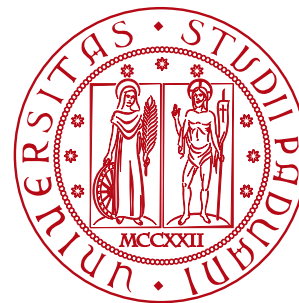


Progettazione e implementazione di un sistema di Network Detection and Response

Discussione Tesi di Laurea in Informatica

Laureando: Elia Pasquali

22/09/2023



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

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



WINTECH

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



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

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

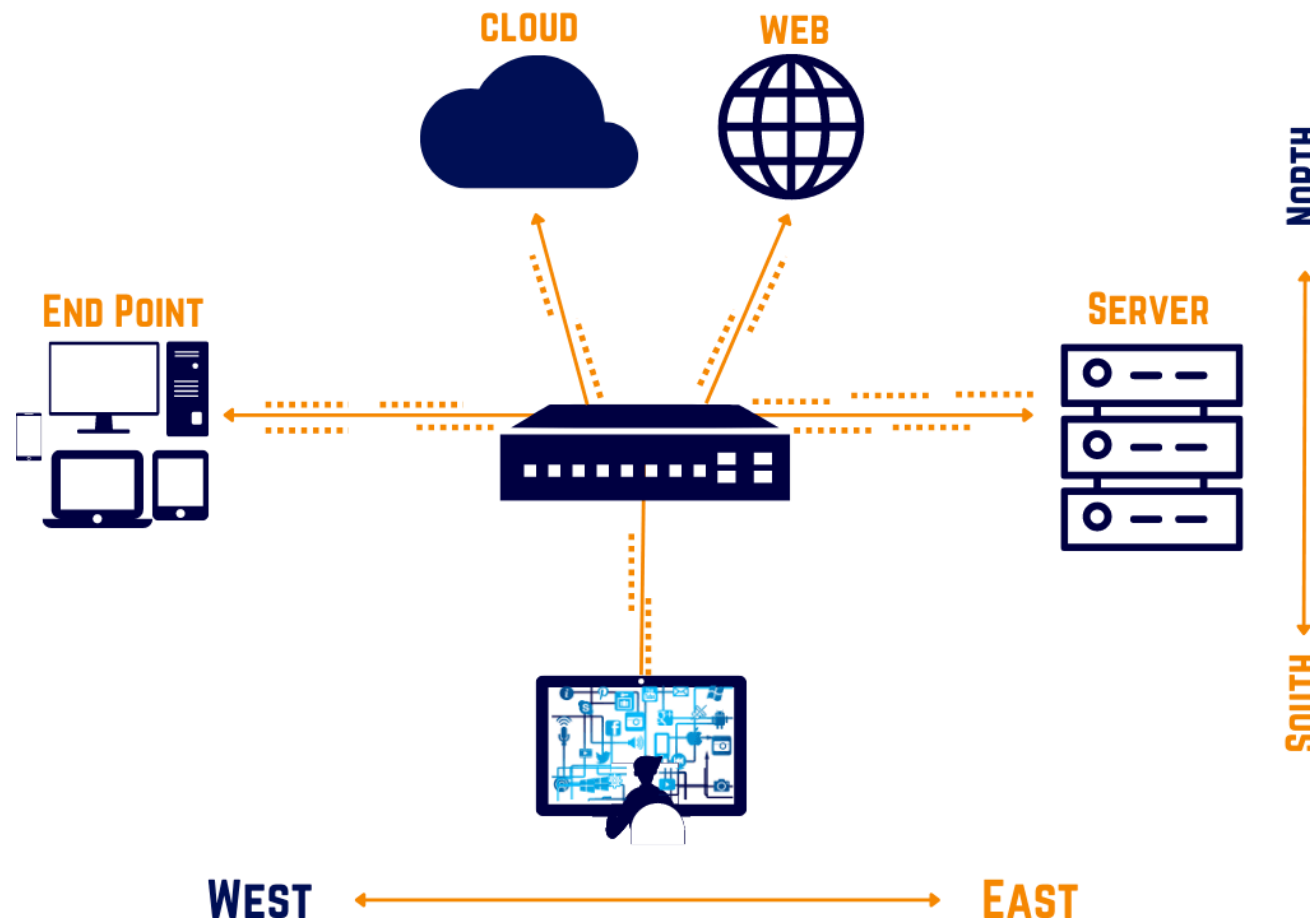


Tramite StageIT conosco Wintech e mi viene proposto un progetto di stage per portare in produzione il sistema *CyberCommand* di Sangfor

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*)



Obbligatorî:

- *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

Obbligatorî:

- *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

Obbligatorî:

- *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:

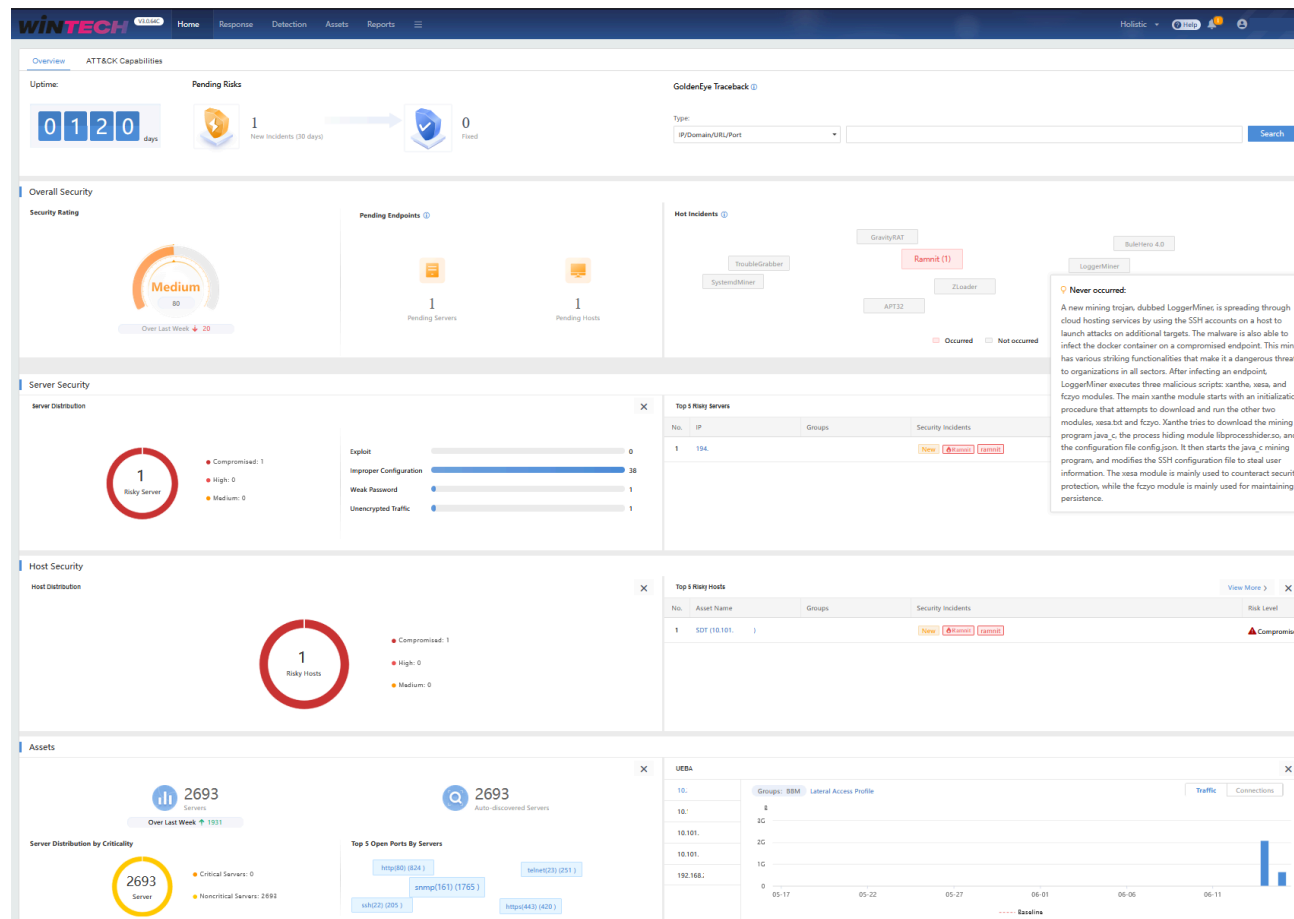
- Integrazione con prodotti già presenti in azienda

Facoltativi:

- *Bypassare* il sistema di rilevazione

CyberCommand, il sistema NDR offerto da Sangfor.

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

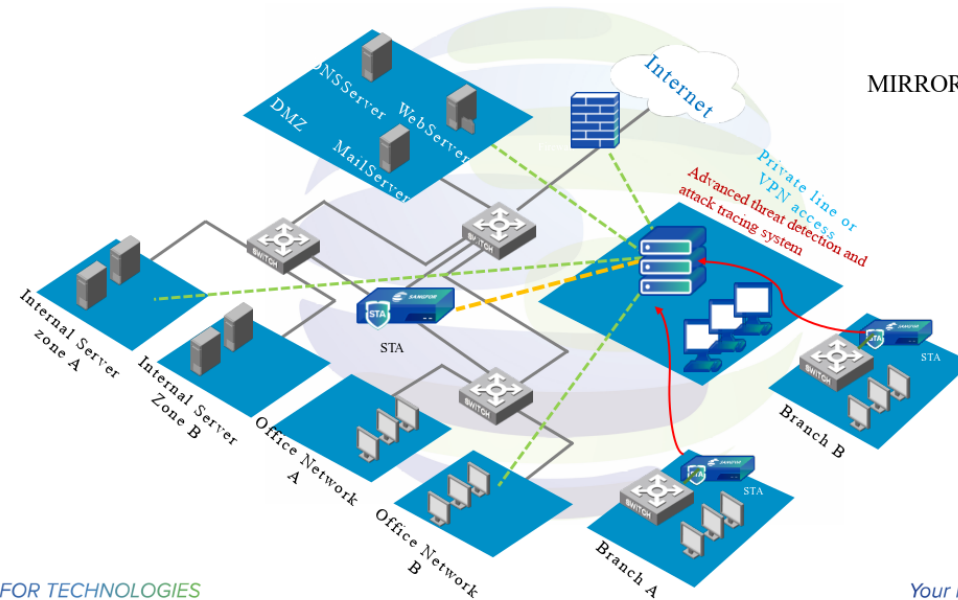


CyberCommand sfrutta le sonde STA inserite all'interno della rete per analizzare il traffico di rete e rilevare eventuali anomalie.

Deployment Guide



MIRROR MODE



SANGFOR TECHNOLOGIES

Your Future-Proof IT Enabler

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

Whitelists

Audit Whitelist: Traffic that matches the whitelist will not be audited.
Security Whitelist: No alerts or incidents will be generated for the logs that matches the whitelist.
Traffic data is filtered based on the audit whitelist first and then the security whitelist. Traffic that is not whitelisted is then analyzed, and alerts are generated.

Traffic

→

Audit Whitelist

→

Security Whitelist

→

Analyze

Edit Whitelist Entry

Description:

- 1. If multiple conditions are specified, the whitelist will take effect only when all the conditions are met.
- 2. The traffic that matches this whitelist entry will not be audited.
- 3. Only Stealth Threat Analytics (STA) V3.0.34 or later is supported. When STA is connected to two platforms, STA takes effect for the audit whitelist of only the primary platform.

Src IP:

Src Port:

Dst IP:

Dst Port:

Log Type:

Remarks:

Edit Security Alert Whitelist

Notes:

- 1. If multiple conditions are specified, the whitelist entry will take effect only when all the conditions are met.
- 2. After the whitelist entry is added, no alert will be triggered for the logs hitting this entry.

*Threat Type:

Rule ID:

Src IP:

Src Type:

Dst IP:

Dst Type:

Dst Port:

Domain Name/URL:

*Apply To:

*Schedule:

Remarks:

Edit Weakness Scan Whitelist

* IP Address:

URL:

Username:

Rule ID:

* Groups:

* Risk Type:

Remarks:

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

Incident Details

Infected with ramnit (worm)

Status: Pending Threat Type: **Worm** Severity: High
Detected By: **STA-NUC-** Attack Stage: **C&C** Incident ID: **1145000009**

Integration

Threats Hit Rules Attacker Analysis Forensics Recommendations

All Targets (1)

Select

SDT (194.) Compromised
Attacks: 2
Last Detected: 2023-06-15 08:58:36

1 in all < 1 >

Attacker	Victim	Attack Result	Last Detected
72.52.178.23(-)	SDT (194)	Compromised	2023-06-15 08:58:36

Details Original Logs

Details

1 Requested Malicious Domain Name: ttco...

2 Returned Response IP

Protocol: dns

Server: 194 SDT Port: 35739

Victim

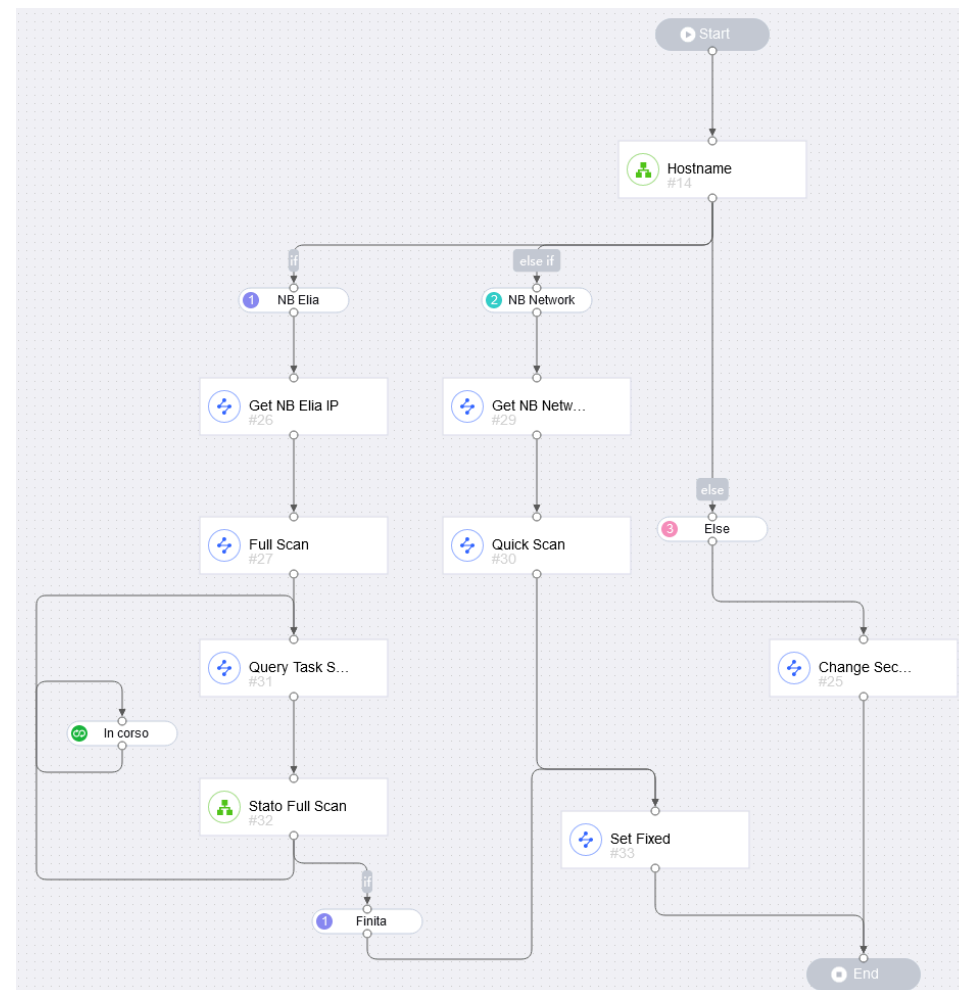
DNS Server

Latest Attack Details

indicator	ttconf.pw	name_server	8.8.8.8
answers_ip	72.52.178.23		

GoldenEye Traceback | Threat Intelligence

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



- ✓ NDR inserito in produzione, configurato e testato

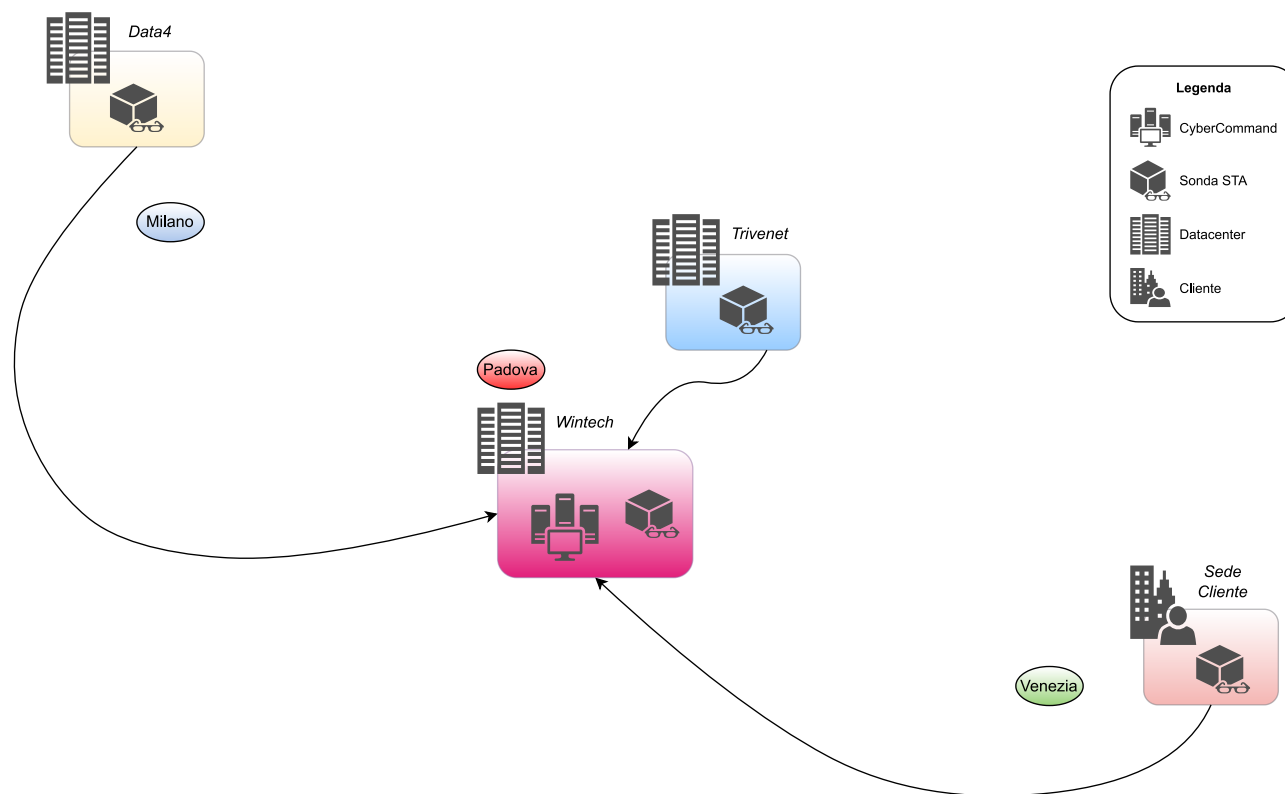
- ✓ NDR inserito in produzione, configurato e testato
- ✓ Documentate *best practices* e problemi riscontrati

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

- ✓ 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

- ✓ 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

- ✓ 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*



Sonde presenti in:

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

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 dimostrato efficace nella rilevazione dei problemi