

Esercitazione Fine modulo 5

Security Operation & Threat Intelligence

Progetto

Fabio Benevento - 24/03/2024

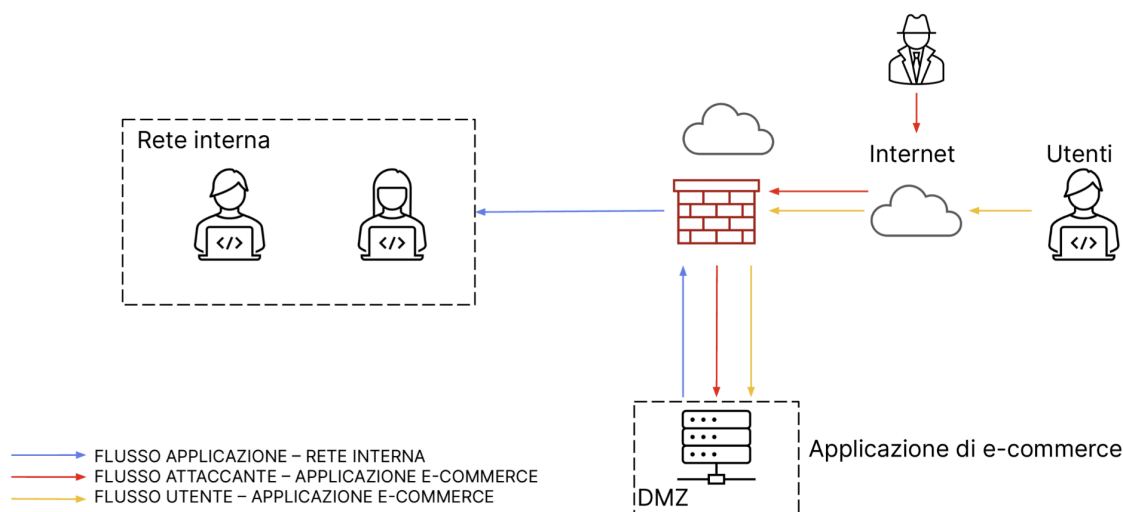
Traccia

Con riferimento alla figura, 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 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.



Svolgimento

1. Azioni preventive

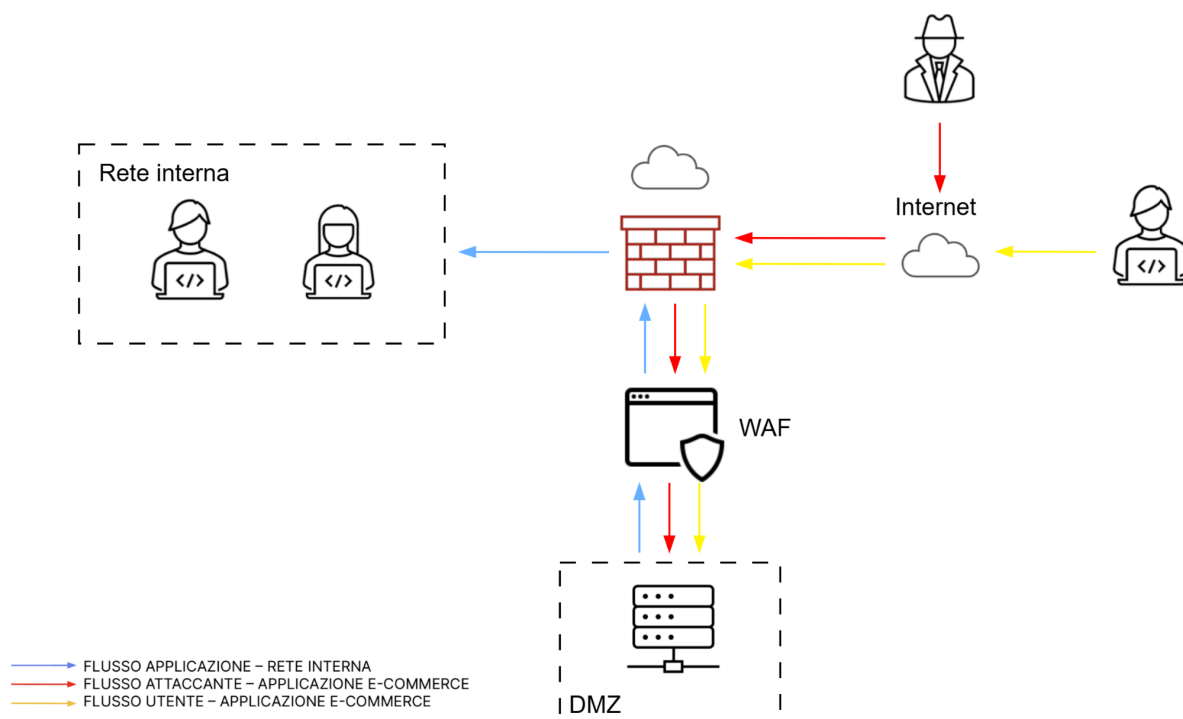
Al fine di proteggere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato, sarebbe possibile utilizzare uno specifico tipo di firewall denominato **Web Application Firewall (WAF)**. L'obiettivo principale di questo tipo di firewall è proprio quello di proteggere le applicazioni web da una varietà di minacce, come attacchi di tipo injection (SQL injection, XSS), cross-site scripting (XSS), e altre vulnerabilità che potrebbero essere sfruttate da malintenzionati.

Nel caso l'applicazione sia prodotta internamente all'azienda è importante sensibilizzare il reparto sviluppo nell'adozione di best-practice nella scrittura del codice e nell'adozione di maggiori controlli preventivi al fine di ridurre le potenziali vulnerabilità sfruttabili da un utente malevolo (**S-SDLC**: secure software development life cycle).

Ciò può essere ottenuto eseguendo periodicamente, soprattutto prima del rilascio di una nuova versione, sessioni di **analisi statica/dinamica del codice** tramite appositi tool al fine di evidenziare immediatamente eventuali vulnerabilità e porvi rimedio.

Nel caso invece si adottino applicazioni di terze parti, è bene, da parte del reparto IT, monitorare il rilascio di patch di sicurezza o nuove versioni del software, ed eseguire gli aggiornamenti in tempi rapidi ove possibile.

Allo stesso modo è importante eseguire periodicamente **cicli/sessioni di vulnerability assessment / penetration testing** al fine di evidenziare vulnerabilità generali della rete aziendale.



2. Impatti sul business

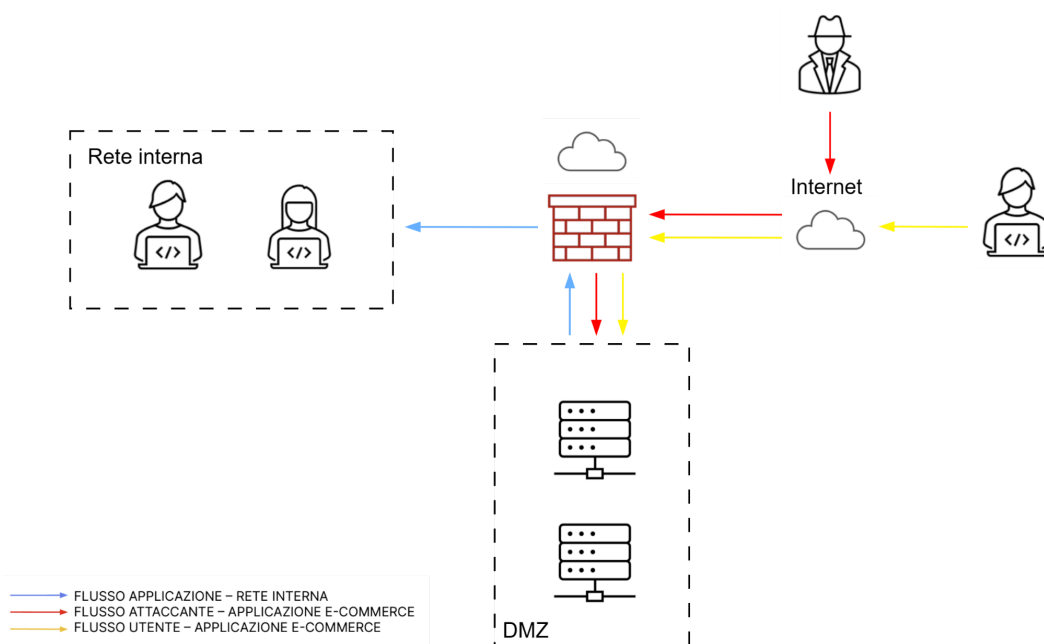
Considerando una spesa media per minuto da parte degli utenti di 1500€, un'attacco DDos che causa un disservizio di 10 minuti provoca un costo per l'azienda per singolo avvenimento (SLE: Single Loss Expectancy) di

$$\text{SLE} = 1500\text{€/min} \times 10 \text{ min} = 15000\text{€}$$

Ad esso andrebbero aggiunti costi più difficilmente quantificabili causati dalla pubblicità negativa in seguito all'evento e dal malcontento/sfiducia nei clienti che potrebbero portare gli utenti a preferire altri competitor.

Al fine di garantire la business continuity e limitare i disservizi in caso di attacco, è importante per l'azienda rendere l'applicazione maggiormente resiliente e tollerante agli errori, ridondando l'applicazione tramite quello che viene chiamato **"failover cluster"** come illustrato in figura.

In una configurazione di questo tipo, il server secondario dove è replicata l'applicazione, normalmente "dormiente", in caso di malfunzionamenti del server primario, diventa attivo secondo un processo denominato per l'appunto "failover", garantendo la continuità di disponibilità dell'applicazione e dei servizi core e quindi del business.



Naturalmente andranno fatte opportune valutazioni da parte del management per capire se ha senso applicare la soluzione in termini di costo/benefici o se è preferibile accettare/demandare il rischio

In quest'ottica, considerando una azienda di medie/piccole dimensioni, sarebbe possibile valutare l'adozione di servizi in cloud in luogo di quelli on-premise secondo quello che è il paradigma di Disaster Recovery as a Service come ad esempio il servizio **Azure Site Recovery** offerto da Microsoft. Questo tipo di soluzione permette di ottenere un duplice vantaggio:

- in primo luogo permette un contenimento dei costi rispetto alla soluzione on-premise dato che non è necessario comprare ulteriori apparati hardware per implementare la soluzione ma il costo è legato solo all'effettivo utilizzo del servizio
- in secondo luogo ciò garantisce anche una diversificazione geografica difficilmente ottenibile per aziende di piccole dimensioni, con una sola sede fisica, rendendo quindi il servizio maggiormente tollerante a minacce anche di tipo ambientale

Lo svantaggio rispetto ad una soluzione on-premise sta principalmente nei tempi superiori di ripristino del sistema, per cui bisognerà assicurarsi che essi rispettino la regola $RTO \leq MTD$, ovvero che il tempo per recuperare un sistema o una funzionalità critica in caso di disastro sia minore del tempo limite durante il quale un business può

non essere operativo senza causare danni irreparabili al business stesso.

L'adozione di queste soluzioni non esula dall'esecuzione di procedure di backup, che devono essere svolte manualmente dal personale o tramite sistemi automatizzati al fine da avere sempre a disposizione una copia dei dati, dei sistemi e delle configurazioni attualmente in produzione da cui ripartire a fronte di un disastro irreparabile.

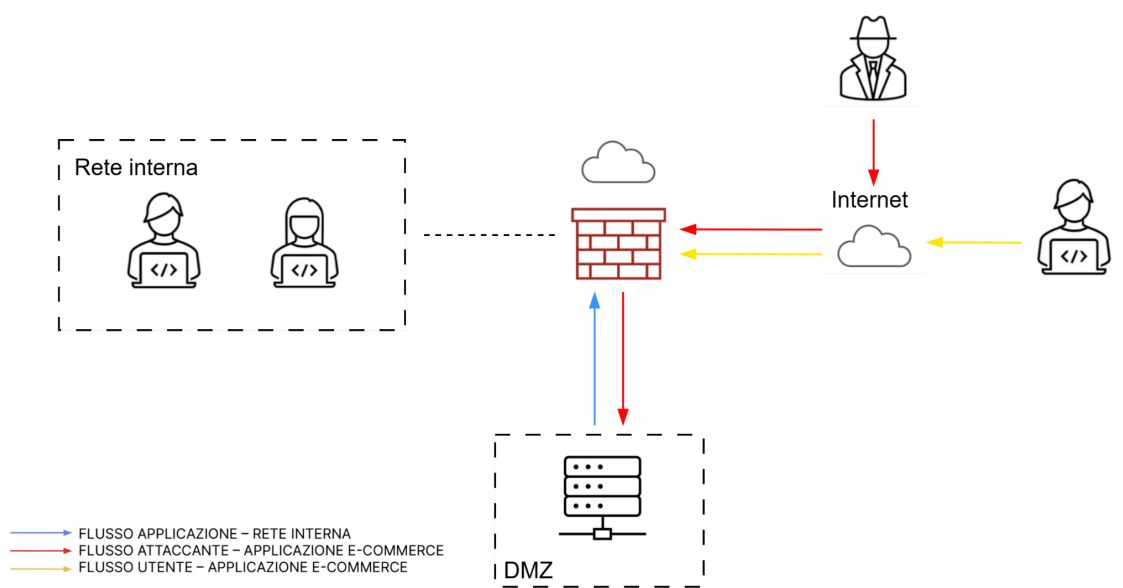
3. Response

Nel caso l'applicazione risulti compromessa da un malware, bisogna in primo luogo isolare o rimuovere tempestivamente il sistema infetto al fine di evitare che il malware possa propagarsi nella rete e creare danni ad altri nodi.

Ciò si ottiene segmentando la rete in maniera da separare il sistema infetto dal resto della rete e permettere quindi di procedere con le fasi di analisi e ripristino

Nella configurazione iniziale l'applicazione/sistema infetto risulta essere già su una sottorete diversa (DMZ) rispetto al resto della rete (rete interna) ma non isolata da essa in quanto la rete interna risulta essere raggiungibile dalla rete DMZ.

Nell'ipotesi che la DMZ contenga la sola applicazione infetta, come soluzione primaria più semplice è quindi necessario modificare le policy del firewall al fine interrompere la comunicazione tra DMZ e rete interna come illustrato in figura. Essendo l'applicazione ormai compromessa è inoltre importante bloccare gli accessi anche da parte dei normali utenti, agendo sempre sul firewall per bloccare la comunicazione.

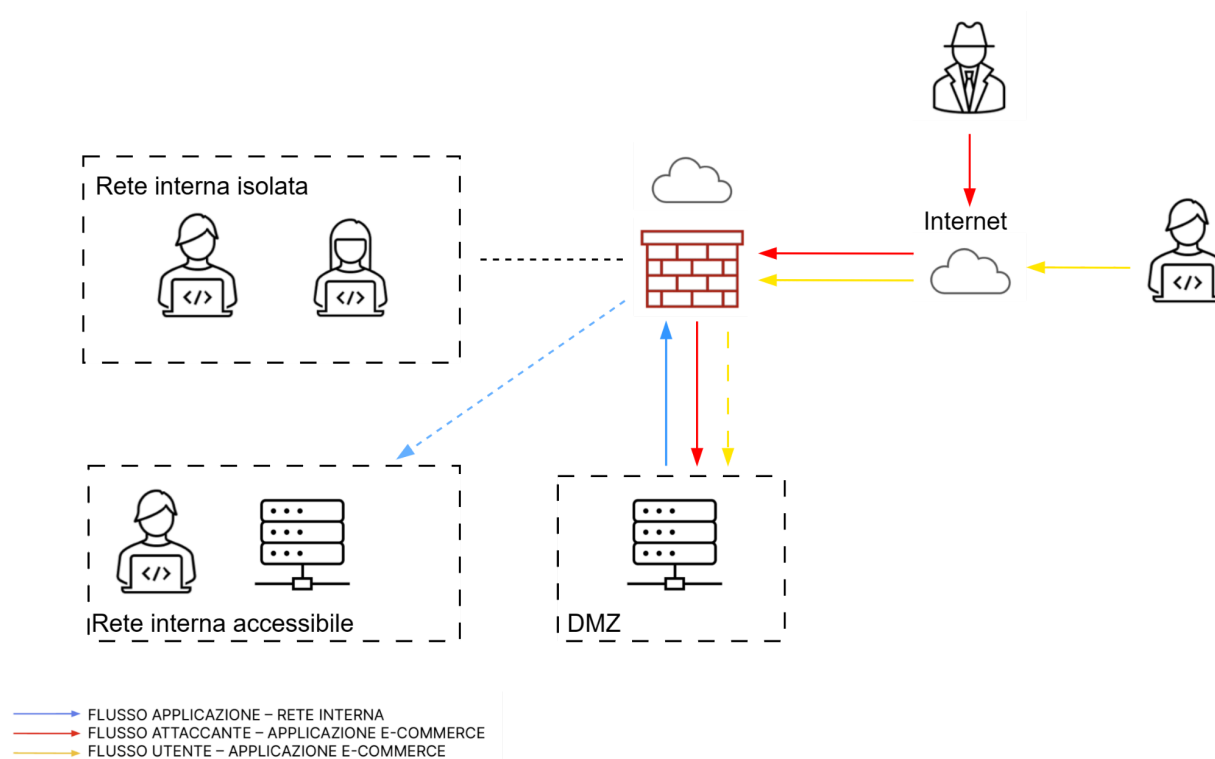


In seguito alla fase di contenimento si passa alla fase di rimozione, con il ripristino del sistema/applicazione e l'esecuzione di tutte le contromisure ad evitare che l'attacco possa verificarsi nuovamente (applicazione delle patch dove disponibili, revisione delle politiche dei firewall, etc..)

In ottica preventiva, nel caso l'applicazione abbia effettivamente necessità di accedere alla rete interna (ad esempio ivi sono collocati giustamente componenti non direttamente accessibili dall'esterno come backend applicazione, database, etc..) è auspicabile segmentare ulteriormente la rete al fine di adottare una politica zero-trust e rendere accessibile alla DMZ solo i componenti necessari.

4. Soluzione completa

Riepilogando quanto illustrato nei punti precedenti è possibile ipotizzare la seguente architettura finale (azione preventiva + azione risolutiva), in cui la rete interna è stata ulteriormente segmentata secondo la soluzione citata in precedenza. Le frecce tratteggiate stanno ad indicare il senso della comunicazione dopo il ripristino del sistema in seguito all'attacco.



5. Modifica «più aggressiva» dell'infrastruttura

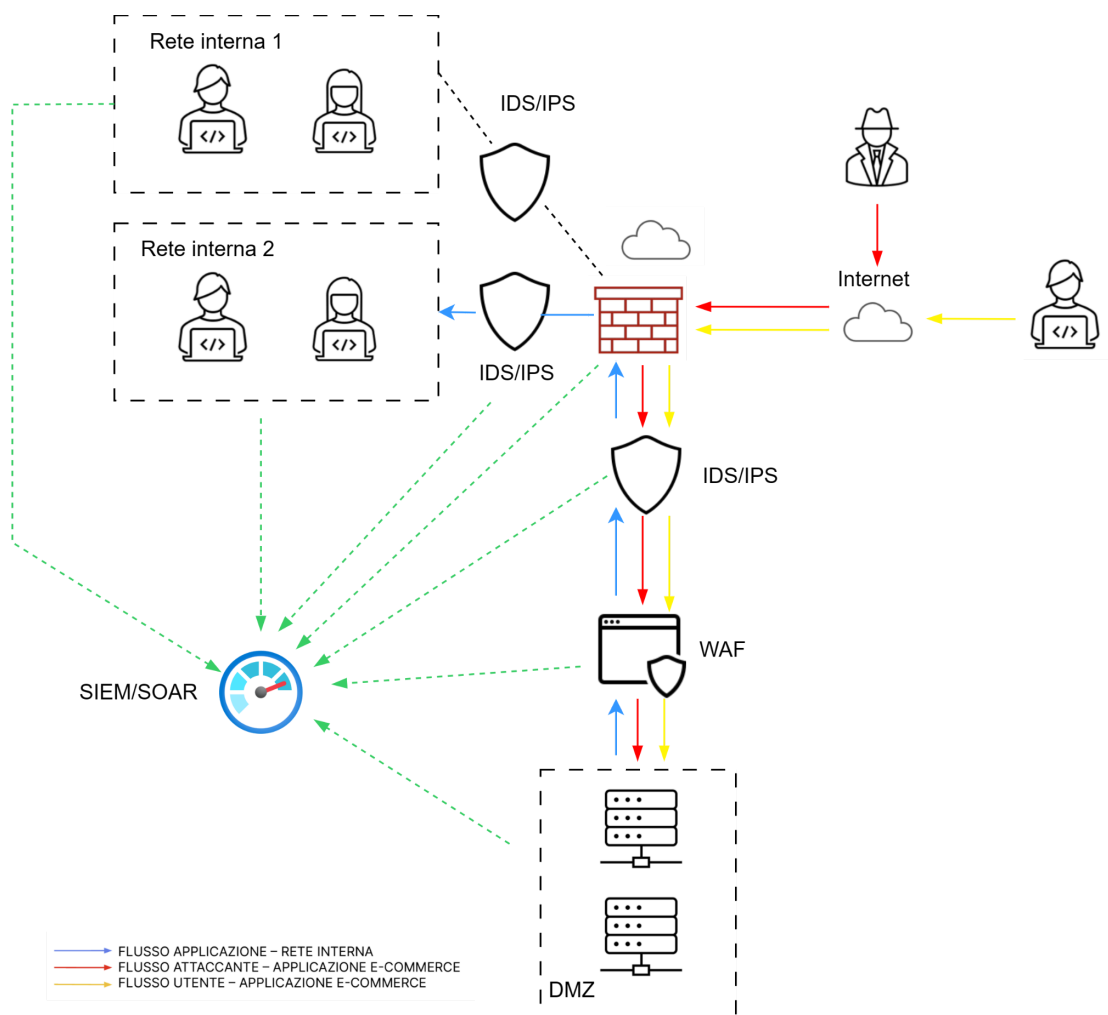
Per rendere l'applicazione ancora più sicura e tollerante agli errori è possibile in primo luogo adottare la soluzione di ridondanza (failover "cluster") proposta al punto 2.


Come illustrato in precedenza è importante

E' possibile inoltre fare uso di sistemi di **IDS/IPS** al fine rilevare e prevenire diverse tipologie di attacchi oltre a quelli specifici indicati al punto 1.

La principale differenza tra i due è che un IDS rileva solo le intrusioni e genera avvisi, mentre un IPS rileva e blocca le intrusioni in tempo reale. Molto spesso questi strumenti sono integrati all'interno dei firewall più sofisticati (Next Generation Firewall)

Inoltre è possibile monitorare in maniera centralizzata ed integrata tutti i log e gli allarmi raccolti adottando un sistema **SIEM** al fine di avere un quadro più ampio e generale di ciò che accade nei dispositivi della rete specialmente in caso di attacco.





Un sistema SIEM raccoglie, normalizza, analizza e correla i dati provenienti da varie fonti di sicurezza, come registri di sistema, registri di sicurezza, dispositivi di rete, sistemi di rilevamento delle intrusioni e molto altro ancora, offrendo quindi visione completa e in tempo reale della sicurezza informatica di un'organizzazione.

Ipotizzando sempre che l'azienda sia di medie/piccole dimensioni, è possibile fare ricorso a strumenti di questo tipo offerti in Cloud al fine di ridurre i costi di gestione.

Facendo sempre riferimento all'ecosistema Microsoft Azure è possibile usare il servizio **Azure Sentinel** come "log collector" il quale estende le funzionalità di SIEM con quelle di SOAR (Security Orchestration, Automation, and Response) aggiungendo capacità di orchestrazione e automazione avanzate per migliorare la gestione degli incidenti di sicurezza e ridurre i tempi di risposta agli eventi di sicurezza.

Relativamente agli strumenti anti-intrusione è possibile fare ricorso ad **Azure Firewall** che offre funzionalità avanzate di IDS/IPS.

Entrambi gli strumenti permettono la gestione di architetture ibride on-premise/cloud con integrazione anche di servizi ospitati in cloud di terze parti (AWS, Google, etc...).

E' di recente l'integrazione con strumenti di intelligenza artificiale (AI) al fine di coadiuvare e semplificare il lavoro degli analisti di sicurezza informatica (Microsoft Azure Copilot for Security)