

Projectplan

Bryan Poleunis

Thomas Deboel



Orange
Cyberdefense

THOMAS
MORE

Inhoud



- Wat doet Orange cyberdefense
- Doel project
- Plan
- Onderzoek
- Oplevering
- Stand van zaken



Orange
Cyberdefense



Orange
Cyberdefense

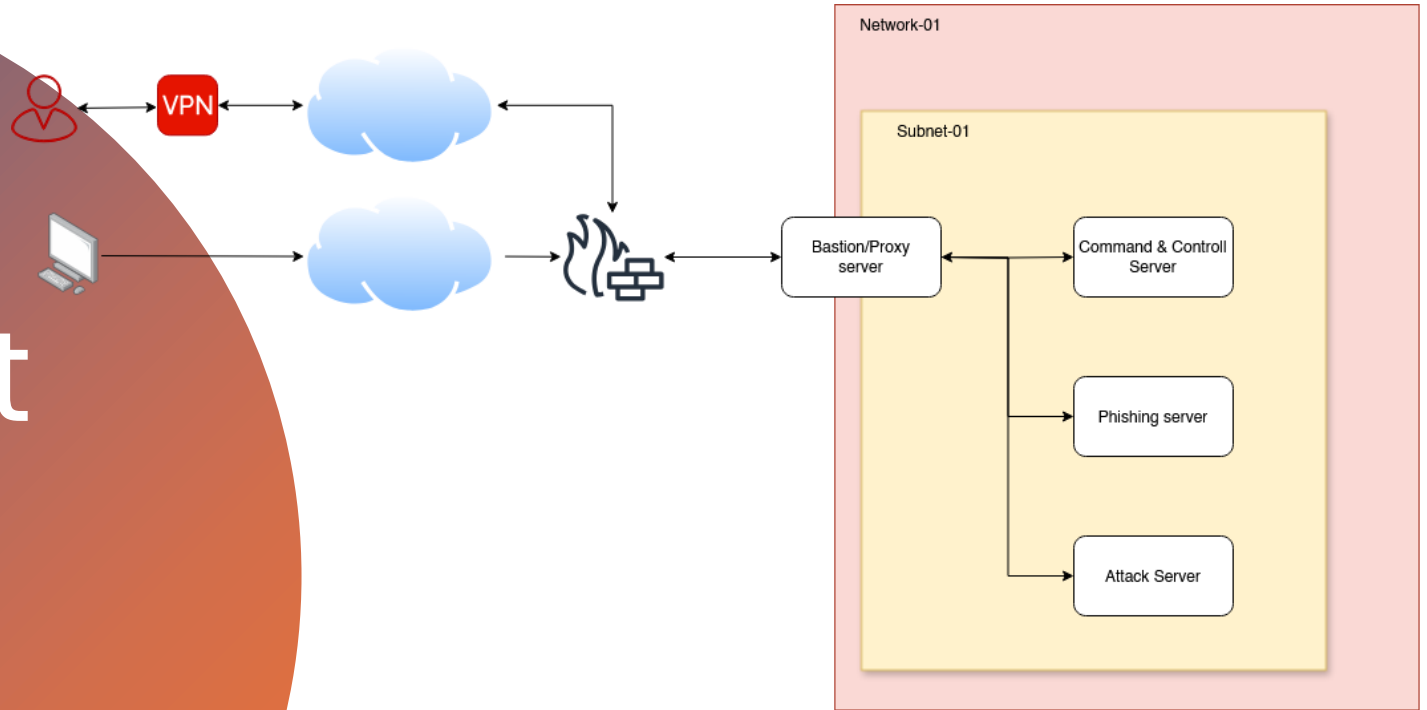


Orange Cyberdefense

Orange Cyberdefense is een leverancier van cybersecuritydiensten en -oplossingen en maakt deel uit van de internationale Orange Cyberdefense groep. Het bedrijf richt zich op het beschermen van organisaties tegen digitale dreigingen via diensten zoals advies, managed security, incident response en training.

Doel project

- Red team environment
 - Veiligheid en isolatie
 - Herbruikbare infrastructuur
 - Bruikbaar in echte wereld
 - configureerbaar

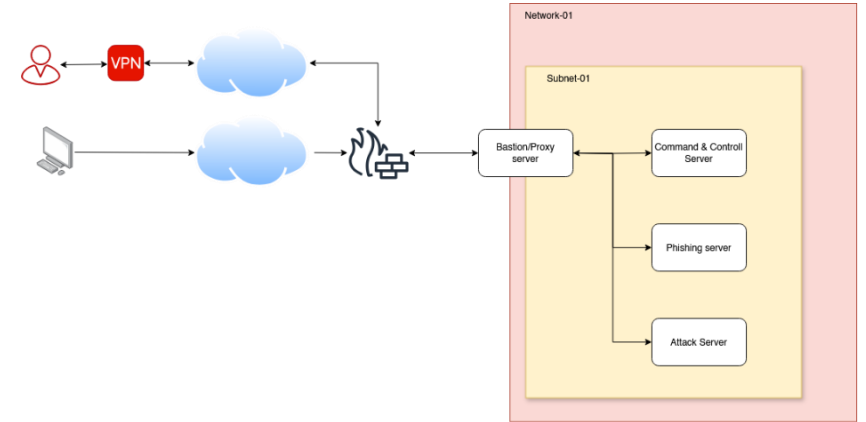


	Network	range
Network-01	10.0.0.0	/16
Subnet-01	10.0.0.0	/16

Ip-Table		
Bastion/proxy	10.0.0.2	/16
Command & Control server	10.0.0.3	/16
Phishing Server	10.0.0.4	/16
Attack Server	10.0.0.5	/24

Doel project

Het doel van het project is het maken van een geautomatiseerde Cloud red team omgeving op te zetten. Met deze omgeving moet je kunnen phishen, moet een command en control server zijn en een attack server hebben. Toegang moet enkel mogelijk zijn met behulp van een vpn.



	Network	range
Network-01	10.0.0.0	/16
Subnet-01	10.0.0.0	/16

Ip-Table		
Bastion/proxy	10.0.0.2	/16
Command & Controll server	10.0.0.3	/16
Phishing Server	10.0.0.4	/16
Attack Server	10.0.0.5	/24



Orange
Cyberdefense

Plan



Onderzoek individuele componenten



Functionaliteit

Ease of use

Automatie mogelijkheden

openSource

VPN



Orange
Cyberdefense

Cloud



Wat moet er in de Cloud

Hoe moet de Cloud functioneren

Wat kan de Cloud

Hoeveel resources moet je hebben

- Storage?
- Ram?
- CPU?
- GPU?

Welke servers moet je hebben voor welke prijs



Orange
Cyberdefense

Automatizing Cloud

Iac: OpenTofu

Proxy : Nginx

VPN: Tailscale

C2: Mythic C2

Phishing: GoPhish en Evilginx

Attack Server: Exegol



OpenTofu⁺

tailscale



Orange
Cyberdefense

Oplevering



Github Repository

Handleiding

Documentatie offensive tools

Demo



Orange
Cyberdefense