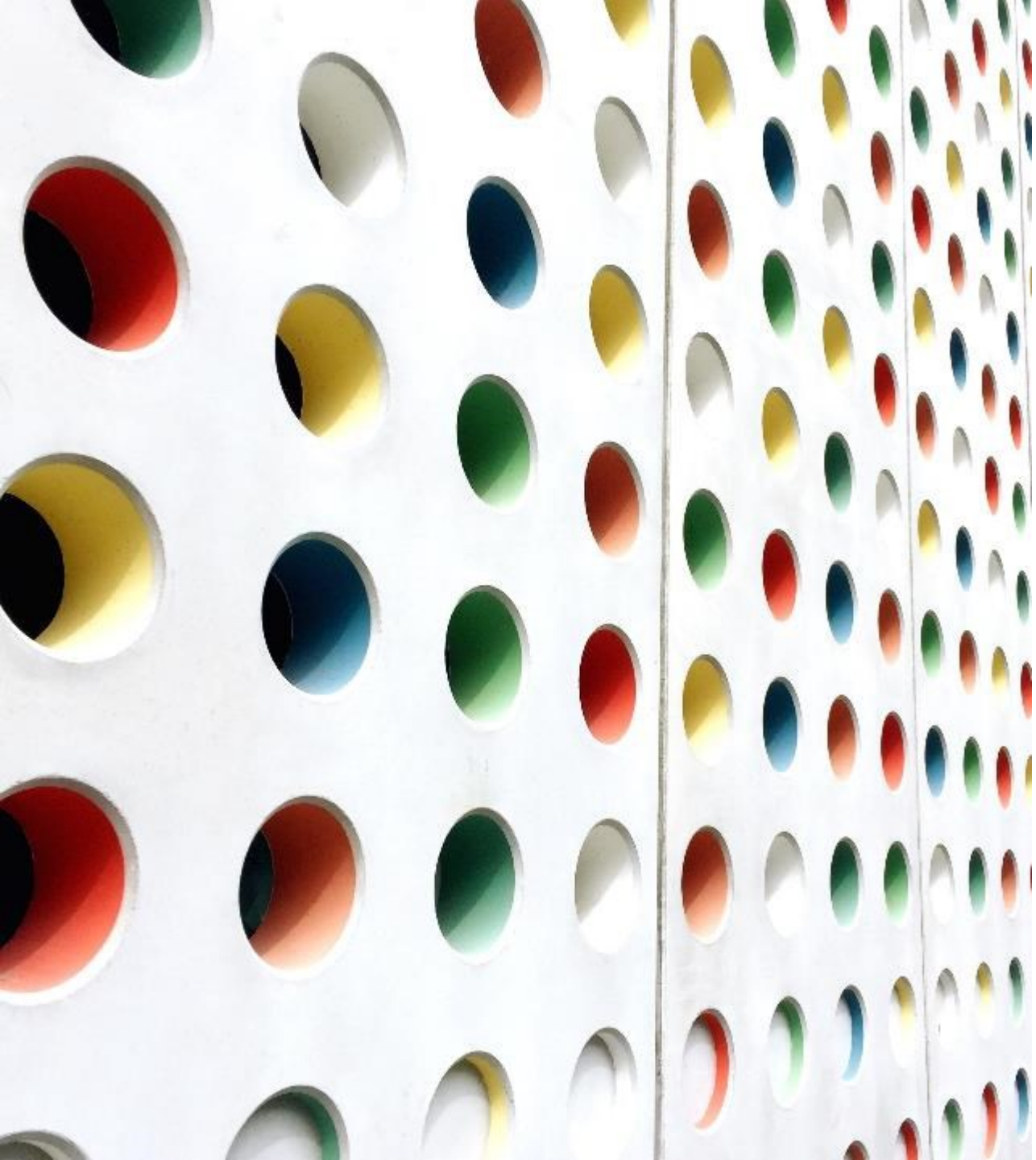


Tecnologie per la Sicurezza Informatica

Risk Assessment

VINCENZO CALABRÒ

Università degli Studi
Mediterranea
di Reggio Calabria

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. Tecnologie per la sicurezza informatica
4. Compliance normativa e regolatoria

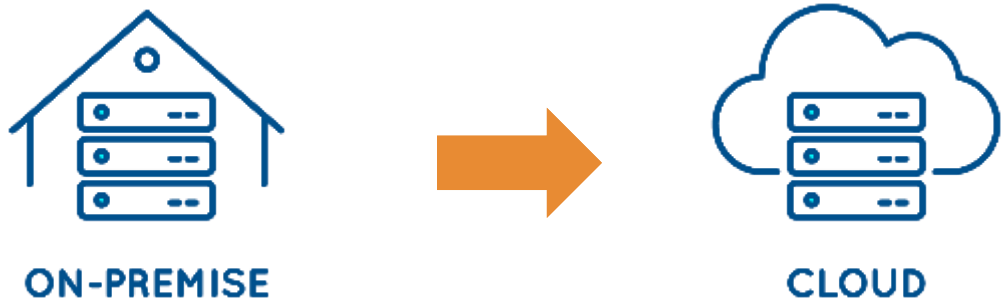
Premesse

- La maggior parte delle attività economiche, produttive, personali e sociali si svolgono con/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 assoluta 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

In sintesi



La sicurezza assoluta non è raggiungibile

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

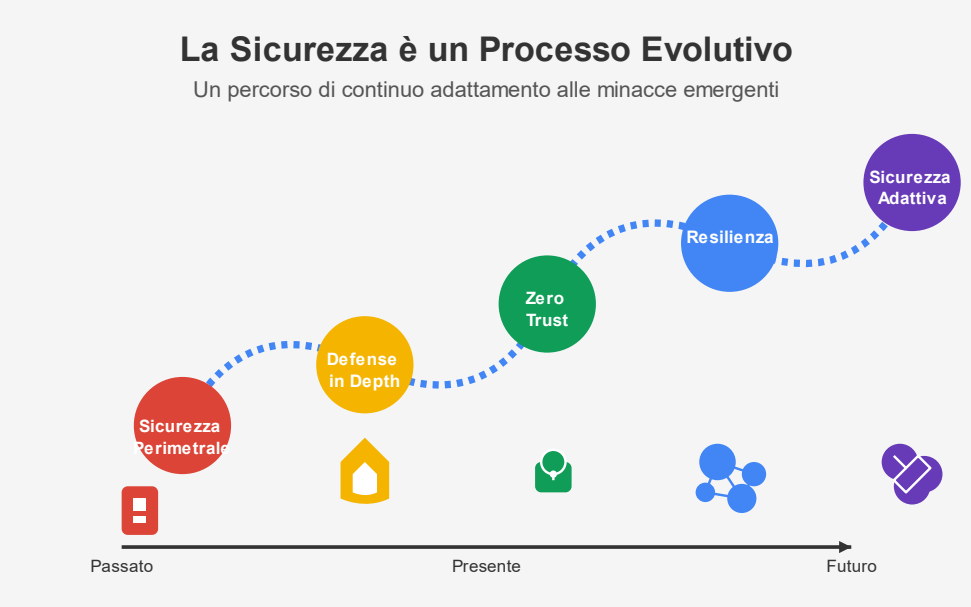
Inoltre, i costi di implementazione e gestione per una sicurezza generalizzata potrebbero risultare economicamente **svantaggiosi**

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

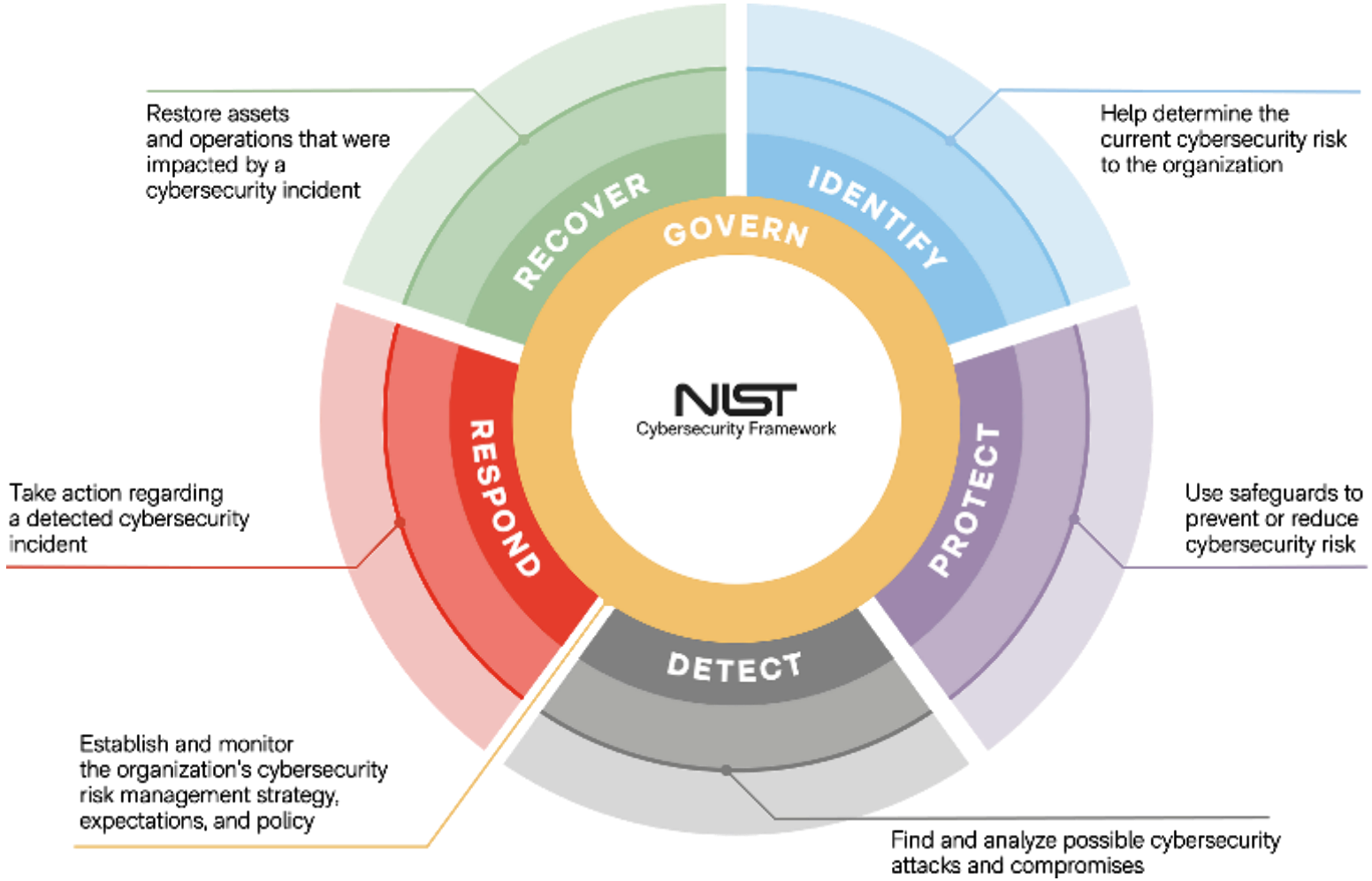
NIST Cybersecurity Framework

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 funzione dedicata alla Governance (Gestione), per la gestione del framework (iterativo) e il miglioramento continuo (evolutivo)



https://www.nist.gov/cybersecurity

Functions and Categories

L'ordine di elencazione rappresenta la sequenza ottimale per rendere operativa la gestione del rischio all'interno dell'organizzazione

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CIS Critical Security Controls

I CIS Critical Security Controls (CIS Controls) sono un'elencazione di best practice, raggruppate in **18 categorie**, che possono essere utilizzate per:

1. Implementare le misure di sicurezza *(no risk based)*
2. Verificare le misure di sicurezza applicate e rafforzare la postura di sicurezza informatica dell'organizzazione

https://www.cisecurity.org/

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

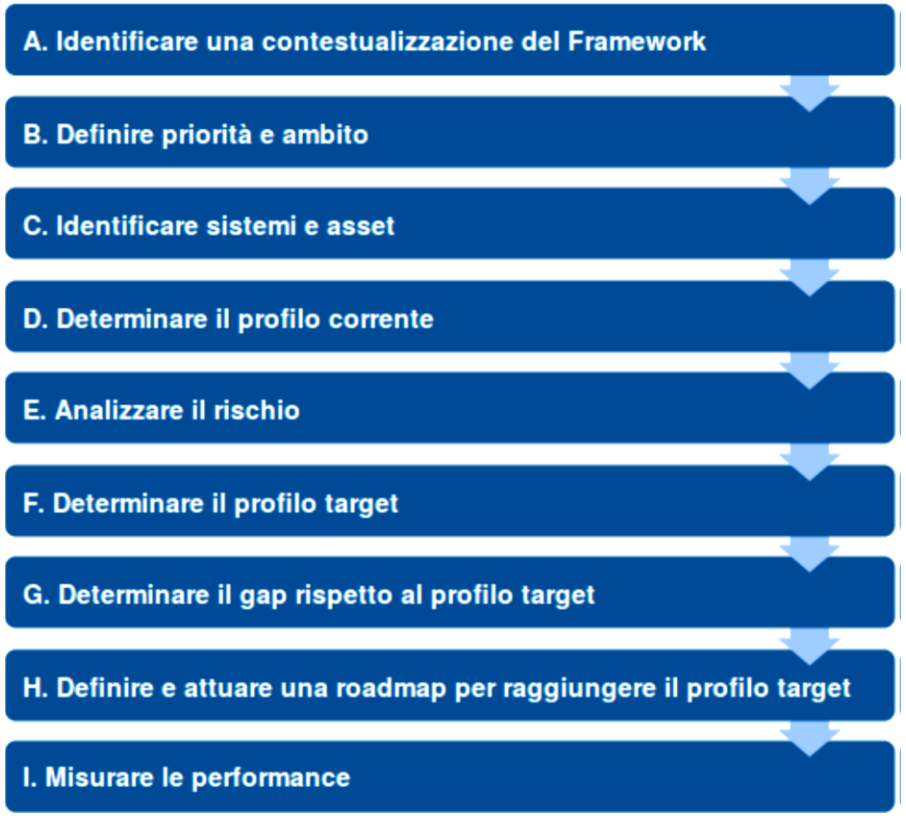
Livello 4 Adattivo

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.

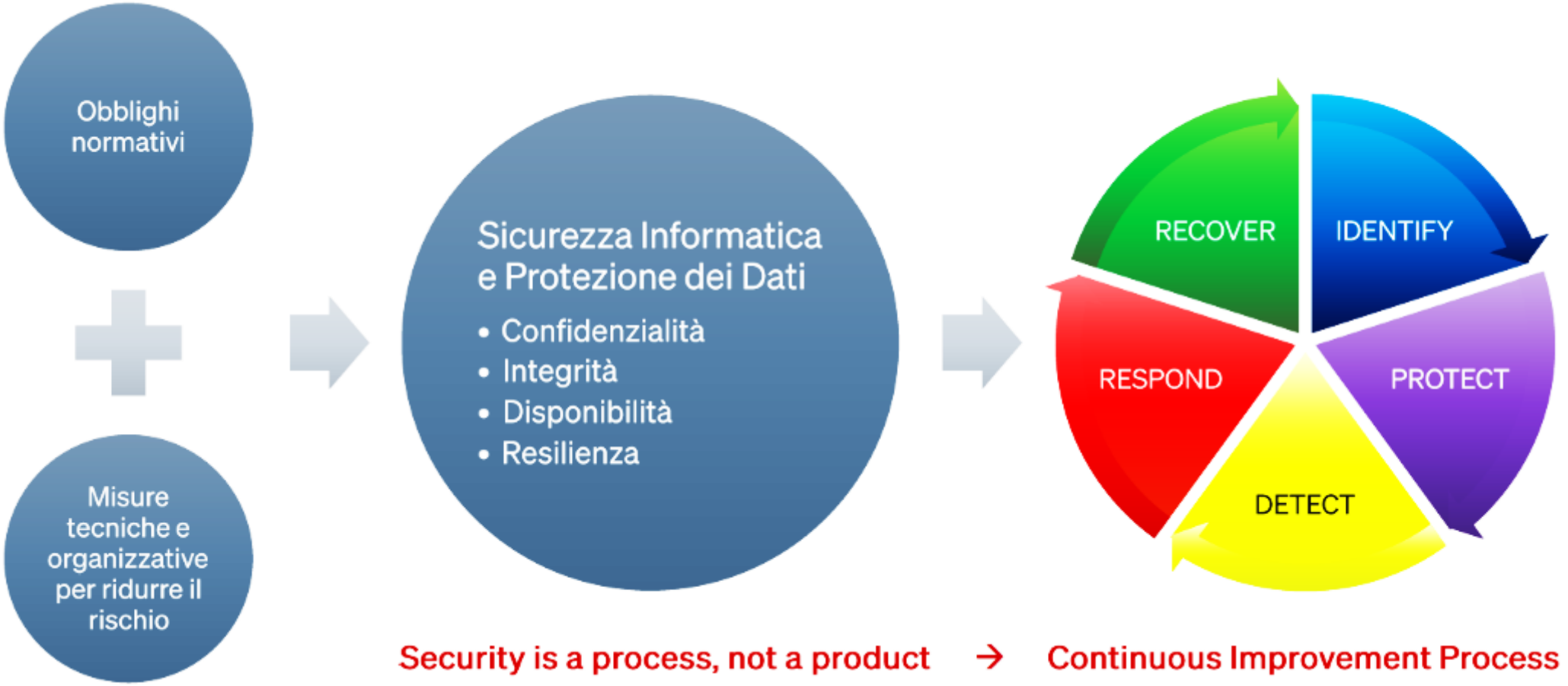
Applicazione del Framework

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

- Migliorare o definire un programma di cybersecurity strutturato e integrato
- Determinare il profilo di cyber maturità corrente e target atteso
- Agevolare e semplificare 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
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
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 incentrate 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**.

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.

Identify / Identificare (ID)

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

Asset Management (ID.AM)

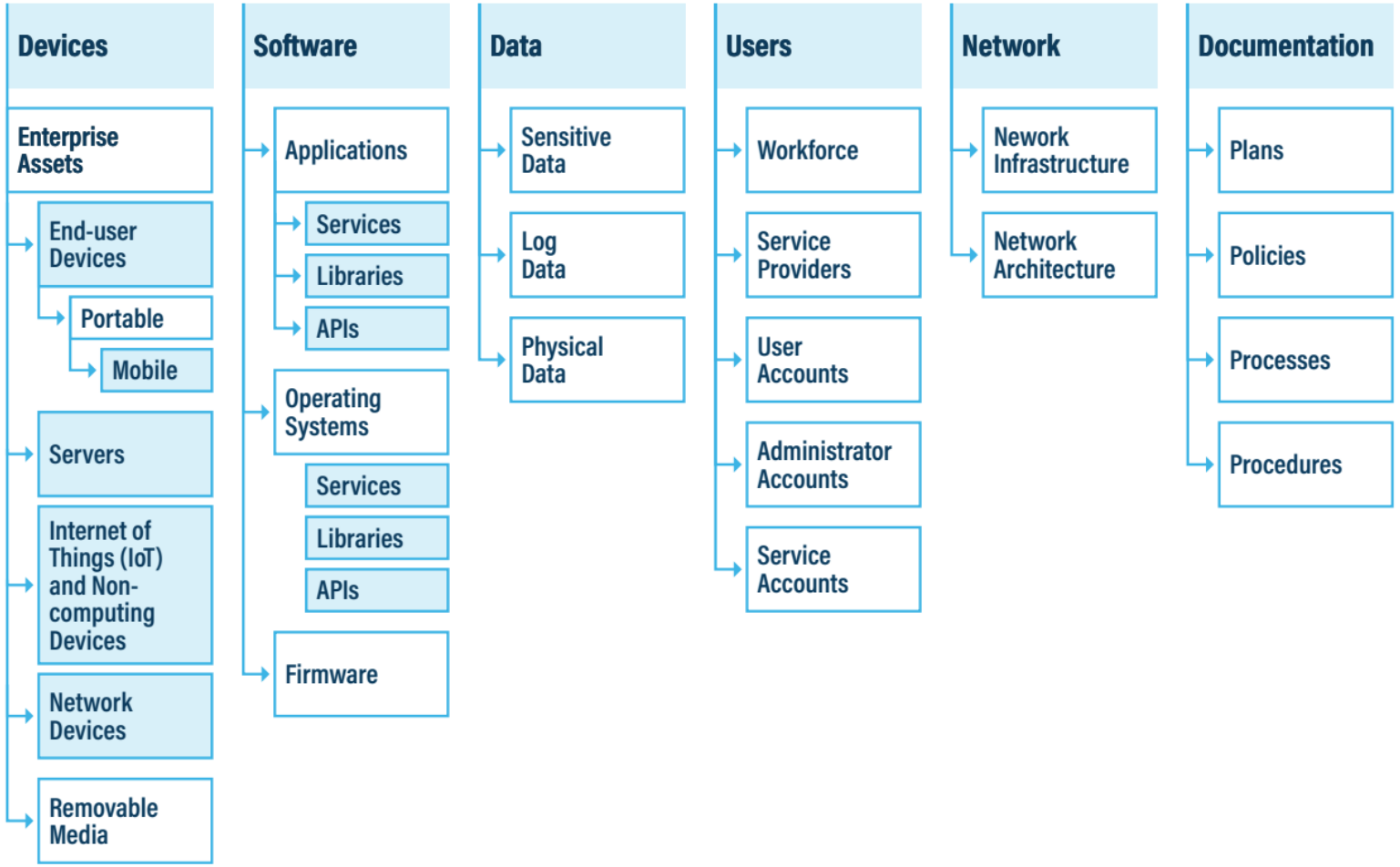
Obiettivo:

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)

Tipi di Asset

Identificare e gestire, per l'intero ciclo di vita, le risorse che consentono all'organizzazione di raggiungere gli scopi aziendali in coerenza con la priorità rispetto agli obiettivi e alla strategia di rischio dell'organizzazione stessa



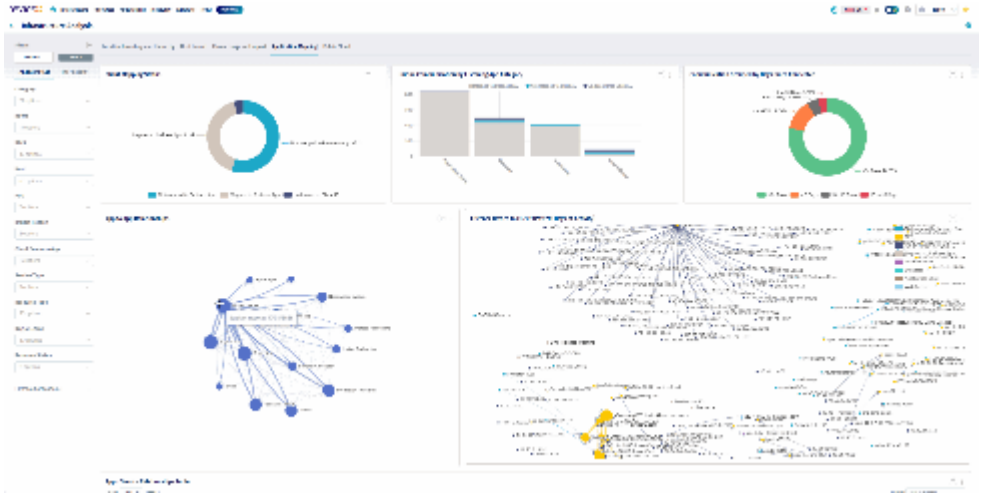
Tool di Asset Management (ITAM)

E' fondamentale indicare:

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

Esempi:

- Snipe-it
- Spiceworks
- Device42
- Asset Management System Microsoft



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

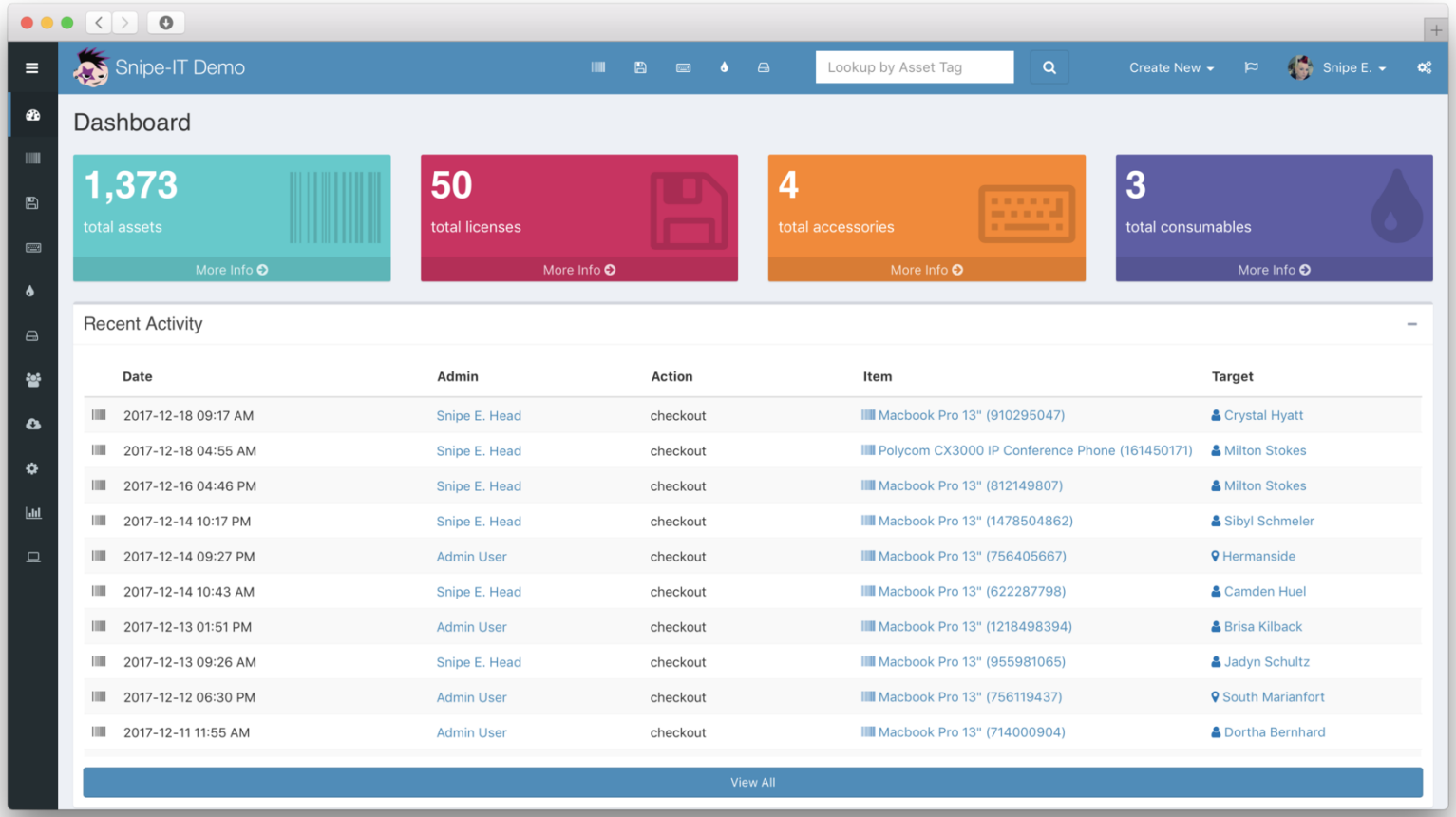
Esempio di implementazione

Asset Management

SNIPE-IT

Asset inventory, consente la gestione dell'intero ciclo di vita degli asset:

- Hosts
- Licenses
- Accessories
- Consumables
- Componentes
- People



Esercitazione SNIPE-IT

- Installare Virtual Box (configurare Rete con NAT)
- Scaricare l'ultima release da https://snipeitapp.com/
- Fare il deployment dell'app su XAMPP
- Avviare SNIPE-IT
- Avviare browser su altra macchina (p.e. Kali linux)
- Collegarsi a https://ip_snipe-it
- N.b. Per VM SNIPE-IT già pronta le credenziali sono: [admin / Change_this1]
- Effettuare una simulazione

Greenbone OpenVAS

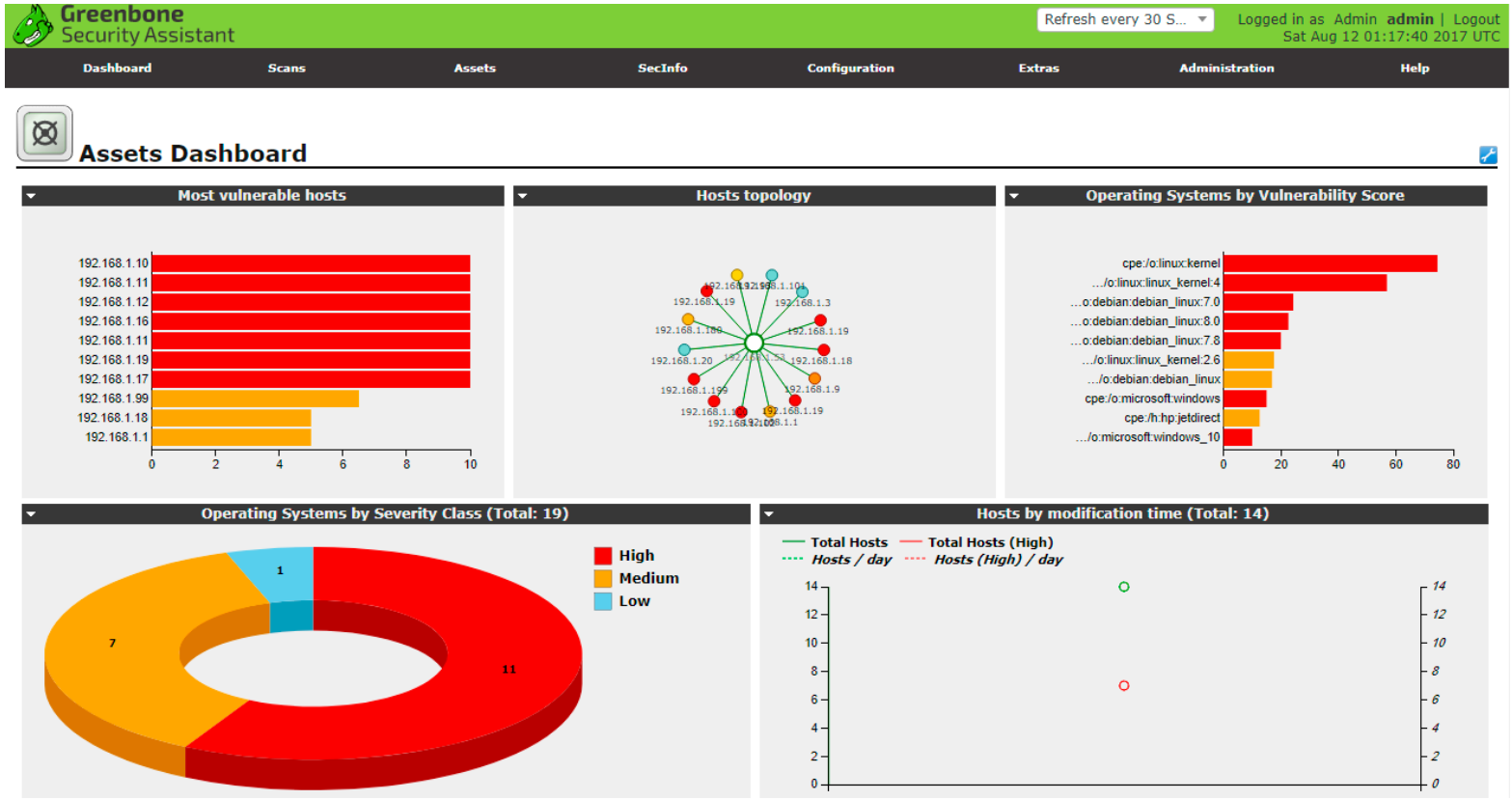
Open Vulnerability Assessment Scanner

Esempio di implementazione

Asset Management

OpenVAS

Vulnerability scanner, consente di individuare gli host di una rete e le vulnerabilità dei software installati confrontandoli con gli elenchi CVE



Esercitazione OpenVAS

- Installare Virtual Box (configurare Rete con NAT)
- Scaricare l'ultima release FREE in formato OVA
- Importare la VM in Virtual Box
- Entrare da console con credenziali [User name: admin | Password: admin]
- Creare un nuovo utente web (da console)
- Accedere via web con un altra VM (p.e. Kali linux) sulla stessa Rete
- Effettuare un assessment di prova sulla subnet configurata

Risk Assessment (ID.RA)

Obiettivo:

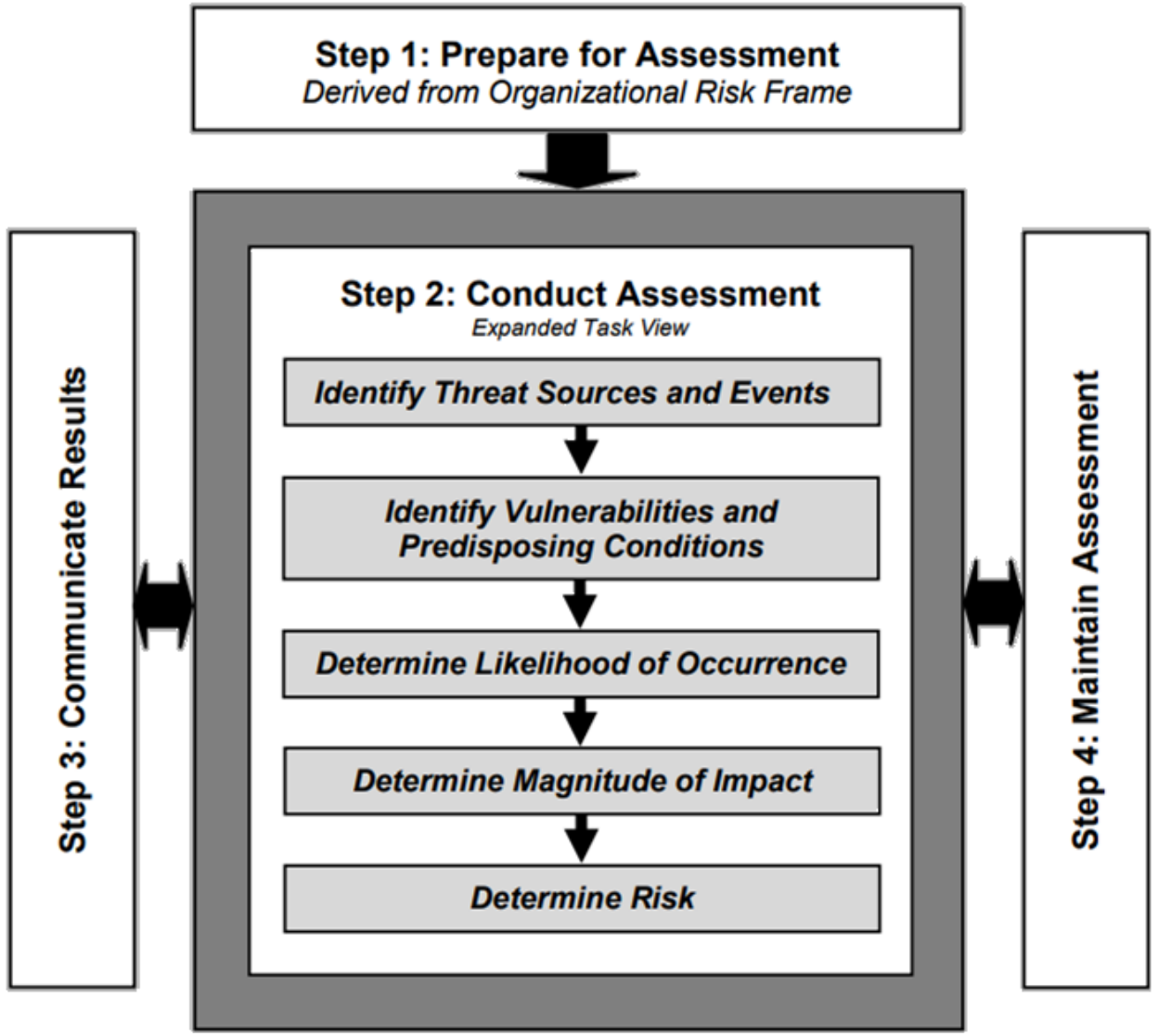
Comprendere il grado di rischio di cybersecurity per l'organizzazione, gli asset e le persone

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

Processo di cybersecurity risk assessment

É un processo che consente di valutare i rischi cyber che incombono sull'organizzazione.

Si tratta di un processo evolutivo, perché le variabili (sorgenti, minacce, vulnerabilità, probabilità di accadimento, impatto) possono variare nel tempo e, pertanto, occorre rivalutarle periodicamente.



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 dallo sfruttamento della vulnerabilità da parte della minaccia in termini di: danno alla confidenzialità, integrità e disponibilità dei dati, danni finanziari e reputazionale, impatti operativi e sulla mission

Si raccomanda di adottare 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 maniera sistematica e coerente

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

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

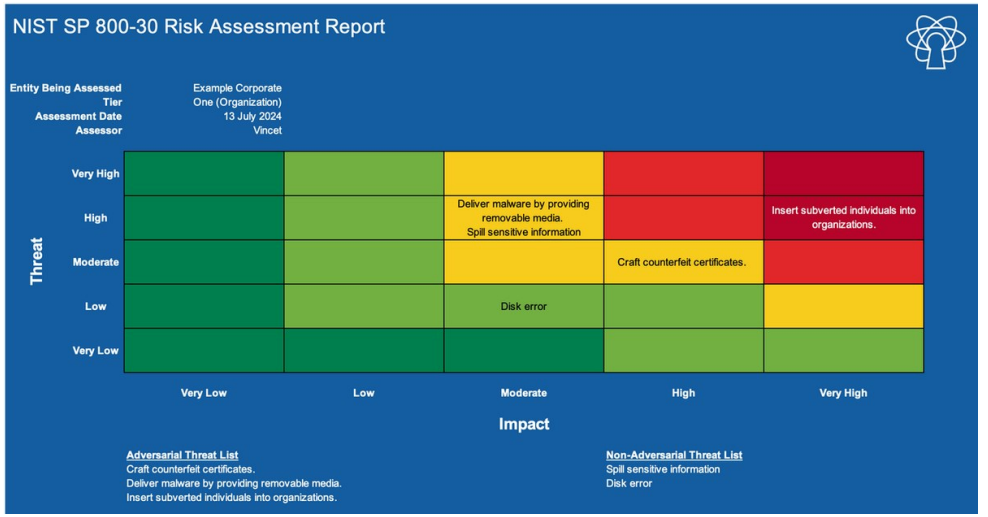
NON MALEVOLI:

- 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

Esempio di calcolo del rischio (NIST RMF)

Il NIST ha predisposto una guida per condurre un risk assesment (NIST SP 800-30 https://csrc.nist.gov/projects/risk-management/) che si sviluppa nei seguenti passi:

1. Identificare le fonti di minaccia
2. Identificare gli eventi avversi
3. Identificare le vulnerabilità
4. Determinare la probabilità
5. Determinare gli impatti negativi
6. Determinare i rischi per la sicurezza delle informazioni



NIST SP 800-30 Risk Assessment Template

Esercitazione NIST RMF

Leggere il **NIST Special Publication 800-30** per comprendere la tassonomia utilizzata per:

1. THREAT SOURCES
2. THREAT EVENTS
3. VULNERABILITIES AND PREDISPOSING CONDITIONS
4. LIKELIHOOD OF OCCURRENCE
5. IMPACT
6. RISK DETERMINATION

Determinare il rischio utilizzando il foglio di calcolo **NIST-800-30-Risk-Assessment-Template**

MITRE ATT&CK

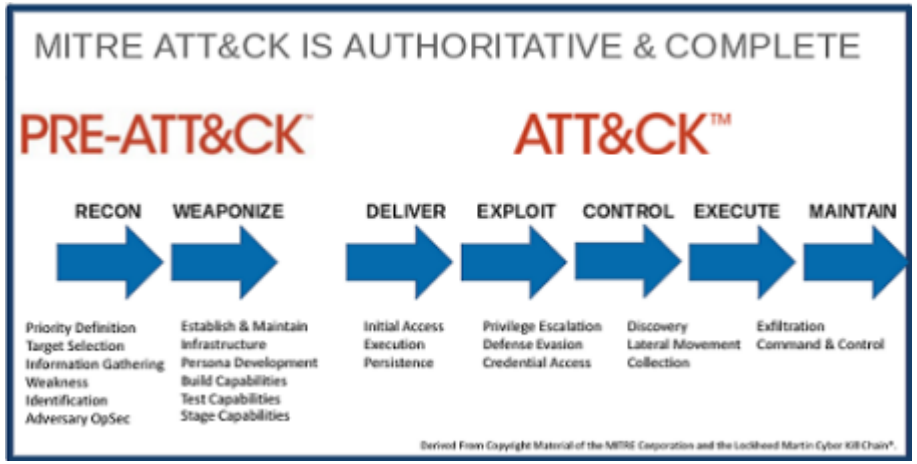
MITRE ATT&CK (*Adversarial Tactics, Techniques and Common Knowledge*) è una risorsa di tattiche e tecniche di attacco basate su osservazioni del mondo reale

- 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 framework sono utilizzate per sviluppare i modelli e le 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

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

Esempio di calcolo del rischio (ISO 27001)

Il Tool VERA "Very Easy Risk Assessment"
di Cesare Gallotti (www.cesaregallotti.it)
è una metodologia che permette di condurre risk assesment con un foglio Excel in cui sono riportate le istruzioni e le formule per il calcolo del livello di rischio, nonché i modelli per redigere il piano di trattamento del rischio e per documentare quelli accettati

		Treath	Business data alteration by malicious user	Malicious software	Bomb attack and use of arms
		Probability	3	3	1
		Parameters	CIA	CIA	A
		Inherent Risk	2,00	2,00	1,00
A.6.2.1 Identification of risks related to external parties	3		X	X	
A.6.2.2 Addressing security when dealing with customers	2		X	X	X
A.7.2.2 Information labelling and handling	1		X		X

Individuare le vulnerabilità

Ecco alcuni dei principali metodi per individuare le vulnerabilità in ambito 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

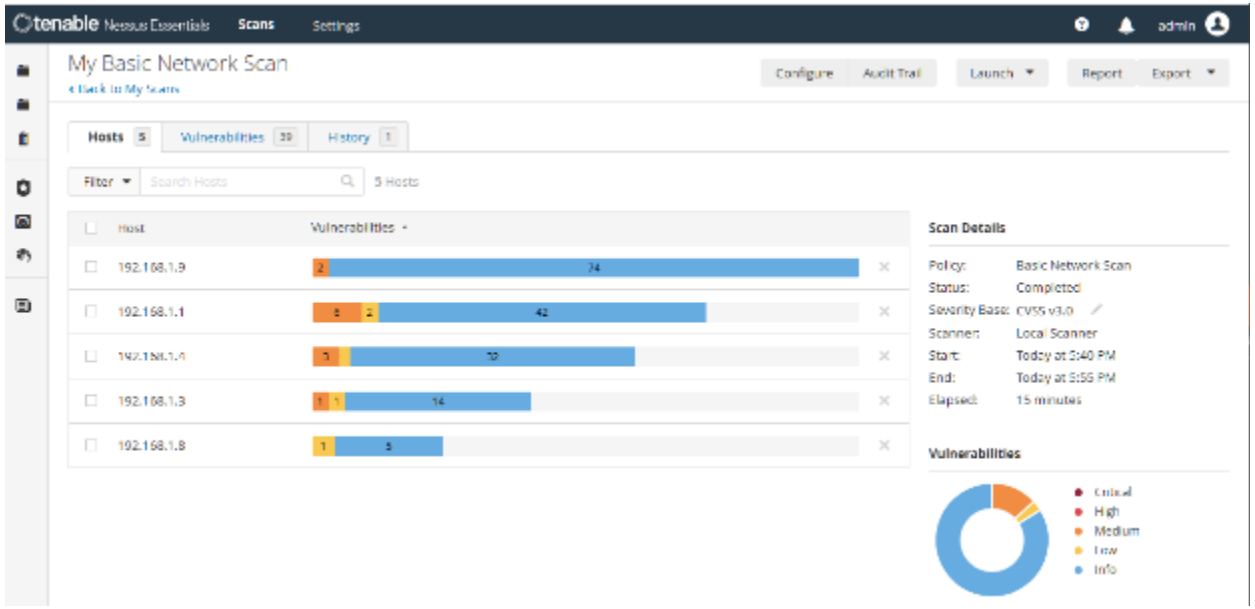
Vulnerability Assessment

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

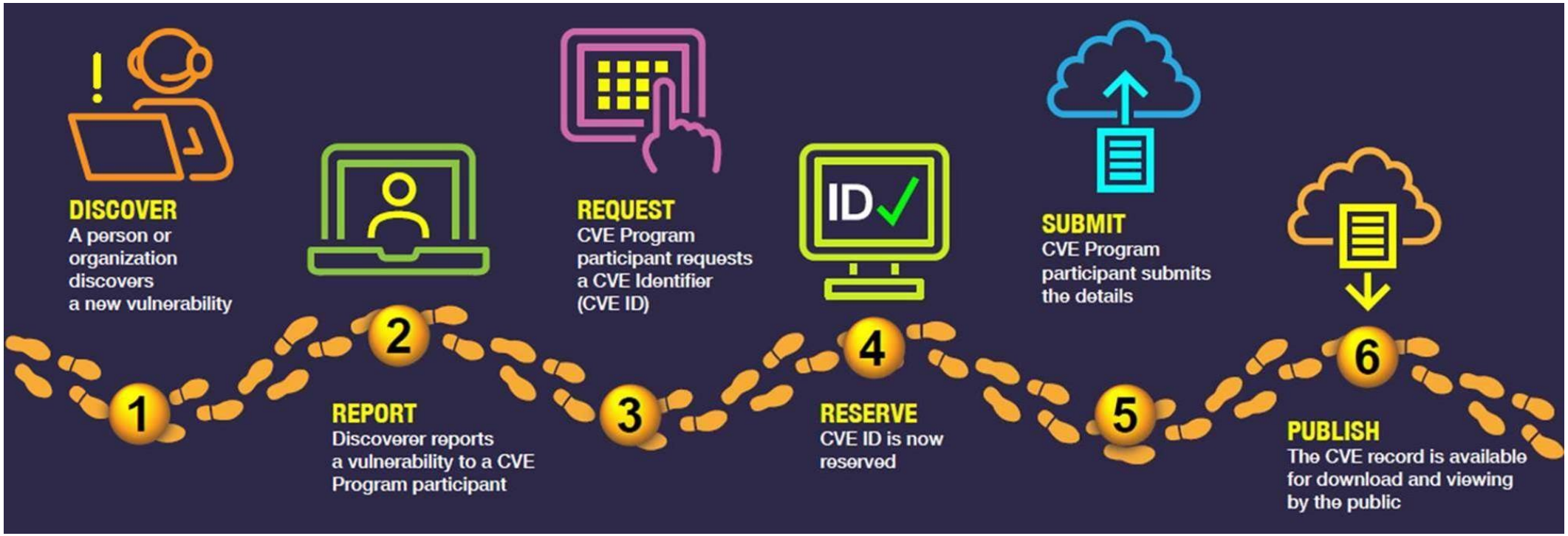


Esercitazione NESSUS

- Installare Virtual Box (configurare Rete con NAT)
- Scaricare l'ultima release **Nessus Essentials for education** in formato OVA
- Chiedere **Activation Code** https://www.tenable.com/tenable-for-education/nessus-essentials
- Importare la VM in Virtual Box
- Attivare la licenza
- Effettuare un testing sulla rete (aggiungere qualche altra macchina virtuale)

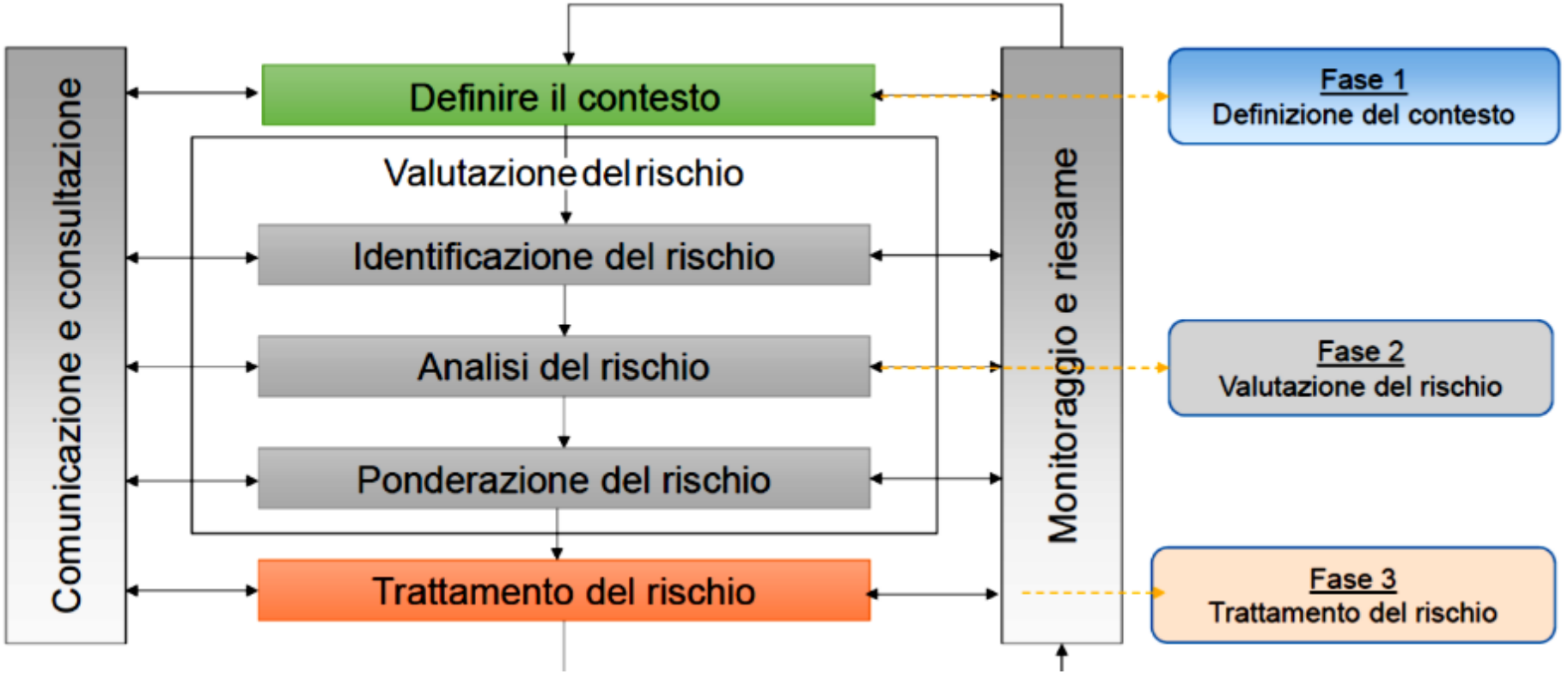
Common Vulnerabilities and Exposures www.cve.org

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

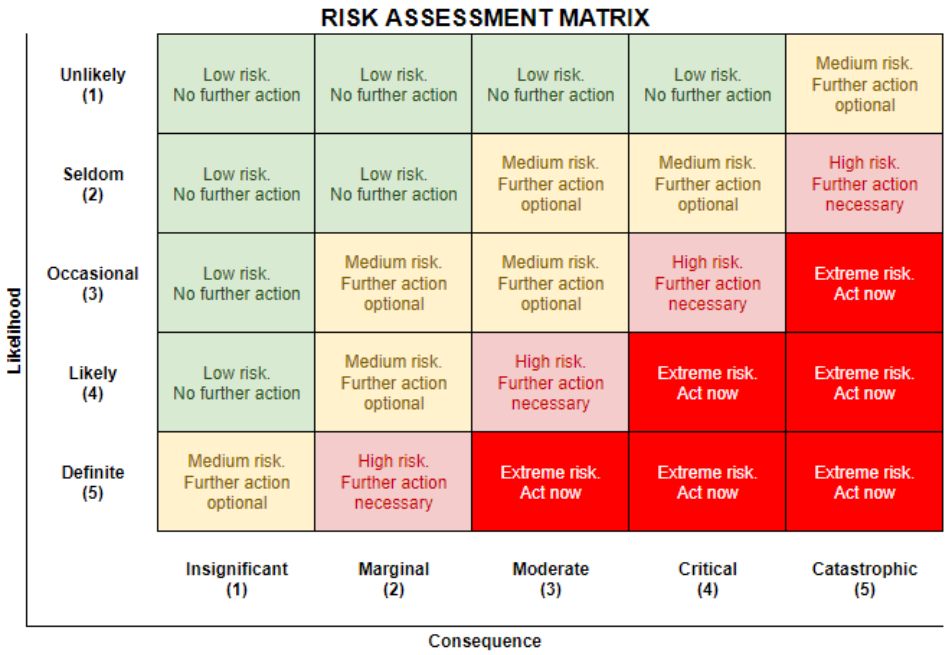


CVE Record Lifecycle

Metodo di cybersecurity risk management



Metodo di trattamento del rischio



Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure — Overheating in server room. **High**	Air conditioning systems 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

Trattamento del rischio

Il risk assessment ci fornisce l'elenco dei rischi residui come possiamo trattare in quattro modi:

1. **Accettazione**: implementazione di misure idonee a contenere le minacce
2. **Monitoraggio**: implementazione di misure adatte a controllare lo stato delle minacce
3. **Reazione**: sviluppare procedure per rispondere qualora il rischio residuo si concretizzi
4. **Trasferimento**: spostare il rischio residuo all'esterno (assicurazione)

Improvement / Miglioramento (ID.IM)

Obiettivo:

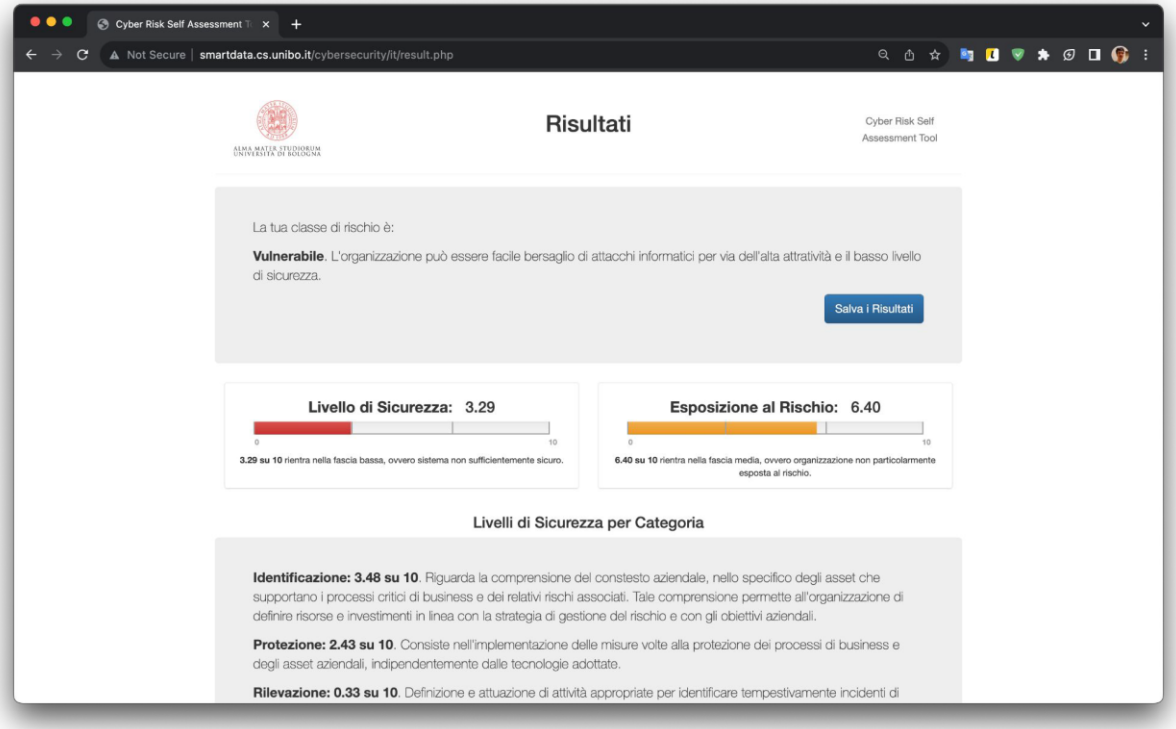
Identificare i miglioramenti apportati ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity in tutte le funzioni aziendali

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

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



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

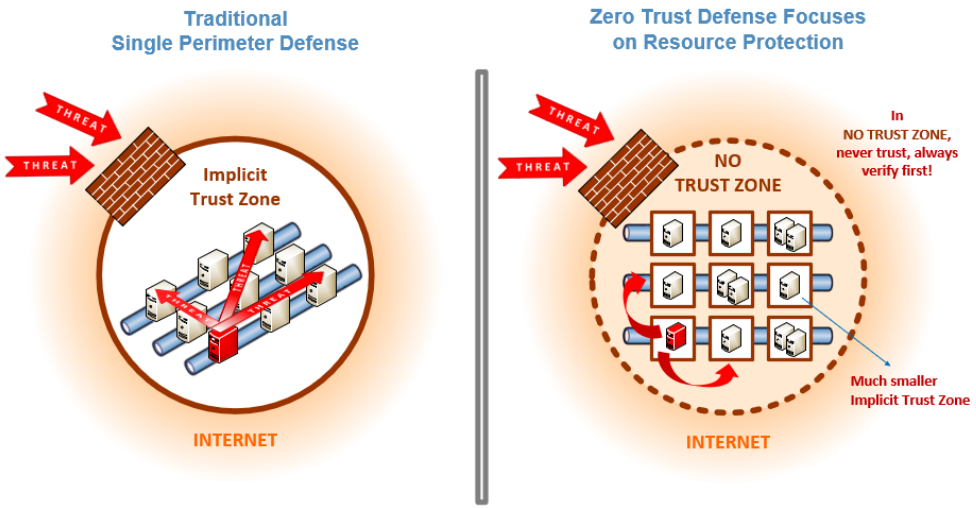
Negli ambienti tradizionali (on-premise) **l'autenticazione utente è affidata alle credenziali di accesso** e, raramente, è effettuata una profilazione che associ i permessi di accesso alle risorse (dati o funzioni) per cui l'utente è effettivamente autorizzato

Con l'avvento delle tecnologie mobile e del 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**

Modelli di autenticazione:

- **Definire regole sull'utilizzo delle identità**: utilizzare credenziali codificate, password complesse e a tempo
- **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

Il paradigma di sicurezza "*Zero Trust*"



È un approccio che sovverte la tradizionale fiducia all'interno delle reti perimetrali "castle-and-moat«. Invece di presumere che tutto ciò che si trova all'interno del perimetro di rete sia sicuro, Zero Trust opera con il principio fondamentale:
«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)

Zero Trust: definizioni

Contesto storico

- Evoluzione rispetto al modello tradizionale perimetrale "castle-and-moat«
- Concetto introdotto da John Kindervag di Forrester Research nel 2010
- Adozione accelerata con la diffusione del cloud computing e il lavoro remoto

Principi fondamentali

- "Mai fidarsi, sempre verificare«
- Ogni richiesta deve essere autenticata e autorizzata indipendentemente dalla provenienza
- Considera tutti gli accessi potenzialmente ostili
- Principio del privilegio minimo
- Fornire accesso solo alle risorse necessarie per svolgere specifiche funzioni
- Limitare l'accesso nel tempo (just-in-time access)
- Verifica continua
- Monitoraggio e validazione costante di tutti gli accessi
- Riautenticazione periodica durante le sessioni attive

Zero Trust: architettura

COMPONENTI CHIAVE

- Gestione delle identità e degli accessi (IAM)
- Micro-segmentazione della rete
- Data protection
- Rilevamento e risposta alle minacce
- Analytics e monitoraggio

MODELLO A PIÙ LIVELLI

- Identità
- Dispositivi
- Rete
- Applicazioni
- Dati

Zero Trust: implementazione pratica

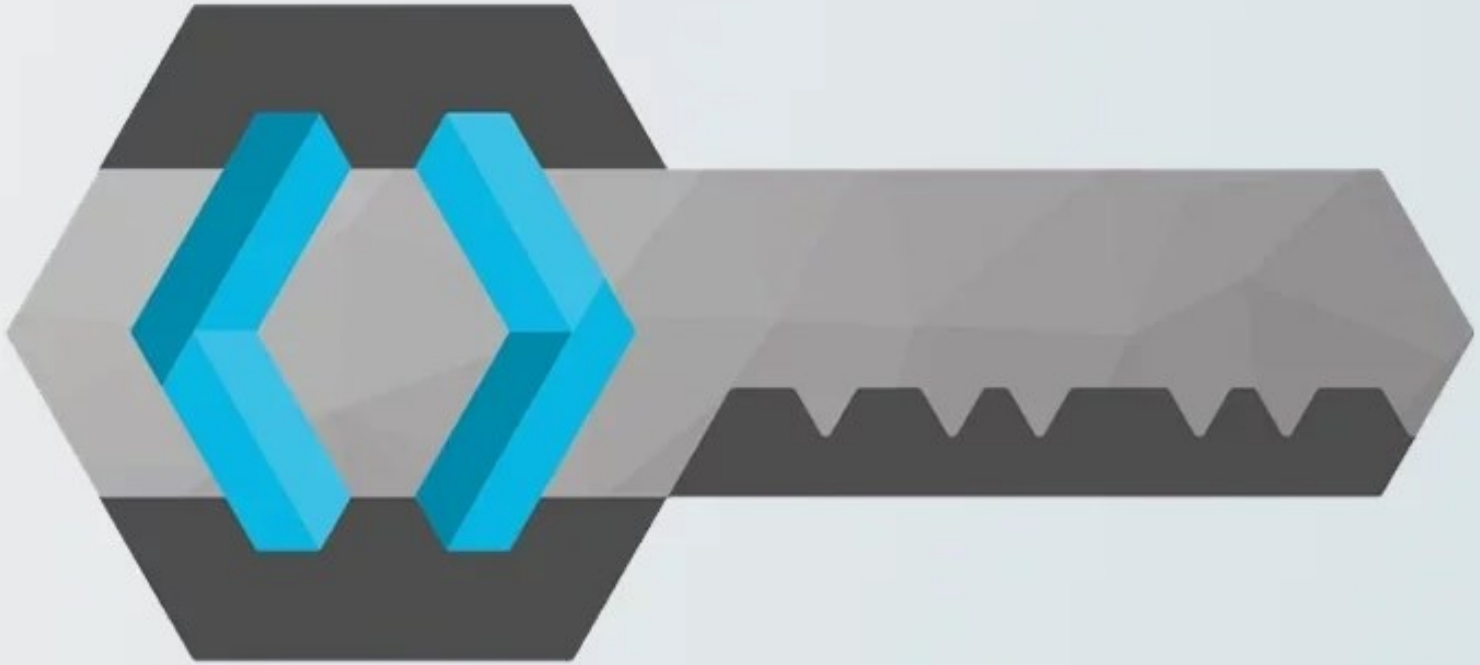
1. PIANIFICAZIONE - Identificare gli asset critici, il loro valore e mappare i flussi di dati e le dipendenze

2. ROADMAP DI IMPLEMENTAZIONE

1. Valutazione della maturità e gap analysis
2. Implementazione delle identità e gestione degli accessi
3. Segmentazione della rete
4. Protezione dei dati
5. Monitoraggio e automazione

3. TECNOLOGIE ABILITANTI

- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)
- Privileged Access Management (PAM)
- Micro-segmentazione
- SIEM e XDR



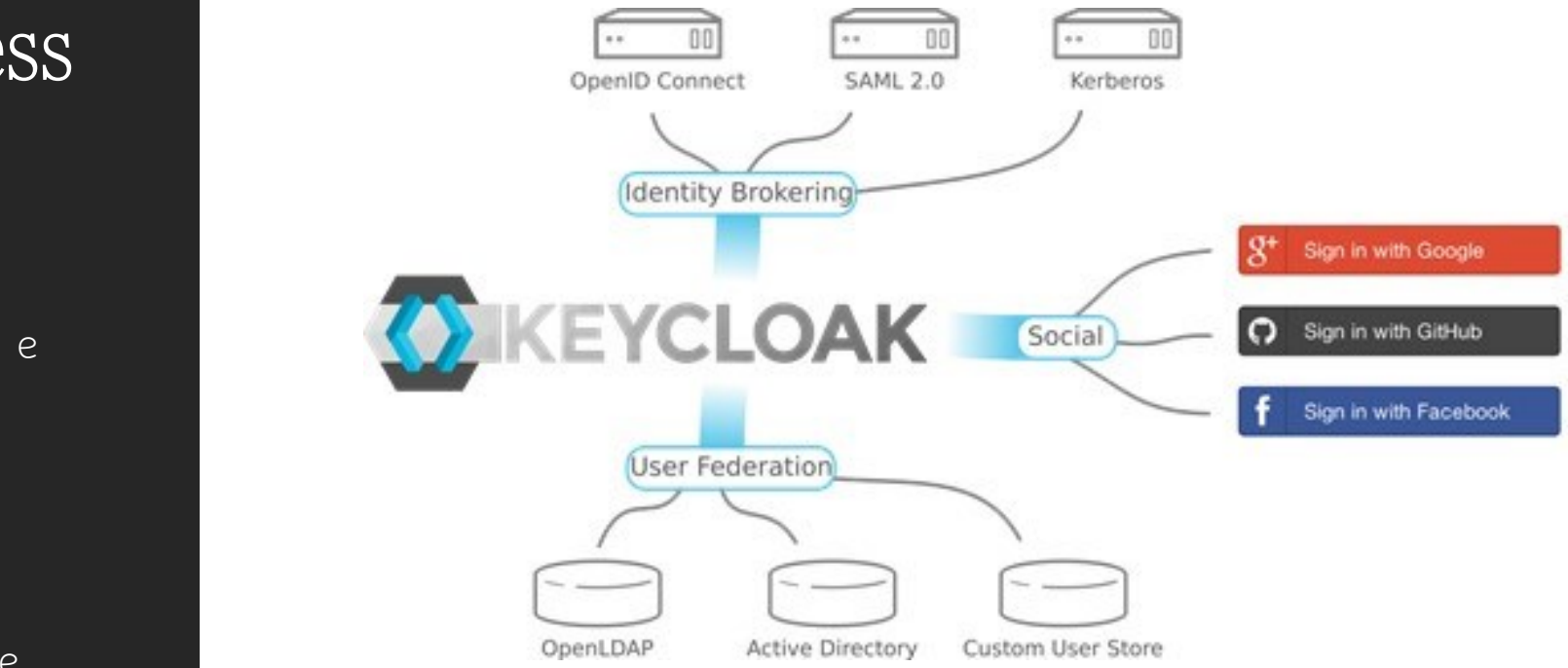
Esempio di implementazione

IAM - Identity and Access Management

Open Source Identity and Access Management

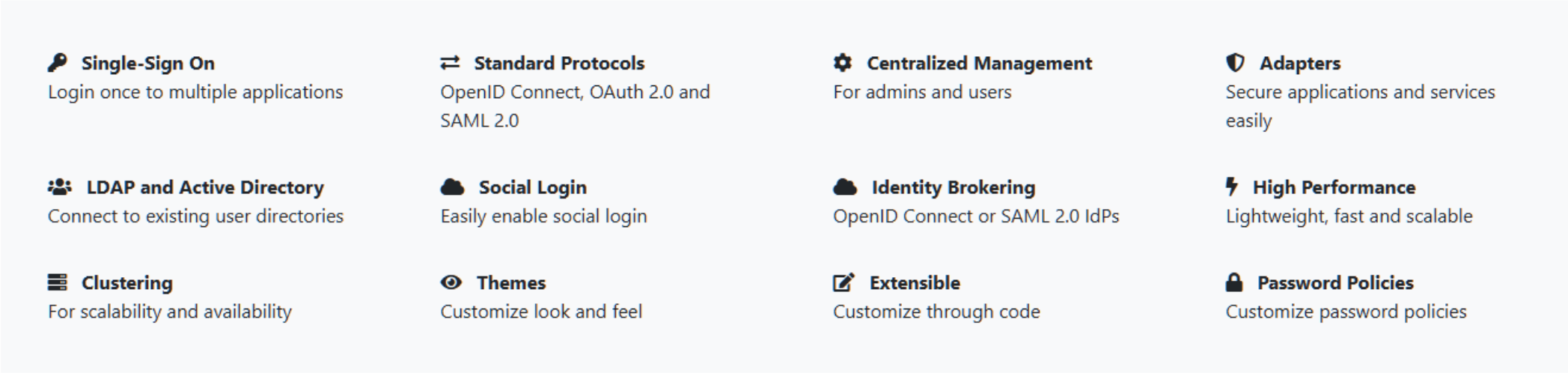
Consente di aggiungere l'autenticazione alle applicazioni e protegge i servizi.

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



Esercitazione Keycloak

- Scaricare Keycloak (*https://www.keycloak.org/*)
- Decomprimere il file di deployment (*zip*)
- Installare OpenJDK 23 (*https://jdk.java.net/archive/)*
- Impostare la variabile di sistema JAVA_HOME=*«path in cui è installato java»*
- Eseguire: ***kc start-dev*** (la prima volta *avviare in modalità development*)
- Aprire url: *http://localhost:8080*
- Creare profili

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

Personale

Formazione

- Creare pillole formative per aumentare l'awareness sui temi dei rischi cyber
- Coinvolgere il personale per affrontare incidenti cyber o social engineering tramite la gamification (individuali e a squadre)
- Utilizzare casi d'uso extra-lavorativa (casi personali) per aumentare la partecipazione

Formalizzazione

- La formalizzazione delle responsabilità incrementa la consapevolezza del rischio
- Aiuta a comprendere i ruoli e le attività per aumentare la postura cyber
- Deve essere accompagnata da sistemi di controllo e valutazione

Il personale solitamente rappresenta la catena debole della cybersecurity, allo stesso tempo può diventare la prima avamposto per la cyber defence

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

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 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 di avviare la collaborazione
- **Software Bill of Materials (SBOM)**: inventario dettagliato di tutti i componenti software utilizzati dai fornitori
- **Controllo degli accessi**: limitare l'accesso dei fornitori ai soli sistemi necessari per lo svolgimento dell'incarico
- **Monitoraggio continuo**: sorveglianza delle attività dei fornitori nei propri sistemi
- **Clausole contrattuali**: requisiti di sicurezza esplicitamente definiti nei contratti
- **Zero Trust**: implementar un approccio di verifica costante di 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, 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, valutare l'importanza dei principi di

- 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 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 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 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 per le 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 verificarne l'efficacia
- **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

La gestione delle configurazioni e degli aggiornamenti dei software e dei sistemi

La gestione delle configurazioni e degli aggiornamenti può essere effettuata attraverso piattaforme come Configuration Management (CM) o Software Configuration Management (SCM).
Ecco alcune delle più diffuse:

- Ansible - Soluzione open source per automazione, configurazione e gestione dei sistemi che utilizza
- YAML per definire le configurazioni.
- Puppet - Strumento che permette di gestire configurazioni tramite un linguaggio dichiarativo, adatto per ambienti di grandi dimensioni.
- Chef - Piattaforma di automazione che utilizza "ricette" per descrivere configurazioni e gestire l'infrastruttura.
- SaltStack - Sistema basato su event-driven automation che consente la gestione centralizzata della configurazione.
- Microsoft System Center Configuration Manager (SCCM) - Soluzione per ambienti Windows che gestisce distribuzione di software, aggiornamenti e conformità.
- Red Hat Satellite - Piattaforma di gestione per sistemi Linux che facilita provisioning, patching e configurazione.
- JFrog Artifactory - Gestore di repository binari che supporta la distribuzione di software.
- GitLab/GitHub con CI/CD - Integrazione di sistemi di controllo versione con pipeline di integrazione continua per gestire configurazioni come codice.
- Jenkins - Strumento di automazione open source che può essere utilizzato per implementare pipeline di configurazione.
- IBM UrbanCode - Soluzione enterprise per deployment di applicazioni e gestione configurazioni.

Queste piattaforme consentono di centralizzare la gestione, implementare configurazioni come codice e automatizzare gli aggiornamenti, migliorando efficienza e consistenza degli ambienti IT.

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

Il paradigma «DevOps»

DevSecOps integra la sicurezza in ogni fase del ciclo di vita dello sviluppo software.
Combina **sviluppo** (Dev), **sicurezza** (Sec) e **operazioni** (Ops) in un **unico approccio integrato**.
L'obiettivo è incorporare la sicurezza fin dall'inizio del processo di sviluppo, anziché considerarla solo nelle fasi finali.

Principi chiave del DevSecOps

1. **Sicurezza come codice**: La sicurezza è implementata, testata e applicata come codice, rendendola ripetibile, scalabile e condivisibile.
2. **Automazione**: I controlli di sicurezza sono automatizzati per non rallentare i cicli di sviluppo e deployment.
3. **Collaborazione trasversale**: Sviluppatori, team di sicurezza e operatori IT lavorano insieme anziché in silos separati.
4. **Responsabilità condivisa**: La sicurezza è responsabilità di tutti, non solo del team di sicurezza.
5. **Miglioramento continuo**: Feedback e apprendimento costanti per migliorare sia il prodotto che i processi.

Open Web Application Security Project

OWASP è un'organizzazione internazionale non-profit dedicata al miglioramento della sicurezza del software. Fondata nel 2001, fornisce risorse gratuite e aperte utilizzate da sviluppatori, tester, professionisti della sicurezza per identificare e mitigare le vulnerabilità di sicurezza nel software

Ecco alcuni contributi di OWASP:

- OWASP Top 10 - Una lista delle dieci vulnerabilità di sicurezza web più critiche
- OWASP Testing Guide - Una guida completa per testare la sicurezza delle applicazioni web
- OWASP Application Security Verification Standard (ASVS) - Un framework per i requisiti di sicurezza e verifica
- OWASP ModSecurity Core Rule Set - Regole per il firewall applicativo ModSecurity.
- OWASP Generative AI Security Project - Supporta coloro che stanno progettando, costruendo e mettendo in sicurezza i sistemi di intelligenza artificiale generativa

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)

Esempi di misure di sicurezza attiva

- **Firewall perimetrale**: blocca gli accessi esterni non autorizzati
- **Intrusion detection system IDS**: rileva i tentativi di intrusione
- **Intrusion prevention system (IPS)**: rileva e blocca i tentativi di intrusione
- **Web Application Firewall (WAF)**: blocca le sequenze/chiamate ai servizi web non autorizzate
- **Endpoint Detection and Response (EDR)**: rileva, monitora e protegge gli endpoint
- **Anti Denial of Service (DOS)**: rileva e blocca i tentativi di attacchi DOS
- **Anti Malware**: rileva e blocca la diffusione di codice malevolo

Tools per le misure di sicurezza attiva

FIREWALL

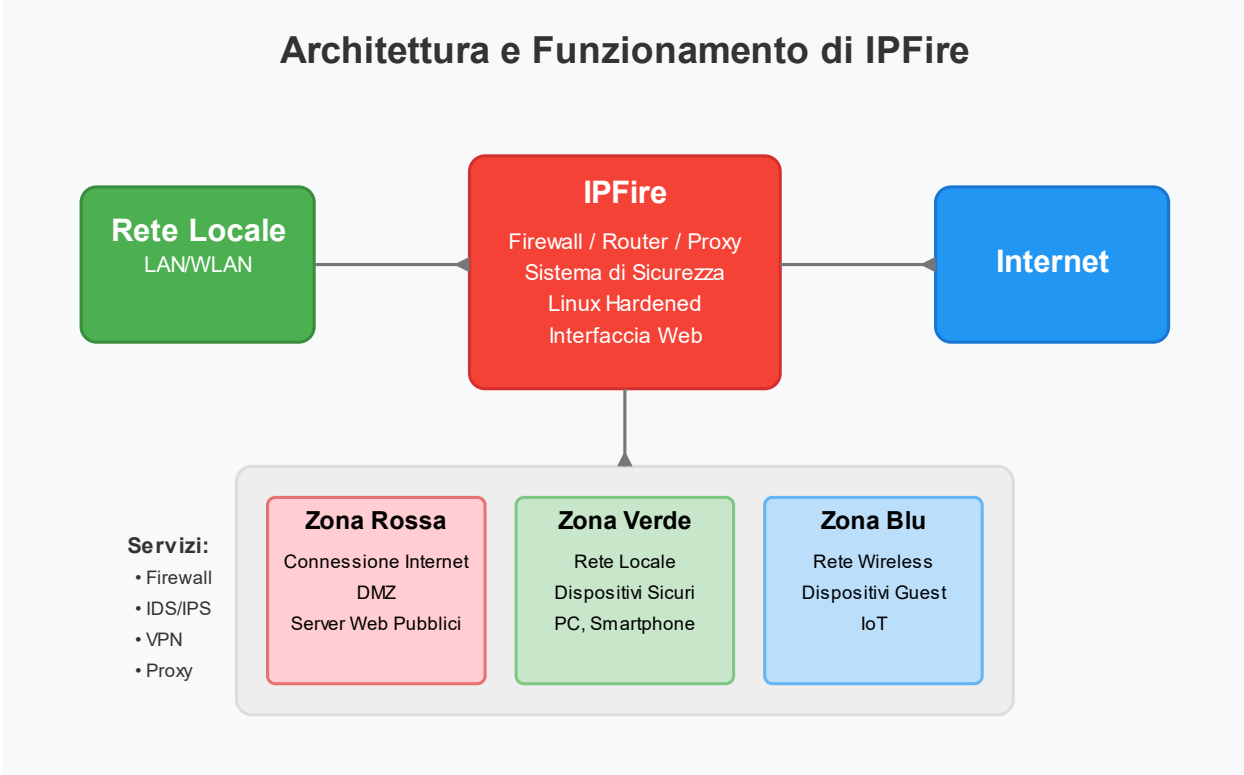
1. **pfSense** - Distribuzione basata su FreeBSD che offre firewall completo, routing e funzionalità VPN con interfaccia web.
2. **OPNsense** - Fork di pfSense con focus su sicurezza, aggiornamenti regolari e interfaccia moderna.
3. **IPFire** - Distribuzione Linux specializzata in firewall con funzionalità di proxy, filtro contenuti e VPN.
4. **ClearOS** - Soluzione completa con funzionalità firewall, gateway e altre funzioni di sicurezza di rete.
5. **UFW (Uncomplicated Firewall)** - Interfaccia semplificata per iptables su sistemi Linux.

IDS/IPS

1. **Snort** - Uno dei più popolari IDS/IPS open source, capace di analisi in tempo reale e logging dei pacchetti.
2. **Suricata** - IDS/IPS multithread ad alte prestazioni con supporto per identificazione di protocolli e file.
3. **Zeek** (precedentemente Bro) - Potente IDS focalizzato sull'analisi del traffico di rete e sulla sicurezza.
4. **OSSEC** - IDS host-based che fornisce monitoraggio in tempo reale, rilevamento delle intrusioni e analisi di log.
5. **Security** Onion - Distribuzione Linux che integra diversi strumenti di rilevamento e monitoraggio, tra cui Suricata, Zeek e Wazuh.
6. **Fail2ban** - Strumento che monitora i log di sistema e blocca gli IP che mostrano comportamenti sospetti.

Firewall

- Segmentare la rete per livelli di criticità
- Associare ogni segmento ad un profilo:
  - Green: rete interna
  - Red: rete esterna
  - Orange: DMZ (server farm)
  - Blu: Wi-fi (guest)
- Configurare i servizi e i port da
- Impostare le regole di filtering



Intrusion Detection System (IDS)

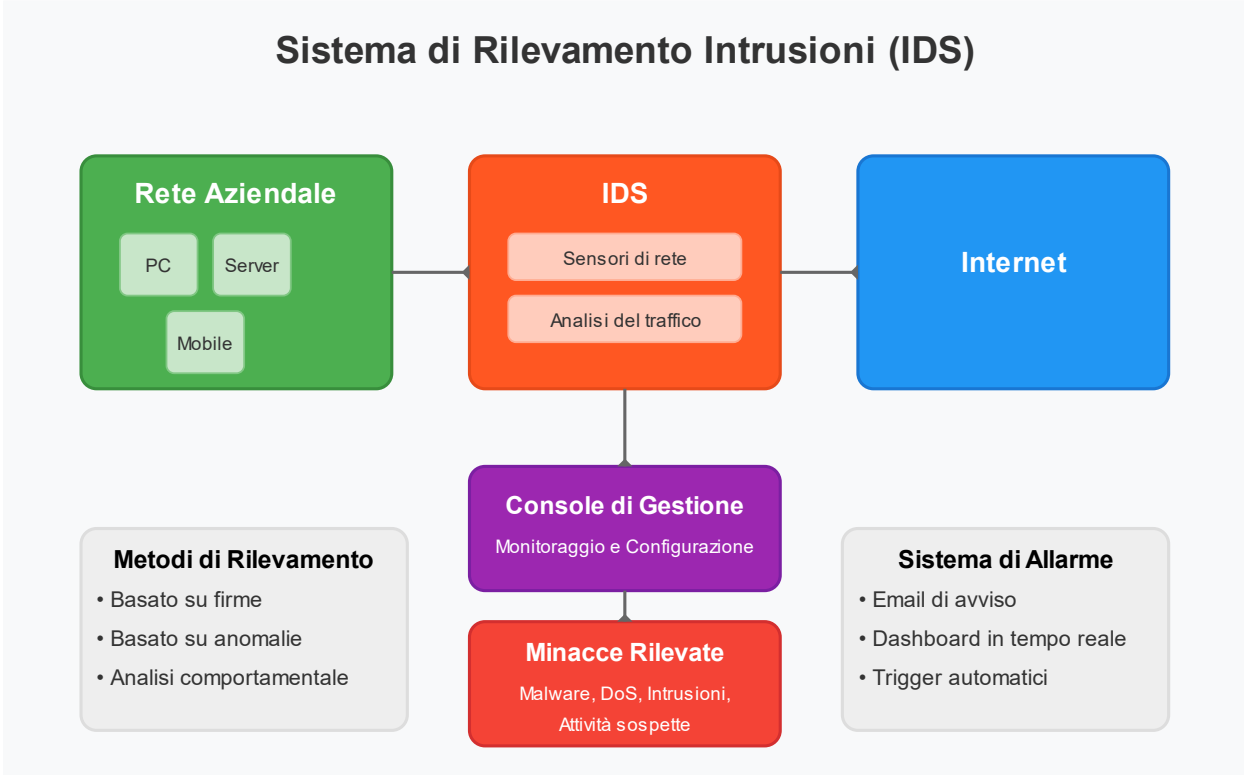
È un dispositivo o un'applicazione software che monitora una rete o un sistema per individuare attività dannose o violazioni delle policy di sicurezza.

Ecco gli elementi fondamentali:

- Monitoraggio del traffico di rete o delle attività del sistema
- Analisi dei dati raccolti per identificare pattern sospetti
- Generazione di alert per rilevate possibili intrusioni
- Registrazione degli eventi per analisi forensi

Metodologie di rilevamento

- Basato su firme (Signature-based): Confronta il traffico con un database di firme di attacchi noti
- Basato su anomalie (Anomaly-based): Stabilisce un comportamento normale e segnala le deviazioni
- Basato su comportamento (Behavior-based): Analizza pattern di attività per individuare comportamenti sospetti

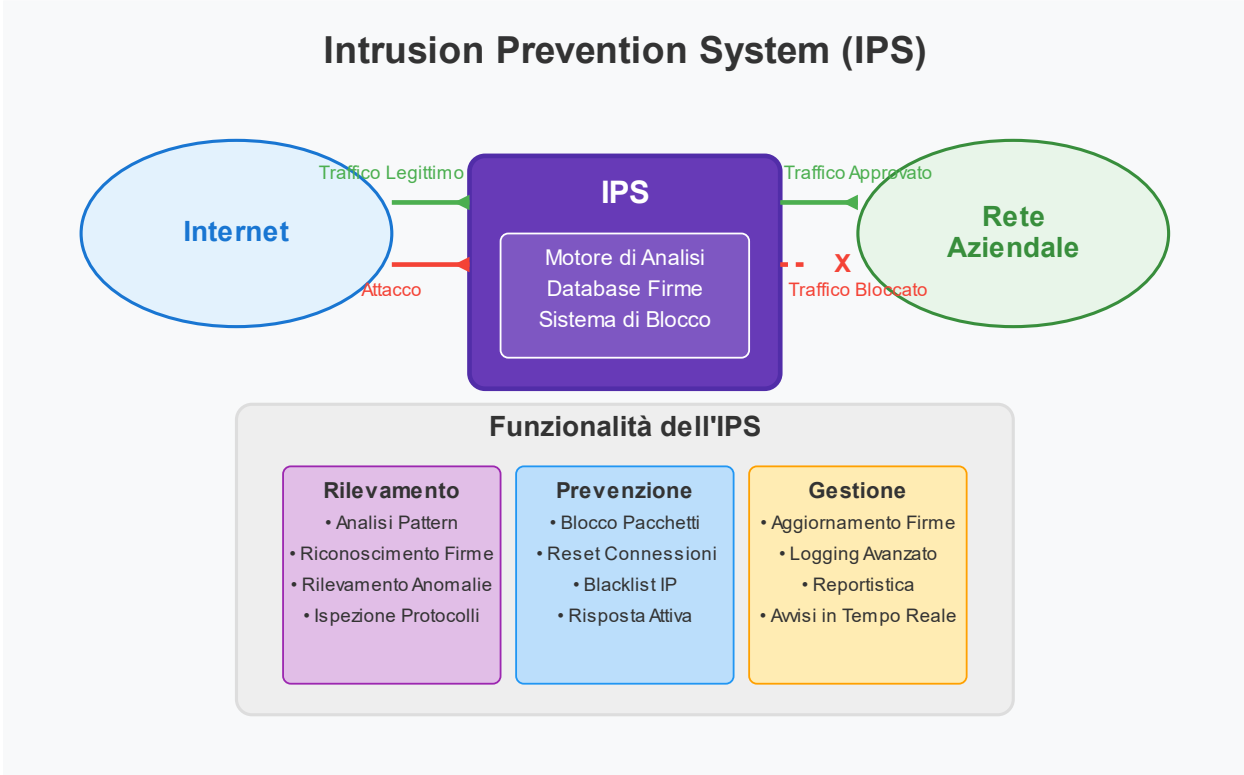


Intrusion Prevention System (IPS)

È un sistema di sicurezza di rete che monitora attivamente il traffico per identificare e bloccare le minacce in tempo reale. A differenza di un IDS (Intrusion Detection System) che si limita a rilevare, l'IPS interviene attivamente per prevenire gli attacchi.

Azioni preventive:

- Blocco di pacchetti sospetti
- Terminazione forzata delle connessioni
- Blacklisting temporaneo o permanente degli IP malevoli
- Logging e notifiche in tempo reale

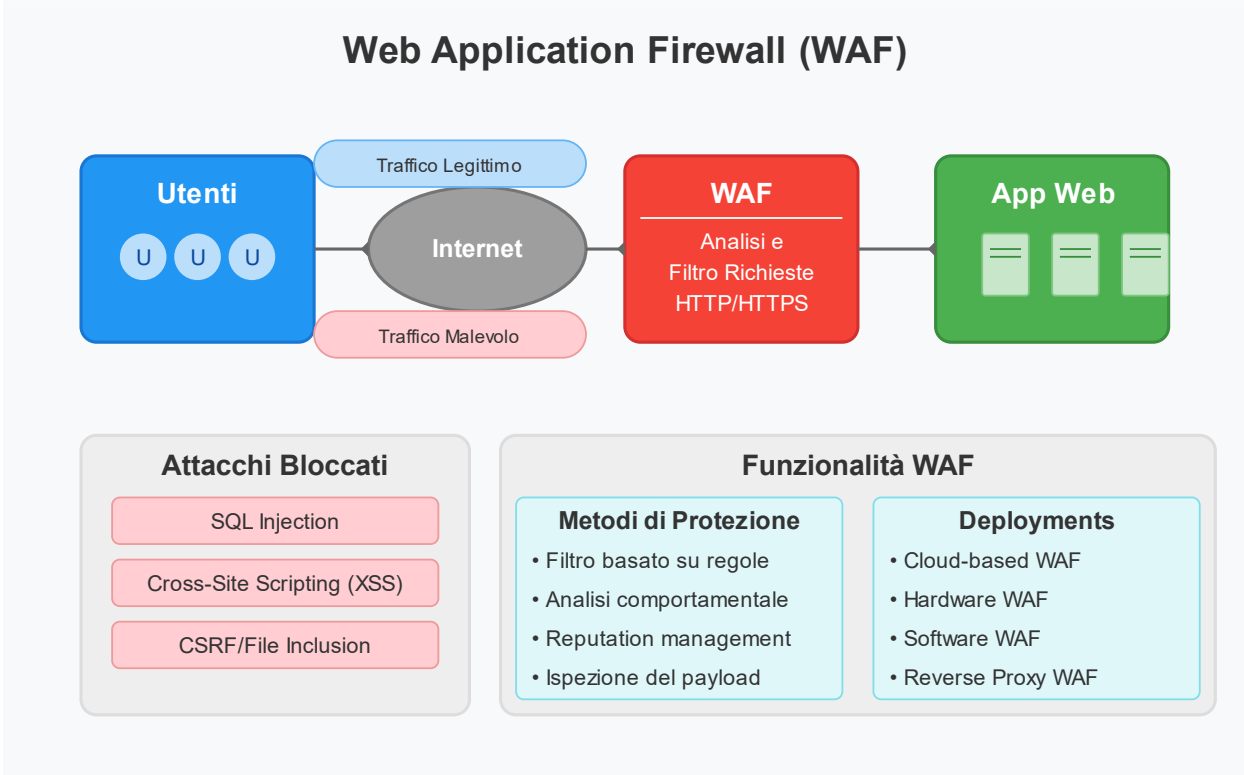


Web Application Firewall (WAF)

È una soluzione di sicurezza che monitora, filtra e blocca il traffico HTTP/HTTPS dannoso verso applicazioni web, proteggendole da vari attacchi.
Un WAF opera tra i client (utenti) e le applicazioni web, esaminando il traffico in entrata e in uscita. Distingue tra traffico legittimo e richieste malevole utilizzando vari metodi di analisi:

- Filtraggio basato su regole (signatures): Confronta il traffico con pattern noti di attacchi
- Analisi comportamentale: Identifica anomalie rispetto al comportamento normale
- Machine learning: Rileva pattern complessi e adatta le protezioni in tempo reale
- Reputation filtering: Blocca traffico da origini note come dannose

Un WAF è particolarmente efficace contro le vulnerabilità OWASP Top 10.



Endpoint Detection and Response (EDR)

È una soluzione di sicurezza avanzata che va oltre i tradizionali antivirus, offrendo capacità di monitoraggio continuo, rilevamento e risposta alle minacce sui dispositivi endpoint

Rilevamento

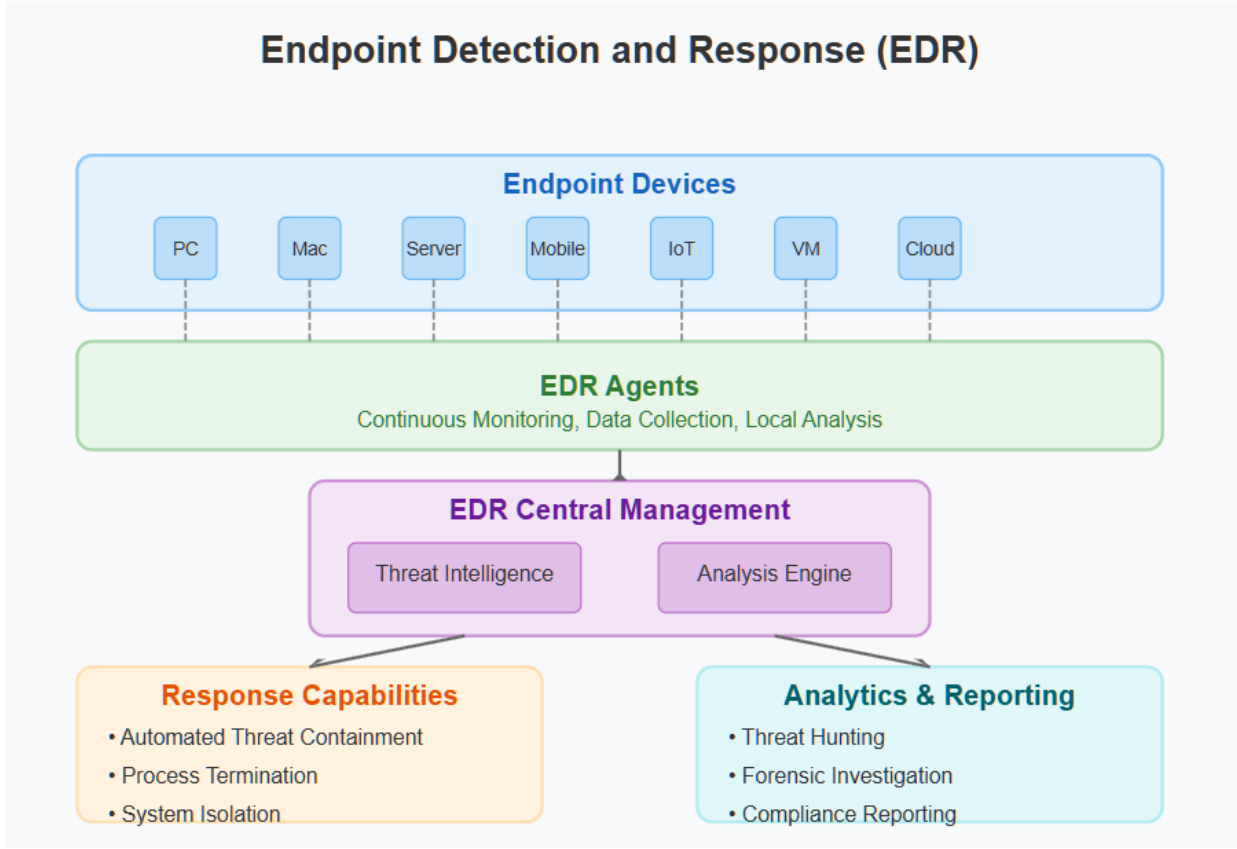
- Analisi comportamentale avanzata
- Rilevamento di minacce senza firma (zero-day)
- Monitoraggio delle attività di sistema, processi, connessioni di rete
- Identificazione di comportamenti anomali e sospetti

Risposta

- Contenimento automatico delle minacce
- Isolamento di endpoint compromessi dalla rete
- Terminazione di processi malevoli
- Rimozione di file dannosi
- Ripristino di sistemi compromessi

Analisi e reporting

- Visualizzazione completa della catena di attacco
- Capacità di threat hunting
- Analisi forense dettagliata
- Dashboard e reportistica per conformità normativa



Anti DOS

I sistemi Anti-DoS (Denial of Service) e Anti-DDoS (Distributed Denial of Service) sono soluzioni progettate per proteggere le risorse online da attacchi mirati a renderle inaccessibili. **Tipologie di attacchi DoS/DDoS**

Per volume

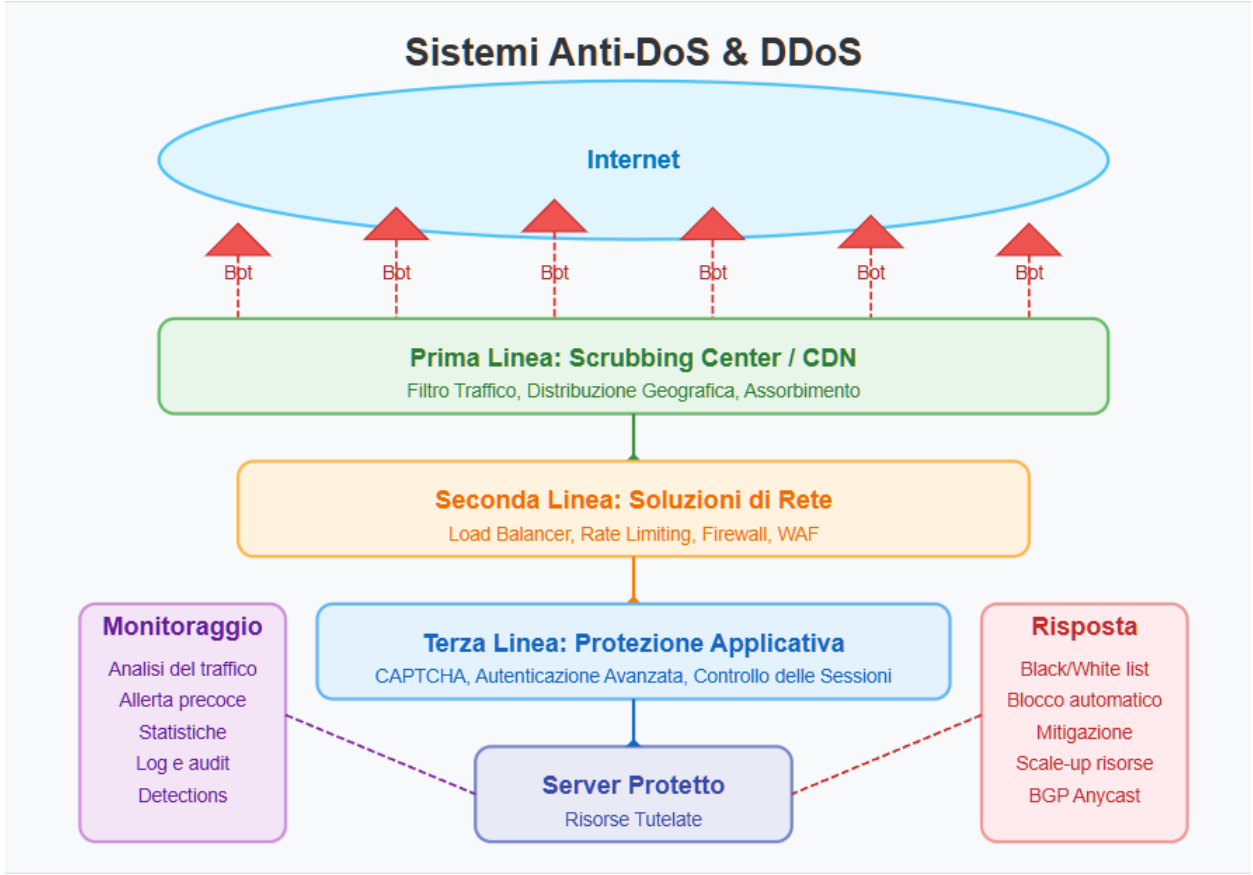
- **Flood di pacchetti**: Sovraccarico della rete con enormi quantità di traffico
- **UDP Flood**: Invio di pacchetti UDP a porte casuali
- **ICMP Flood**: Bombardamento con richieste ICMP (ping)

Per protocollo

- **SYN Flood**: Sfruttamento del meccanismo TCP handshake
- **Reflection/Amplification**: Uso di server terzi per amplificare l'attacco
- **Frammentazione di pacchetti**: Invio di pacchetti malformati

Per applicazione

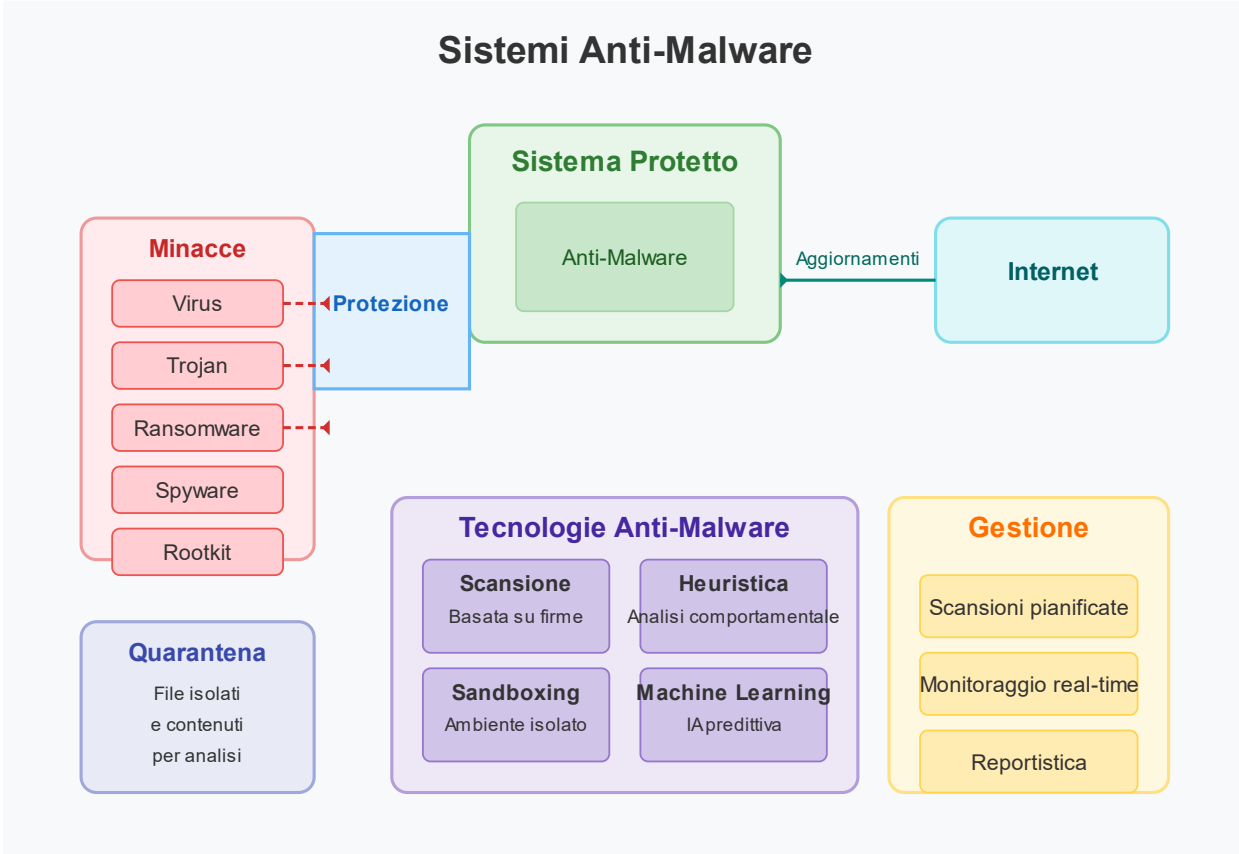
- **HTTP Flood**: Eccesso di richieste HTTP/HTTPS legittime
- **Slow Loris**: Mantenimento di connessioni aperte a lungo
- **Layer 7 Attacks**: Attacchi mirati alle applicazioni web



Anti Malware

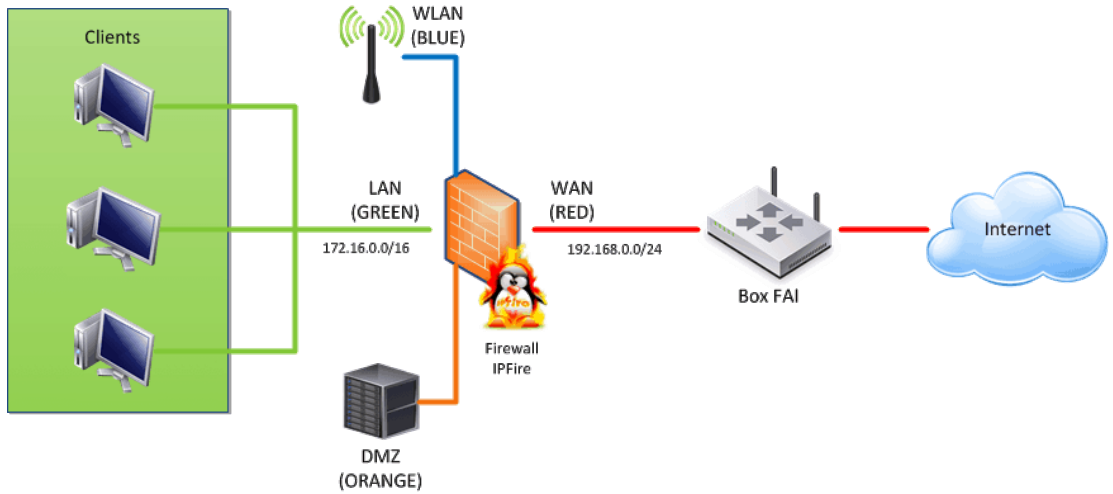
I sistemi anti-malware sono soluzioni software progettate per rilevare, prevenire e rimuovere codice malevolo dai sistemi informatici. Ecco una panoramica completa del loro funzionamento:

- Rilevamento basato su firme
- Analisi euristica
- Analisi comportamentale
- Sandboxing
- Machine Learning e IA



IPFire.org

- Network security
- Network Features
- Web Proxy
- WAN Features
- VPN
- Quality of Service (QoS)
- Intrusion Prevention System
- DNS



https://www.ipfire.org/

Configurazione ottimale:
Linux 4.x, 4 GB RAM, 8 GB HDD, 4 schede di rete

Esercitazione IPFire

- Installare Virtual Box (configurare DUE schede di rete: Rete con NAT->GREEN e NAT->RED)
- Scaricare l'ultima release IPFire
- Installare IPFire da ISO
- Associare scheda con GREEN RED (ip da dhcp)
- Collegarsi da altra VM (p.e. Kali) configurato sulla

Web Application Firewall (WAF)

Un Web Application Firewall (WAF) è un sistema di sicurezza che protegge le applicazioni web filtrando e monitorando il traffico HTTP (e HTTPS) tra un'applicazione web e Internet. Agisce come una barriera protettiva, analizzando ogni richiesta in entrata e ogni risposta in uscita, e bloccando quelle che considera dannose o sospette.

Differenza tra un WAF da un firewall di rete:

- **Un firewall tradizionale opera a livello di rete** (livelli 3 e 4 del modello OSI) e si concentra sul controllo del traffico in base a indirizzi IP e porte.
- **Un WAF opera a livello applicativo** (livello 7 del modello OSI) e analizza il contenuto specifico del traffico HTTP/HTTPS, comprendendo il contesto delle richieste web.

Funzioni principali di un WAF:

- **Filtraggio del traffico malevolo**: Identifica e blocca gli attacchi comuni come SQL injection, cross-site scripting (XSS), file inclusion, e altri exploit noti
- **Protezione da attacchi DDoS** (Distributed Denial of Service): Può aiutare a mitigare attacchi che mirano a sovraccaricare l'applicazione web rendendola inaccessibile.
- **Prevenzione di accessi non autorizzati:** Blocca tentativi di accesso a risorse protette da parte di utenti non autorizzati.
- **Patching virtuale:** In caso di vulnerabilità note in un'applicazione web per cui non è ancora disponibile una patch, un WAF può implementare regole temporanee per bloccare gli exploit.
- **Visibilità e logging:** Fornisce registri dettagliati del traffico web e degli attacchi bloccati, utili per l'analisi e il monitoraggio della sicurezza.
- **Gestione dei bot**: Può identificare e bloccare bot dannosi, consentendo invece il traffico di bot legittimi (come i crawler dei motori di ricerca).

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) è una categoria di strumenti di sicurezza informatica progettati per monitorare, rilevare, analizzare e rispondere alle minacce avanzate che colpiscono gli endpoint di una rete.

In sostanza, l'EDR va oltre le tradizionali soluzioni antivirus focalizzandosi sulla visibilità continua e in tempo reale di ciò che accade su ciascun endpoint. Raccoglie e analizza costantemente dati dettagliati sull'attività degli endpoint per identificare comportamenti sospetti, attività dannose e potenziali minacce che potrebbero eludere le difese di sicurezza convenzionali.

Funzionalità chiave di una soluzione EDR:

- **Monitoraggio Continuo e Raccolta Dati**: Gli agenti raccolgono i dati su processi in esecuzione, connessioni di rete, modifiche al registro di sistema, attività dei file, autenticazioni utente e altro ancora
- **Rilevamento Avanzato delle Minacce**: L'EDR utilizza varie tecniche di analisi, tra cui l'analisi comportamentale, l'apprendimento automatico (Machine Learning), l'intelligenza sulle minacce (Threat Intelligence) e l'analisi forense per identificare attività anomale e indicatori di compromissione (IOC)
- **Analisi e Investigazione**: L'EDR fornisce una visibilità completa sugli eventi degli endpoint, consentendo loro di indagare a fondo sugli allarmi, tracciare la progressione degli attacchi, comprendere la portata del danno e identificare la causa principale
- **Risposta e Remediation**: l'EDR offre funzionalità di risposta per contenere e neutralizzare l'attacco. Queste possono includere l'isolamento degli endpoint infetti, la terminazione di processi dannosi, la quarantena o l'eliminazione di file sospetti e il ripristino delle configurazioni
- **Threat Hunting**: L'EDR consente ai team di sicurezza di condurre attività di "caccia alle minacce" proattive, cercando attivamente comportamenti sospetti o indicatori di compromissione che potrebbero non aver ancora attivato un allarme automatico
- **Analisi Forense e Storica**: L'EDR conserva i dati storici degli eventi degli endpoint per condurre analisi forensi dettagliate per comprendere meglio l'attacco, identificare gli aggressori e migliorare le difese future

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 noti, 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.

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