Report Progetto

W20-D5

Redatto da Andrea Sciattella

05/07/2024

INDICE

Indice **2**

1. Traccia **3**

2. Azioni preventive **4**

3. Impatti sul business **5**

4. Response **6**

5. Soluzione completa **7**

6. Modifica «più aggressiva» dell'infrastruttura **8**

1. TRACCIA

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti:

1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

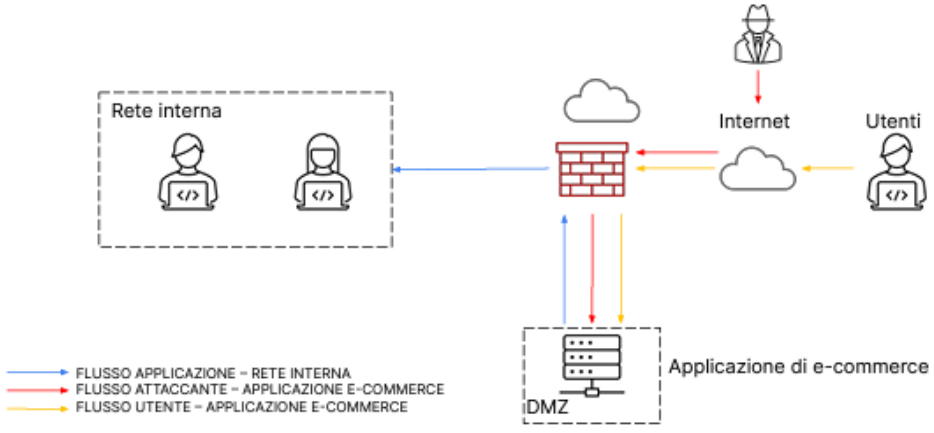
3. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide due con la soluzione proposta.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2).**

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



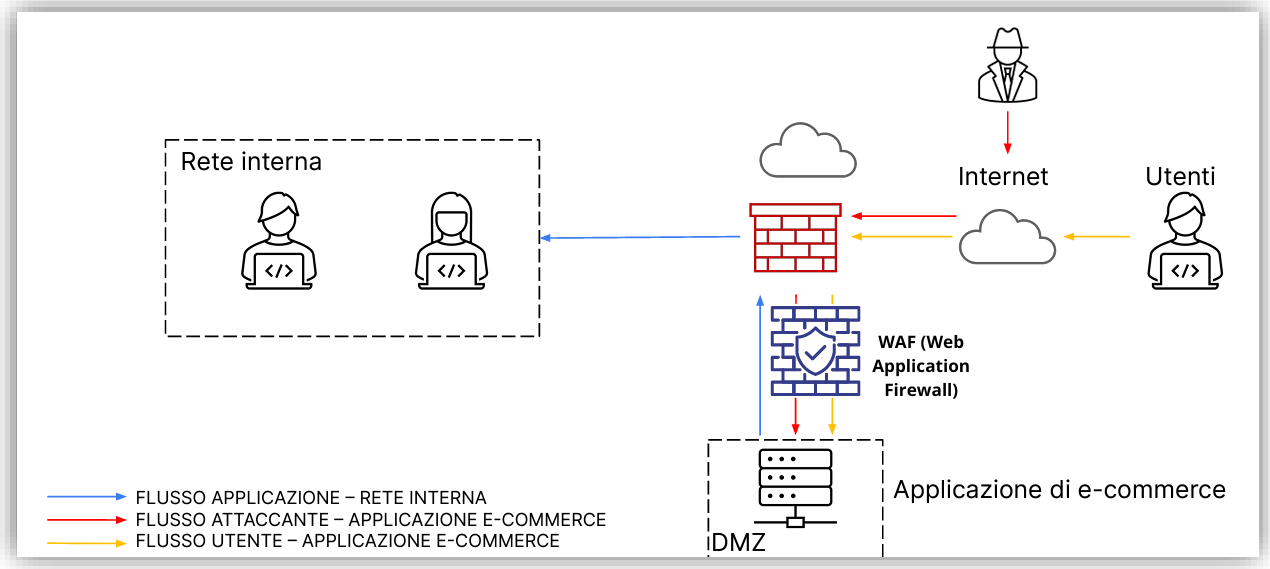
2. AZIONI PREVENTIVE

"Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni."

Per difendere l'applicazione web dagli attacchi **SQL Injection (SQLi) e Cross-Site Scripting (XSS),** possiamo implementare diverse azioni preventive, tra cui le più valide:

1. **Validazione e sanificazione degli input**: Anche se spesso viene dato per scontato e di conseguenza trascurato, bisogna assicurarsi che tutti i dati forniti dagli utenti siano correttamente validati e sanificati durante l'input nei campi della Web App per prevenire l'iniezione di comandi SQL o script dannosi.
2. **Utilizzo di prepared statements (SQL parametrizzati)**: Per prevenire gli attacchi SQLi, utilizzare le query SQL parametrizzate ci permette di non concatenare stringhe di query SQL, e utilizzare dei segnaposto per i parametri di input dell'utente.
3. **Firewall per applicazioni web (WAF)**: La soluzione più semplice e meno dispendiosa, è l'utilizzo di un firewall per applicazioni web che può identificare e bloccare i tentativi di attacco SQLi e XSS.
4. **Aggiornamenti, patching, monitoraggio e logging**: Assicurarsi che tutti i software e i framework utilizzati siano aggiornati con le ultime patch di sicurezza, il tutto affiancato da sistemi di monitoraggio e logging per rilevare attività sospette.

Come richiesto dal quesito n.1, nella nostra architettura di rete andremo ad implementare la soluzione numero 3, ***un Web Application Firewall*** che a differenza dei soliti Firewall viene utilizzato appositamente per Web App. Lo posizioniamo tra la DMZ (Demilitarized Zone) e l'accesso ad internet, in modo da proteggere dal traffico in entrata da internet (sia utenti che attaccante).



3. IMPATTI SUL BUSINESS

"L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per dieci minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce."

Calcoliamo dell'impatto sul business dovuto a un attacco ***DDoS (Distributed Denial of Service***) che rende l'applicazione non raggiungibile per dieci minuti. Tenendo conto che gli utenti spendono *€1.500* ogni minuto sulla piattaforma e in caso di attacco DDoS la piattaforma di e-commerce si fermerebbe per 10 minuti:

- **Spesa al minuto**= €1.500/ Minuto
- **Tempo**= 10 minuti di irraggiungibilità

Possiamo constatare che:

- **Impatto**= 10 * 1.500= *€15.000*

Le *migliori azioni preventive* per attacco DDoS potrebbero essere:

- **Utilizzo di CDN (Content Delivery Network)**: Una rete di server distribuiti geograficamente che lavorano insieme per fornire rapidamente contenuti Internet in modo da ridurre latenza e aumentare velocità tramite la vicinanza dei server CDN distribuendo il traffico su diversi server, riducendo l'impatto di un attacco DDoS.
- **Servizi di mitigazione DDoS**: Utilizzare servizi specifici per la mitigazione degli attacchi DDoS, che possono identificare e filtrare il traffico dannoso come i servizi offerti da Cloudflare, che comprende server CND e WAF.
- **Bilanciamento del carico**: Implementare un sistema di bilanciamento del carico (hardware o software) per distribuire equamente il traffico tra i vari server per garantire la disponibilità continua dei servizi.

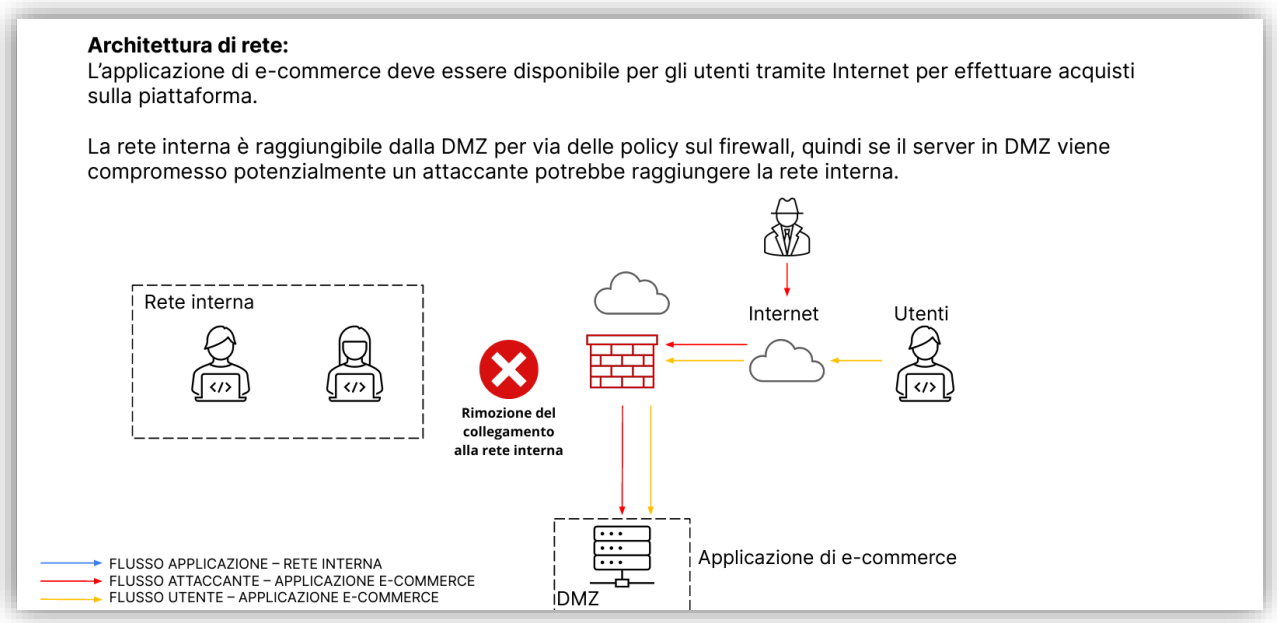
4. RESPONSE

"L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide due con la soluzione proposta."

Data la priorità alla rete interna, come primo passo andremo ad **isolare immediatamente il server** infetto dalla rete per impedire la diffusione del malware.

Questo può essere fatto **disabilitando la connessione di rete** del server alla rete interna tramite:

- Cavo fisico;
- Disabilitando la connessione della scheda rete;
- Implementando una policy firewall per bloccare l'indirizzo IP.

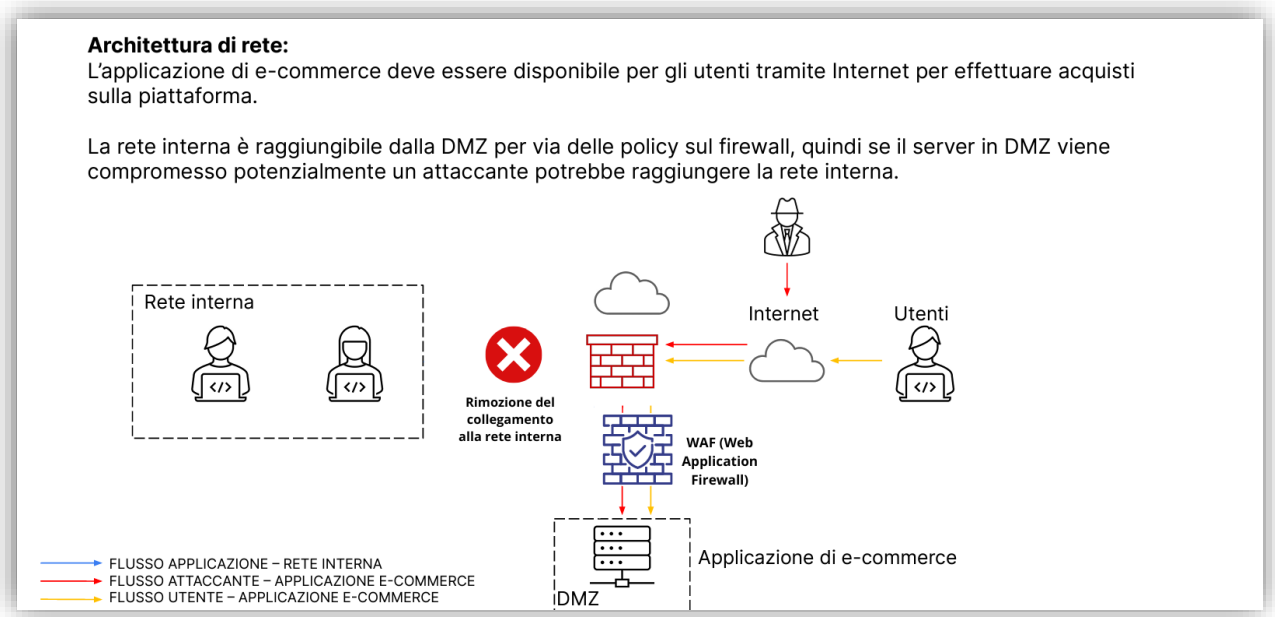


Un'altra possibile soluzione è il ***Disaster Recovery as a Service*** (DRaaS), una soluzione di continuità operativa che offre servizi di replica e hosting di server e sistemi in una posizione geografica diversa, per consentire il ripristino dei servizi critici in caso di disastro.

Implementando il *DRaaS* alla struttura, si **migliorerà significativamente la resilienza** di tutto il complesso, garantendo che i dati e le applicazioni critiche siano sempre protetti e recuperabili in caso di "disastro".

5. SOLUZIONE COMPLETA

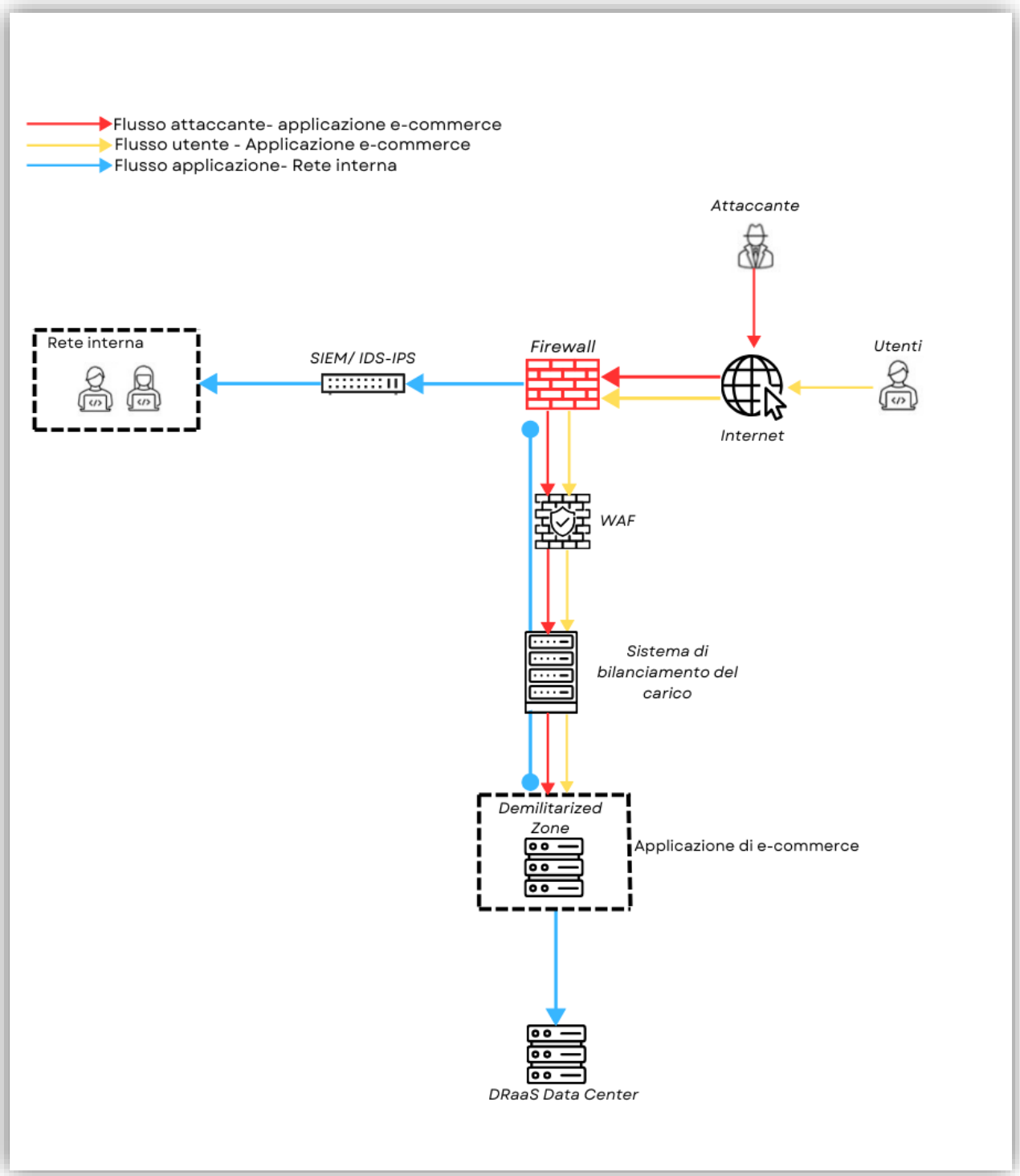
"Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)."



In questa fase abbiamo unito le due architetture di sistema create nelle precedenti fasi, creando così una struttura più solida e sicura:

- Tramite la prima soluzione, abbiamo aggiunto un **WAF (Web Application Firewall)** come protezione in entrata e in uscita per la Web App di e-commerce presente nel server della DMZ.
- Nella seconda soluzione invece abbiamo **rimosso il collegamento dalla DMZ alla rete interna**, in caso di infezione da malware che si propagherebbe da un attaccante, al server della Web App e infine alla rete interna, creando danni e problemi di entità grave alla struttura dell'azienda.

6. MODIFICA «PIÙ AGGRESSIVA» DELL'INFRASTRUTTURA



Abbiamo implementato diverse soluzioni per migliorare la sicurezza, la disponibilità e le prestazioni dell'architettura di rete. Le aggiunte che hanno rivoluzionato la nostra struttura sono:

1. Load Balancer:

Un dispositivo o software che distribuisce il traffico di rete o delle applicazioni tra più server che ha diversi vantaggi:

- Con la distribuzione del carico **evita che i server si sovraccarichino** distribuendo uniformemente il traffico tra più server, come in caso di attacchi *DDoS* (Soluzione punto 2).
- L'alta disponibilità che in caso di guasto di un server, **reindirizza il traffico ai server funzionant**i, riducendo il rischio di downtime.
- La scalabilità facilita **l'aggiunta di nuovi server** senza interruzioni del servizio.
- **Ottimizza la velocità di risposta** delle applicazioni, migliorando l'esperienza utente.

2. DRaaS (Disaster Recovery as a Service)

Una soluzione che replica e ospita server fisici e virtuali da un'altra posizione geografica per garantire il ripristino rapido in caso di disastro ed apporta i seguenti vantaggi:

- La continuità del Servizio assicura che i dati e le applicazioni critiche siano **sempre disponibili** anche in caso di disastro.
- Il failover automatico **mantiene l'applicazione operativa** senza interruzioni significative, minimizzando il downtime.
- La **replica continua copia e mantiene i dati in una posizione sicura**, riducendo il rischio di perdita di dati.

3. WAF (Web Application Firewall)

Un dispositivo di sicurezza che monitora, filtra e blocca il traffico HTTP e HTTPS verso e dalle applicazioni web, che porta come vantaggi:

- **Blocca attacchi come SQL injection e Cross-Site Scripting (XSS)**, proteggendo i dati sensibili degli utenti.
- **Mitiga le vulnerabilità** senza necessità di aggiornamenti immediati al codice sorgente.
- Aiuta a **rispettare le normative di sicurezza dei dati**, come GDPR e PCI-DSS.

4. SIEM (Security Information and Event Management)

Il SIEM è uno strumento fondamentale per la raccolta, l'analisi e la gestione dei log di sicurezza e degli eventi di rete. L'implementazione di un SIEM nell'architettura di rete permette di centralizzare il monitoraggio della sicurezza, rilevare minacce e rispondere agli incidenti in modo più efficiente

soprattutto se integrato ad un sistema IDS (Intrusion Detection System) e IPS (Intrusion Prevenction System). Tra i benefici apportati abbiamo:

- Il SIEM **offre una visibilità centralizzata** (monitoraggio centralizzato) di tutti i log di sicurezza e delle attività di rete, facilitando il monitoraggio e l'analisi degli eventi di sicurezza.
- **Analizza i dati raccolti in tempo reale** per rilevare attività sospette o anomalie che potrebbero indicare una violazione della sicurezza.
- **Correla eventi di sicurezza provenienti da diverse fonti** per identificare attacchi complessi e multivettore che potrebbero sfuggire a sistemi di sicurezza isolati.
- **Genera report dettagliati e analisi forensi** per supportare le indagini di sicurezza e fornire insights per migliorare le difese della rete.

5. IDS (Intrusion Detection System) e IPS (Intrusion Prevention System)

Un Intrusion Detection System (IDS) è un dispositivo o software che monitora il traffico di rete per rilevare attività sospette o potenzialmente dannose mentre un Intrusion Prevention System (IPS) è un dispositivo o software complementare all'IDS che previene attività sospette o potenzialmente dannose. Le loro funzioni sono:

- **L'IDS e l'IPS lavorano insieme per rilevare e prevenire minacce** prima che possano danneggiare i sistemi interni, creando così una protezione proattiva.
- Forniscono una sorveglianza costante della rete, identificando e rispondendo rapidamente agli attacchi.
- **Mitigano il rischio di violazioni di sicurezza**, proteggendo la rete da attacchi noti e sconosciuti.
- **Migliorano la visibilità** sulle attività di rete e offrono un **maggiore controllo** sulle politiche di sicurezza.