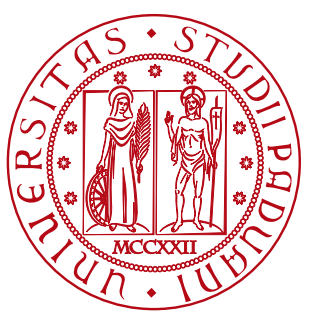
Progettazione e implementazione di un sistema di Network Detection and Response

Discussione Tesi di Laurea in Informatica

Laureando: Elia Pasquali

22/09/2023



Università degli Studi di Padova

Indice

1. L’azienda
2. Il progetto
3. Il prodotto
4. Obiettivi raggiunti
5. Conclusioni

L'azienda

WINTECH

Nasce nel 1987 come *System Integrator* che opera nel settore *ICT*

Stage svolto all'interno del *team* di *Network Operation Control*

Nascita dello stage

L’azienda cerca un sistema di NDR sul mercato che trova in Sangfor e attiva un *proof of concept* con una singola sonda all’interno della rete aziendale

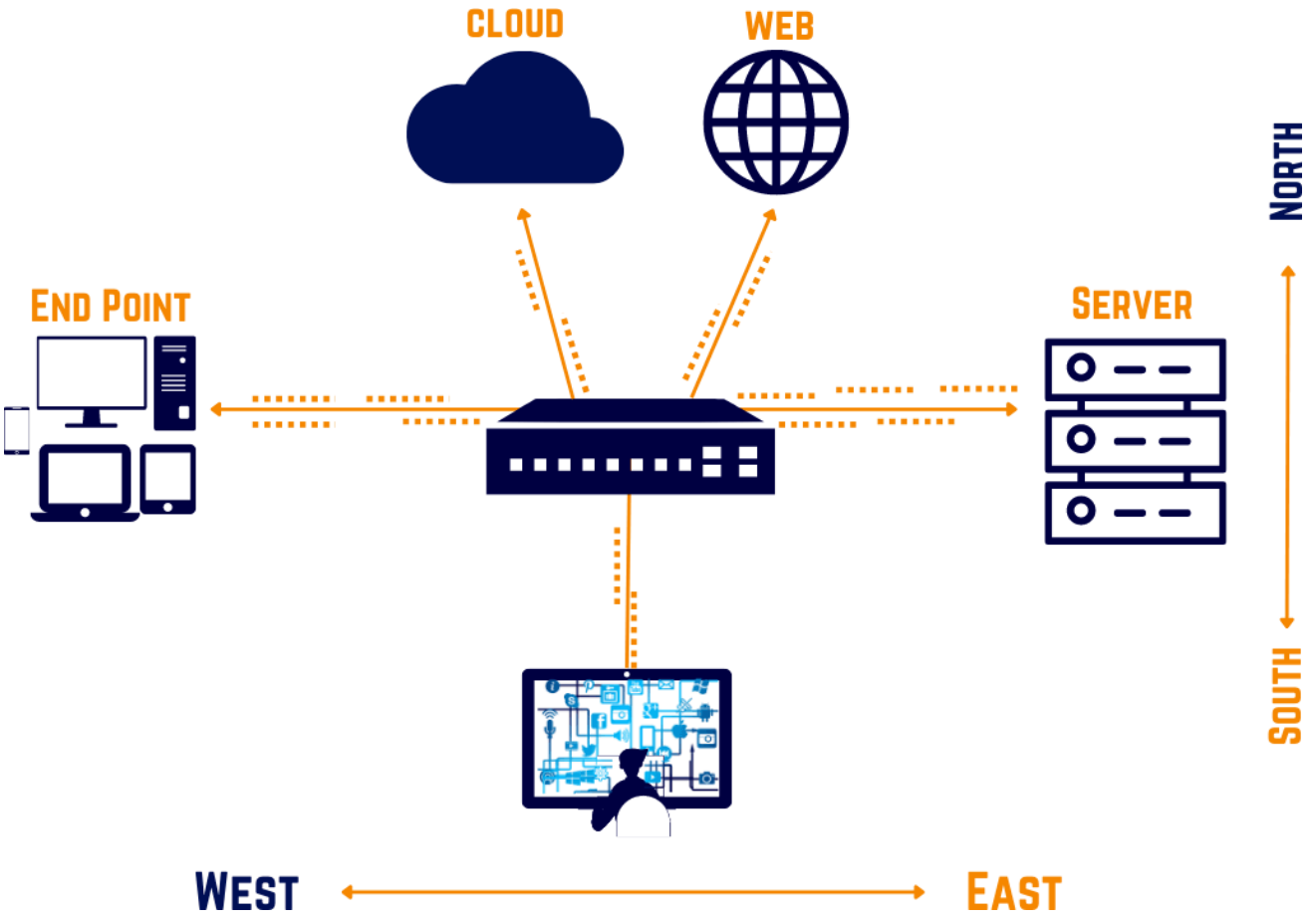
SANGFOR

Tramite StageIT conosco Wintech e mi viene proposto un progetto di stage per portare in produzione il sistema *CyberCommand* di Sangfor

Network Detection and Response

Prodotti di sicurezza informatica che analizzano il traffico di rete e rilevano eventuali anomalie (*Network Detection*).

Possono rispondere automaticamente alle minacce (*Network Response*)



Risultati attesi

Obbligatori:

- *Deploy* e configurazione del sistema NDR all'interno della rete aziendale
- Test e analisi del prodotto
- Configurazione della funzionalità di risposte automatiche
- Documentazione di scelte prese, problemi e configurazioni

Risultati attesi

Obbligatori:

- *Deploy* e configurazione del sistema NDR all'interno della rete aziendale
- Test e analisi del prodotto
- Configurazione della funzionalità di risposte automatiche
- Documentazione di scelte prese, problemi e configurazioni

Desiderabili:

- Integrazione con prodotti già presenti in azienda

Risultati attesi

Obbligatori:

- *Deploy* e configurazione del sistema NDR all'interno della rete aziendale
- Test e analisi del prodotto
- Configurazione della funzionalità di risposte automatiche
- Documentazione di scelte prese, problemi e configurazioni

Desiderabili:

- Integrazione con prodotti già presenti in azienda

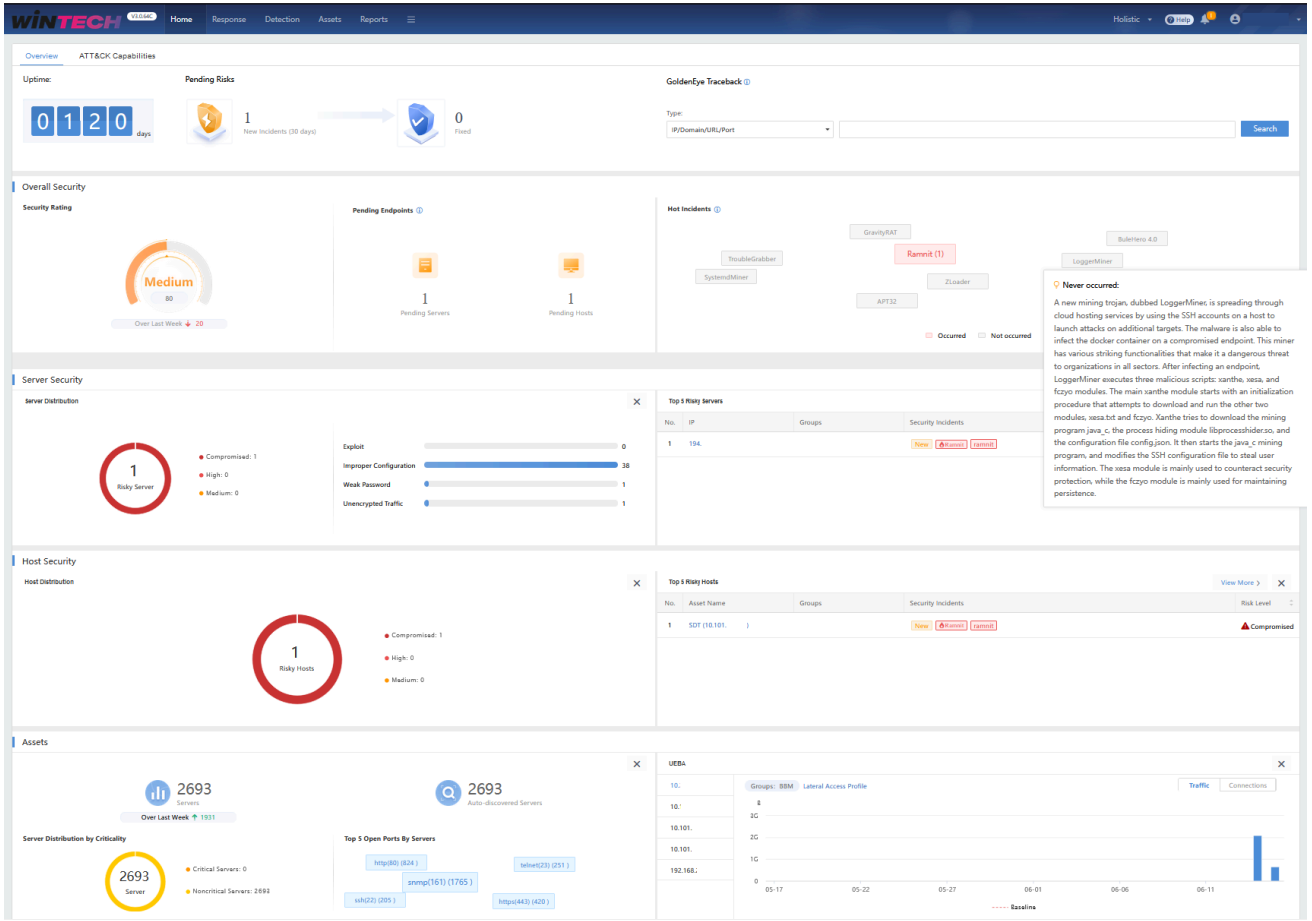
Facoltativi:

- *Bypassare* il sistema di rilevazione

Il prodotto Sangfor

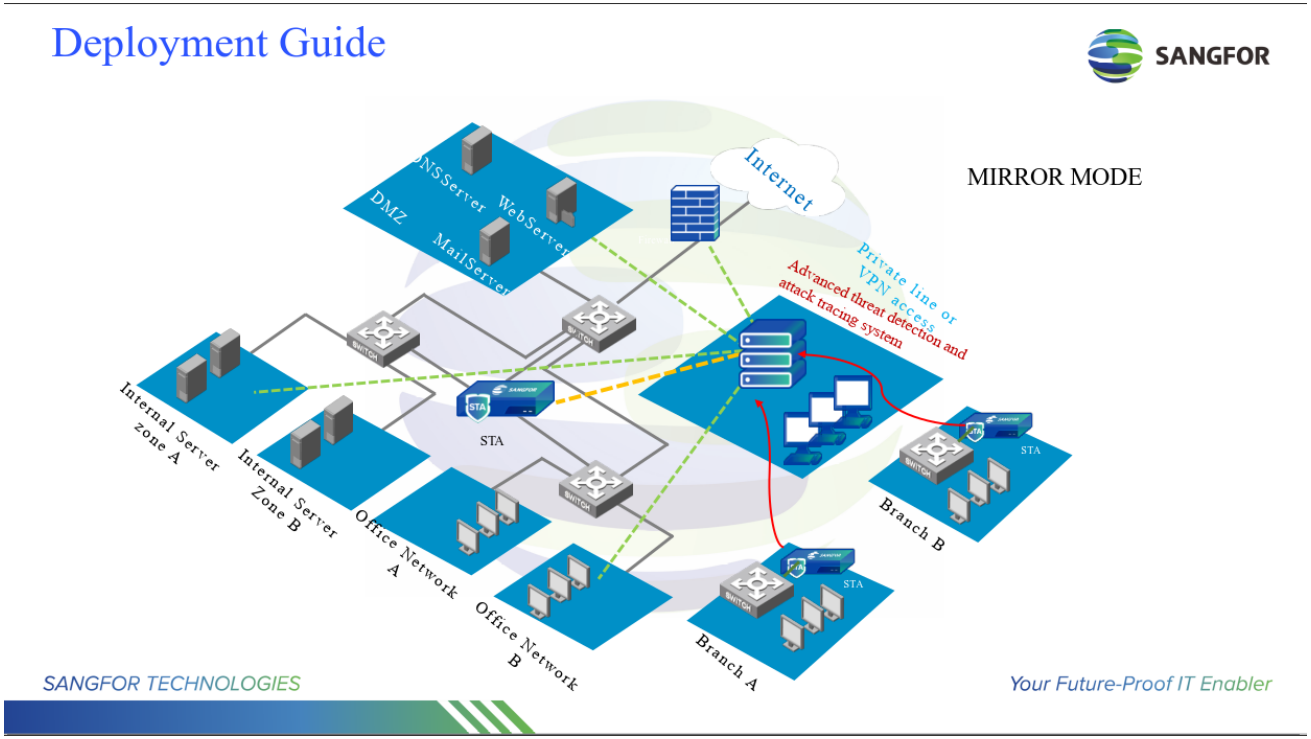
CyberCommand, il sistema NDR offerto da Sangfor.

Dalla dashboard è possibile visualizzare tutte le informazioni sulle minacce rilevate e lo stato della rete.

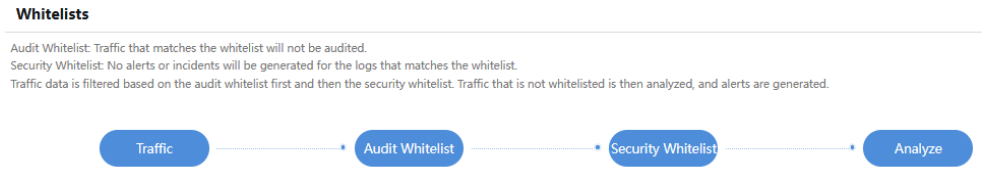


Sistema di sonde

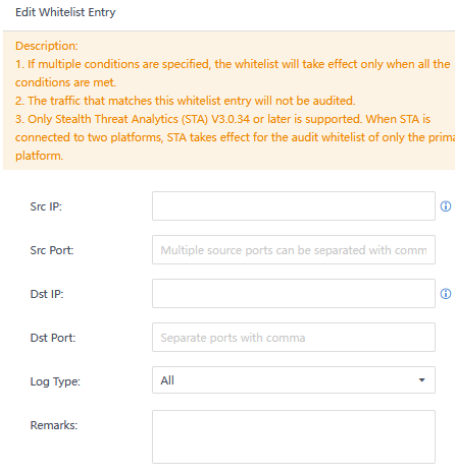
CyberCommand sfrutte le sonde STA inserite all'interno della rete per analizzare il traffico di rete e rilevare eventuali anomalie.

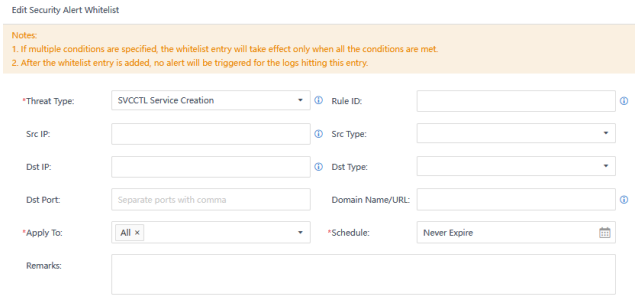


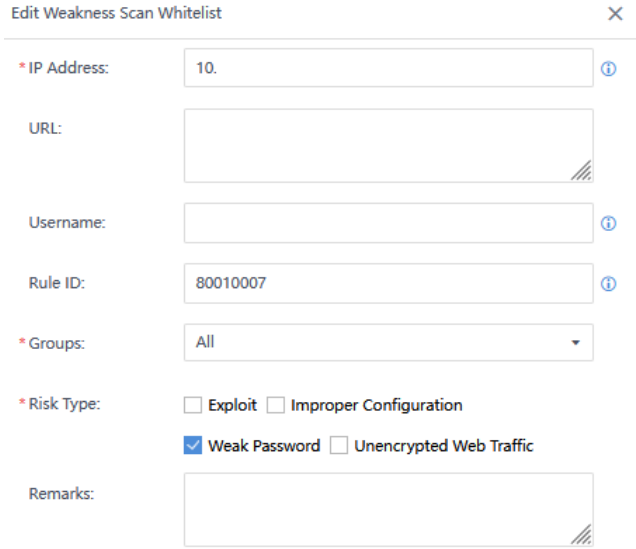
Flusso di analisi e whitelist



Possono essere definite delle regole per filtrare il traffico in modo da ottenere un'analisi più precisa.

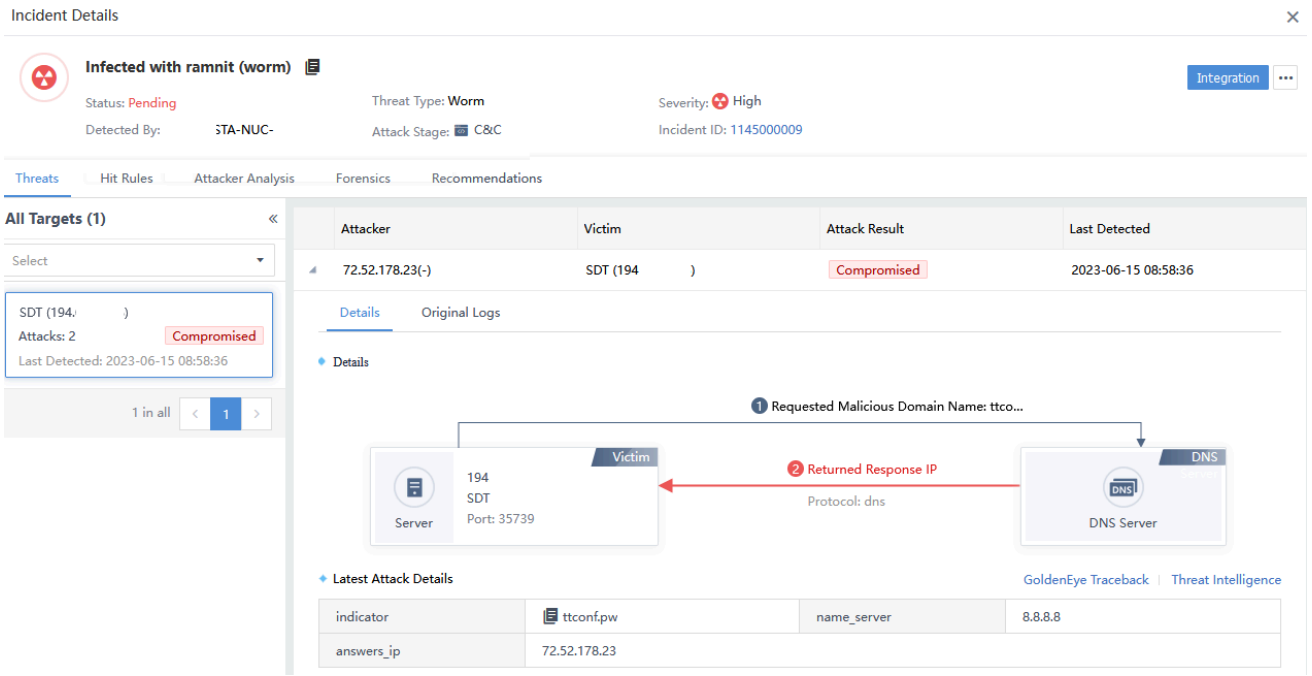






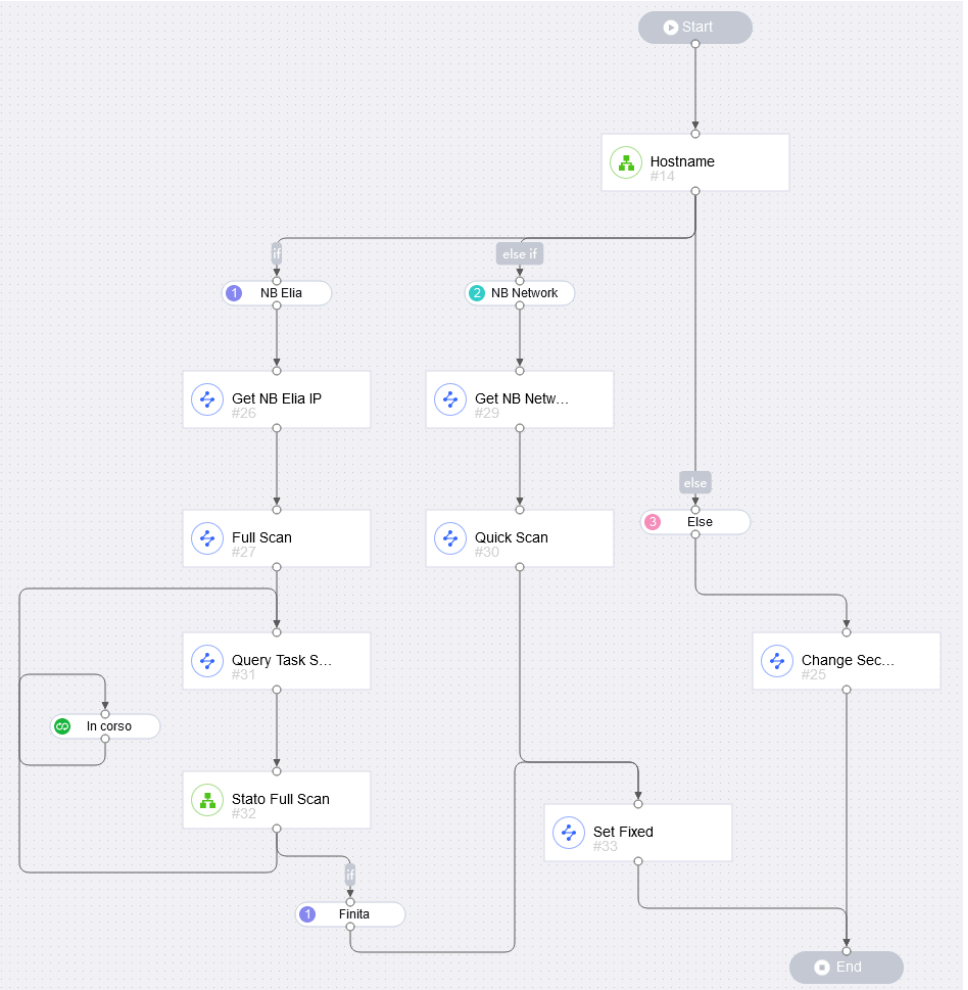
Segnalazioni

Le segnalazioni rilevate vengono visualizzate con tutti i dettagli e i *log* a loro associati.



Risposte automatiche

Il sistema NDR può rispondere automaticamente alle minacce rilevate seguendo un algoritmo costituito da *action node* e *decision node*



Obiettivi raggiunti

- ✔ NDR inserito in produzione, configurato e testato

Obiettivi raggiunti

- ✔ NDR inserito in produzione, configurato e testato
- ✔ Documentate *best practices* e problemi riscontrati

Obiettivi raggiunti

- ✔ NDR inserito in produzione, configurato e testato
- ✔ Documentate *best practices* e problemi riscontrati
- ✔ Risolti problemi rilevati con la definizione delle regole

Obiettivi raggiunti

- ✓ NDR inserito in produzione, configurato e testato
- ✓ Documentate *best practices* e problemi riscontrati
- ✓ Risolti problemi rilevati con la definizione delle regole
- ✓ Definite risposte automatiche e integrate con EDR

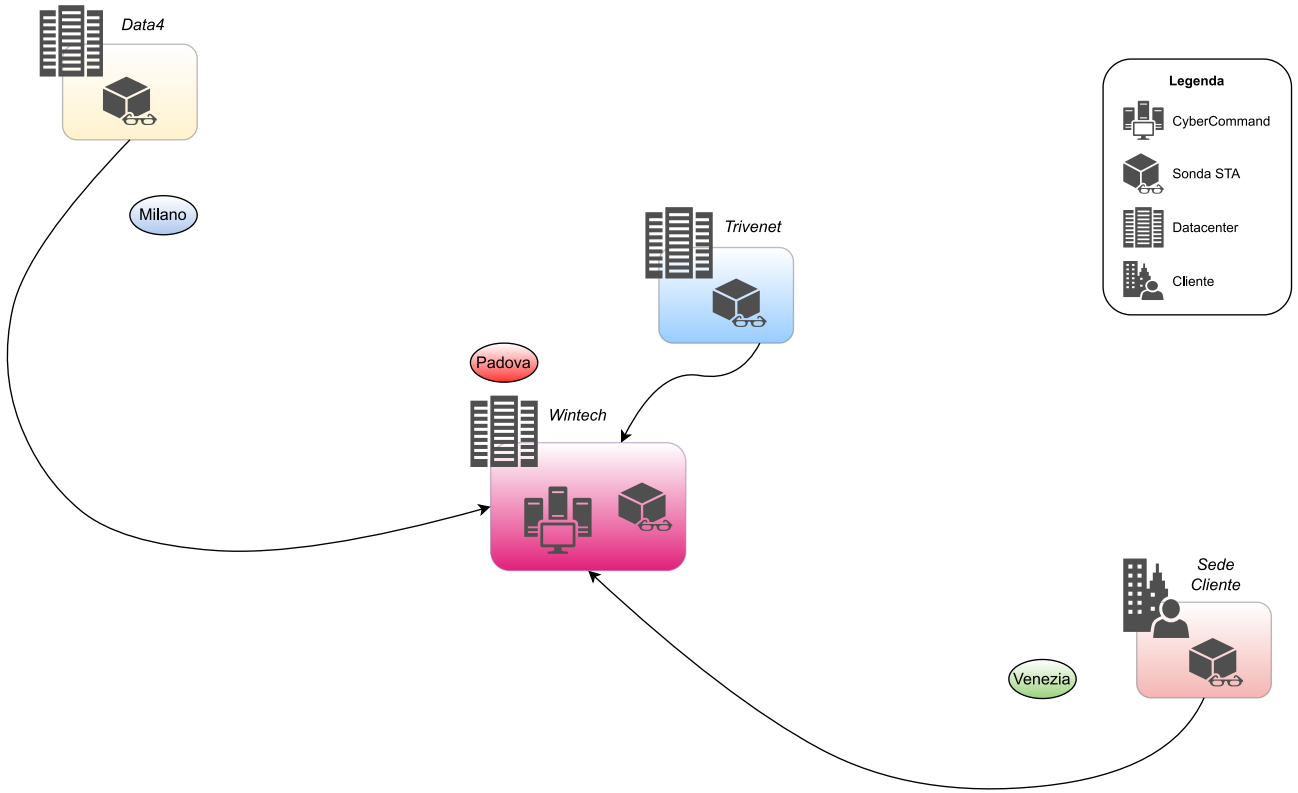
Obiettivi raggiunti

- ✓ NDR inserito in produzione, configurato e testato
- ✓ Documentate *best practices* e problemi riscontrati
- ✓ Risolti problemi rilevati con la definizione delle regole
- ✓ Definite risposte automatiche e integrate con EDR
- ✗ *Bypass* del sistema di rilevazione

Obiettivi raggiunti

- ✓ NDR inserito in produzione, configurato e testato
- ✓ Documentate *best practices* e problemi riscontrati
- ✓ Risolti problemi rilevati con la definizione delle regole
- ✓ Definite risposte automatiche e integrate con EDR
- ✗ *Bypass* del sistema di rilevazione
- ✗ Integrazione con prodotti già presenti in azienda impossibile con attuale versione di *CyberCommand*

Rete ottenuta a fine stage



Sonde presenti in:

- Sede Wintech (PD)
- Datacenter Trivenet (PD)
- Datacenter Data4 (MI)
- Sede cliente (VE)

Resoconto finale

Lato personale:

- Esperienza di lavoro in un team aziendale
- Conoscenza di un prodotto all'avanguardia di sicurezza di rete
- Formazione nell'ambito di rete e sicurezza con strumenti professionali e in un contesto reale

Lato aziendale:

- Segnalati problemi e possibili miglioramenti al prodotto
- Il sistema si è dimostato efficace nella rilevazione dei problemi