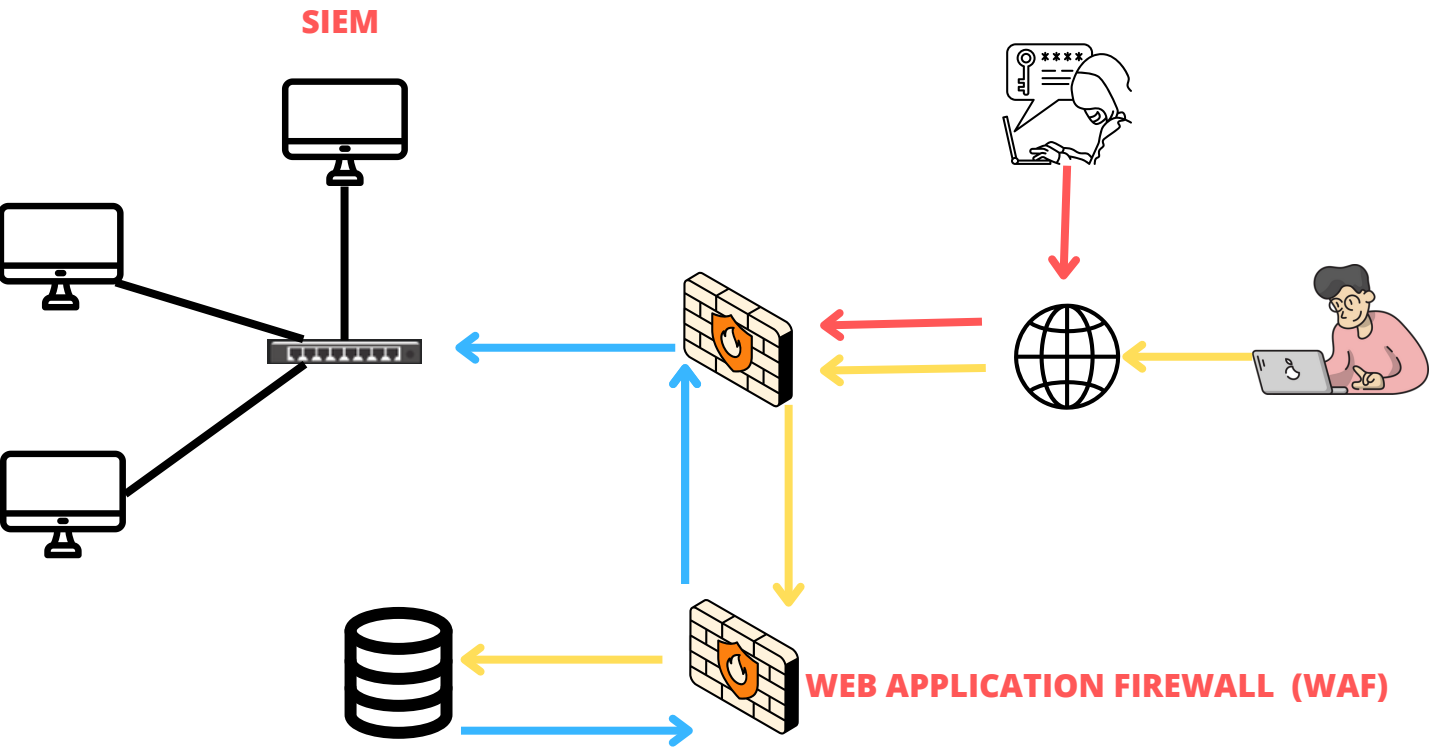
Esercizio 1

Eseguire azioni preventive per difendere l'app web da XSS e SQLi



Flusso applicazione - rete interna

Flusso attaccante - app e-commerce

Flusso utente - app e-commerce-

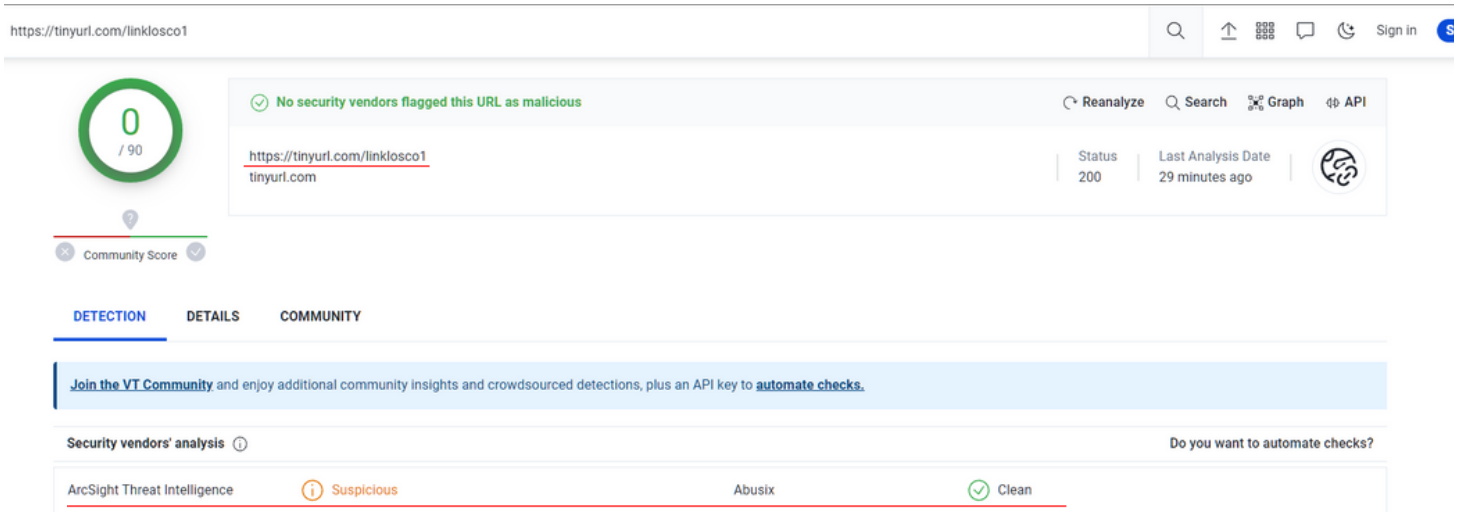
Per prevenire attacchi di tipo SQL Injection (SQLI) e Cross-Site Scripting (XSS) in un'applicazione e-commerce si può inserire un WAF per filtrare e bloccare attività sospette.
Si può inserire anche SIEM per tenere traccia di tutti i log.

Esercizio 2

Analisi dei link:
https://tinyurl.com/linklosco1
https://tinyurl.com/linklosco2

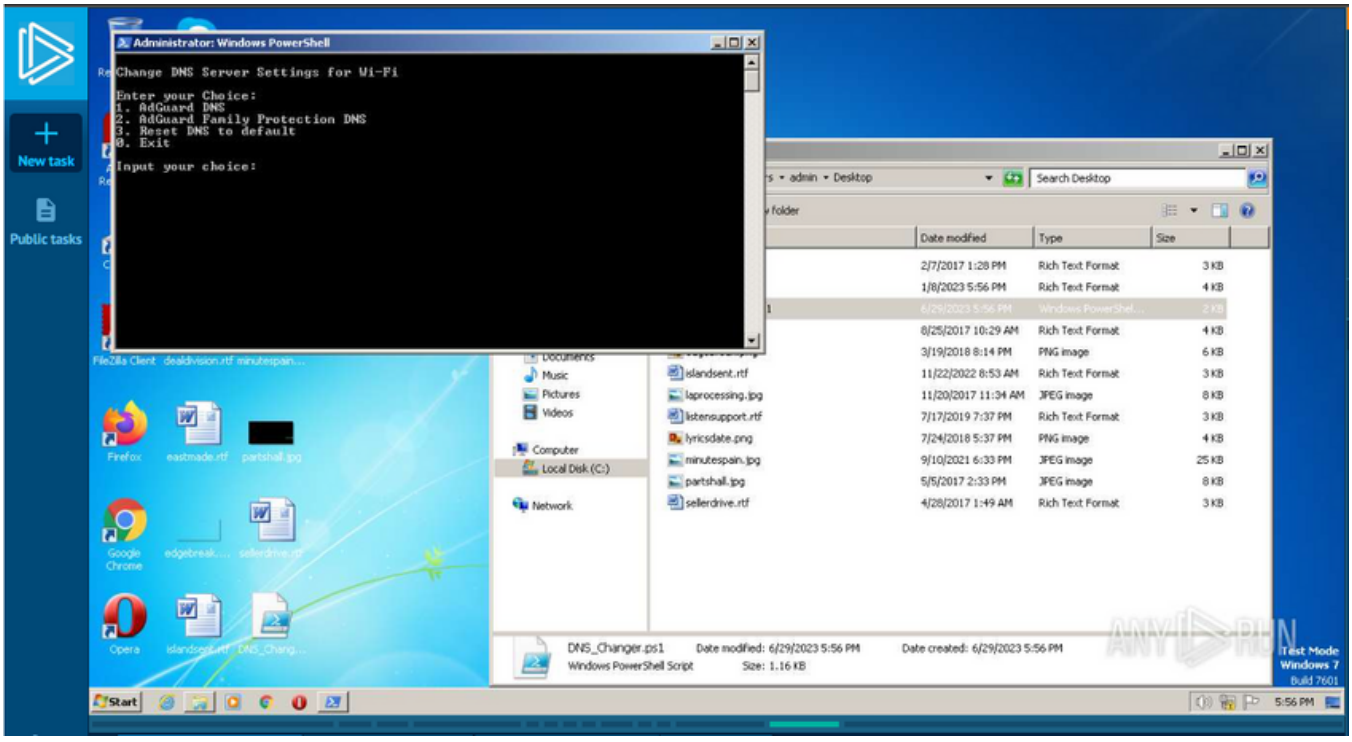
1) https://tinyurl.com/linklosco1

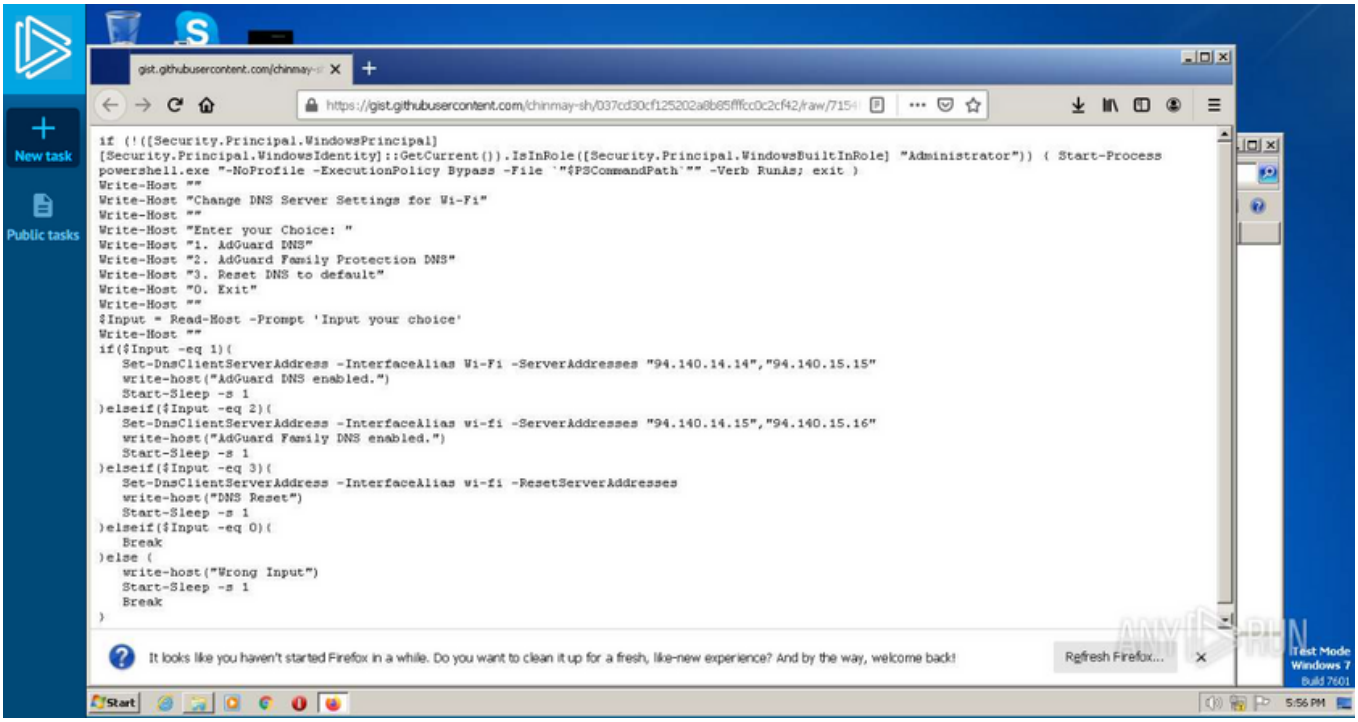
Analizzando la prima URL vado ad inserirla su Virus total



Virus total ci dice che è un link sospetto. Avverto i dipendenti di non aprire quel determinato link. Se è già stato aperto consiglio loro di cambiare tutte le password per una sicurezza preventiva.

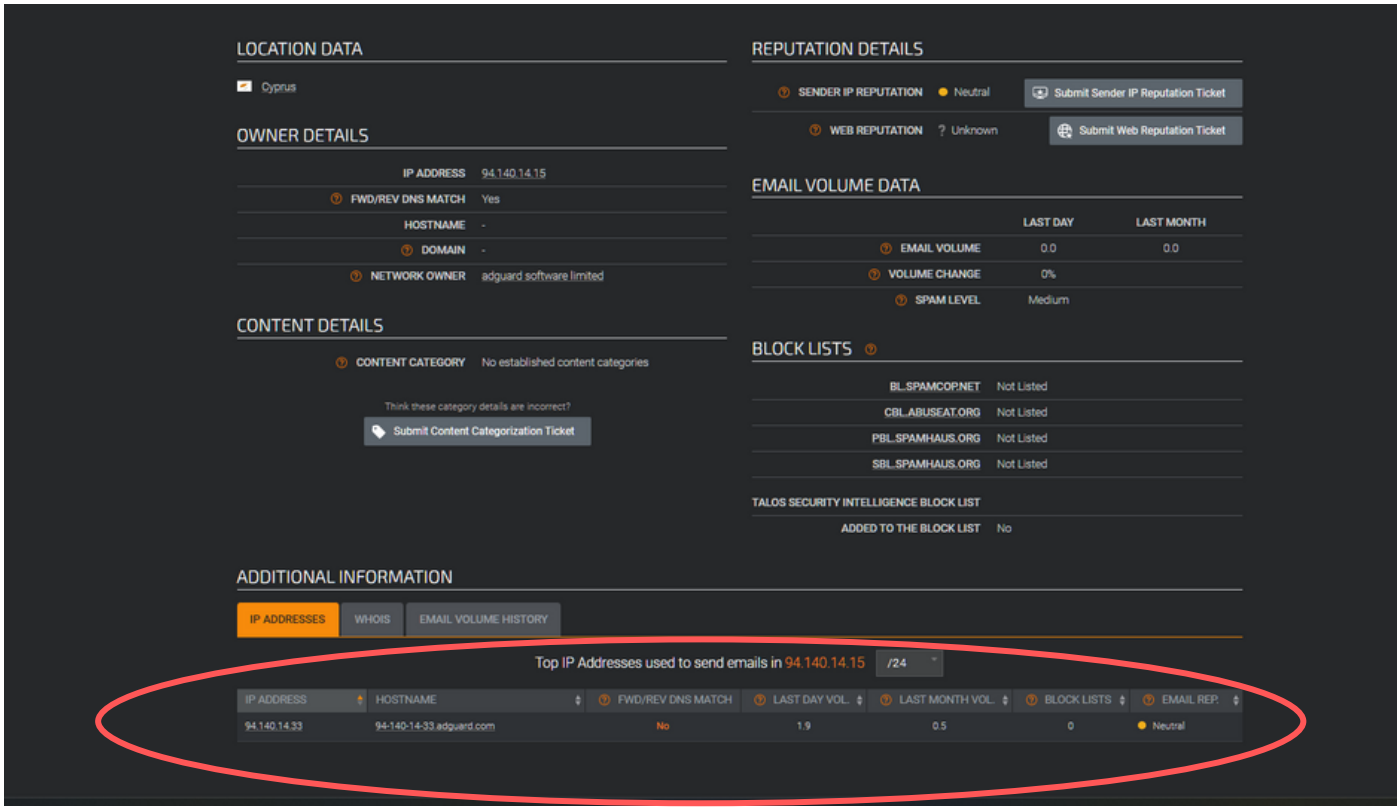
Apro il link e mi ritrovo su anyrun dove posso analizzare l'eventuale minaccia.
Il primo link si tratta di una PowerShell che gestisce le impostazioni del server DNS..
Questa PoweShell ha un menù a scelta come si vede nella figura seguente.



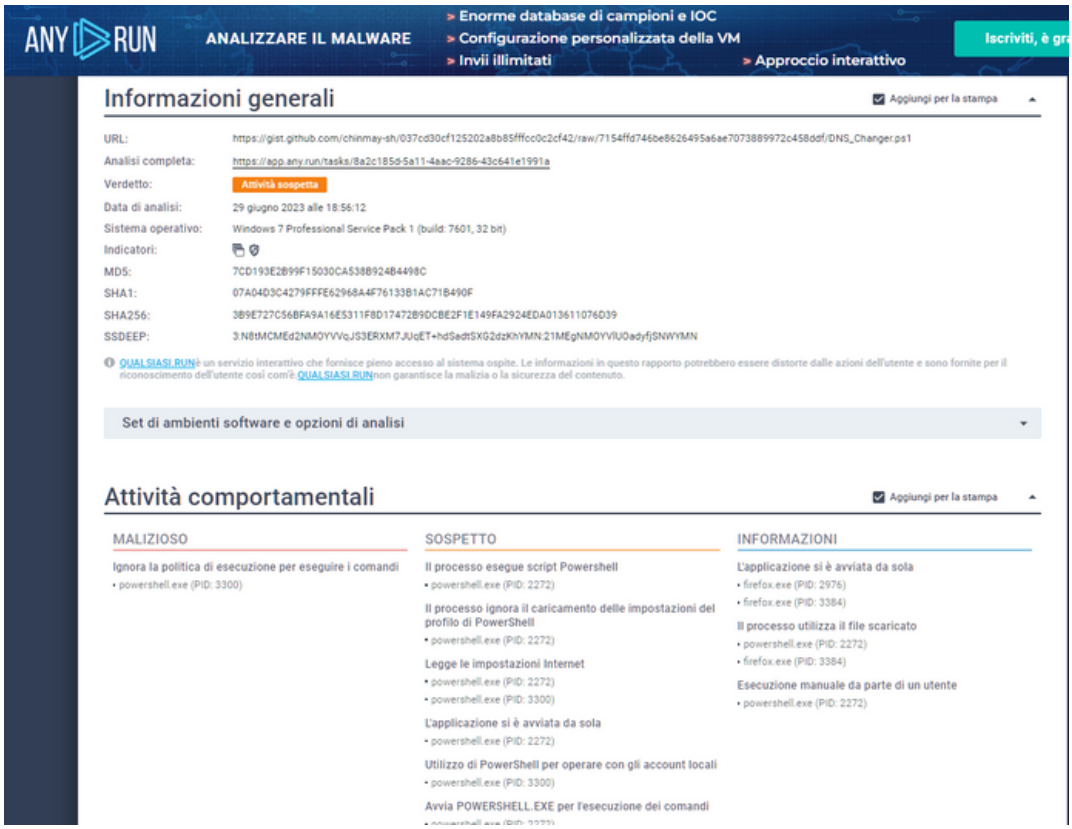


Come si puo vedere nella figura precedente digitando 1 o 2 cambierà il dns in "94.140.14.15" o "94.140.14.16"

Facendo un analisi approfondita inserisco l'indirizzo ip su https://talosintelligence.com/



https://talosintelligence.com/ dice che l'indirizzo ip è neutrale ovvero non ha rilevato alcuna minaccia.

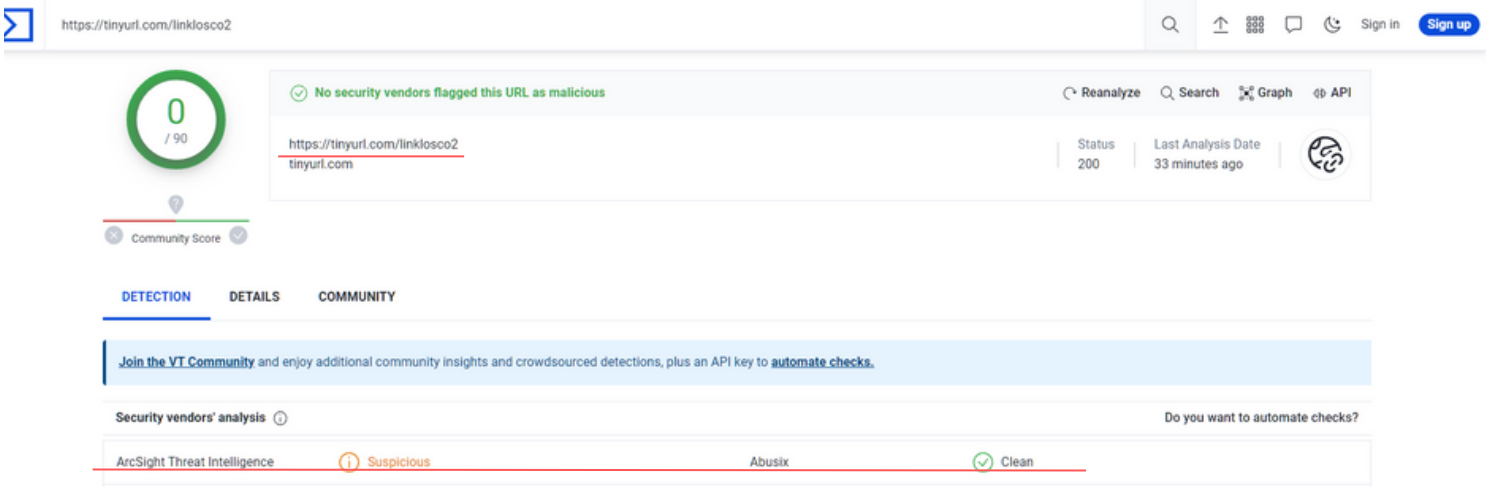


Any run ci dice che è un attività sospetta infatti essa puo essere eseguita in automatico ma soprattutto comunicare con gli account locali

Fase di contenimento,rimozione e recupero

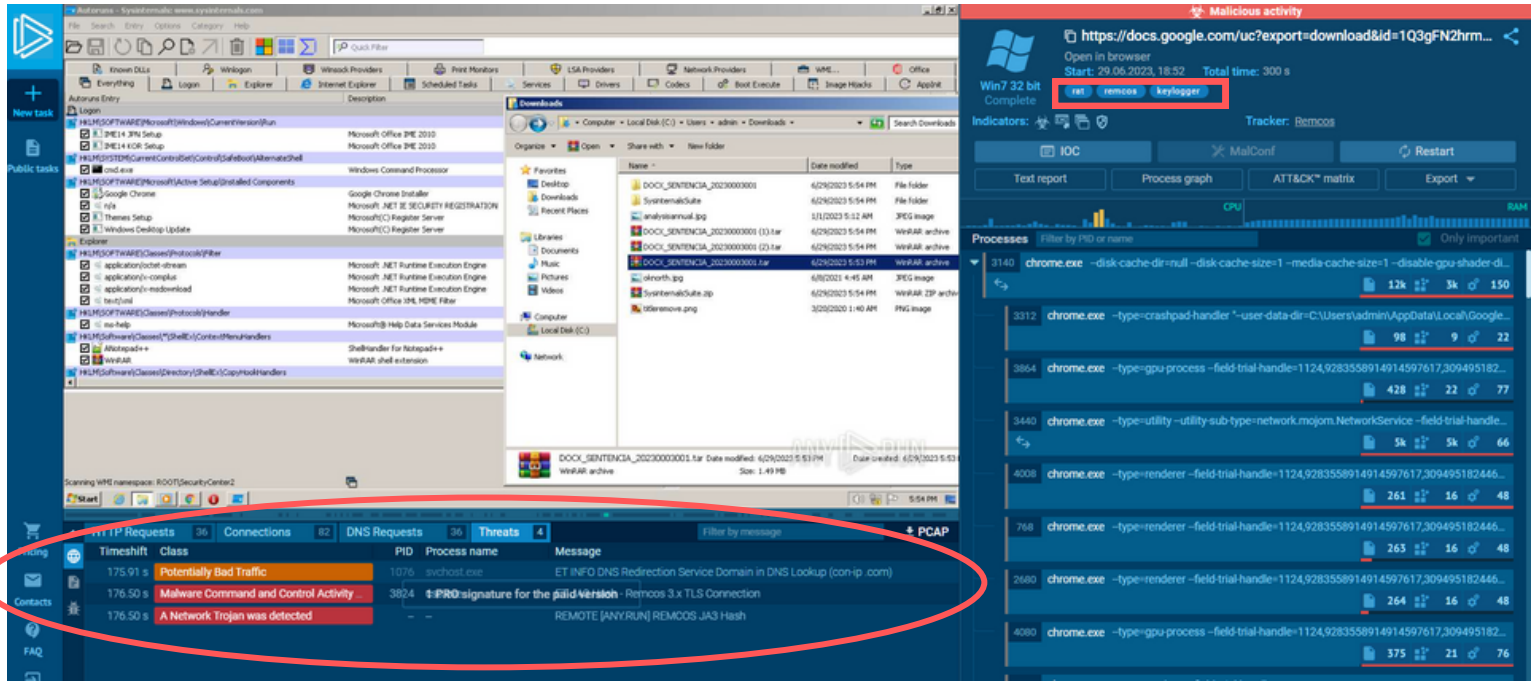
1)Se un dipendente ha aperto il link dividere la rete in diverse Vlan
2)Avvertire l'azienda
3)Recupero dati causati da eventuali danni
4)Ripulire completamente il dispositivo danneggiato

2) https://tinyurl.com/linklosco2

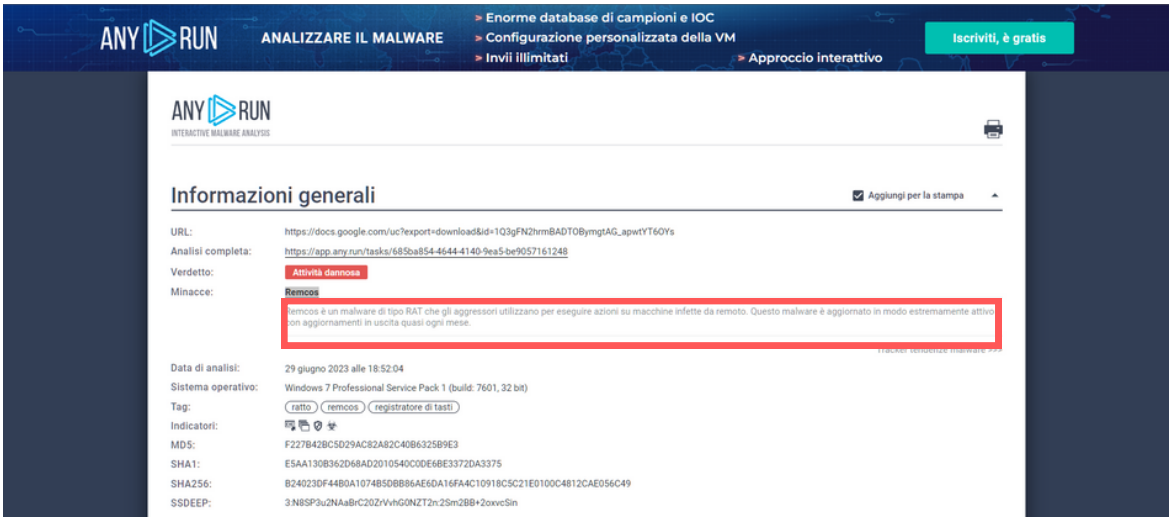


Virus total ci dice che è un link sospetto. Avverto i dipendenti di non aprire quel determinato link. Se è già stato aperto consiglio loro di cambiare tutte le password per una sicurezza preventiva.

Apro il link e mi ritrovo su anyrun dove posso analizzare l'eventuale minaccia,



Analizzando l'eventuale minaccia Anyrun ci dice che siamo difronte ad un malware chiamato Remocs.
1)Potenziale traffico cattivo
2)Un keylogger
3)Ha rilevato un trojan

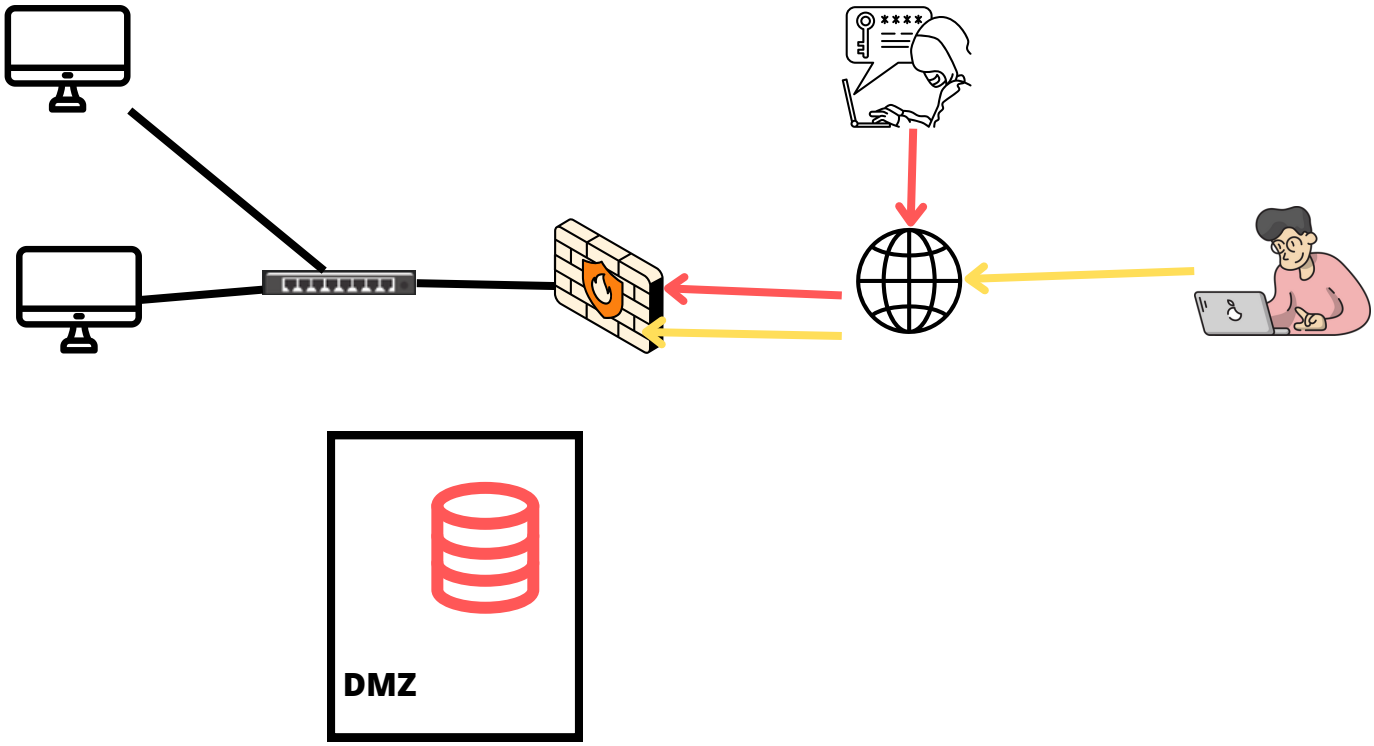


Fase di contenimento,rimozione e recupero

1)Se un dipendente ha aperto il link dividere la rete in diverse Vlan
2)Avvertire l'azienda
3)Recupero dati causati da eventuali danni
4)Ripulire completamente il dispositivo danneggiato

Esercizio 3

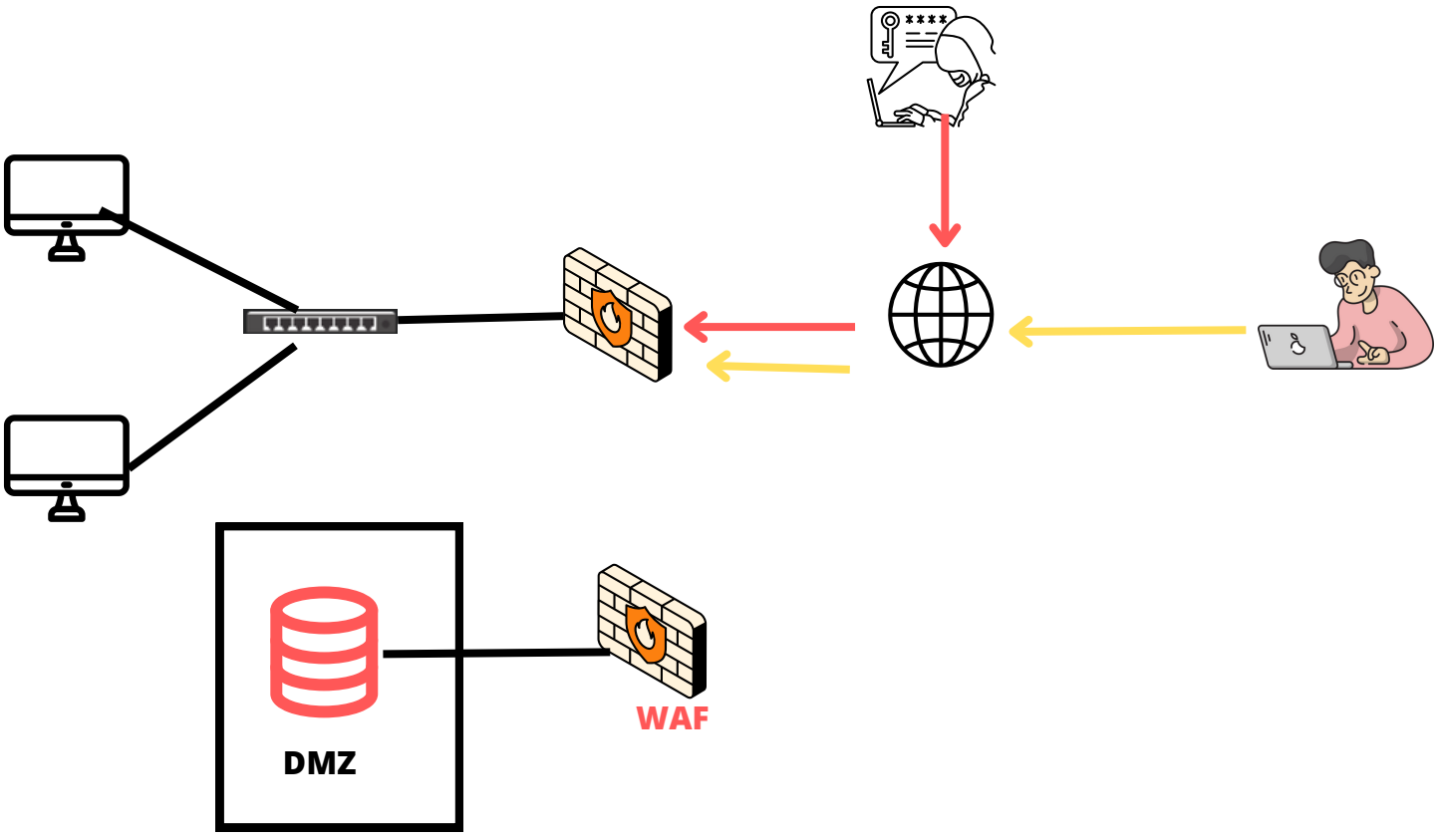
L'applicazione Web è stata infettata da un malware. Il malware non si deve propagare sulla rete e non devono essere divulgate info sensibili.



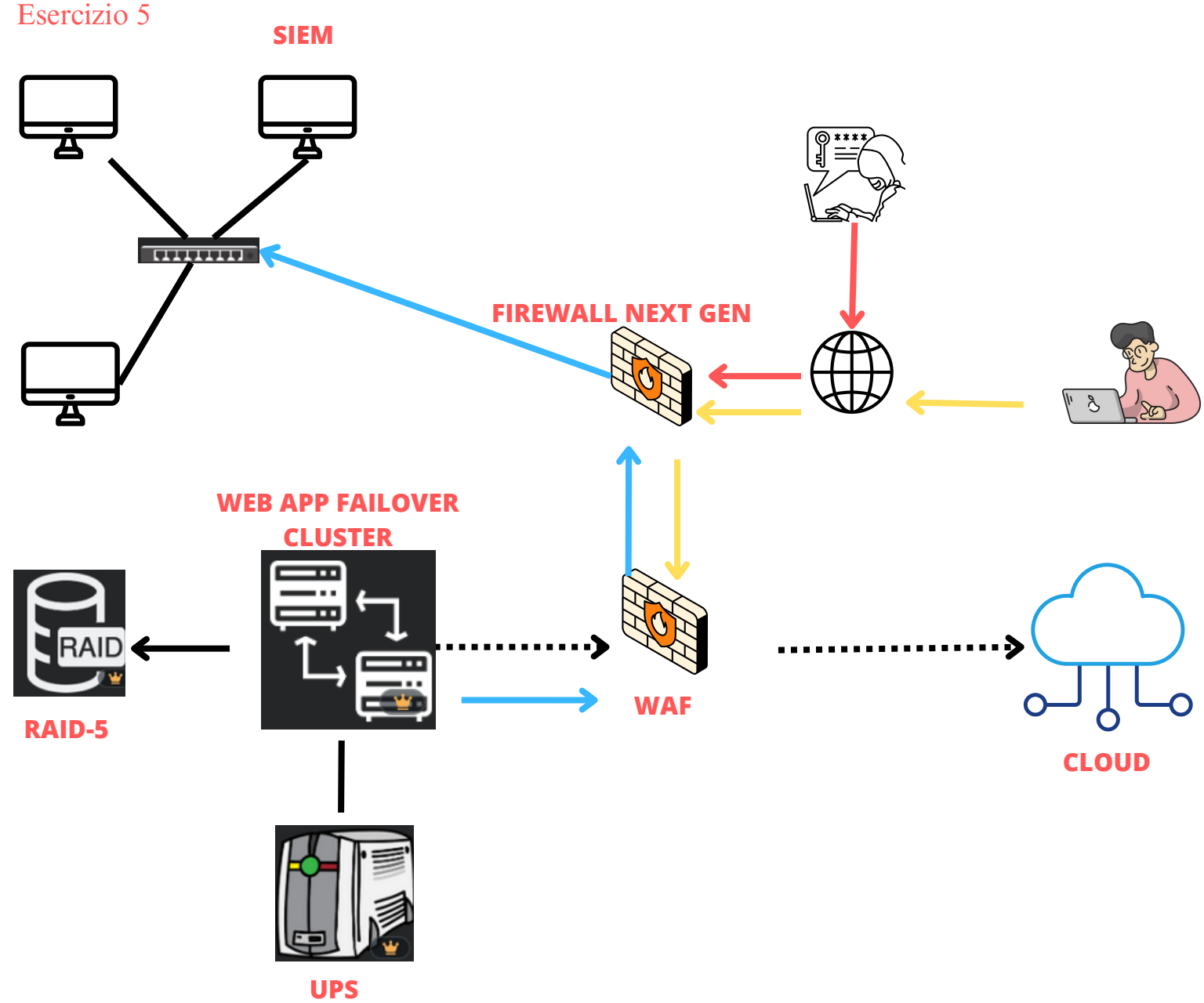
La priorità è che il malware non si propaghi sulla nostra rete, dopo l'attacco e non divulgare dati sensibili, quindi andiamo bloccare la web app rendendola inaccessibile.
Andiamo a creare una zona di quarantena dove ci sarà la nostra Web App.

Esercizio 4

Unisco le azioni preventive e la response



Esercizio 5



Per implementare la sicurezza dell'infrastruttura di seguito sono riportati alcuni consigli

Piano di disaster recovery

-Creazione di un EXECUTIVE SUMMARY
-Configurazione di un RAID-5
-Acquisto di un UPS per il servizio critico
-Acquisto di un Cloud
-Backup
-In questo modo si ha una triplice copia, due locazioni per il backup e una off-site

Acquisto di ulteriori hardware/software

-Firewall next gen effettua un analisi su tutti i livelli iso/osi. Include un ids per il filtraggio di connessioni malevoli.
-Acquisto di un software SIEM per il continuo monitoraggio dei log (SPLUNK)
-Ridondanza di un applicativo e-commerce, utile se la web app principale è infettata da un malware.