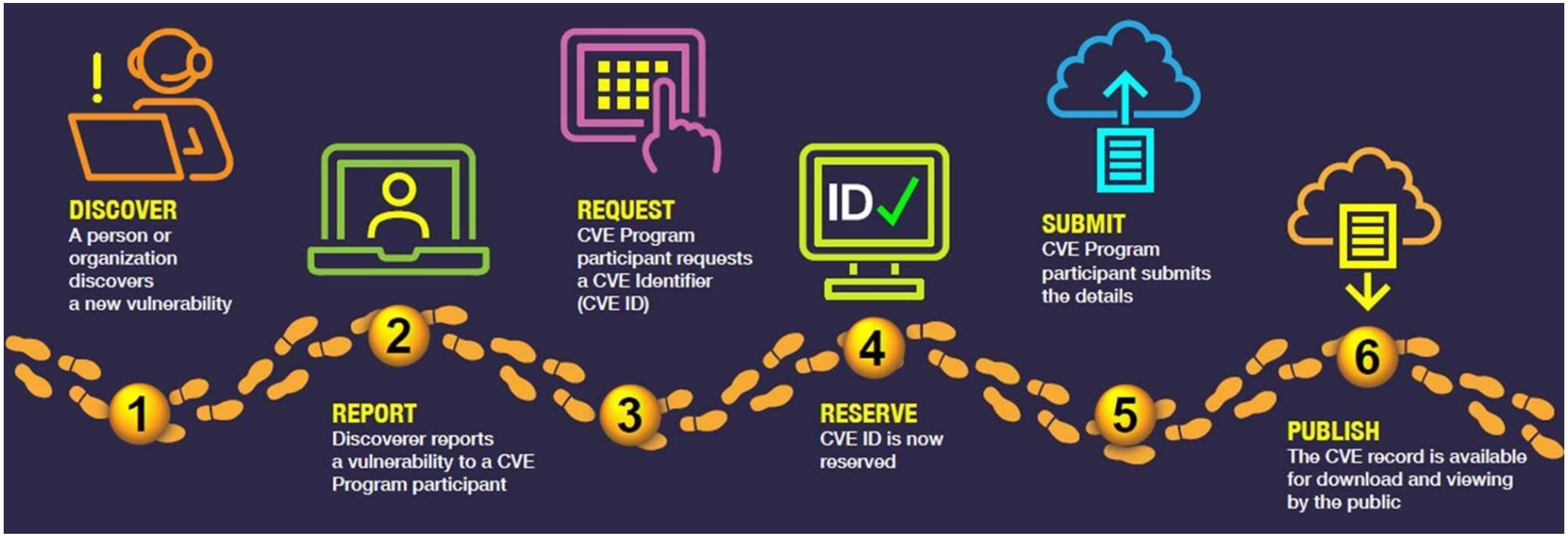
Evidenziare e classificare le minacce: utilizza un set di sistemi di valutazione, come CVSS v4, EPSS e VPR, per classificare le vulnerabilità per le attività di contenimento

Colmare le lacune di conoscenza: fornisce una serie di consigli e suggerimenti pratici per implementare gli step di remediation successivi



Common Vulnerabilities and Exposures www.cve.org

Il CVE è un framework per identificare, definire, catalogare e pubblicare le vulnerabilità di cybersecurity



CVE Record Lifecycle

Macro-modello di calcolo del rischio

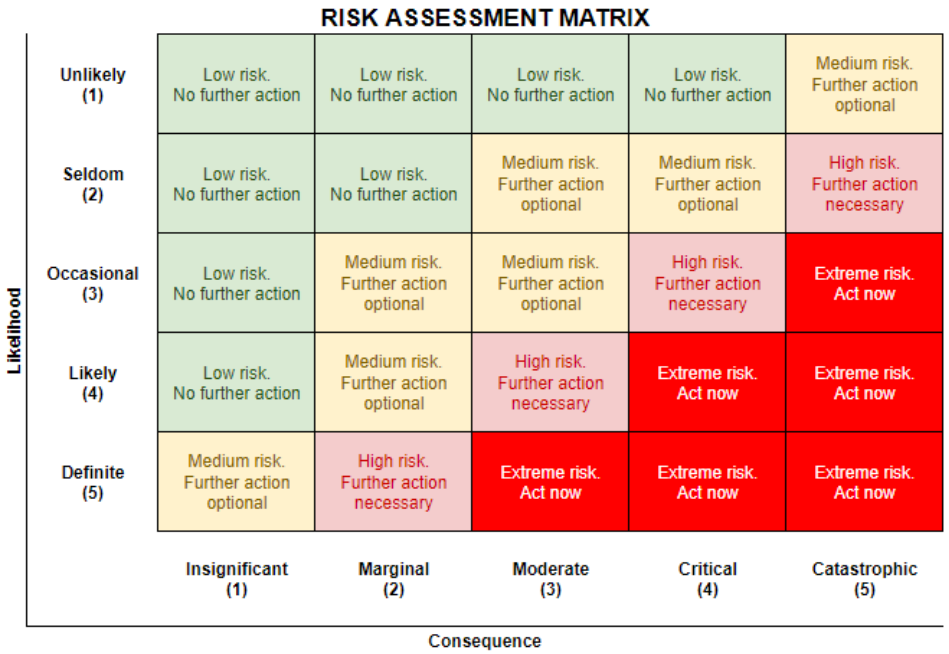
CARATTERISTICHE SERVIZI
A seconda delle caratteristiche primarie dei servizi erogati, è determinato il livello di criticità intrinseca (Profilo di Criticità) · Le caratteristiche primarie e secondarie consentono di selezionare le Misure di Sicurezza da implementare (controlli di tipo amministrativo, sicurezza logica e fisica,) e dunque determinare le Vulnerabilità.

BENCHMARK
Il benchmark consente di valutare il fattore di Esposizione alla singola minaccia

IMPATTO
Consente di valutare gli impatti per ciascun servizio erogato dalla PA in caso di perdita di **Riservatezza (R), Integrità (I) e Disponibilità (D).** A partire dagli impatti sui singoli servizi erogati dalla PA, sarà poi calcolato l'impatto R,I,D

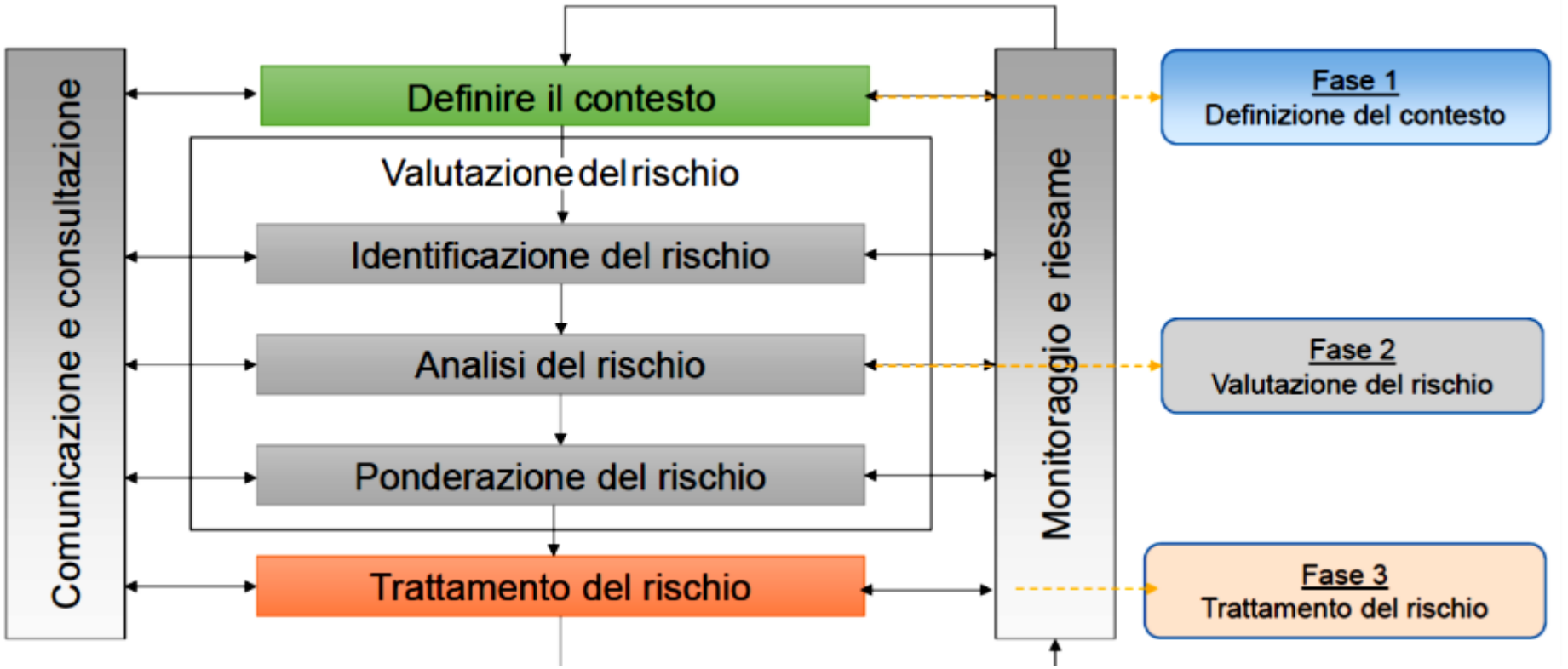
CYBER RISK = PROBABILITÀ DI ACCADIMENTO X IMPATTO

Metodo di cybersecurity risk management



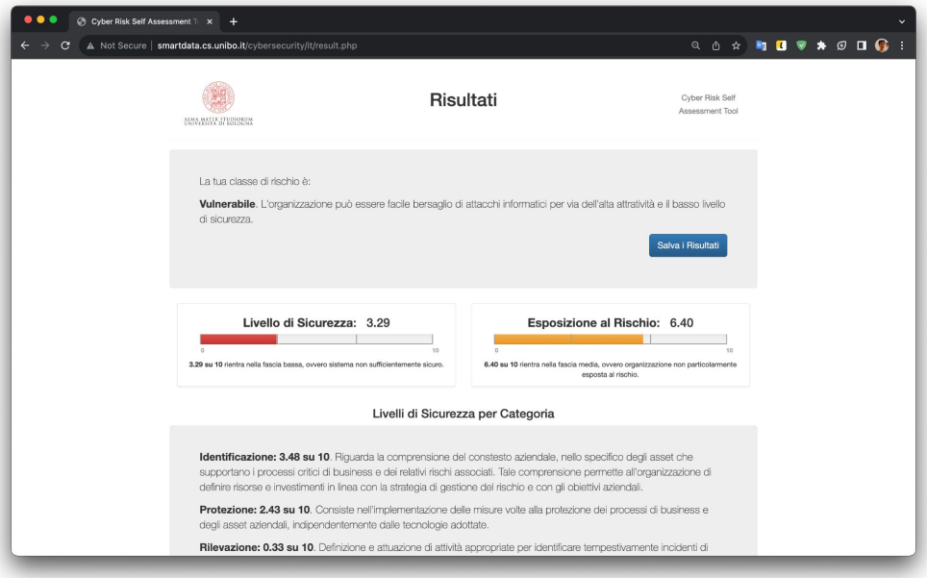
Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure — Overheating in server room. **High**	Air conditioning system is ten years old. **High**	All services (website, email, etc.) will be unavailable for at least 3 hours. **Critical**	**High** Potential loss of $50,000 per occurrence.	Buy a new air conditioner ($3,000 cost)
Malicious human (interference) — distributed denial-of-service (DDoS) attack. **High**	Firewall configured properly and has good DDOS mitigation. **Low**	Website resources will be unavailable. **Critical**	**Moderate** Potential loss of $5000 per hour of downtime	Monitor the firewall
Natural disasters — flooding **Moderate**	Server room is on the 3rd floor **Very low**	All services will be unavailable **Critical**	**Very low**	No action needed
Accidental human interference — accidental file deletions **High**	Permissions are configured properly; IT auditing software is in place; backups are taken regularly **Low**	All services (website, email, etc.) will be unavailable for at least 3 hours **Moderate**	**Low**	Continue monitoring permissions changes, privileged users and backups

Metodo di cybersecurity risk management



Tool di Valutazione del livello di sicurezza e esposizione al rischio

- Cyber Risk Self Assessment Tool - Free
  http://smartdata.cs.unibo.it/cybersecurity/
  basato su NIST Cybersecurity Framework 2.0
- Cyber Risk Management – Free (PA)
  https://rischiocyber.acn.gov.it/cyber/index.html
  basato su ISO 31000 e IRAM2
- Cyber Security Assessment Tool - $$$
  https://azuremarketplace.microsoft.com/en/marketplace/apps/qs-solutions.cyber-security-assesment-tool



Improvement / Miglioramento (ID.IM)

Obiettivo:

Identificare i miglioramenti apportati ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity in tutte le funzioni aziendali

Attività
Identificare i miglioramenti dalle valutazioni effettuate
Identificare i miglioramenti dai test e dalle esercitazioni di sicurezza, compresi quelli effettuati in coordinamento con i fornitori e le terze parti interessate
Identificare i miglioramenti dall'esecuzione dei processi operativi, delle procedure e delle attività
Stabilire, comunicare, manutenere e migliorare i piani di risposta agli incidenti e gli altri piani di cybersecurity che influenzano le operazioni

In questa fase si avverte l'importanza
della funzione di governance/coordinamento

Riepilogo

Al termine di questa fase otteniamo:

- Inventario degli asset (hardware, dispositivi, dati, allocazione temporale, personale e software)
- Mappatura dei rischi
- Grado di esposizione/vulnerabilità

Queste informazioni sono utili a:

- Stabilire il profilo di cybersecurity
- Valutare le misure di contenimento
- Trasferire il rischio residuo
- Dialogare con il top management

Protect / Proteggere (PR)

Implementazione delle misure volte alla protezione dei processi di business e degli asset aziendali

Gestione dell'identità, autenticazione e controllo degli accessi (PR.AA)

Obiettivo:

Limitare l'accesso agli asset fisici e logici, ed alle relative risorse, al personale, ai processi e ai dispositivi autorizzati, e gestire, in maniera coerente con la valutazione del rischio, l'accesso non autorizzato alle attività ed alle transazioni autorizzate

Attività
Gestire le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati dall'organizzazione
Verificare e collegare le identità alle credenziali in base al contesto delle interazioni
Autenticare gli utenti, i servizi e l'hardware
Proteggere, trasmettere e verificare le asserzioni di identità
Definire i permessi di accesso, i diritti e le autorizzazioni in una politica, gestirli, applicarli e rivederli; incorporare i principi del minimo privilegio e della separazione dei compiti
Gestire, monitorare e fatto rispettare l'accesso fisico alle risorse in base al fattore di rischio

L'importanza dell'autenticazione

Negli ambienti tradizionali (on-premise) l'autenticazione utente è affidata alle credenziali di accesso e, raramente, è effettuata una profilazione che associ i permessi di accesso alle risorse (dati o funzioni) per cui l'utente è autorizzato.

Con l'avvento delle tecnologie mobile e cloud, le previsioni normative in materia di trattamento dei dati, la proliferazione degli attacchi informatici (compresi quelli rivolti al furto di identità o allo spoofing) si è reso necessario adottare politiche di autenticazione e autorizzazione granulari, più robuste e sicure.

- **Single Sign-On (SSO)**: sistemi di autenticazione condivisa
- **Multi-Factor Authentication** (MFA): richiede più fattori di autenticazione (biometria)
- **Role-based access control** (RBAC): gestione degli accessi basata sui ruoli
- **Self-Sovereign Identity** (SSI): accesso senza una parte fidata centralizzata
- **Identity and Access Management** (IAM) sistema gestionali per le politiche di accesso
- **Secure Access Service Edge** (SASE): autenticazione basato sul cloud

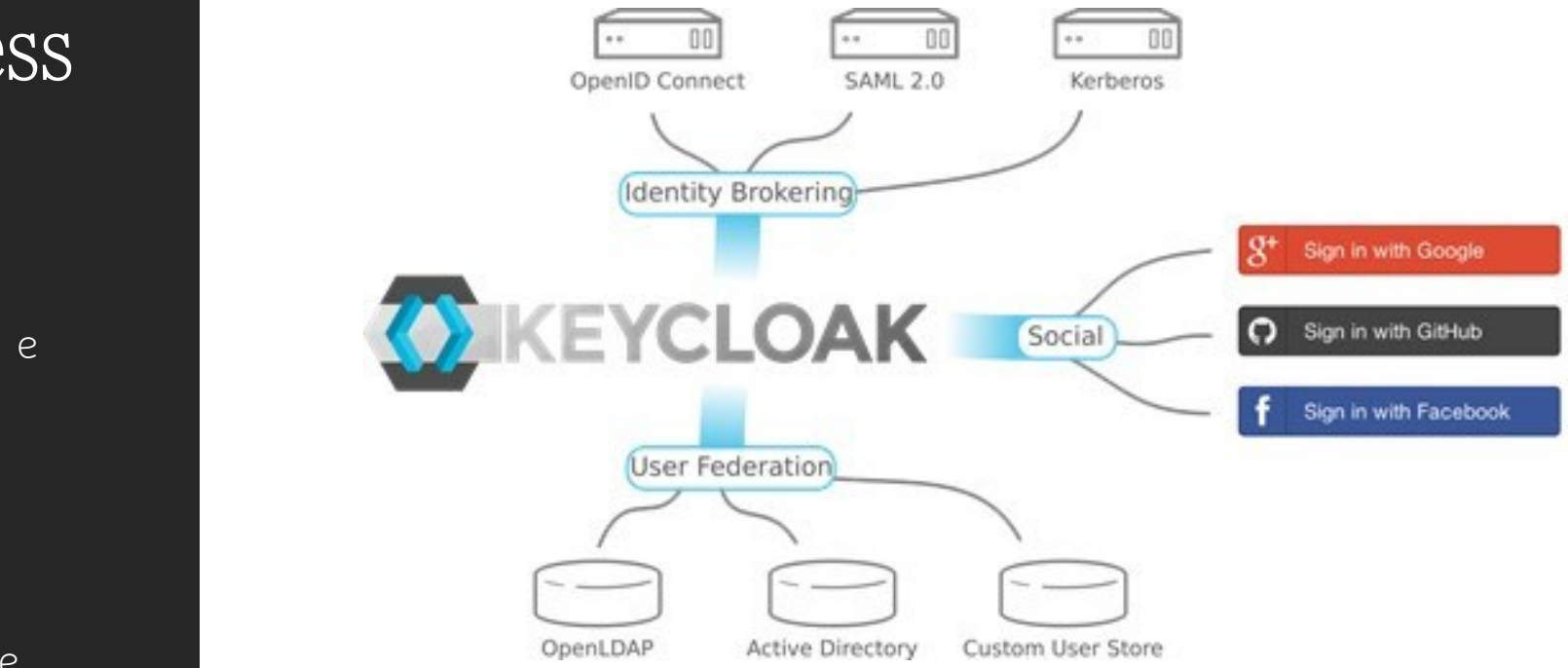
Esempio di implementazione

IAM - Identity and Access Management

Open Source Identity and Access Management

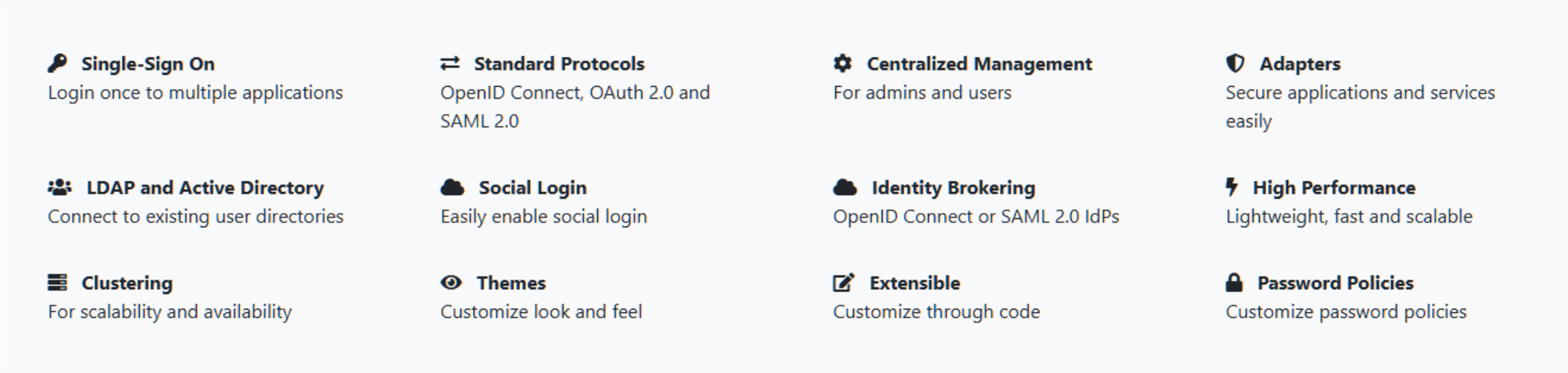
Consente di aggiungere l'autenticazione alle applicazioni e protegge i servizi.

Può gestire gli utenti e la loro autenticazione in base ai ruoli. Inoltre, offre la federazione con altre LDAP, l'autenticazione forte, la gestione degli utenti, l'autorizzazione a grana fine e l'integrazione con altri servizi cloud.



Modelli di autorizzazione

Un sistema di Identity and Access Management consente di definire le autorizzazioni in base ai ruoli oppure di selezionarle su ogni singola funzionalità
Questo permette di gestire le autorizzazioni in una console di amministrazione e definire esattamente le politiche di accesso ai singoli servizi o funzionalità



Il paradigma di sicurezza "*Zero Trust*"

È un approccio che sovverte le tradizionali nozioni di fiducia all'interno delle reti aziendali.
Invece di presumere che tutto ciò che si trova all'interno del perimetro di rete sia sicuro,
Zero Trust opera con il principio fondamentale che **«non ci si fida di nessuno, si verifica tutto»**

1. **Nessuna fiducia implicita**: ogni utente, dispositivo o applicazione, è considerato potenzialmente una minaccia
2. **Verifica continua**: l'identità e l'accesso sono verificati costantemente, non solo al momento dell'accesso iniziale
3. **Principio del minimo privilegio**: gli utenti e i dispositivi ricevono solo i permessi necessari per svolgere le loro funzioni, limitando il potenziale danno in caso di compromissione
4. **Micro segmentazione**: la rete è suddivisa in segmenti più piccoli, limitando il movimento laterale degli aggressori
5. **Monitoraggio e registrazione**: le attività sono monitorate e registrate per rilevare anomalie e potenziali minacce

È un modo di progettare la sicurezza dell'identità per ambienti aperti e dinamici (cloud, edge, mobile)

Sensibilizzazione e formazione (PR.AT)

Obiettivo:

Sensibilizzare e addestrare tutto il personale in materia di cybersecurity affinché possa svolgere i propri compiti o ruoli connessi alla cybersecurity

Attività
Sensibilizzare e formare il personale in modo da possedere le conoscenze e le competenze necessarie per svolgere le mansioni generali tenendo conto dei rischi di cybersecurity
Sensibilizzare e formare coloro che ricoprono ruoli specializzati in modo da possedere le conoscenze e le competenze necessarie per svolgere i compiti pertinenti tenendo conto dei rischi di cybersecurity
Far comprendere alle terze parti interessate (ad esempio, fornitori, clienti, partner) i loro ruoli e le loro responsabilità.
Far comprendere agli alti dirigenti i loro ruoli e le loro responsabilità

È fondamentale, in alcuni casi è un obbligo, formare il personale sui temi cyber, regolamentare la gestione dei dati e delle funzioni, formalizzare i livelli di responsabilità e i compiti connessi alla cyber

Supply chain: il problema delle terze parti

Il problema della supply chain in ambito cyber rappresenta una delle sfide più complesse e critiche per la sicurezza informatica moderna.

Il rischio della supply chain si riferisce alle vulnerabilità introdotte attraverso le relazioni commerciali con fornitori, partner, e altri soggetti terzi che hanno accesso ai sistemi informatici o forniscono componenti software/hardware utilizzati nell'infrastruttura IT di un'organizzazione.

Principali problematiche

- **Effetto a cascata**: un attacco a un singolo fornitore può compromettere centinaia o migliaia di clienti simultaneamente.
- **Superficie d'attacco estesa**: ogni fornitore e partner estende la superficie d'attacco dell'organizzazione.
- **Asimmetria di sicurezza**: fornitori più piccoli potrebbero avere standard di sicurezza inferiori rispetto ai loro clienti di grandi dimensioni.
- **Componenti compromessi**: inserimento di codice malevolo o backdoor direttamente nei componenti software o hardware durante il processo di sviluppo o distribuzione.
- **Difficoltà di verifica**: impossibilità pratica di verificare completamente ogni componente di terze parti utilizzato nei sistemi.

Strategie di mitigazione

- **Due diligence dei fornitori**: valutazione approfondita della sicurezza dei fornitori prima della collaborazione
- **Software Bill of Materials (SBOM)**: inventario dettagliato di tutti i componenti software utilizzati
- **Controllo degli accessi**: limitare l'accesso dei fornitori ai soli sistemi necessari
- **Monitoraggio continuo**: sorveglianza delle attività dei fornitori nei propri sistemi
- **Clausole contrattuali**: requisiti di sicurezza esplicitamente definiti nei contratti
- **Zero Trust**: implementazione di un approccio che verifica costantemente ogni accesso, indipendentemente dalla provenienza
- **Segmentazione della rete**: isolamento dei sistemi accessibili ai fornitori per limitare potenziali danni

In alcuni contesti è un obbligo normativo

Sicurezza dei dati (PR.DS)

Obiettivo:

Gestire i dati in maniera coerente con la strategia di rischio per garantire la riservatezza, l'integrità e la disponibilità delle informazioni

Attività
Preservare la riservatezza, l'integrità e la disponibilità dei dati a riposo
Preservare la riservatezza, l'integrità e la disponibilità dei dati in transito
Preservare la riservatezza, l'integrità e la disponibilità dei dati in uso
Creare, proteggere, manutenere e testare i backup dei dati

Le policy di protezione devono tenere conto del grado di classificazione assegnato al dato e delle normative vigenti

Classificazione dei dati per livello di criticità

Classificazione dei dati per livello di criticità

Livello 1 - Pubblico: Dati che possono essere liberamente divulgati, Impatto minimo se compromessi (informazioni di marketing, materiali educativi pubblici)

Livello 2 - Interno: Dati non destinati alla divulgazione pubblica, ma con impatto limitato se esposti (politiche interne, organigrammi, procedure operative standard)

Livello 3 - Confidenziale: Dati la cui divulgazione potrebbe danneggiare l'organizzazione (informazioni finanziarie non pubbliche, dati dei clienti non sensibili, strategie aziendali)

Livello 4 - Riservato: Dati altamente sensibili la cui divulgazione causerebbe danni significativi (proprietà intellettuale, piani di sviluppo strategici, alcuni dati personali)

Livello 5 - Critico: Dati la cui compromissione potrebbe minacciare la sopravvivenza dell'organizzazione (segreti commerciali, credenziali di accesso ai sistemi critici, dati sanitari)

Mappatura secondo i principi CIA

Per ciascun livello di criticità, si valuta l'importanza dei tre principi CIA

Confidenzialità (C):

- Livello 1: Bassa (0-1)
- Livello 2: Bassa-Media (2-3)
- Livello 3: Media (4-6)
- Livello 4: Alta (7-8)
- Livello 5: Molto Alta (9-10)

Integrità (I):

- Livello 1: Bassa-Media (2-3)
- Livello 2: Media (4-5)
- Livello 3: Media-Alta (6-7)
- Livello 4: Alta (8-9)
- Livello 5: Molto Alta (10)

Disponibilità (A):

- Livello 1: Variabile (1-7, dipende dal caso)
- Livello 2: Media (4-6)
- Livello 3: Media-Alta (6-8)
- Livello 4: Alta (8-9)
- Livello 5: Molto Alta (9-10)

Implementazione mappatura dei dati

1. Creazione di una matrice di classificazione:
   - Combinare livelli di criticità con valutazioni CIA
   - Esempio: un dato classificato come Livello 4 (Riservato) potrebbe avere C:8, I:9, A:7
2. Etichettatura dei dati:
   - Implementare sistemi di etichettatura automatica dove possibile
   - Formare gli utenti sulla corretta classificazione dei dati
3. Controlli di sicurezza adeguati:
   - Mappare i controlli di sicurezza necessari per ciascun livello di classificazione
   - Esempio: i dati di Livello 5 potrebbero richiedere crittografia avanzata, controlli di accesso rigorosi e backup regolari
4. Revisione periodica:
   - Rivalutare periodicamente la classificazione dei dati
   - Adeguare i controlli di sicurezza in base ai cambiamenti nel valore o nella criticità dei dati

Questa mappatura consente di allocare risorse di sicurezza in modo efficiente, concentrando gli sforzi di protezione sui dati più critici secondo le specifiche esigenze di confidenzialità, integrità e disponibilità.

Il ruolo della crittografia: riservatezza e integrità

La crittografia svolge un ruolo fondamentale nella sicurezza dei dati:

1. **Confidenzialità**: protegge le informazioni da accessi non autorizzati, garantendo che solo le persone autorizzate possano accedere ai dati. Anche se i dati vengono intercettati, rimangono illeggibili senza la chiave di decrittazione
2. **Integrità**: può essere utilizzata per verificare che i dati non siano stati alterati durante la trasmissione o l'archiviazione. Le funzioni hash crittografiche, ad esempio, generano un'impronta digitale univoca dei dati, che può essere utilizzata per rilevare qualsiasi modifica
3. **Autenticazione**: può essere usata per verificare l'identità di un utente o di un dispositivo. Le firme digitali, ad esempio, utilizzano la crittografia per garantire che un messaggio provenga da una fonte attendibile
4. **Non ripudio**: può essere utilizzata per impedire a una persona di negare di aver inviato o ricevuto un messaggio. Le firme digitali, ad esempio, forniscono una prova inconfutabile dell'origine e della destinazione di un messaggio

Policy di backup: disponibilità e resilienza

L'importanza di politiche di backup sicure:

- **Protezione dei dati**: prevenire la perdita di dati critici a causa di guasti hardware, errori umani, attacchi informatici o disastri naturali
- **Continuità operativa**: garantire la disponibilità dei dati e delle applicazioni per mantenere la continuità delle operazioni aziendali
- **Conformità normativa**: soddisfare i requisiti di conservazione dei dati previsti dalle normative e dai contratti
- **Ripristino rapido**: ridurre i tempi di inattività e i costi associati al ripristino dei dati

In sintesi, le politiche di backup sono fondamentali per la protezione dei dati e la continuità operativa

Elementi chiave di una politica di backup efficace

- **Identificazione dei dati critici**: determinare quali dati sono essenziali e necessitano di backup regolari
- **Frequenza dei backup**: stabilire quando eseguire i backup in base alla criticità dei dati e alla frequenza delle modifiche
- **Tipi di backup**: scegliere il tipo di backup a seconda delle esigenze di ripristino
- **Supporti di archiviazione**: selezionare i supporti di archiviazione appropriati
- **Conservazione dei backup**: definire per quanto tempo conservare i backup, in conformità con le normative e le esigenze aziendali
- **Test di ripristino**: eseguire test di ripristino per verificare l'efficacia dei backup
- **Sicurezza dei backup**: proteggere i backup da accessi non autorizzati, crittografandoli e archiviandoli in luoghi sicuri
- **Documentazione**: documentare le procedure di backup e ripristino per garantire la coerenza e la facilità di esecuzione

Sicurezza della piattaforma (PR.PS)

Obiettivo:

Gestire l'hardware, il software (ad esempio: firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali in maniera coerente con la strategia di rischio per garantire la loro riservatezza, integrità e disponibilità.

Attività
Stabilite e applicare le pratiche di gestione della configurazione
Manutenere, sostituire e rimuovere il software in base al rischio
Manutenere, sostituire e rimuovere l'hardware in base al rischio
Generare i registri e renderli disponibili per il monitoraggio continuo
Impedire l'installazione e l'esecuzione di software non autorizzato
Integrare e monitorare le pratiche di sviluppo sicuro del software e le loro prestazioni durante l'intero ciclo di vita del software

Le stesse regole andrebbero estese ai fornitori,
di hardware, software e servizi, classificati critici

Gestione dei sistemi informativi

La regola fortemente consigliata è ***«Prevention is better than cure»****.* Ecco alcune best practice per la manutenzione di hardware e software, che possono essere integrate nel contesto del NIST Cybersecurity Framework 2.0

Manutenzione dell'Hardware

1. Aggiornare l'Inventario
2. Programmare la manutenzione preventiva
3. Gestire l'obsolescenza dei dispositivi
4. Controllare l'accesso fisico ai data center
5. Effettuare regolarmente backup e adottare politiche di ridondanza

Manutenzione del Software

1. Gestire il deployment delle patch
2. Gestire le configurazioni
3. Effettuare il monitoraggio e il logging
4. Gestire le licenze
5. Effettuare il decommissioning sicuro

Ciclo di vita dei sistemi informativi

Il paradigma ***security by design e security by default*** rappresenta un approccio fondamentale allo sviluppo di sistemi informativi che incorpora la sicurezza come elemento essenziale fin dalle prime fasi di progettazione.

Security by Design

Questo principio prevede che la sicurezza sia considerata come requisito fondamentale durante tutto il ciclo di vita dello sviluppo del sistema:

- **Analisi dei requisiti**: identificare i requisiti di sicurezza con i requisiti funzionali
- **Architettura**: progettare un'architettura che riduca la superficie d'attacco
- **Threat modeling**: identificazione proattiva delle potenziali minacce
- **Codifica sicura**: implementazione di pratiche di programmazione sicura
- **Testing di sicurezza**: validazione continua dei controlli di sicurezza
- **Manutenzione**: aggiornamenti regolari per affrontare nuove vulnerabilità

Security by Default

Questo principio prevede che le configurazioni predefinite dei sistemi siano già sicure senza necessità di interventi aggiuntivi:

- **Principio del privilegio minimo**: accesso limitato alle sole risorse necessarie
- **Autenticazione robusta**: meccanismi di autenticazione forte abilitati di default
- **Crittografia abilitata**: protezione dei dati sensibili attiva per impostazione predefinita
- **Connessioni sicure**: protocolli di comunicazione sicuri configurati automaticamente
- **Funzionalità non necessarie disabilitate**: riduzione della superficie d'attacco
- **Logging attivo**: registrazione degli eventi di sicurezza abilitata di default

Resilienza infrastrutture tecnologiche(PR.IR)

Obiettivo:

Gestire le architetture di sicurezza con una strategia risk-based per garantire la riservatezza, l'integrità e la disponibilità delle risorse e la resilienza organizzativa

Attività
Proteggere le reti e gli ambienti dall'accesso logico e dall'utilizzo non autorizzato
Proteggere le risorse tecnologiche dalle minacce ambientali
Implementare meccanismi per raggiungere i requisiti di resilienza in situazioni normali e avverse
Assicurare le risorse adeguate per garantire la disponibilità

Misure di sicurezza

Sicurezza logica

1. Hardening dei dispositivi, dei sistemi e delle reti
2. Firewall perimetrali e interni
3. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
4. Segmentazione della rete in VLAN separate
5. VPN per accessi remoti
6. Filtri anti-spam e anti-malware
7. Firewall applicativi (WAF)
8. Proxy per il controllo della navigazione web
9. DNS filtering
10. Network Access Control (NAC)
11. Protezione DDoS
12. Protezione degli endpoint e Soluzioni EDR
13. Controllo dispositivi USB e periferiche
14. Gestione centralizzata dei dispositivi mobili (MDM)

Sicurezza fisica

1. Controllo degli accessi con badge, sistemi biometrici o chiavi
2. Videosorveglianza nelle aree critiche e nei perimetri
3. Sistema di allarme anti-intrusione
4. Registri di accesso per visitatori e personale
5. Barriere fisiche (porte blindate, gabbie per server)
6. Guardie di sicurezza
7. Illuminazione di sicurezza perimetrale
8. Sistemi anti-incendio specifici per ambienti IT
9. Compartimentazione degli spazi con diversi livelli di accesso
10. Protezione contro minacce ambientali (inondazioni, sovratensioni)

Misure di resilienza

Resilienza operativa

1. Ridondanza infrastrutturale
2. Backup e ripristino dati
3. Continuità operativa
4. Disaster Recovery
5. Gestione delle crisi
6. Gestione della supply chain
7. Adattabilità organizzativa
8. Testing

Resilienza tecnologica

1. Architettura distribuita
   - Microservizi con deployment indipendenti
   - Sistemi distribuiti geograficamente
   - Architetture cloud multi-regione
   - Bilanciamento del carico e autoscaling
2. Resilienza delle applicazioni
   - Circuit breaker per prevenire fallimenti a cascata
   - Retry con backoff esponenziale
   - Graceful degradation delle funzionalità
   - Design per il fallimento

Riepilogo

I principi di sicurezza hanno modificato il paradigma dei sistemi informativi:

- In passato i sistemi informatici erano prevalentemente on-premise e, soprattutto, l'infrastruttura tecnologica e il perimetro di sicurezza erano chiari e definiti

- I sistemi informativi moderni sono dinamici e indefiniti, perché sono la sommatoria di diverse componenti, eterogenee tra loro e dislocate in ambienti diversi, che collaborano tra di loro (cloud, mobile, edge, iot) e possono cambiano in maniera disgiunta

Di conseguenza, sono dovute cambiare le strategie di protezione.
Si è passati dalla sicurezza perimetrale, ad un modello di sicurezza Zero Trust basato su controlli più granulari, più sensibili e continui, in grado di adattarsi al cambiamento e alle nuove minacce.

Processo di Gestione della Sicurezza

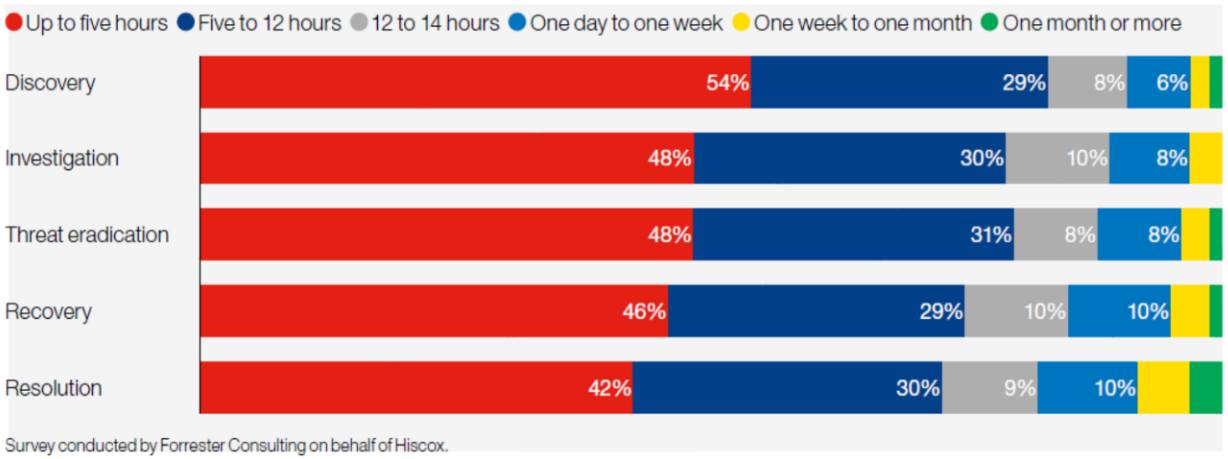
	Function	Obiettivo
Gestione del rischio	IDENTIFY	La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea 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

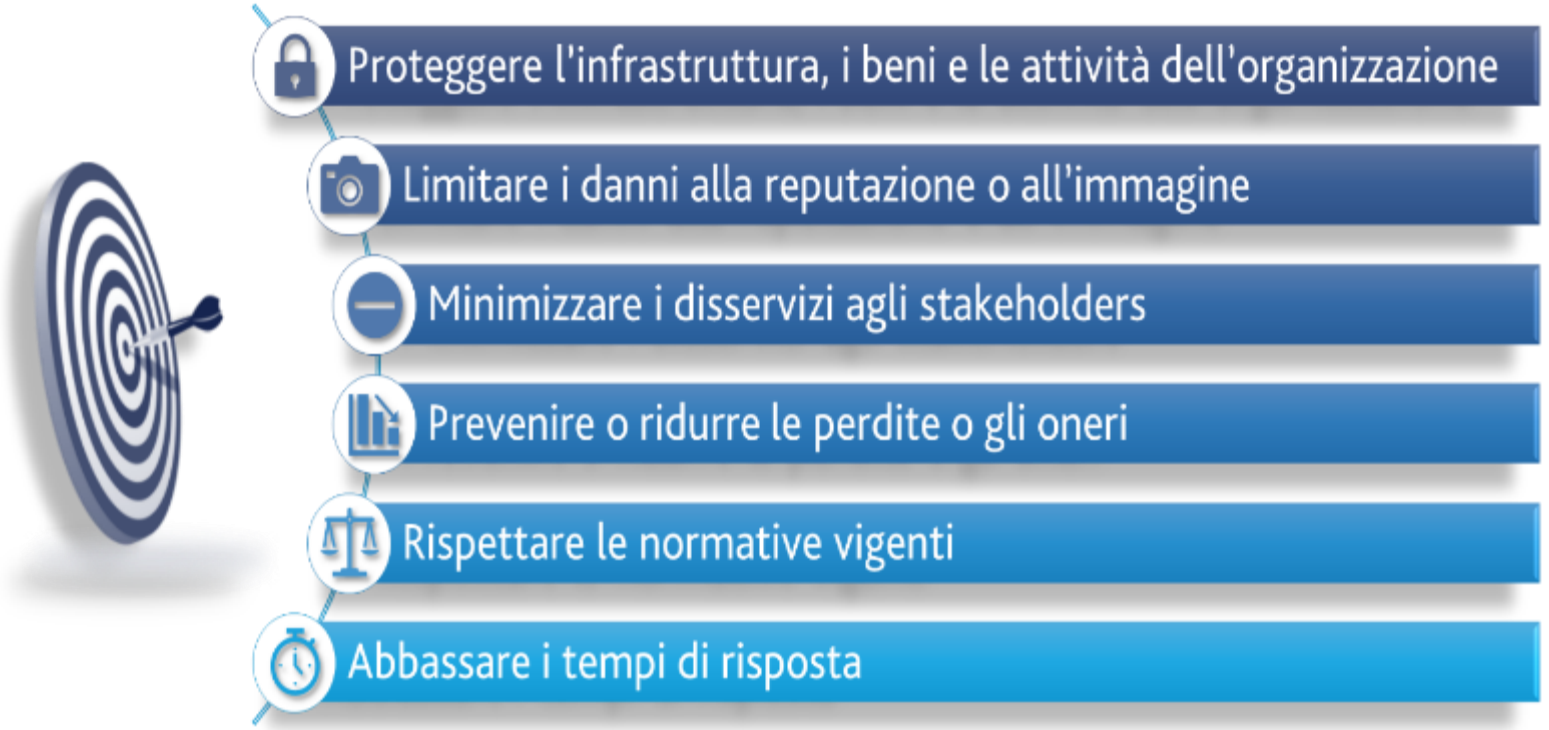
- processo coordinato per reagire alle conseguenze di un incidente finalizzato al ripristino dell'operatività
- normalmente articolato in una sequenza di fasi:

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

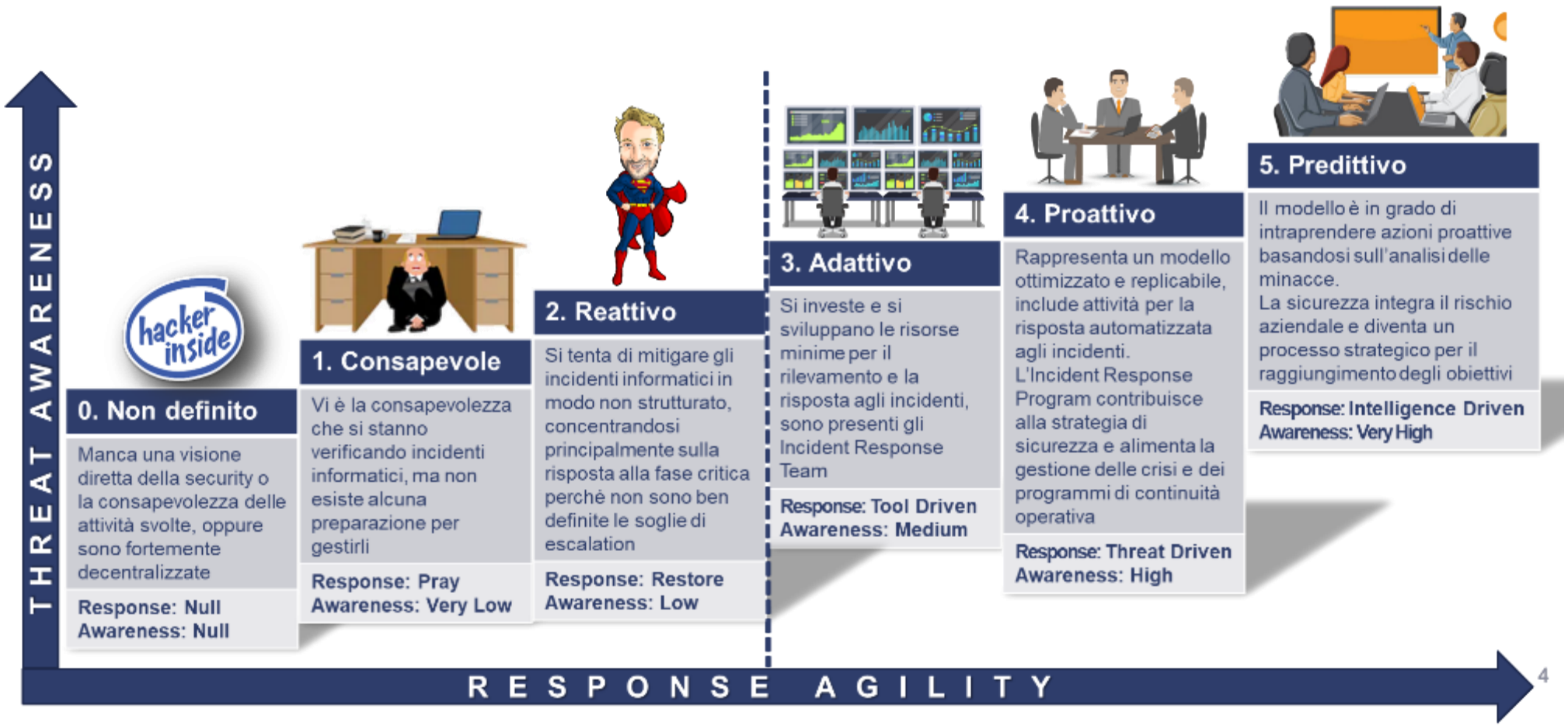
Il tempo è prezioso



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

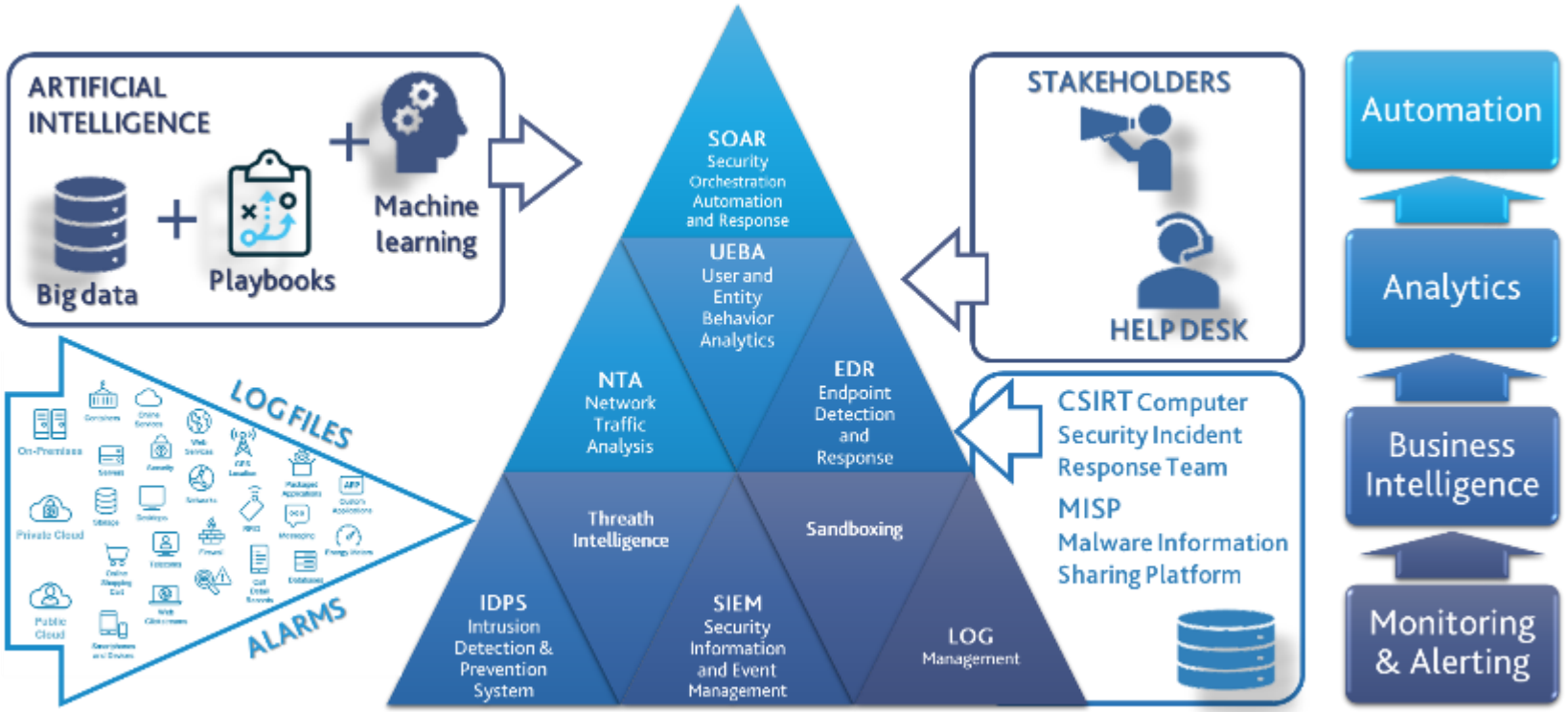
COME SI SVILUPPA UN I.R.PLAN?

- 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

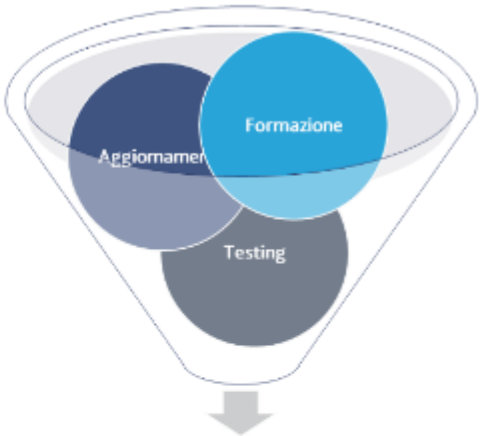
Cosa fare prima: Tech
Incident Response Platform



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

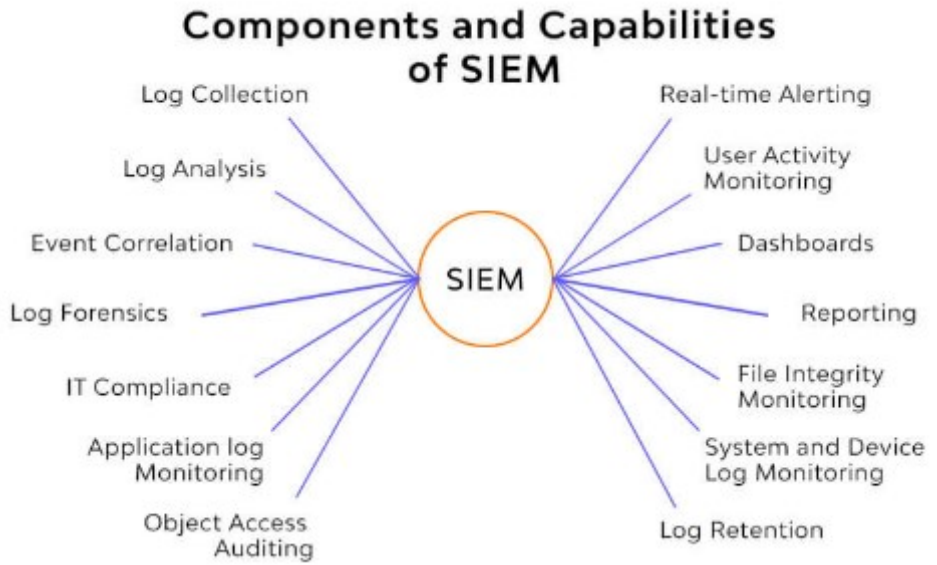
In questa fase è fondamentale la condivisione delle informazioni di sicurezza tra organizzazione dello stesso settore (p.e. minacce, incidenti e indicatori di compromissione) per aumentare l'efficacia di detection

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:

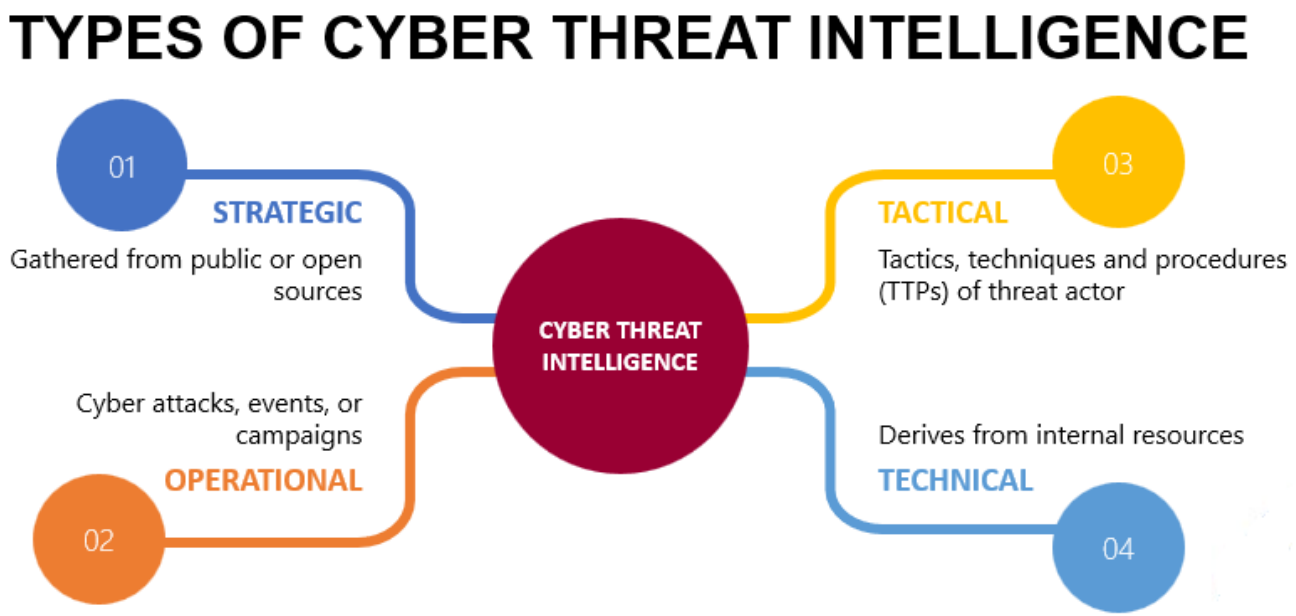
Analizzare le anomalie, gli indicatori di compromissione e gli altri eventi potenzialmente avversi per caratterizzare gli eventi per essere in grado di rilevare gli incidenti di cybersecurity

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

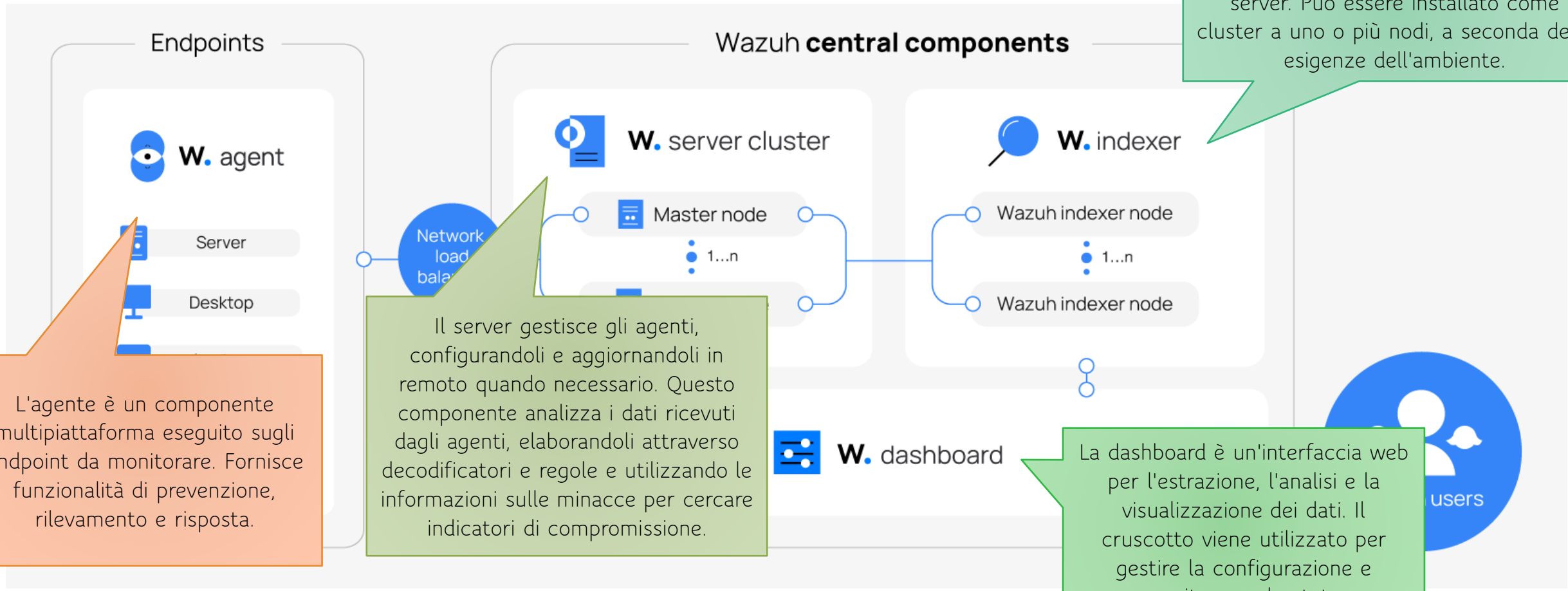
SIEM

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.

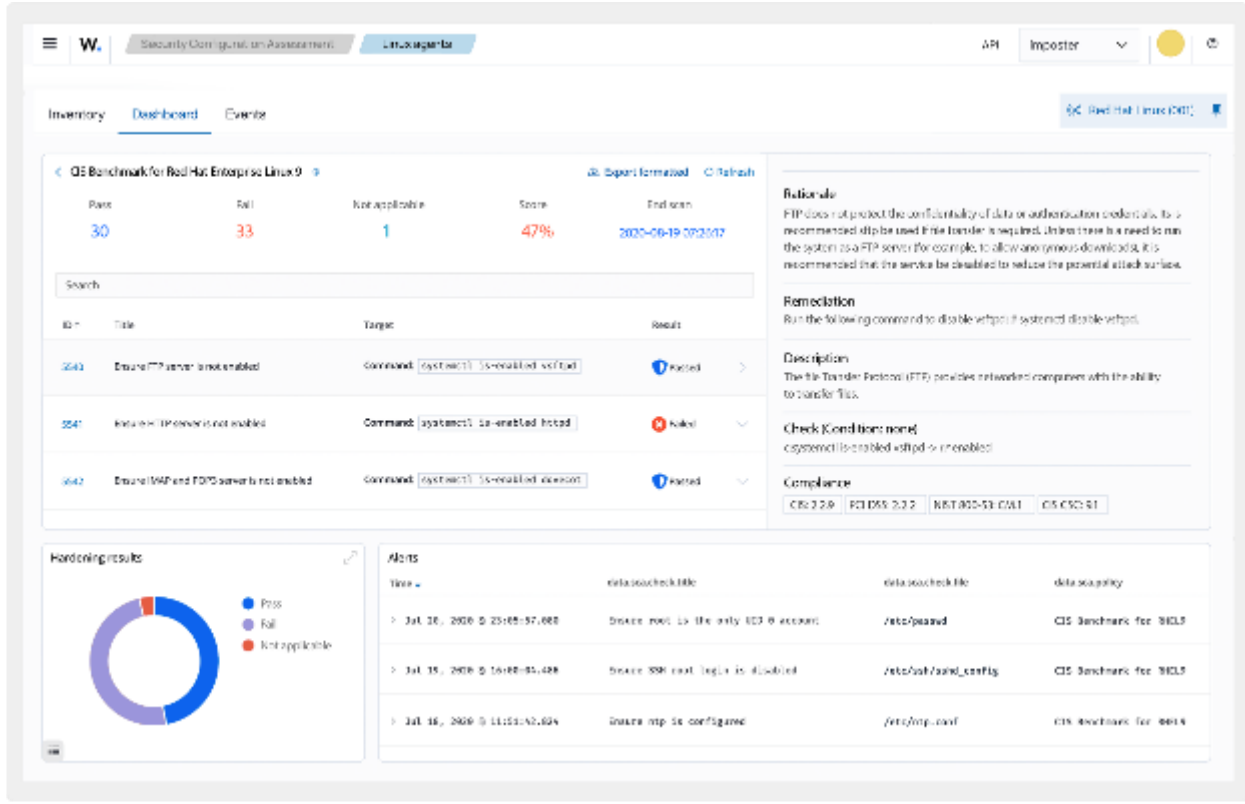
Il server gestisce gli agenti, configurandoli e aggiornandoli in remoto quando necessario. Questo componente analizza i dati ricevuti dagli agenti, elaborandoli attraverso decodificatori e regole e utilizzando le informazioni sulle minacce per cercare indicatori di compromissione.

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.

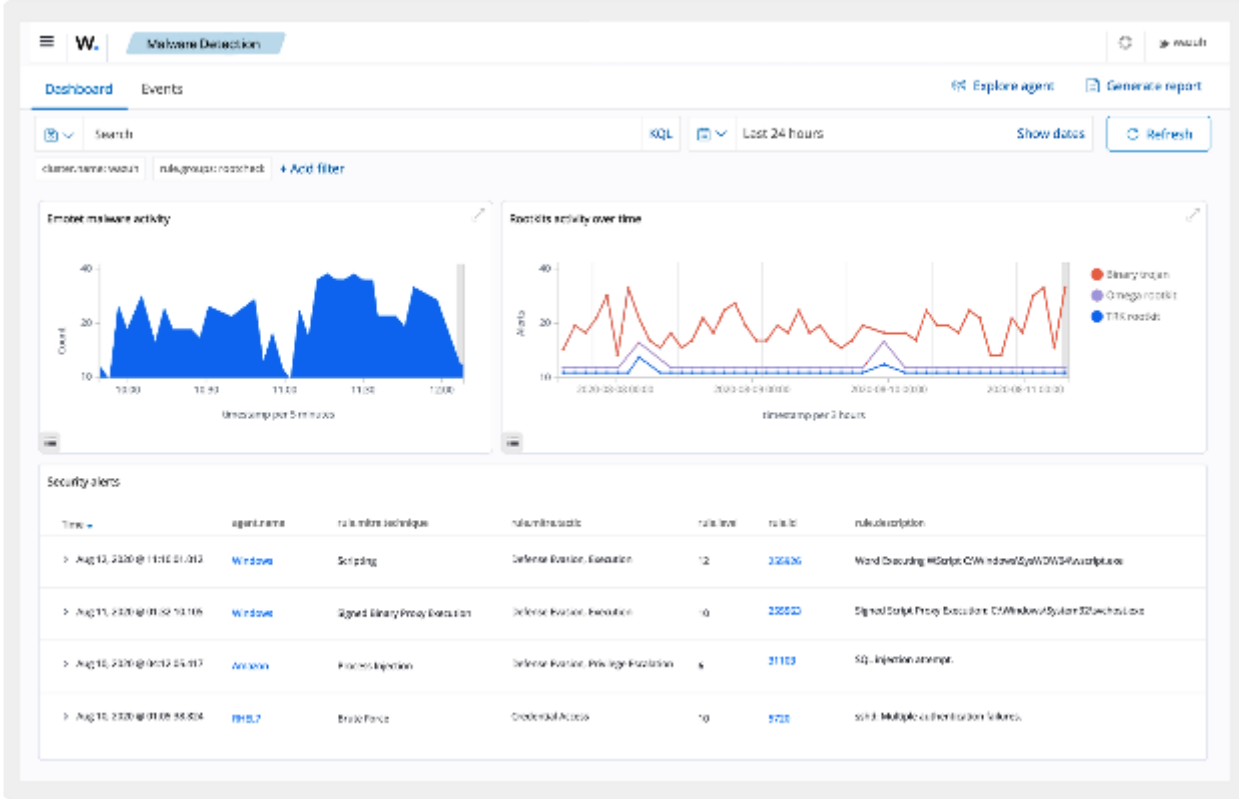
Configuration Assessment

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.



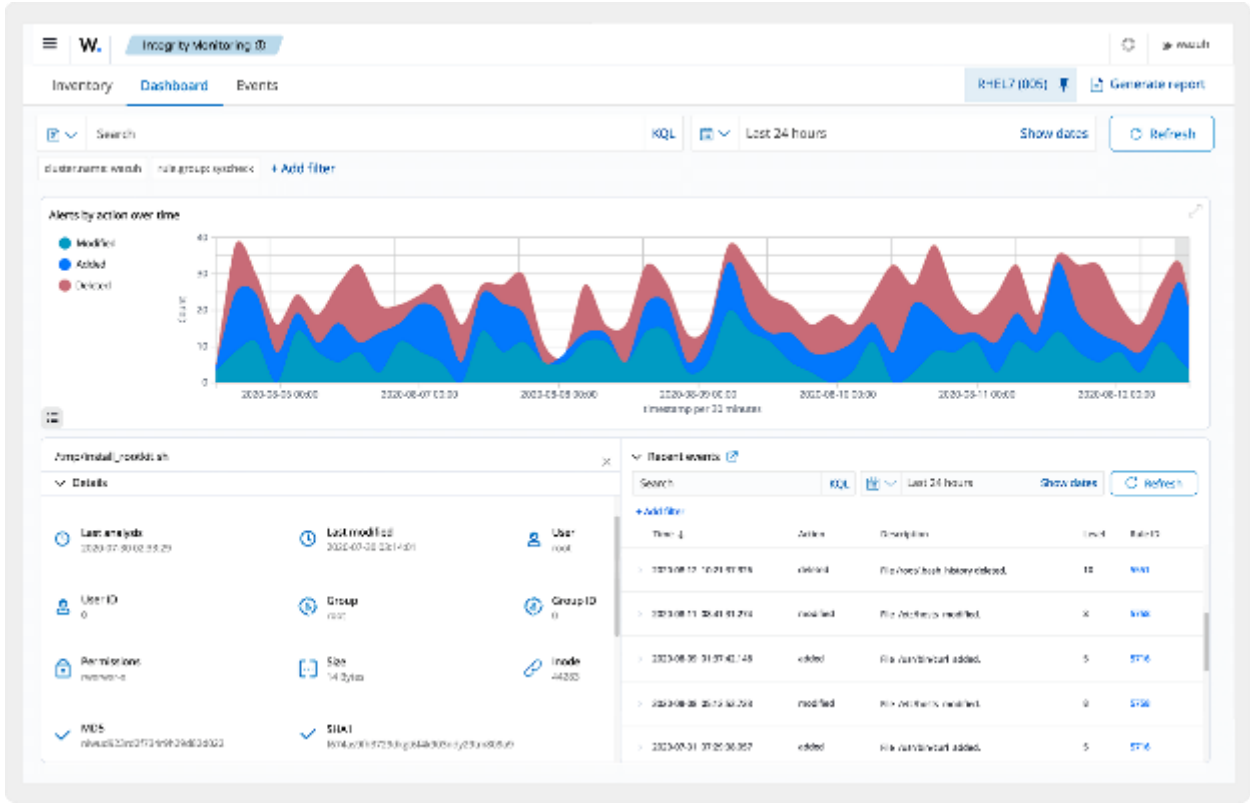
Malware Detection

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.



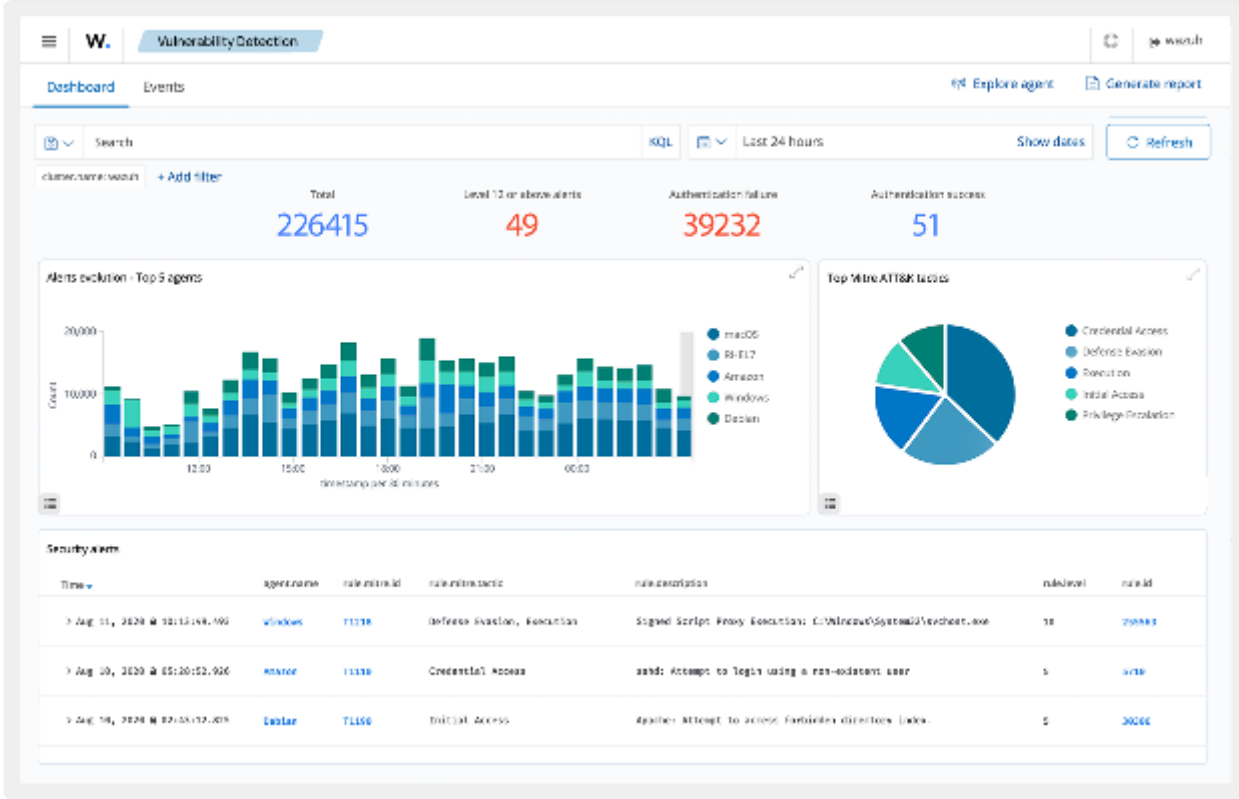
File Integrity Monitoring

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.



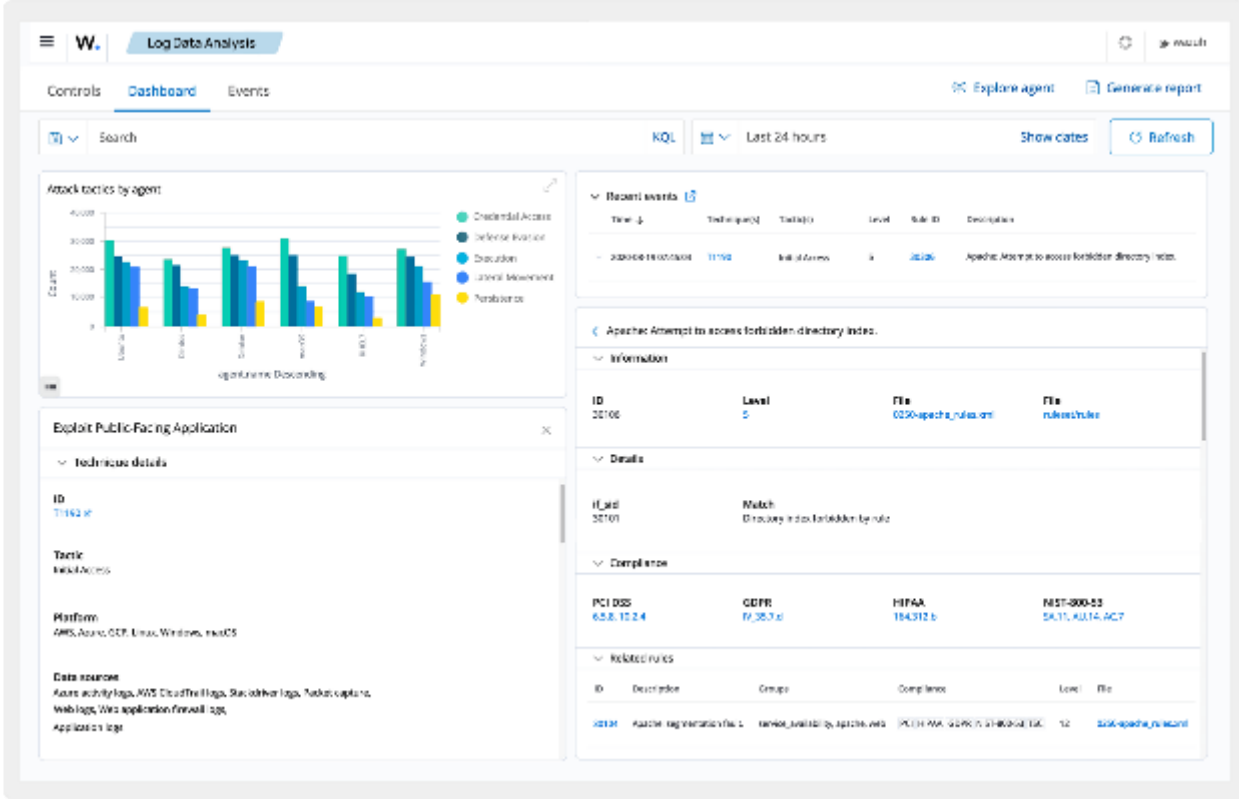
Threat Hunting

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.



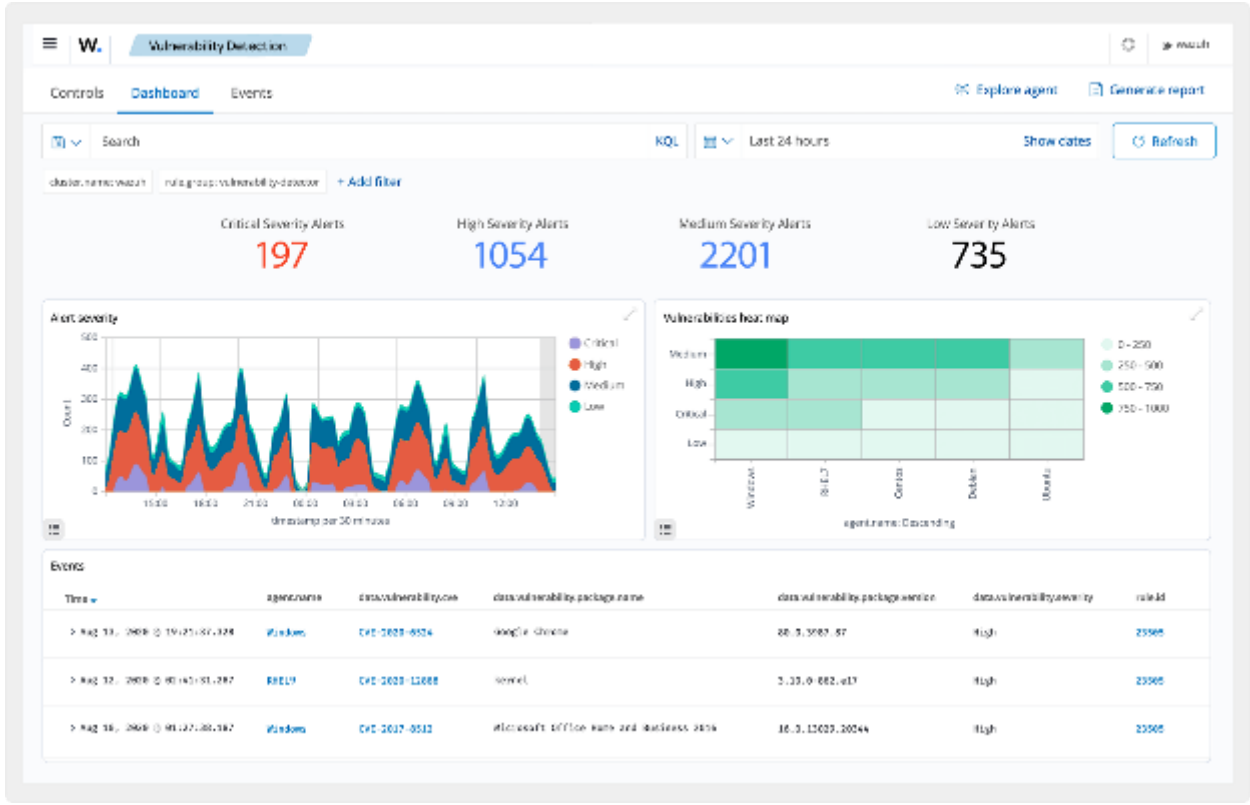
Log Data Analysis

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.



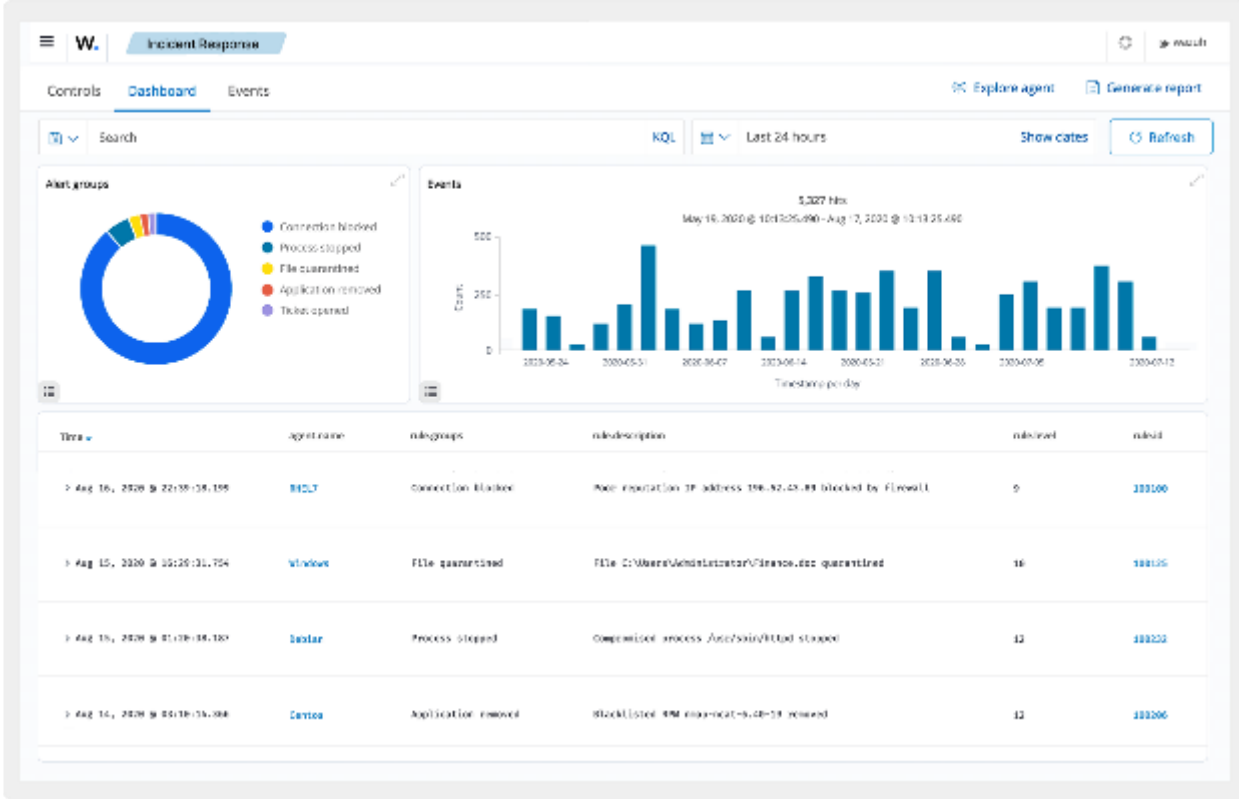
Vulnerability Detection

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.



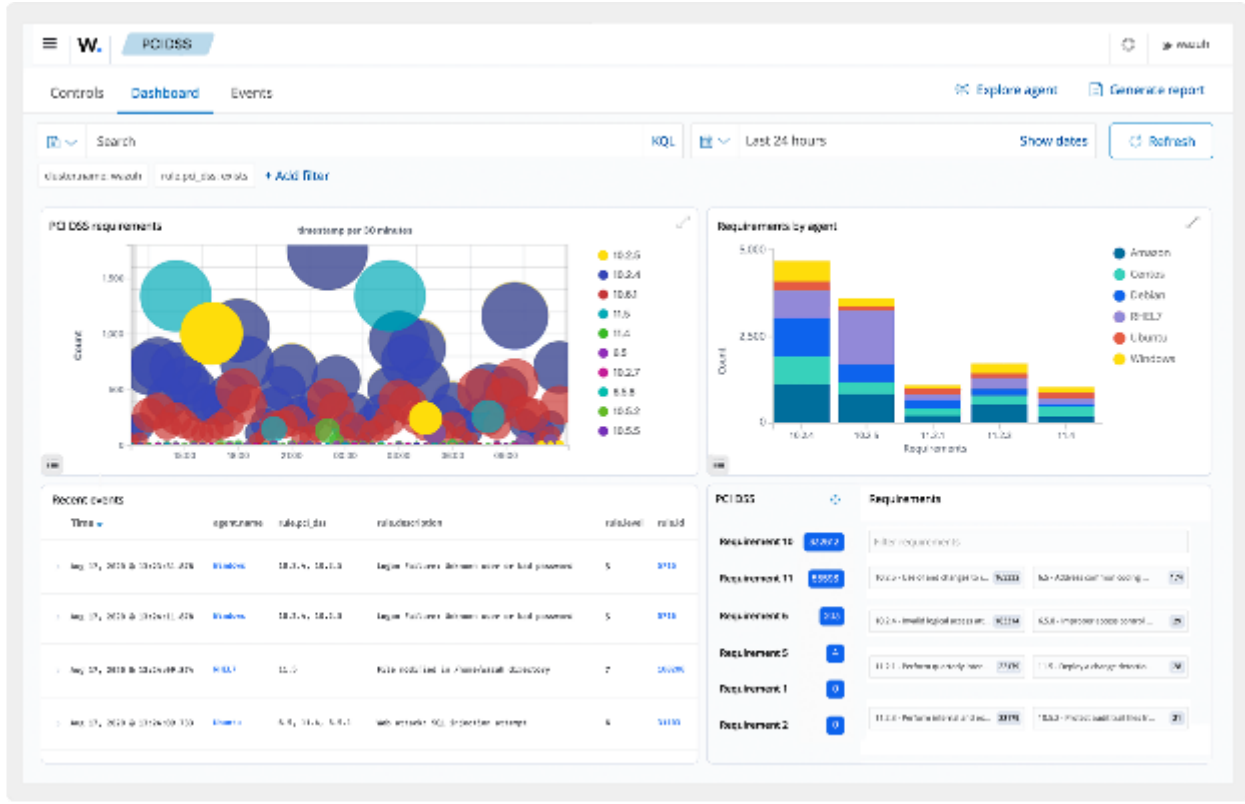
Incident Response

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.



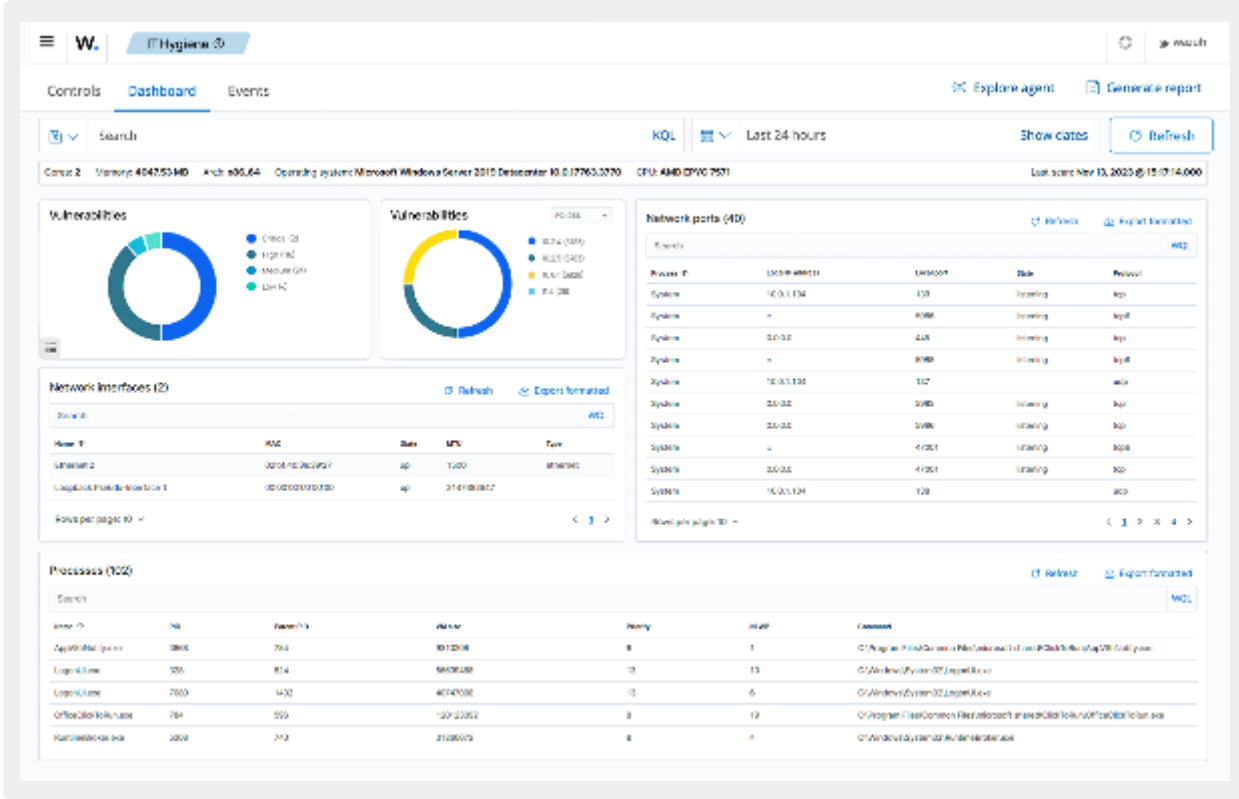
Regulatory Compliance

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.



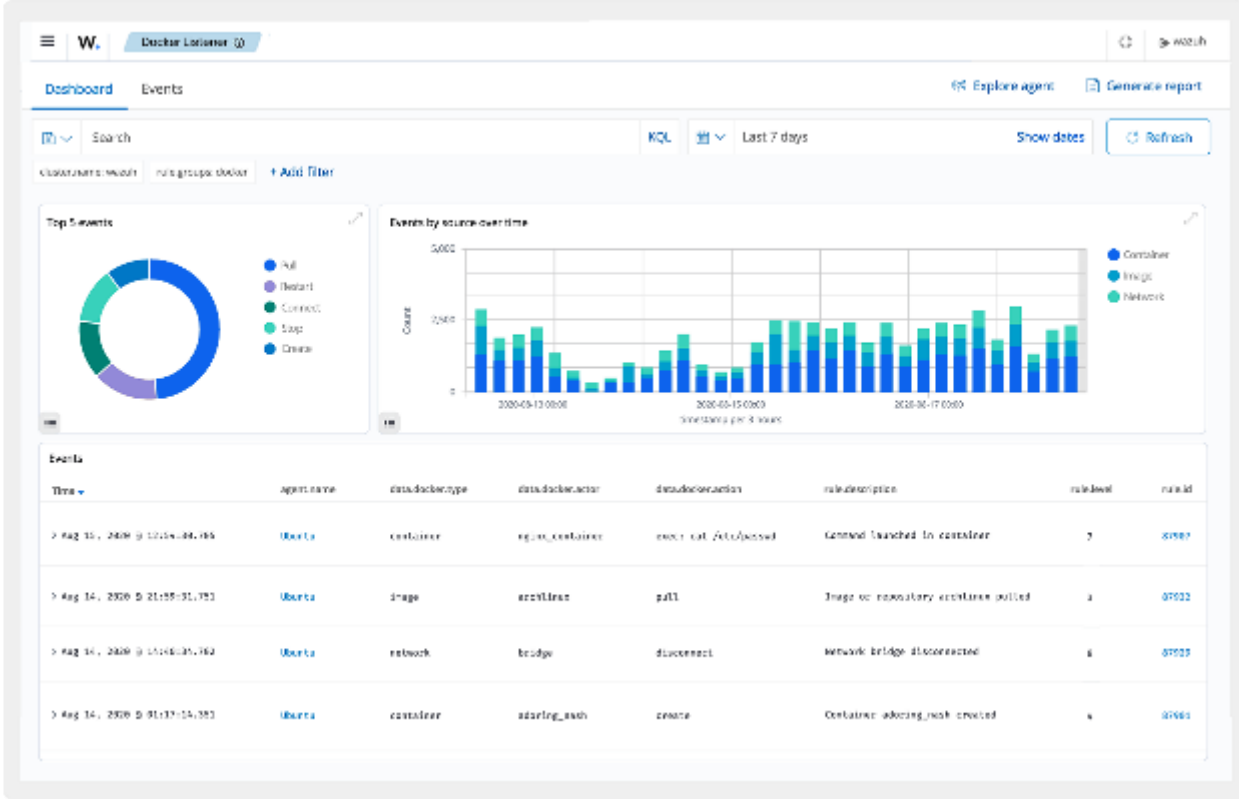
IT Hygiene

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.



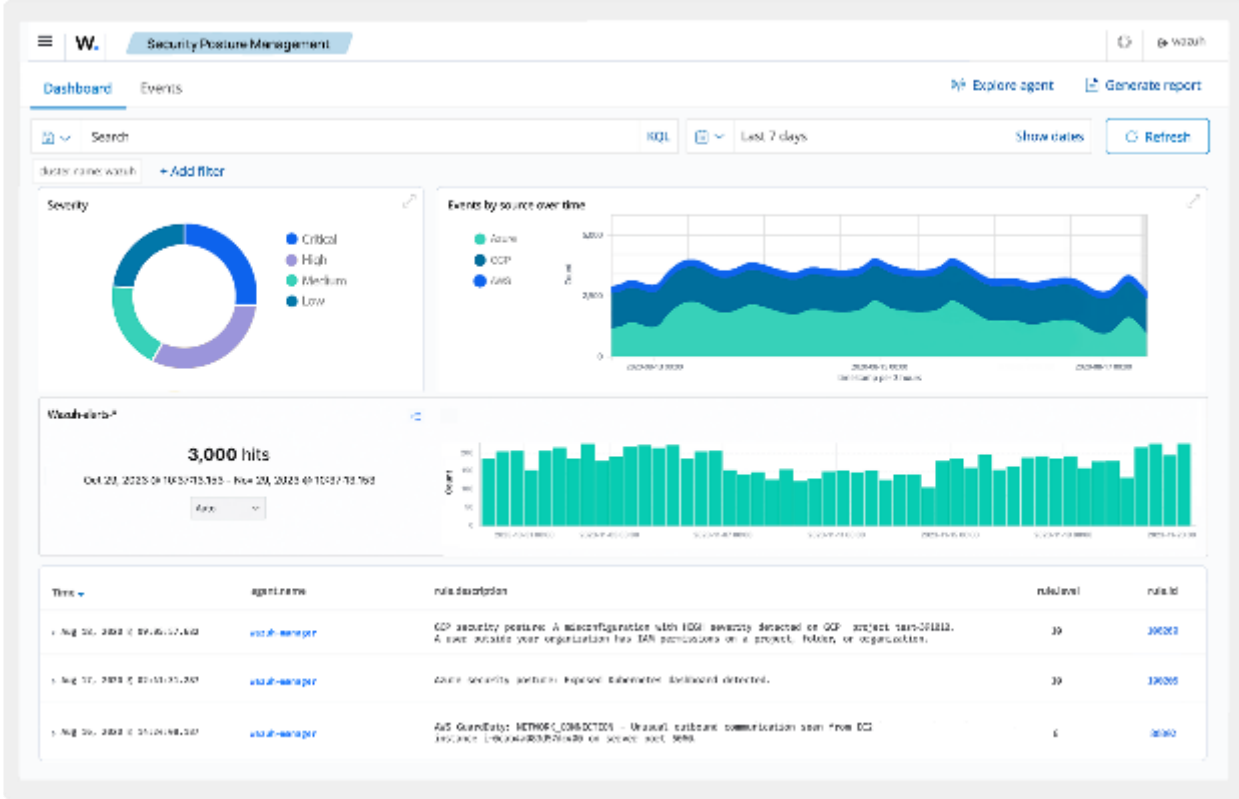
Containers Security

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.



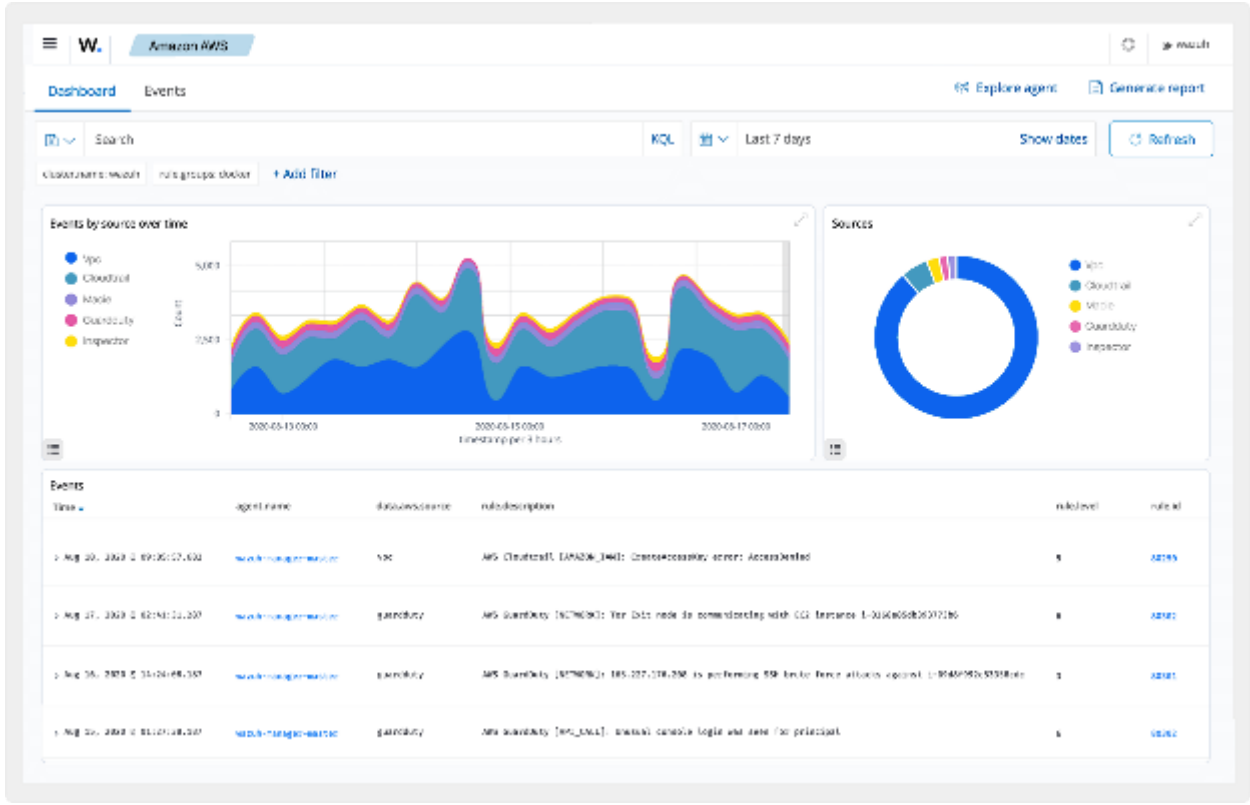
Posture Management

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.



Riepilogo

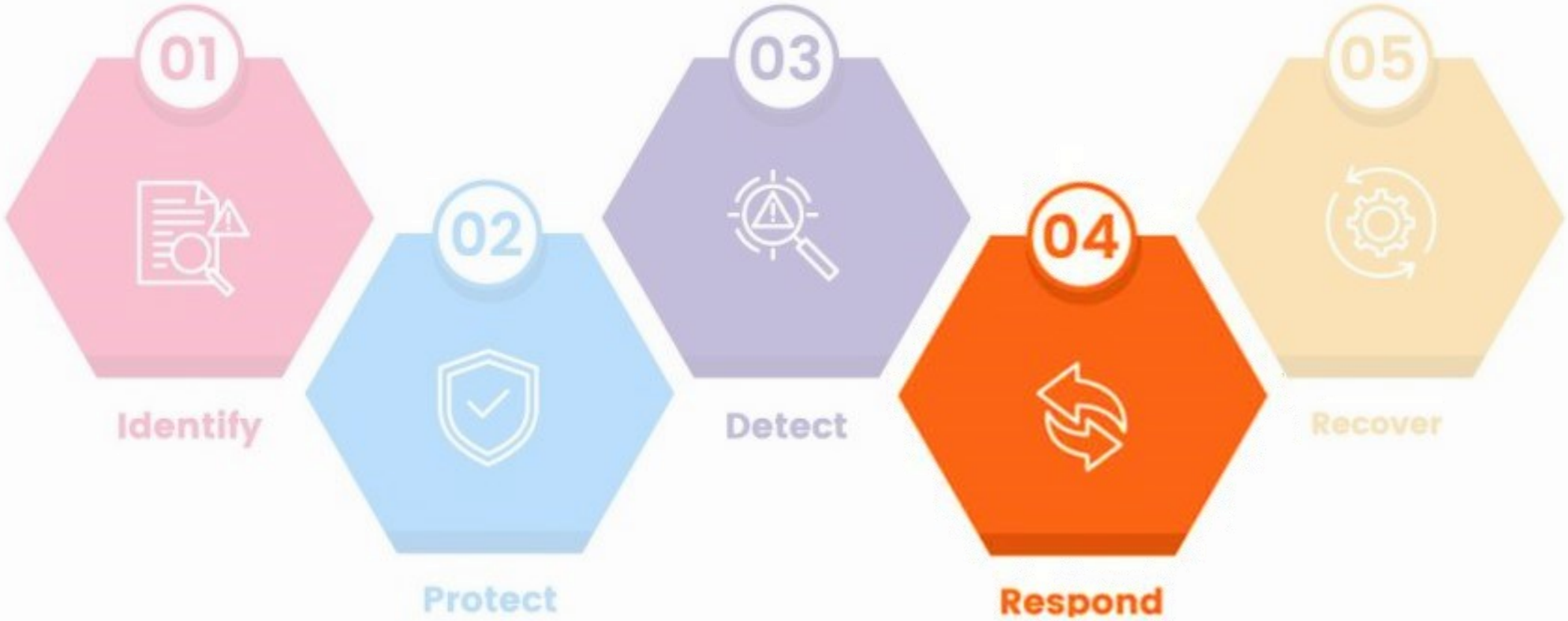
Il monitoraggio rappresenta un fattore abilitante per garantire la sicurezza dei sistemi in ambienti complessi, eterogenei, variabili e indefiniti.

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)

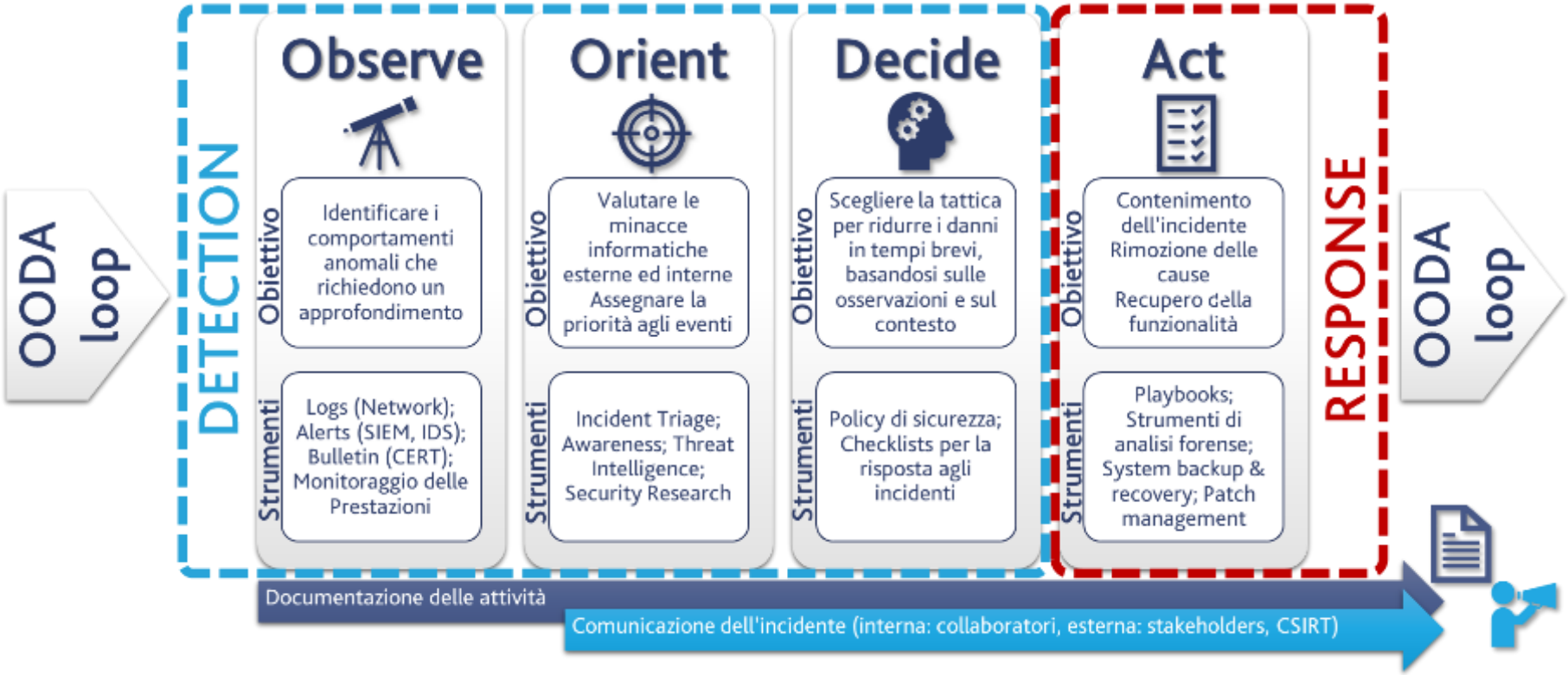
Obiettivo:

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

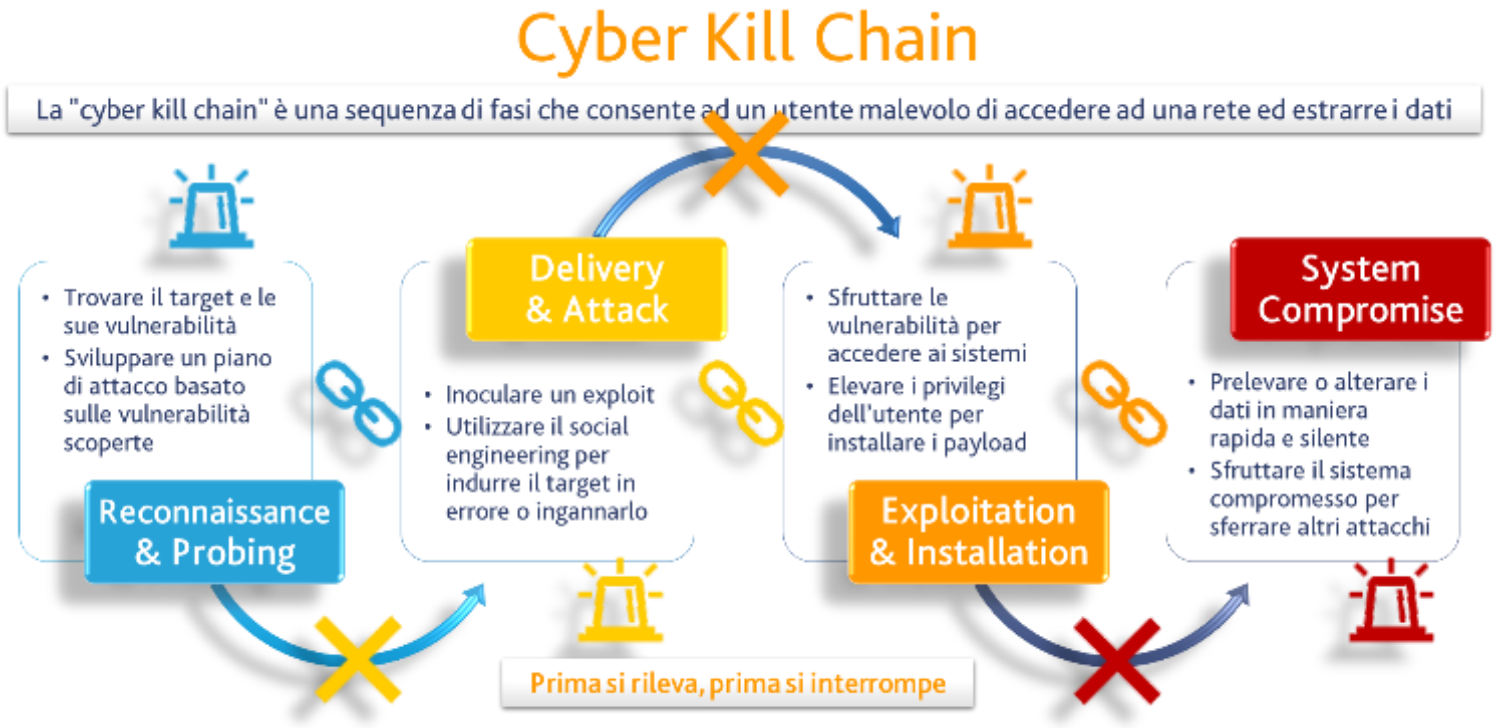
Attività
Contenere gli effetti degli incidenti
Eliminare gli effetti degli incidenti

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

Esempio di Detection & Response



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
Distributed 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
Distributed 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

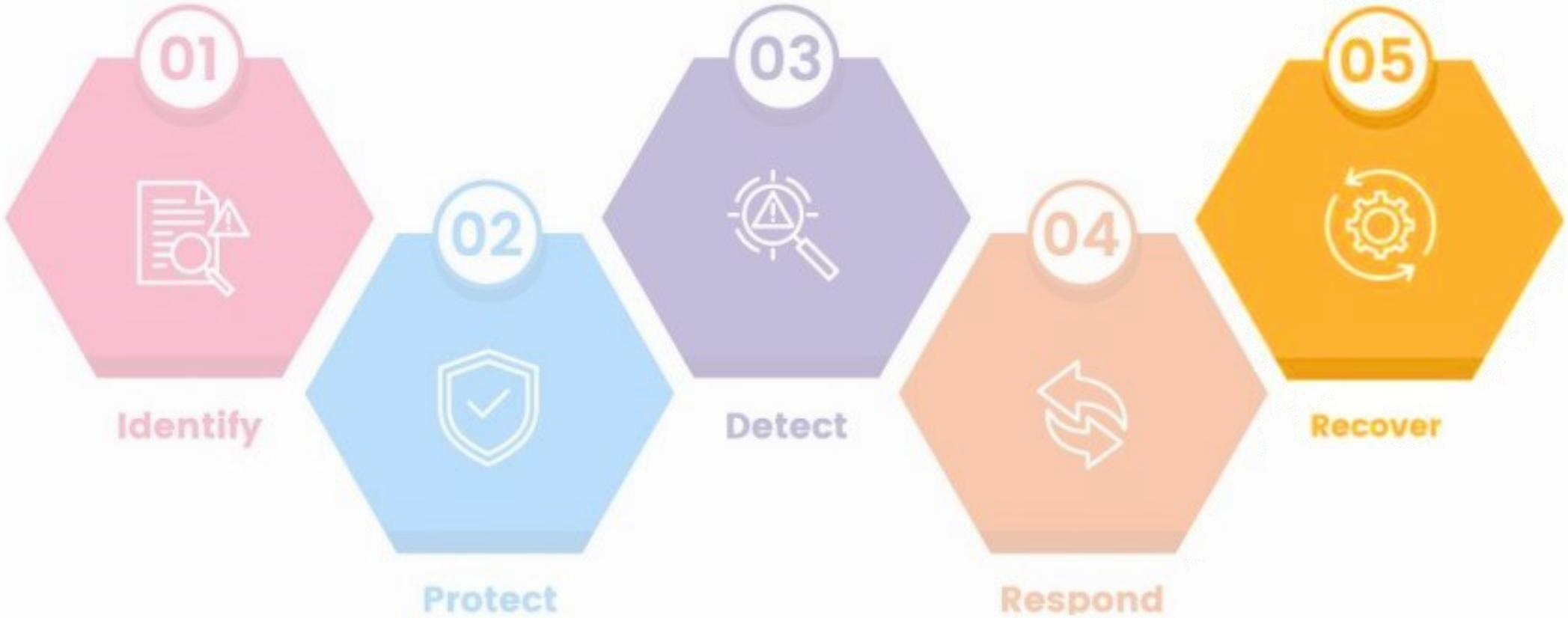

Indagare sull'incidente in maniera approfondita
Segnalare l'incidente agli stakeholder e alle agenzie governative
Realizzare una revisione del piano di incident response
Condividere e approfondire la lezione appresa

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)

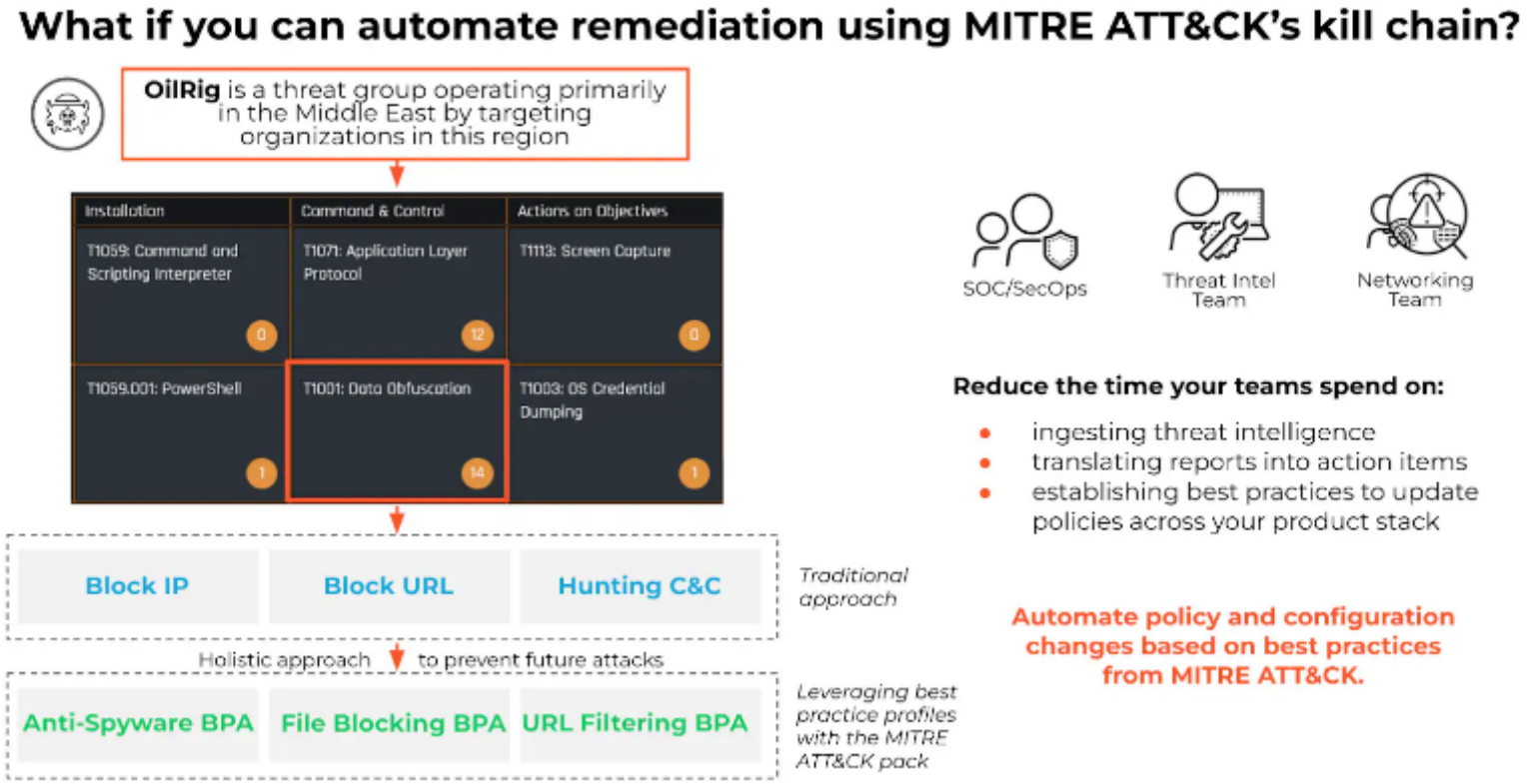
Obiettivo:

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 che in caso di incidente reale



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 metodolgie 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

Who am I?

Formazione

- Laureato in Ingegneria Informatica (Sapienza, Roma) e Sicurezza Informatica (Statale, Milano)
- Specializzato in Advanced Cybersecurity presso la School of Engineering - Stanford University
- Certificato in Cybersecurity Engineering e Digital Forensics presso il Software Engineering Institute - Carnegie Mellon University

Esperienza professionale

- Funzionario alla Sicurezza CIS presso il Ministero dell'Interno
- Professore a.c. di Tecnologie per la Sicurezza Informatica presso l'Università Mediterranea di RC
- Consulente in Sicurezza Informatica e Informatica Forense
- Ricercatore, trainer e autore di articoli e white paper sui temi della cybersecurity

LinkedIn vincenzocalabro.it