Fondamenti di Cybersicurezza

Francesco Pugliese, PhD

neural1977@gmail.com

Fondamenti di Cybersicurezza

- La **Cybersecurity** si occupa della protezione di sistemi connessi ad Internet come hardware, software e dati provenienti dalle minacce informatiche.
- Questo insieme di tecniche è usato da individui e imprese per proteggersi contro accessi non autorizzati ai data center e altri sistemi computerizzati.
- Pertanto la **Cybersecurity** è la prassi per proteggere i sistemi, le reti e i programmi da attacchi digitali.
- Gli **attacchi informatici** sono solitamente finalizzati all'accesso, alla trasformazione, o alla distruzione di informazioni sensibili, nonchè all'estorsione di denaro dagli utenti o all'interruzione dei normali processi aziendali.

Fondamenti di Cybersicurezza

- ✓ Una **Potente Strategia di Cybersicurezza** può fornire una buona sicurezza contro attacchi malevoli progettati per accedere, modificare, cancellare o estorcere i dati sensibili delle organizzazioni e dei sistemi degli utenti.
- ✓ La **Cybersicurezza** è anche funzionale nel prevenire gli attacchi che hanno lo scopo di disabilitare o disgregare le operazioni di un sistema o di un dispositivo.
- ✓ L'implementazione di misure di **Cybersicurezza** efficaci è particolarmente impegnativa oggi perchè ci sono più dispositivi a disposizione degli hacker che stanno diventando sempre più innovativi.

Perchè la Cybersicurezza è importante

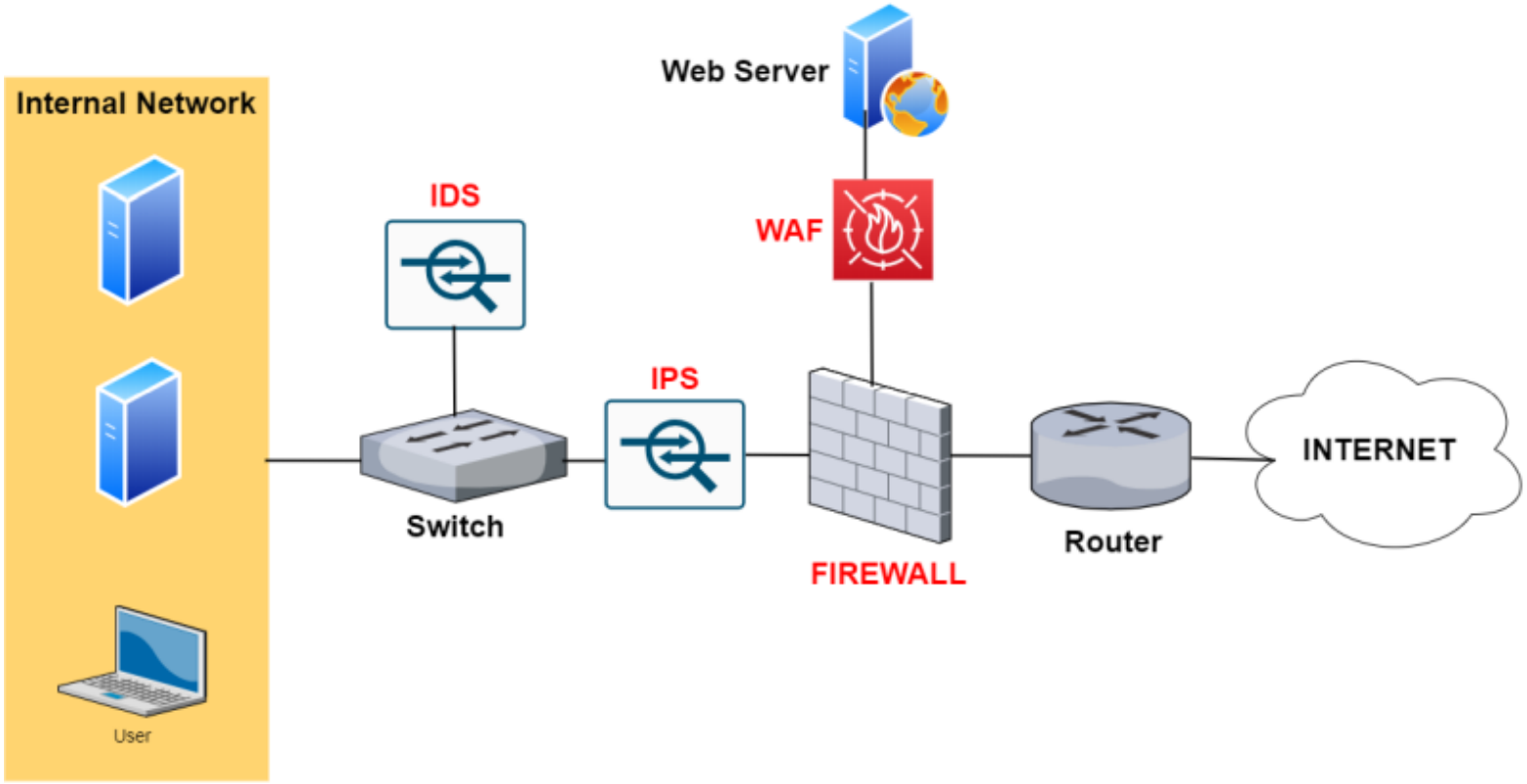
- ✓ Con l'incremento del numero di utenti, dispositivi e programmi nell'impresa moderna, l'importaanza della cybersicurezza continua a crescere.
- ✓ Con l'aumentare del diluvio dei dati, molti di essi sono sensibili e confidenziali.
- ✓ Il crescente volume e la sofisticazione degli attacchi informatici e delle tecniche di attacco composto, il problema dei cyber attacchi diventa sempre più importante.
- ✓ Il campo della **Cybersicurezza** può essere suddiviso in diverse sezioni, il coordinamento delle quali all'interno dell'organizzazione è cruciale per il successo di un programma di cybersicurezza.
- ✓ Mantenere la Cybersicurezza è un terreno in costante evoluzione ed una sfida per tutte le organizzazioni e le company. Gli approcci reattivi tradizionali, in cui le risorse sono messe sul piatto per proteggere i sistemi contro le più grandi minacce conosciute, mentre le minacce meno conosciute sono indifese.

Classificazione dei diversi tipi di Cybersicurezza

- Sicurezza delle Applicazioni
- Sicurezza dei dati e delle informazioni
- Sicurezza di rete
- Pianificazione del Disaster Recovery
- Pianificazione della continuità di Business
- Sicurezza Operazionale
- Sicurezza del Cloud
- Sicurezza delle Infrastrutture critiche
- Sicurezza Fisica
- Educazione dell'Utente Finale

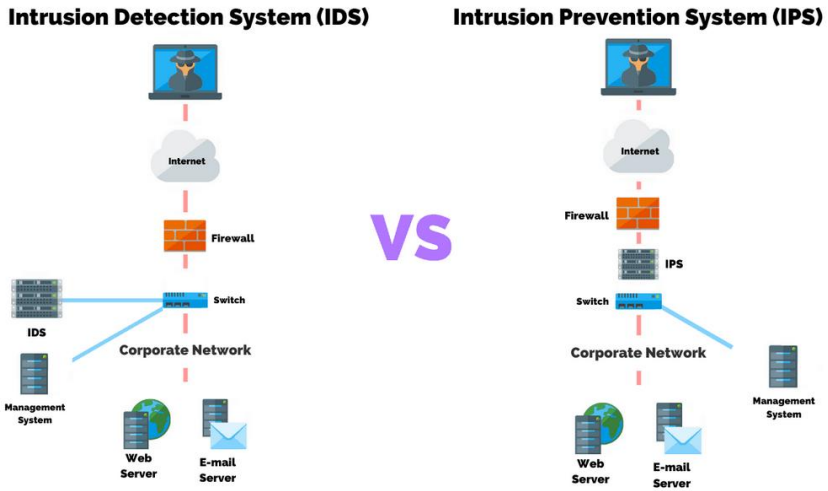
Sistemi di sicurezza (IPS/IDS, Firewall, WAF, Endpoint protection…

- I sistemi di sicurezza come **IPS/IDS**, **Firewall**, **WAF** e **Endpoint Protection**, sono strumenti e tecnologie utilizzati per proteggere le reti informatiche e i dispositivi dagli attacchi informatici.



Sistemi di sicurezza (IPS/IDS, Firewall, WAF, Endpoint protection…

- **IPS/IDS** (Intrusion Prevention System/Intrusion Detection System): Gli **IPS** e gli **IDS** sono sistemi progettati per rilevare e prevenire gli attacchi informatici. Gli **IDS** monitorano il traffico di rete o i log dei sistemi per identificare attività sospette o anomalie che potrebbero indicare una violazione di sicurezza. Gli **IPS**, oltre a rilevare le intrusioni, possono anche intraprendere azioni attive per impedire che tali attacchi avvengano o si propaghino. Ad esempio, possono bloccare il traffico proveniente da indirizzi **IP** malevoli o applicare regole di sicurezza per impedire l'accesso non autorizzato.

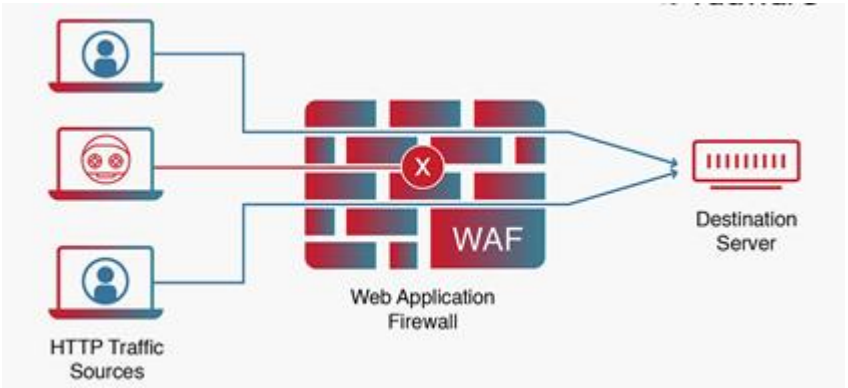


Sistemi di sicurezza (IPS/IDS, Firewall, WAF, Endpoint protection…

- **Firewall**: Un firewall è un componente di sicurezza di rete che filtra e controlla il traffico di rete in entrata e in uscita tra una rete privata e una rete pubblica. Funziona come una barriera di protezione, impedendo a determinati tipi di traffico di passare attraverso. I firewall possono essere basati su software o su hardware e utilizzano regole predefinite per consentire o bloccare il traffico sulla base di indirizzi IP, porte di rete o protocolli specifici. Il firewall aiuta a proteggere la rete da accessi non autorizzati, attacchi di rete e traffico dannoso.

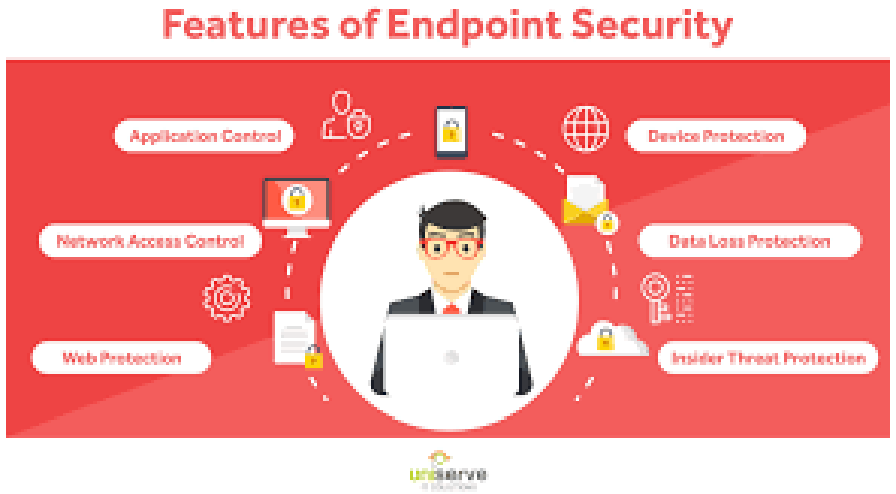
Sistemi di sicurezza (IPS/IDS, Firewall, WAF, Endpoint protection…

- **WAF** (Web Application Firewall): Il **WAF** è un tipo di firewall specificamente progettato per proteggere le applicazioni web da attacchi come SQL injection, cross-site scripting (XSS) e altri attacchi di livello applicativo. Il WAF monitora il traffico **HTTP/HTTPS** delle applicazioni web, analizza le richieste in arrivo e le risposte, e applica regole di sicurezza per filtrare e bloccare le minacce. Può anche fornire funzionalità aggiuntive come la gestione delle sessioni, la protezione delle credenziali e la prevenzione del furto di dati.



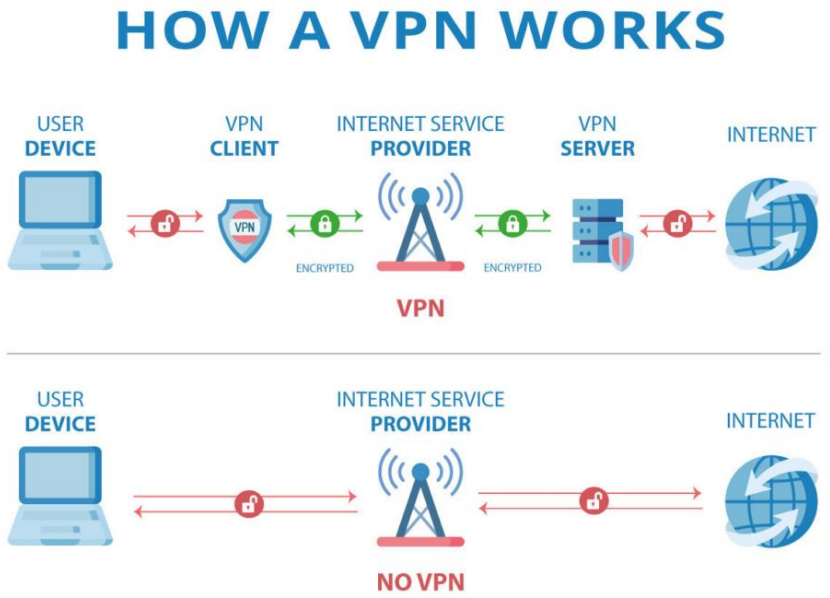
Sistemi di sicurezza (IPS/IDS, Firewall, WAF, Endpoint protection…

- **Endpoint Protection**: L'Endpoint Protection, noto anche come **Endpoint Security**, si riferisce alle soluzioni di sicurezza installate sui dispositivi finali, come computer, laptop, smartphone e tablet. Queste soluzioni includono funzionalità come **antivirus**, **antispyware**, **firewall personale**, **rilevamento delle intrusioni** e **protezione delle applicazioni**. L'Endpoint Protection mira a proteggere i dispositivi dagli attacchi **malware**, **phishing** e altre minacce informatiche, oltre a garantire la sicurezza dei dati e la conformità alle politiche di sicurezza dell'organizzazione.



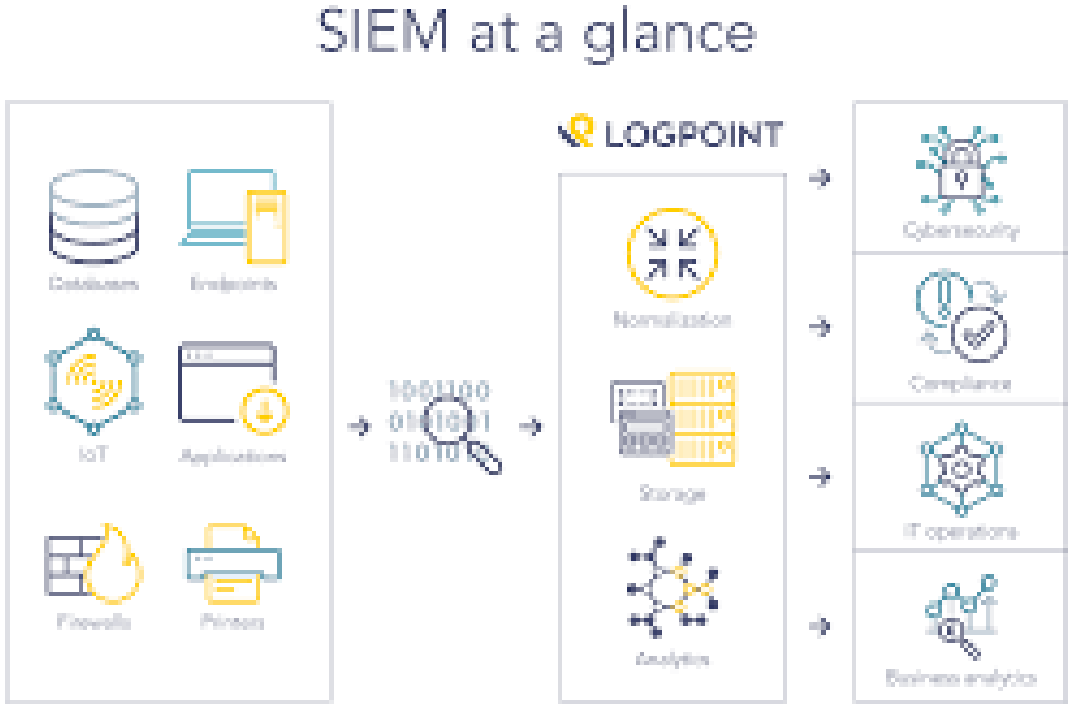
Altri Sistemi di Sicurezza (VPN, SIEM, DLP, HIDS/NIDS…)

- **VPN** (Virtual Private Network): Una VPN è una rete privata virtuale che consente di creare una connessione **sicura** e **crittografata** su una rete pubblica, come Internet. Le **VPN** vengono utilizzate per proteggere la privacy e la sicurezza delle comunicazioni, consentendo agli utenti di accedere in modo sicuro alle risorse di rete da posizioni remote e di crittografare il traffico di rete per prevenire l'intercettazione e l'accesso non autorizzato.



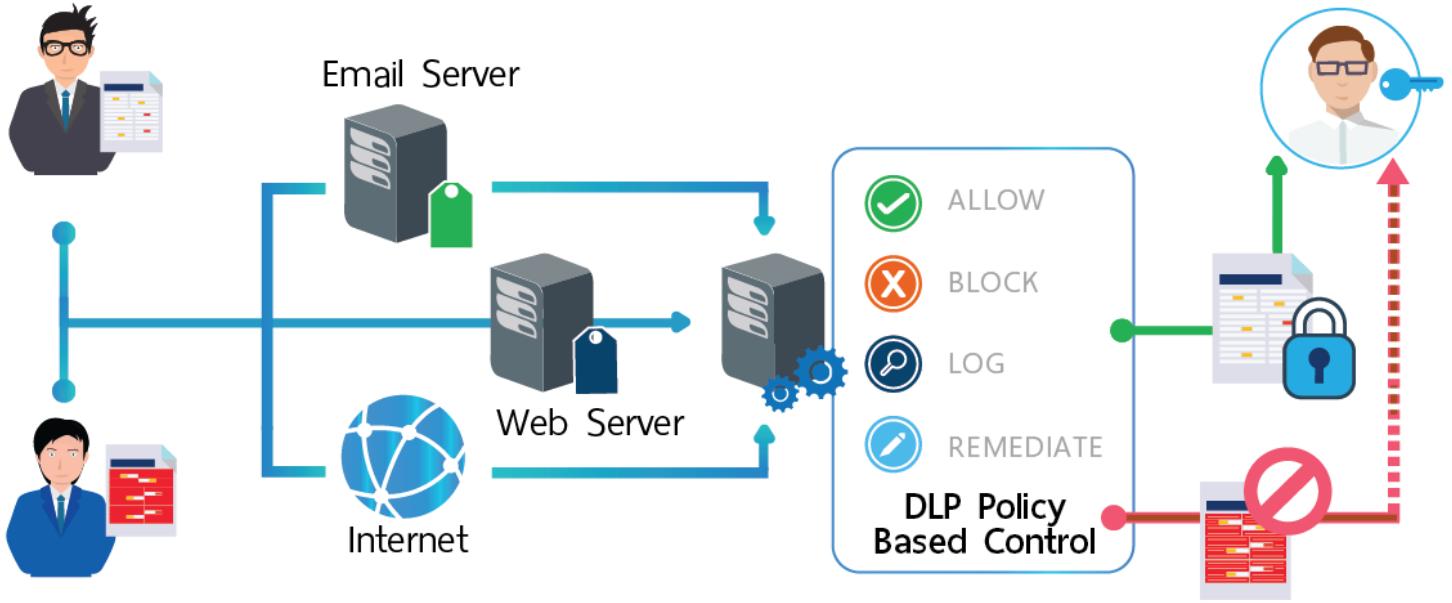
Altri Sistemi di Sicurezza (VPN, SIEM, DLP, HIDS/NIDS…)

- **SIEM** (Security Information and Event Management): Il SIEM è una piattaforma di gestione delle informazioni e degli eventi di sicurezza che raccoglie, analizza e correla i dati da diverse fonti all'interno di un'infrastruttura IT. Il SIEM aiuta a identificare attività sospette o anomalie di sicurezza, genera avvisi in tempo reale e consente di analizzare i dati per rilevare e rispondere agli incidenti di sicurezza.



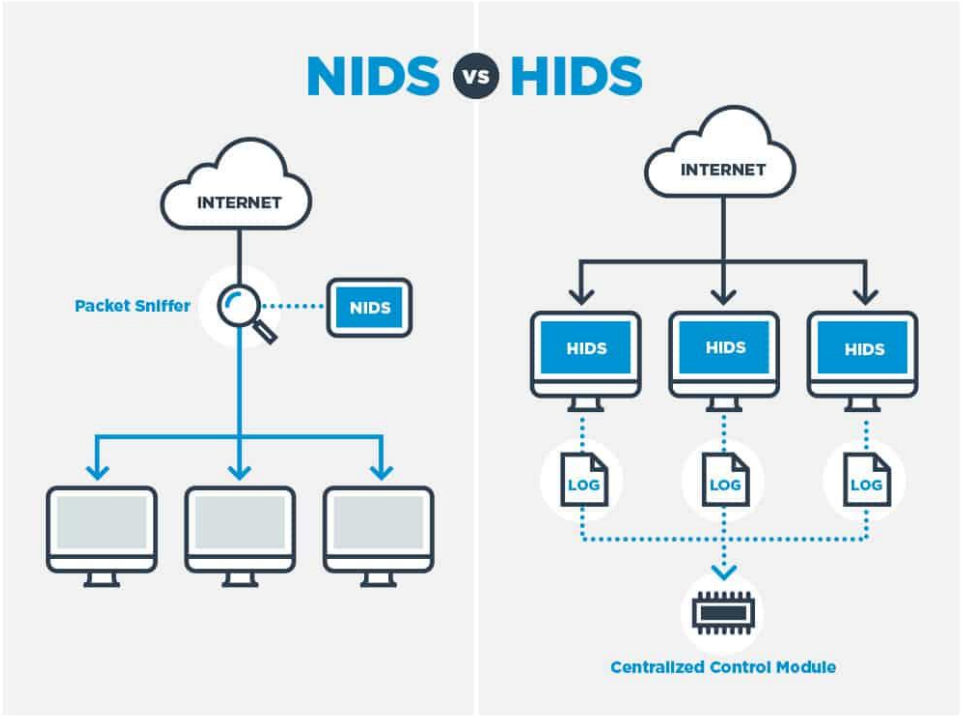
Altri Sistemi di Sicurezza (VPN, SIEM, DLP, HIDS/NIDS…)

- **DLP** (Data Loss Prevention): La soluzione **DLP** è progettata per prevenire la perdita o la divulgazione non autorizzata di dati sensibili. Utilizza tecnologie come il monitoraggio del traffico di rete, la scansione dei dati in movimento e a riposo, la classificazione dei dati e le politiche di protezione per individuare e bloccare le potenziali violazioni di dati sensibili, come la divulgazione di informazioni personali o confidenziali.



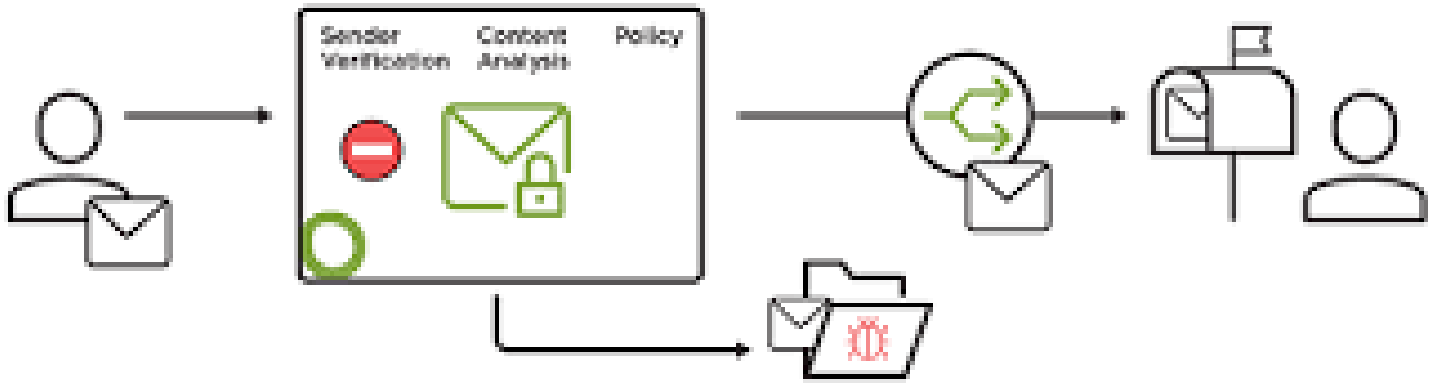
Altri Sistemi di Sicurezza (VPN, SIEM, DLP, HIDS/NIDS…)

- **HIDS/NIDS** (Host-based Intrusion Detection System/Network-based Intrusion Detection System): Gli **HIDS** e i **NIDS** sono sistemi di rilevamento delle intrusioni che monitorano e analizzano l'attività di rete e del sistema operativo per rilevare potenziali **attacchi informatici**. Gli HIDS sono installati su singoli dispositivi finali e rilevano attività sospette sul dispositivo stesso, mentre i NIDS monitorano il traffico di rete per identificare intrusioni o anomalie sulla rete.



Altri Sistemi di Sicurezza (VPN, SIEM, DLP, HIDS/NIDS…)

- **Secure Email Gateway**: Un **Secure Email Gateway** è un sistema che fornisce protezione contro le minacce associate alle email, come phishing, malware e spam. Questi gateway analizzano e filtrano il traffico delle email in arrivo e in uscita, utilizzando tecniche di rilevamento delle minacce, firme antivirus, filtri antispam e regole personalizzabili per bloccare le email dannose e indesiderate.

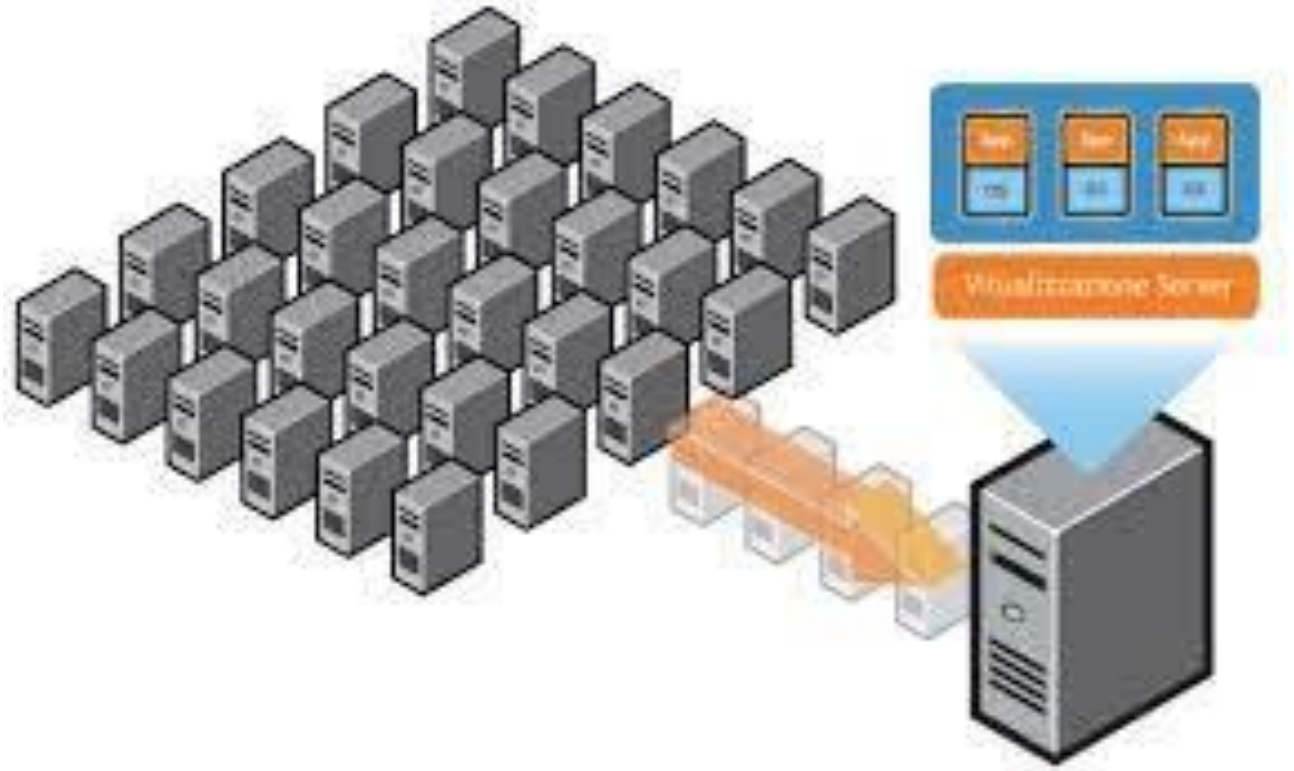


Sistemi di virtualizzazione

- I **sistemi di virtualizzazione** giocano un ruolo significativo nella cybersicurezza, offrendo vantaggi come l'isolamento, la flessibilità e la gestione centralizzata delle risorse. Ecco alcuni esempi di come la virtualizzazione viene utilizzata nella cybersicurezza.
- La **virtualizzazione** offre un modo **flessibile** ed **efficiente** per implementare soluzioni di sicurezza, consentendo di ridurre i **costi**, semplificare la **gestione** e migliorare la **resilienza**. Tuttavia, è importante considerare anche la sicurezza dei componenti virtualizzati stessi, come le vulnerabilità delle VM, la gestione delle credenziali di accesso e le minacce specifiche legate alla virtualizzazione, per garantire una protezione completa.

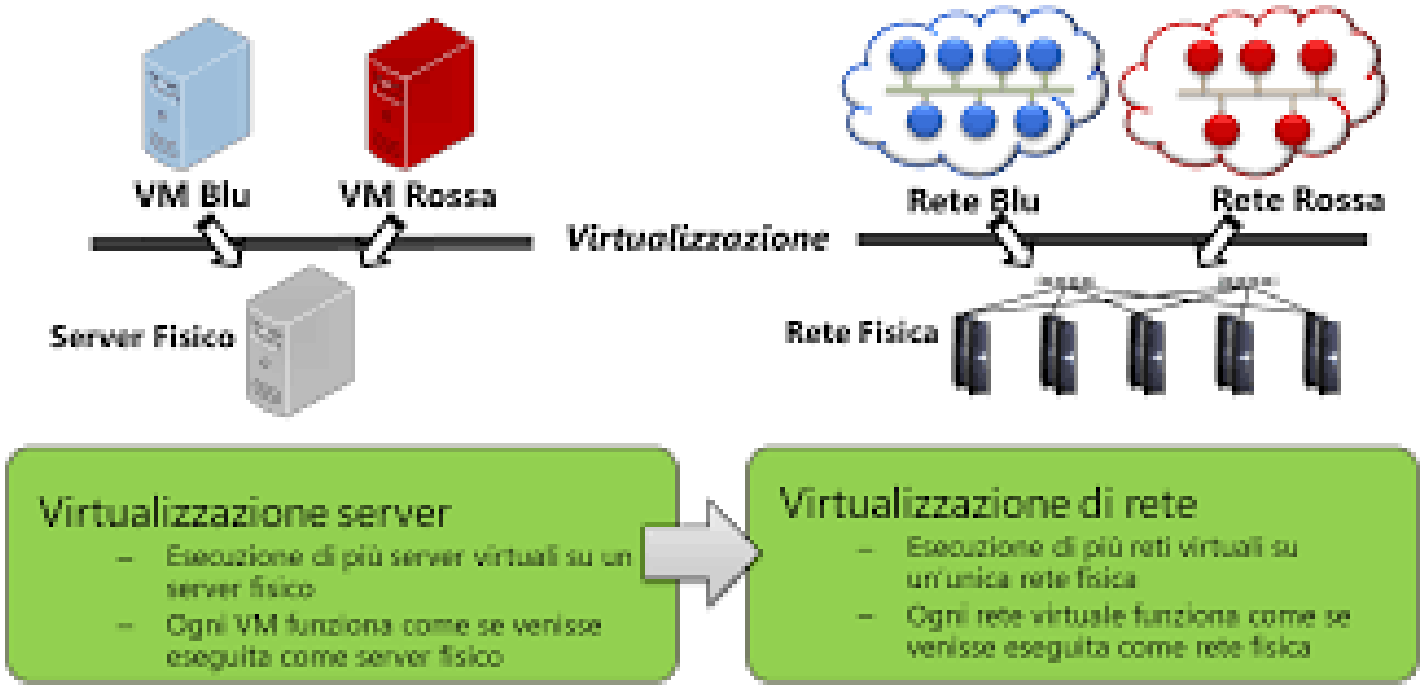
Sistemi di virtualizzazione

- **Virtualizzazione dei server:** La virtualizzazione dei server consente di eseguire più macchine virtuali (VM) su un singolo server fisico. Questo offre un'ulteriore protezione e isolamento tra le diverse applicazioni e i servizi ospitati sullo stesso server. In caso di compromissione di una VM, le altre rimangono intatte, limitando la diffusione di eventuali minacce.



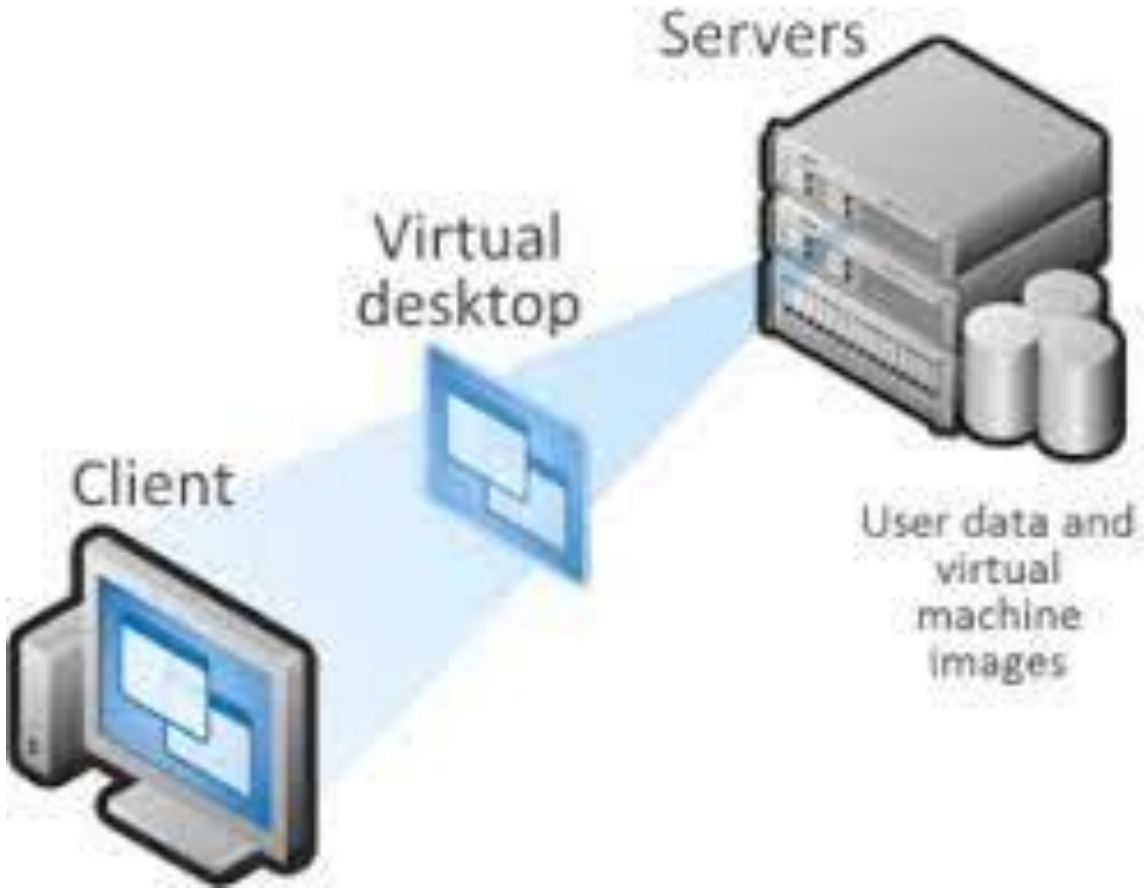
Sistemi di virtualizzazione

- **Virtualizzazione delle reti:** La virtualizzazione delle reti consente di creare reti virtuali separate all'interno di una rete fisica. Questo può contribuire a migliorare la sicurezza separando i diversi segmenti di rete, consentendo una gestione granulare degli accessi e delle politiche di sicurezza per ciascuna rete virtuale.



Sistemi di virtualizzazione

- **Virtualizzazione dei desktop:** La virtualizzazione dei desktop permette agli utenti di accedere a un desktop virtuale ospitato su un server centrale. Questo offre un maggiore controllo sulla sicurezza, poiché i dati e le applicazioni sensibili rimangono nel data center anziché essere distribuiti su dispositivi remoti. In caso di smarrimento o furto del dispositivo, i dati rimangono al sicuro nel server centrale.



Sistemi di virtualizzazione

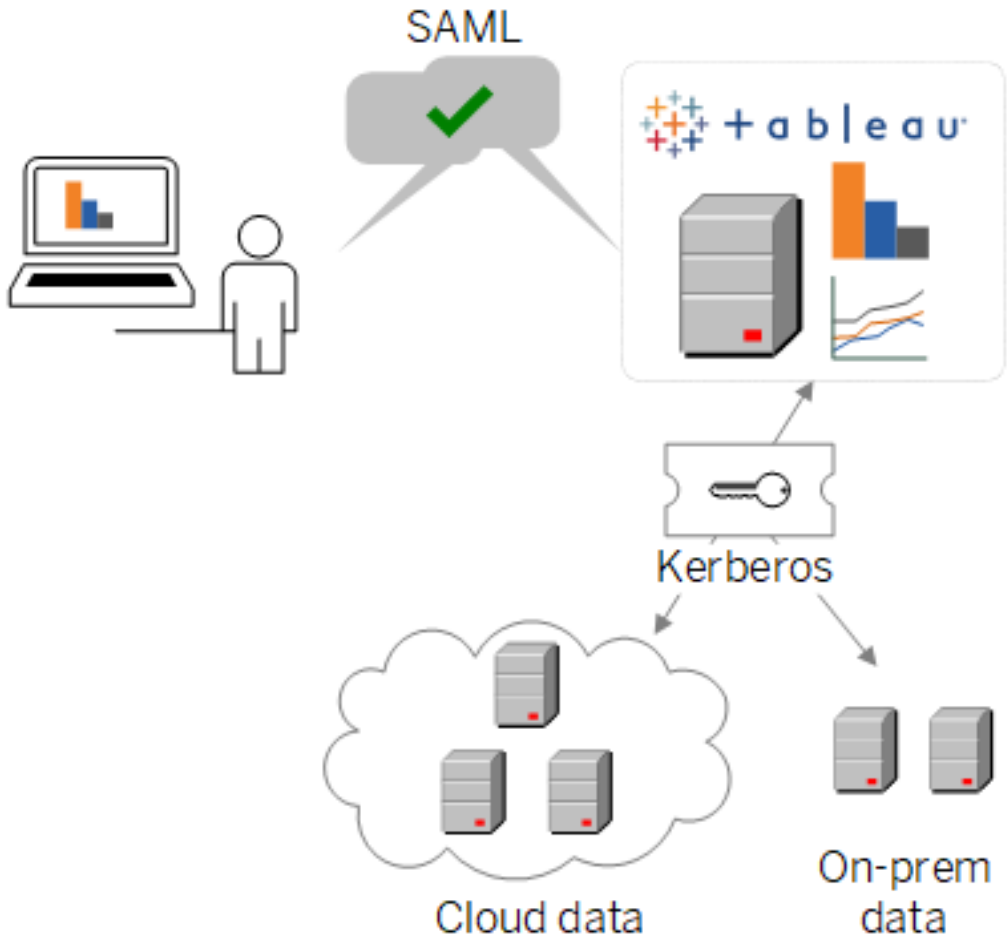
- **Virtualizzazione delle sandbox:** Le sandbox virtuali sono ambienti isolati che consentono di eseguire applicazioni o file sospetti in un ambiente controllato e separato. Questo aiuta a mitigare il rischio di esecuzione di malware o di comportamenti dannosi, poiché qualsiasi attività dannosa viene confinata nella sandbox senza compromettere il sistema ospitante.

Sistemi di virtualizzazione

- **Virtualizzazione dei test di sicurezza:** La virtualizzazione viene ampiamente utilizzata per eseguire test di sicurezza e analisi delle vulnerabilità. I ricercatori di sicurezza e i professionisti del settore possono creare ambienti virtuali per simulare attacchi, testare patch di sicurezza e valutare la resilienza di un sistema o di un'applicazione senza compromettere l'ambiente di produzione.

Sistemi di gestione centralizzati (Active Directory, Sistemi IAM, OAuth 2.0, SAML, Kerberos…)

- I **sistemi di gestione centralizzati** come **Active Directory**, sistemi **IAM** (Identity and Access Management), **OAuth 2.0**, **SAML** e **Kerberos** sono utilizzati per facilitare e controllare l'accesso agli utenti e alle risorse in un ambiente informatico. Ognuno di questi sistemi ha un ruolo specifico nella gestione dell'identità, dell'autenticazione e dell'autorizzazione degli utenti.

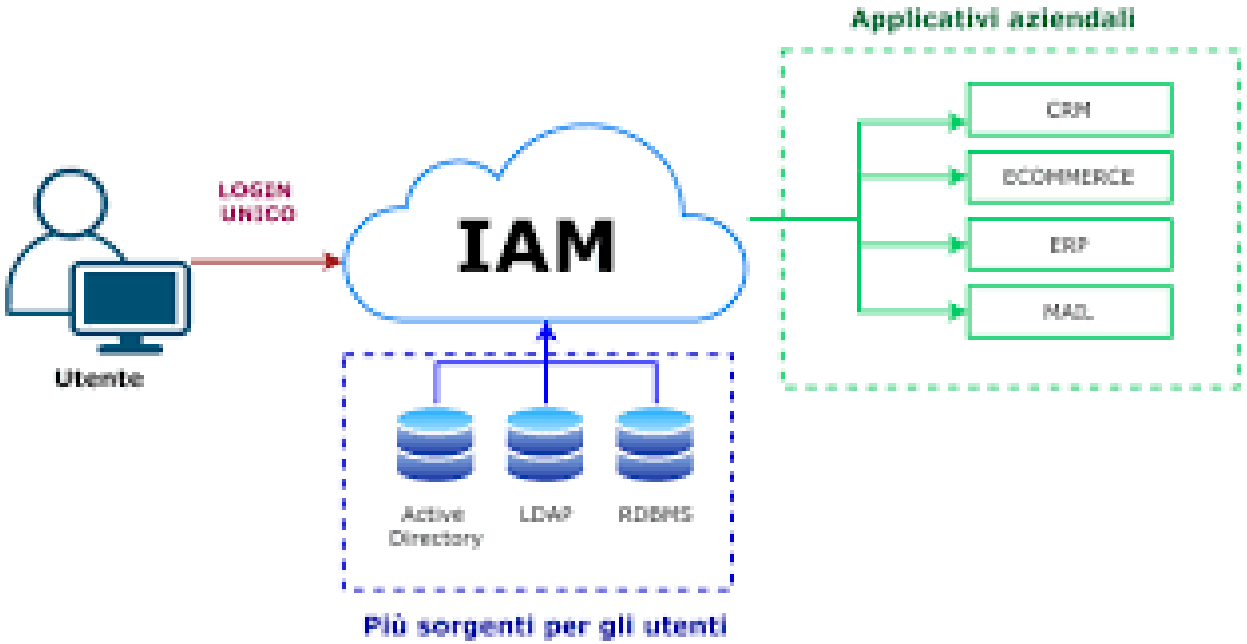


Sistemi di gestione centralizzati (Active Directory, Sistemi IAM, OAuth 2.0, SAML, Kerberos…)

- **Active Directory (AD)**: **Active Directory** è un servizio di directory sviluppato da Microsoft, ampiamente utilizzato nei sistemi operativi Windows. Funziona come un database centralizzato per memorizzare le informazioni sugli utenti, i gruppi e le risorse di rete. AD offre funzionalità di autenticazione, autorizzazione e gestione delle risorse in un dominio Windows.

Sistemi di gestione centralizzati (Active Directory, Sistemi IAM, OAuth 2.0, SAML, Kerberos…)

- **Sistemi IAM** (Identity and Access Management): **IAM** è un framework che gestisce l'identità digitale degli utenti e controlla l'accesso alle risorse. Consente di creare, gestire e revocare le identità degli utenti, di definire i loro ruoli e le autorizzazioni associate. IAM fornisce un controllo centralizzato sull'accesso alle risorse sia all'interno che all'esterno di un'organizzazione.

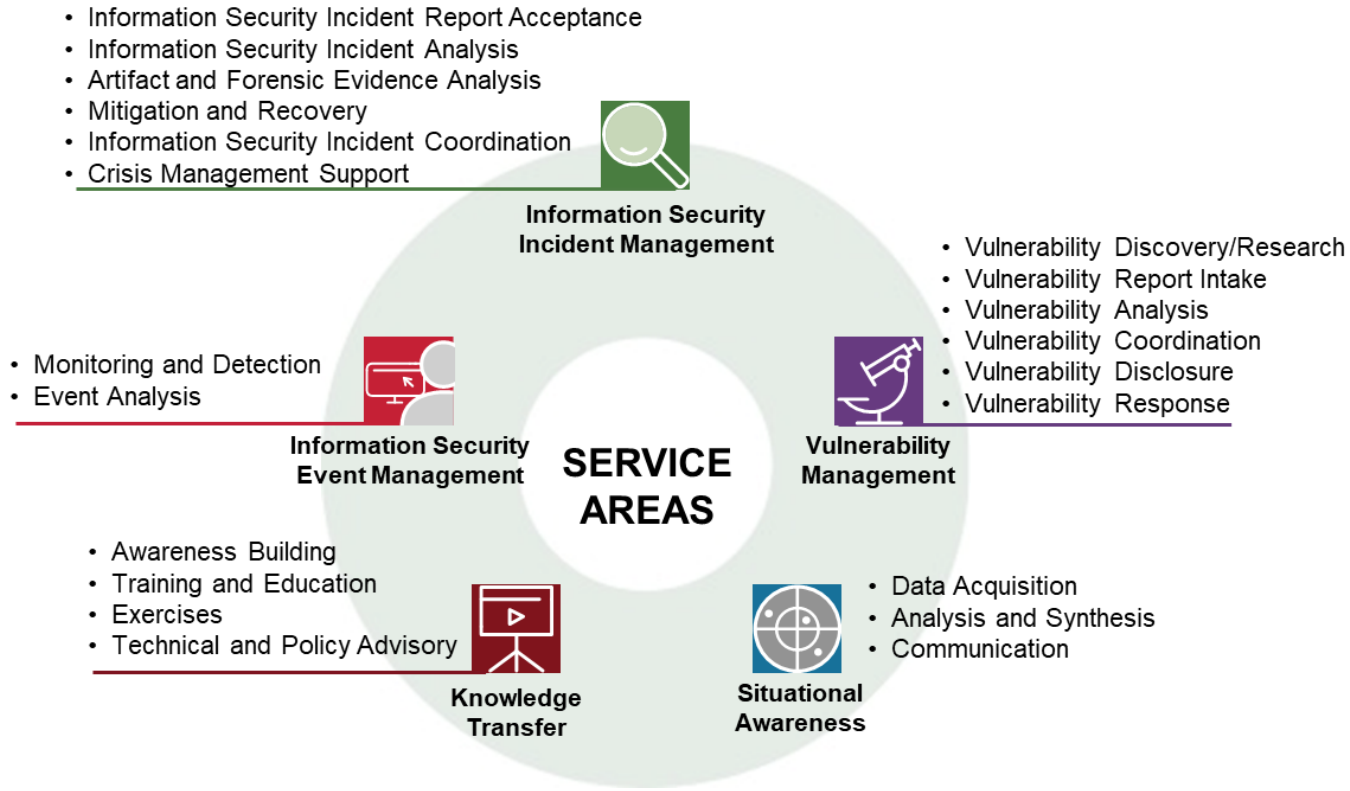


Sistemi di gestione centralizzati (Active Directory, Sistemi IAM, OAuth 2.0, SAML, Kerberos…)

- **OAuth 2.0**: OAuth 2.0 è un protocollo di autorizzazione che consente a un'applicazione di ottenere l'accesso ai dati di un utente su un server di risorse, senza richiedere le credenziali di accesso dell'utente. È ampiamente utilizzato per consentire l'autenticazione e l'autorizzazione sicure tra servizi e applicazioni di terze parti, ad esempio quando si accede a un'app utilizzando le credenziali di accesso di un account Google o Facebook.

Funzioni di CSIRT, SOC e ISAC

- Le funzioni di **CSIRT** (Computer Security Incident Response Team), **SOC** (Security Operations Center) e **ISAC** (Information Sharing and Analysis Center) sono strettamente connesse e spesso lavorano in collaborazione per garantire la sicurezza informatica di un'organizzazione o di una comunità.



Funzioni di CSIRT, SOC e ISAC

- **CSIRT** (Computer Security Incident Response Team): Un **CSIRT** è un team dedicato alla gestione degli incidenti di **sicurezza informatica**. Il suo obiettivo principale è quello di rilevare, rispondere e mitigare gli attacchi informatici. I membri del team **CSIRT** sono addestrati per identificare le minacce, analizzare gli incidenti di sicurezza e coordinare le risposte appropriate. Possono anche fornire consulenza sulla sicurezza informatica e promuovere le migliori pratiche all'interno di un'organizzazione.

Funzioni di CSIRT, SOC e ISAC

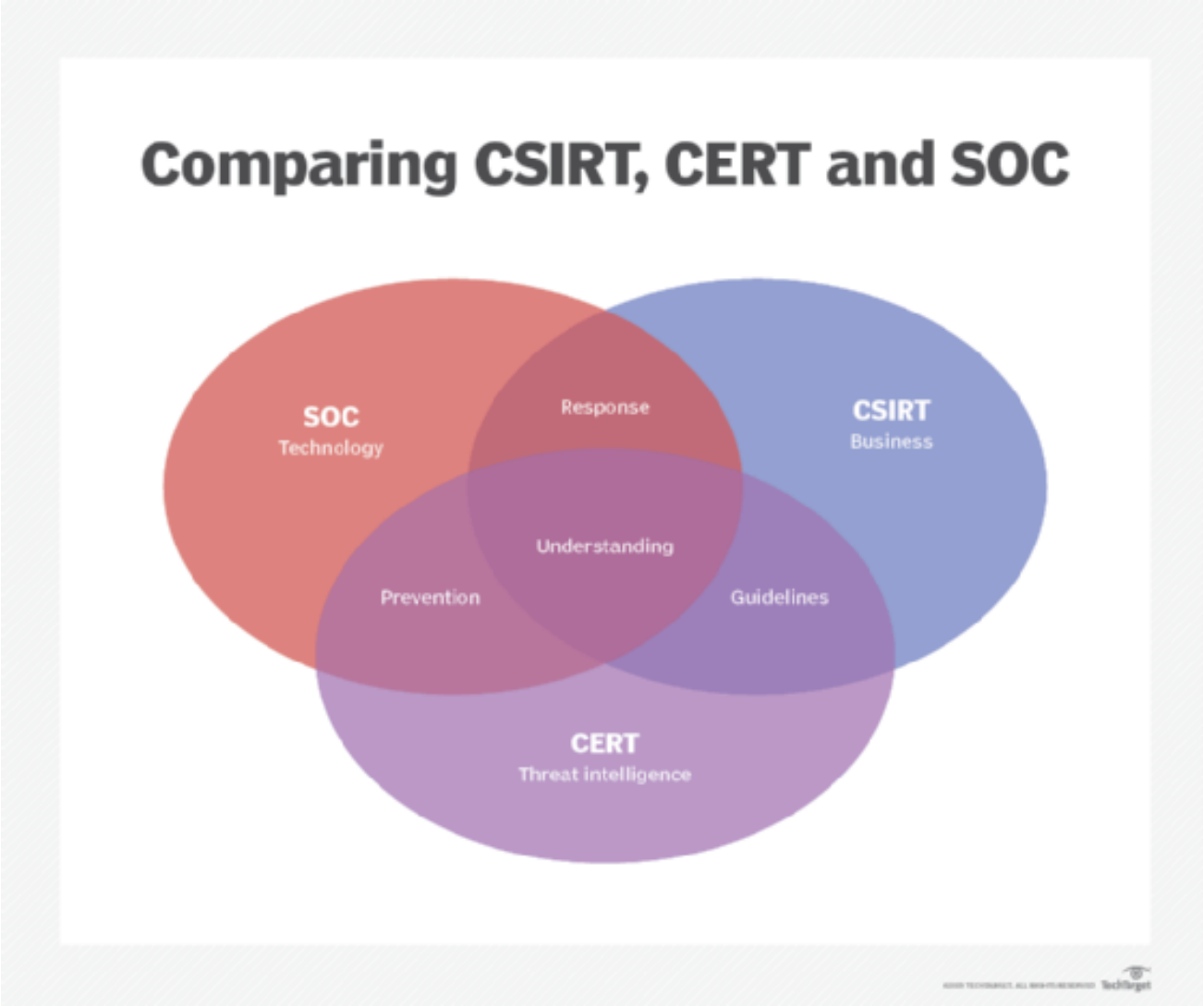
- **SOC** (Security Operations Center): Un **SOC** è un centro operativo specializzato nella gestione della **sicurezza informatica**. Solitamente è composto da un gruppo di esperti che monitorano costantemente gli **eventi di sicurezza**, analizzano le **anomalie** e rispondono agli incidenti. Il SOC utilizza tecnologie avanzate, come i sistemi di rilevamento delle intrusioni (**IDS**) e le soluzioni di gestione delle informazioni e degli eventi di sicurezza (**SIEM**), per monitorare e analizzare il traffico di rete e i log dei sistemi al fine di identificare potenziali minacce. Il SOC svolge anche attività di risposta agli incidenti, collaborando con il team CSIRT o con altre entità interne o esterne all'organizzazione.

Funzioni di CSIRT, SOC e ISAC

- **ISAC** (Information Sharing and Analysis Center): Un **ISAC** è un'organizzazione che facilita lo scambio di informazioni sulla sicurezza informatica tra diverse entità, come organizzazioni governative, aziende, organizzazioni non profit e fornitori di servizi. L'obiettivo principale di un **ISAC** è promuovere la collaborazione e la condivisione di informazioni sulla minaccia cibernetica per migliorare la sicurezza complessiva. Gli ISAC raccolgono, analizzano e diffondono informazioni sulle minacce e sulle migliori pratiche di sicurezza informatica, consentendo alle organizzazioni aderenti di essere più consapevoli dei rischi e di prendere misure preventive appropriate.

Funzioni di CSIRT, SOC e ISAC

- In sintesi, **CSIRT**, **SOC** e **ISAC** rappresentano tre aspetti complementari della sicurezza informatica: il **CSIRT** gestisce gli incidenti di sicurezza, il **SOC** monitora e analizza gli eventi di sicurezza in tempo reale, mentre gli **ISAC** favoriscono la condivisione delle informazioni sulla minaccia tra le organizzazioni.



Bibliografia