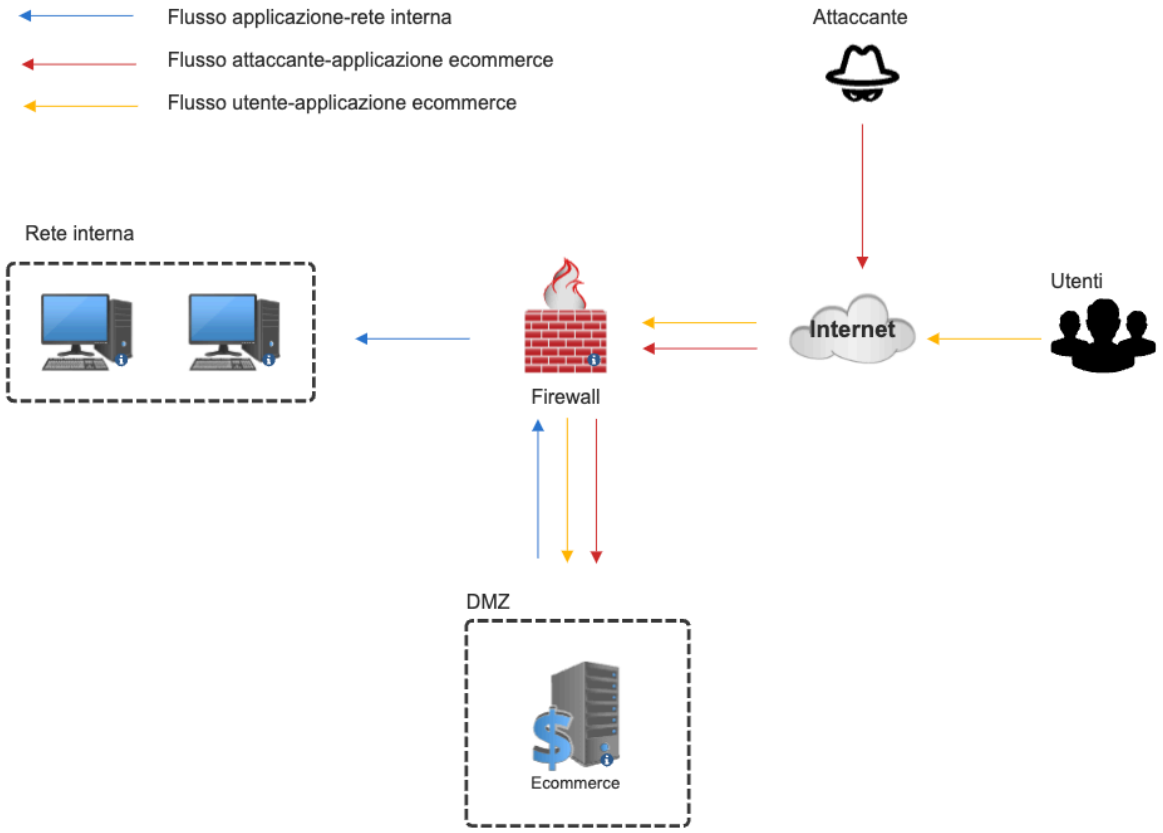
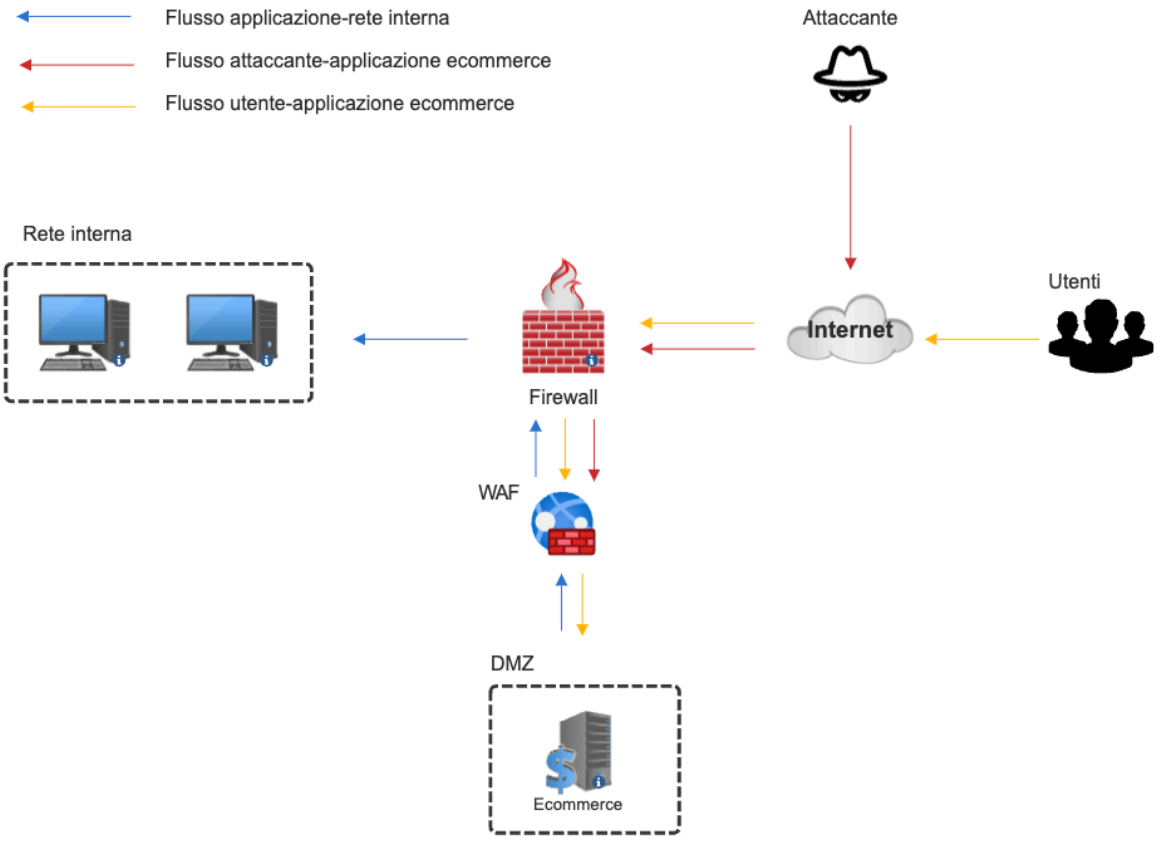
Security Operation Center

Questo progetto è l'analisi di un attacco e successivamente una messa in sicurezza di un'applicazione web di un'azienda che ha un e-commerce, questa è l'infrastruttura del sistema:



Come è possibile notare l'attaccante è riuscito a entrare nel server e-commerce dell'azienda, successivamente analizzeremo la situazione e cercheremo di porre rimedio a questo attacco.
Nei successivi punti analizzeremo l'infrastruttura della rete e proporrò alcune soluzioni per renderla più sicura. Nei prossimi punti possiamo valutare alcuni casi che potremmo riscontrare in caso di attacco:

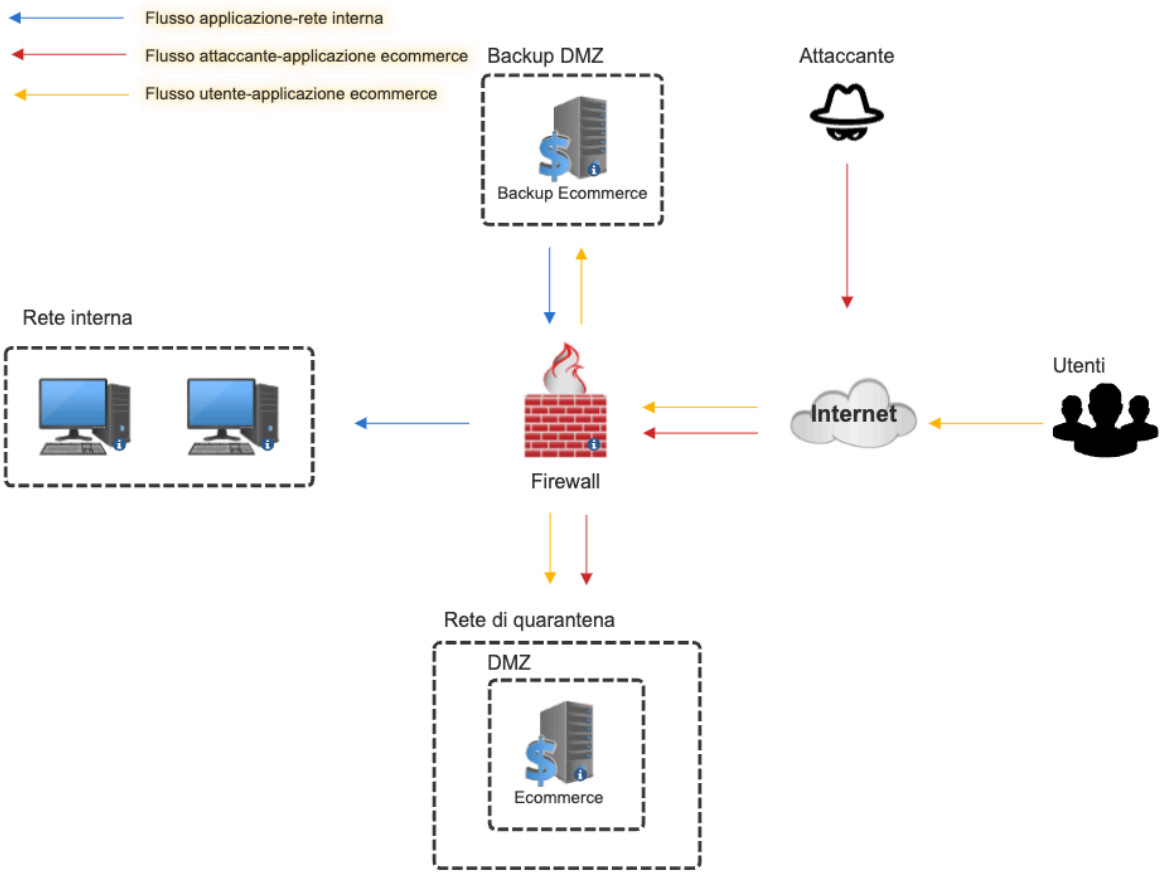
1. **L'applicazione web è vulnerabile agli attacchi SQLi e XSS:**
   Per mitigare questa vulnerabilità esiste un dispositivo specifico creato per le applicazioni web ovvero il web application firewall (WAF).
   Ecco una rappresentazione del sistema con un WAF implementato.



Come è possibile notare l'attacco XSS/SQLi viene bloccato dal WAF, quindi una volta implementato questo dispositivo, il flusso dall'applicazione web alla rete interna risulta sicuro.

2. **Valutazione di un attacco DDoS e impatto economico sull'azienda stessa.**
   L'azienda in questione afferma che in media genera € 1500/minuto, occorre dunque considerare che in caso di attacco ai server o di qualsiasi malfunzionamento ogni minuto che l'azienda non è online perde una cospicua quantità di denaro.
   Se l'azienda rimane non raggiungibile per 10 minuti la perdita potenziale è di € 15.000.
   La soluzione per garantire la business continuity dell'azienda stessa e soddisfare gli utenti finali è quella di implementare un server di backup, che può essere sia cloud che hardware.
   Inoltre è essenziale creare un team in azienda con persone che provengono da più dipartimenti all'interno dell'azienda stessa per creare delle policy che servono in caso di emergenza, in modo tale da poter agire tempestivamente in caso di problemi di questo tipo.

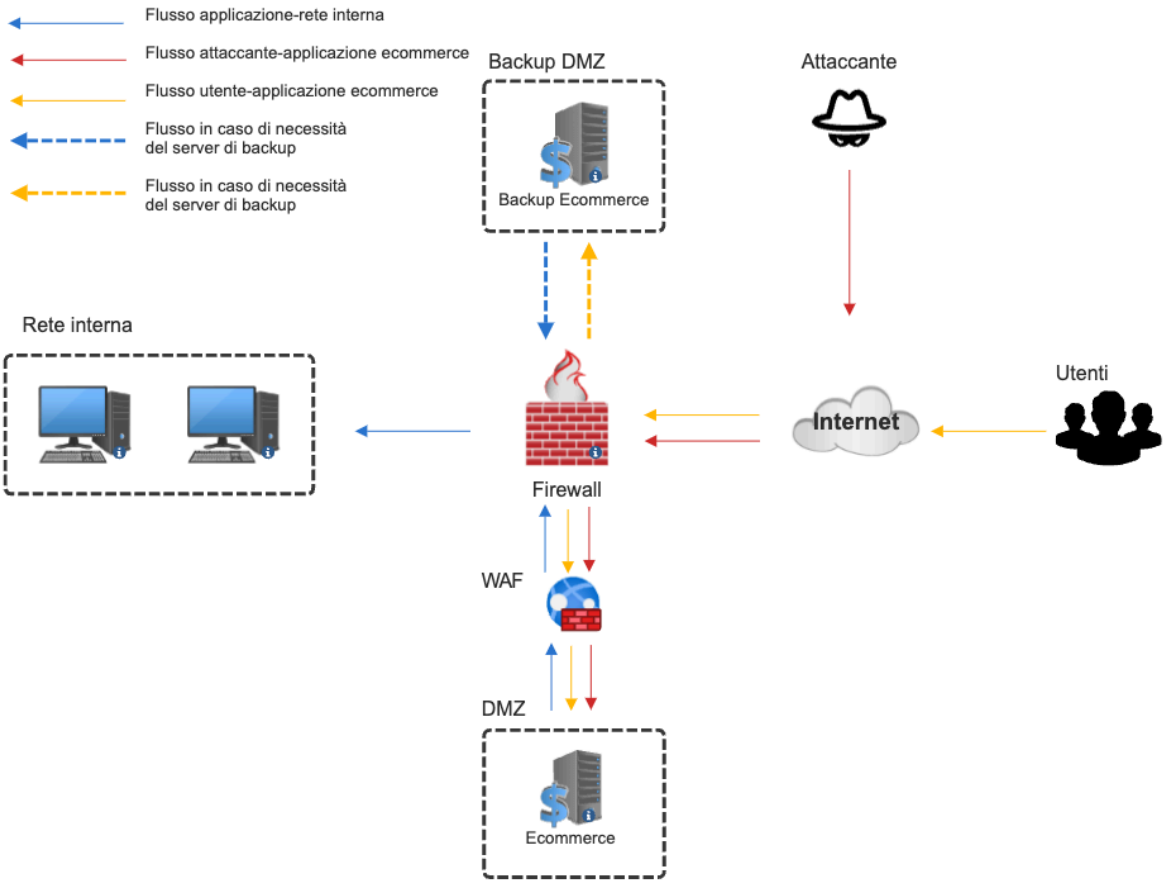
3. **Valutazione di un eventuale attacco hacker.**
   In caso di infezione da parte di un malware la soluzione principale è quella di isolare l'attaccante all'interno della rete.
   Per essere pronti a questo tipo di attacco l'ideale sarebbe effettuare una segmentazione della rete tramite subnetting o vlan, idealmente andrebbe fatto in fase di progettazione della rete, in alternativa è possibile implementare soluzioni diverse come quella proposta nella prossima figura.



   É stata creata una rete di quarantena in modo tale che l'attaccante seppur abbia accesso alla macchina infetta non potrà effettuare altri danni in quanto risulta isolato dalla rete. Isolando la macchina infettata però l'azienda rimarrebbe senza server ecommerce, per questo risulta necessario implementare un server di backup, come detto nel punto precedente questa soluzione risulta necessaria per garantire la business continuity. Il server di backup non deve essere sempre online, ma questo verrà spiegato meglio nel punto 5.

4.Soluzione completa

La soluzione ideale per rendere più sicura l'intera infrastruttura di rete è l'unione del punto 1 e del punto 3, in modo tale da poter far fronte a entrambi i tipi di attacchi e con un grado di sicurezza superiore.
La soluzione illustrata in figura è quella completa.



5. **Modifica aggressiva all'intera infrastruttura.**
È possibile effettuare una valutazione dell'intera infrastruttura in modo da aumentare ancora il grado di sicurezza.
Il budget che l'azienda è disposta a investire è di € 7000.

Ragionando su questo budget ho deciso di implementare un hardware IPS e un Siem dal punto di vista della sicurezza, mentre dal punto di vista della business continuity ho implementato un secondo server di backup.
L'IPS preso in considerazione è un Cisco Firepower al costo di € 1300-1500 che varia in base al modello scelto, questo tipo di apparecchiatura è nuova ma è possibile valutare anche soluzioni entry level nel mercato refurbished dei vari brand.
Per quanto riguarda il Siem si parla di prezzi fuori budget ragionando sui top brand a livello enterprise, ma dato il budget, è possibile valutare sistemi open source oppure soluzioni pensate per le piccole aziende.
Un prodotto che fa a caso nostro è questo: https://utmstack.com/
Questa soluzione ha un costo minimo per ogni host presente all'interno della rete.
Ipotizzando una rete con non più di 50 devices, il siem costerebbe poco più di € 100 al mese.
Il server, come l'IPS è da valutare sia nuovo che usato, come prima propongo una soluzione completamente nuova e parlo di un server Cisco UCS, che in base al modello scelto può costare da € 1500 fino a € 2000.
Un'ulteriore proposta è quella di creare un backup server completamente in cloud, con costi molto più bassi;

considerando un server di una piccola azienda con 50 devices il costo di un cloud server potrebbe costare circa € 50 mensili.
Inoltre i costi si abbattono a quasi zero se questo server non viene utilizzato o meglio se rimane inutilizzato, in quanto i servizi di server cloud vanno a costare solo se accesi e se iniziano a trasferire dati.
Nel totale dei costi ho ipotizzato che un server di backup rimanga acceso, due mesi all'anno per avere una panoramica dei costi, in realtà essendo un server di backup dovrebbe rimanere acceso molto meno.
Riassumendo si potrebbero valutare due proposte
<u>Preventivo più costoso:</u>

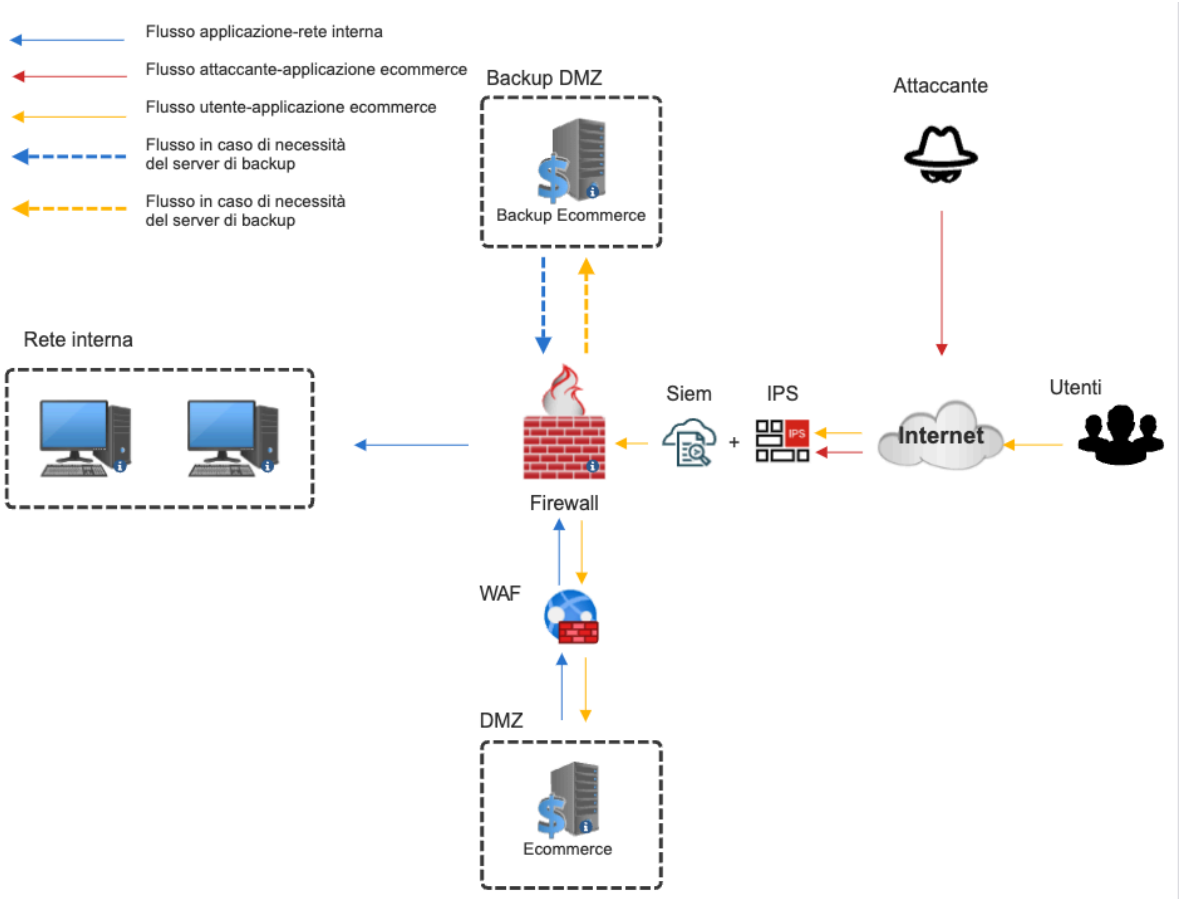
- IPS hardware € 1500
- Server hardware € 1500
- Siem € 100/mensili

Totale di € 3100 subito e € 100 mensili.
Soluzione ottima che va ad esaurire il budget in circa 3 anni dall'implementazione.
<u>Preventivo meno costoso:</u>

- IPS hardware €1500
- Server cloud € 100 annuali
- Siem € 100/mensili

Totale di € 1700 subito, € 100 annuali, € 100 mensili

Soluzione ideale, oltre che ad essere una proposta più economica risulta molto flessibile e con meno costi di manutenzione. Optando per questa soluzione il budget si andrebbe ad esaurire in 4 anni dall'implementazione. Ecco uno schema della soluzione proposta:



Come è possibile notare è stato disposto un server di backup fisico/cloud in parallelo al server principale in modo tale che possa essere attivato all'occorrenza.
Il siem e l'IPS possono essere disposti sia prima che dopo il firewall, in questo caso mi è sembrato più appropriato posizionarli prima in modo tale che le minacce vengano bloccate in partenza e gli utenti all'interno della rete non possano venirne a contatto.
Le soluzioni possono essere molteplici e andrebbero considerati anche i costi di manutenzione dei vari dispositivi hardware per effettuare una stima più appropriata dei costi della business continuity in caso di attacco o malfunzionamento.
Occorre verificare se tutto il resto della rete è predisposto alla business continuity, per esempio se ogni dispositivo ha un relativo ups che gli permetta di rimanere online in caso di sbalzi di tensione o addirittura mancata corrente.
Concludo dicendo che la soluzione più indicata dal punto di vista costi-benefici è la seconda.
Attendo una valutazione e l'eventuale approvazione della proposta.

Bonus 1 - Microsoft Edge download

Il primo report riguarda un download e aggiornamento di internet explorer.
Il sito dal quale viene lanciato il download e l'installazione del programma sembrano legittimi ma in realtà andando ad indagare più a fondo si può notare che è stato scritto sul disco codice malevolo non autorizzato.
Questo tipo di minacce possono essere mitigate inserendo un IPS all'interno della rete in modo tale che possa rilevare questo tipo di intrusioni.

Bonus 2 - Performance booster.

Sembra che l'utente abbia installato questo "Performance booster" ma in realtà dal report si evidenzia che questo software va a modificare alcune directory sensibili, è possibile notare infatti che avvia programmi come ping.exe che risulta sconosciuto alla macchina.
Inoltre proseguendo nel report viene mostrata la configurazione di rete del dispositivo, quindi l'attaccante ha sicuramente raccolto questi dati molto sensibili, successivamente viene eseguita una completa discovery della macchina, quindi è possibile che l'attaccante abbia completamente clonato i dati della macchina.
A seguito di questo attacco l'hacker potrebbe avere pieno controllo della macchina in quanto va a modificare anche i privilegi su alcune directory importanti.
Non è ben chiaro come questo software sia finito all'interno della macchina target, potremmo ipotizzare un download eseguito dall'utente per "aumentare le performance del dispositivo", magari in buona fede, oppure addirittura un attacco voluto dall'utente stesso inserito tramite l'utilizzo di una pen drive.
Questo tipo di attacchi possono essere evitati mettendo delle policy più restrittive sull'utilizzo delle porte usb (disabilitando a livello hardware o software le porte usb), oppure utilizzando un dispositivo come un IPS che rilevi minacce di questo tipo.
L'obiettivo di questo attacco potrebbe essere quello di ottenere l'accesso completo alla macchina in modo tale da poterlo sfruttare a proprio piacimento, magari all'interno di una botnet.

In conclusione, in entrambi i report viene evidenziato che la rete non rileva minacce che possono provenire dall'esterno, la soluzione principale è quello di utilizzare un IPS/IDS, se all'interno dell'azienda c'è un team che monitora la rete si può pensare a un IDS mentre se non c'è un team e si vuole comunque implementare la sicurezza è possibile aggiungere un IPS, in modo tale che vengano effettuate delle remediation actions istantantanee al rilevamento della minaccia.
Un'altro consiglio è quello di creare (se già non è presente) all'interno dell'azienda un team CSIRT, ovvero un team che si occupa della sicurezza informatica all'interno dell'azienda, che può essere temporaneo oppure fisso e che opera attraverso policies definite in fase di pianificazione anche con gli altri reparti aziendali.