BELEID & BEHEER

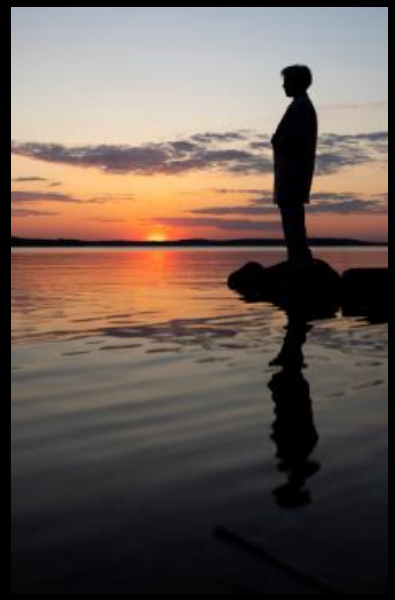
Elien Cardon

Stille Waters

13:30 – 14:15

ANNACON
0X7E8

Sssssssht...niets te zien of te horen hier.....



Agenda

Stille waters

1

Wat zijn APT's?

Kenmerken van APT's en hun tactieken zoals privilege escalation.

2

Insider Threats: Gevaren van binnenuit

Risico dat gevormd wordt door interne medewerkers en hun toegangen tot systemen.

3

Detectie-uitdagingen

Obstakels in security operations bij het detecteren van stille bedreigingen.

4

Use case: de APT en de Insider Threat - a perfect storm

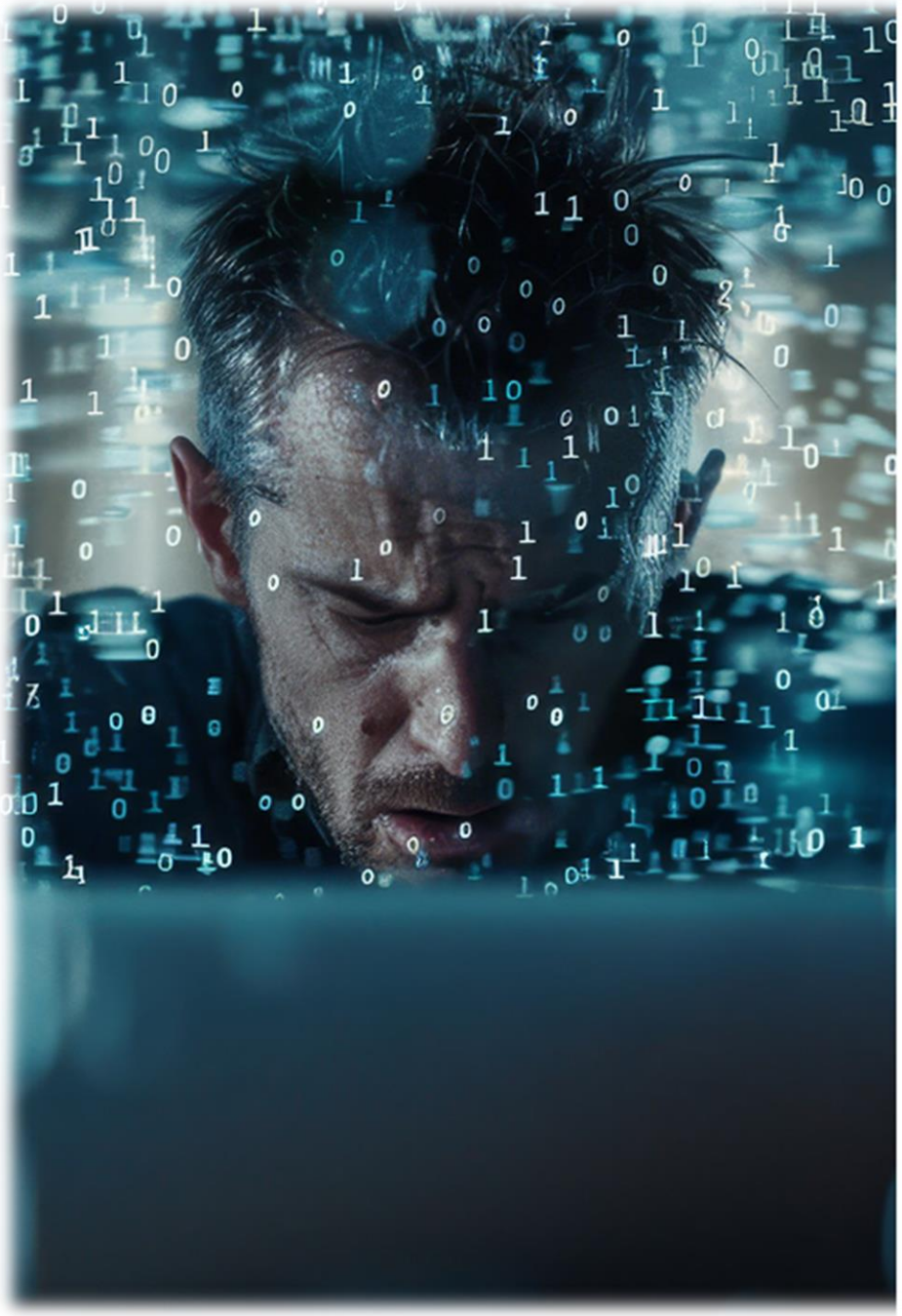
Wat als de APT en de Insider de handen ineen slaan?

5

AI binnen de SOC werking

Wat kan AI betekenen voor de operationele werking?

ANNACON
0X7E8



Wat zijn Advanced Persistent Threats (APT's)?

Definitie, kenmerken en voorbeelden van APT's

Definitie van APT's

Geavanceerde, aanhoudende bedreigingen die langdurige toegang tot netwerken behouden.

Tactiek: Privilege-escalatie

Aanvallers verhogen hun toegangsrechten om gevoelige informatie te bereiken (MITRE T1078).

Tactiek: Laterale beweging

Verplaatsing binnen netwerken om andere systemen te compromitteren (MITRE T1059).

Voorbeeld: SolarWinds-aanval

Malware in software-updates introduceerde langdurige toegang tot duizenden netwerken.

Gevolgen van APT's

Ernstige impact op bedrijfsvoering en databeveiliging, met langdurige schade.

ANNACON
0X7E8

Insider Threats: Gevaren van Binnenuit

Welke werknemer kan een dreiging vormen? Gaat het om mensen met een "speciale badge" of "admin rechten"?

Accidental Insider

Oeie...nu trek ik toch die draden uit zeker...van welk netwerk was welke draad nu ook al weer...?

Negligent Insider

Remote desktop support through LDAP?? But I'm at least 2 seconds faster as Local Admin!

Malicious Insider

Hey, heb je onze nieuwe collega al ontmoet op de anti-witwas afdeling? Fyodor Smirnov. Enfin, hij zegt dat we hem voor het gemak Piet Peeters mogen noemen :-)

Detectie-uitdagingen bij Stille Dreigingen

Uitdagingen in de Operationele Werking

Organisatorisch	Niet alle organisaties beschikken over geavanceerde detectietools, monitoring capaciteit of de nodige in-house technische kennis om deze dreiging te herkennen en mitigeren.
Ontbreken van use cases/logs	APT tactieken dienen met specifieke use cases en logs geïdentificeerd te worden. De meeste klassieke use cases spelen in op de meer "hoorbare" dreigingen (brute force, download van malicious files,...)
Ontbreken van tijd	SOC analisten ontbreekt het vaak aan de nodige tijd om onderzoek te doen naar nieuwe methodes en daaruitvolgend use cases te ontwikkelen.
Identificatie van insider threats	Het ontbreekt organisaties vaak aan een visie omtrent deze specifieke dreiging. Fysieke veiligheid en cybersecurity zijn twee aparte entiteiten.
Cultuur	Net zoals de aanvaller zich hult in de stilte, is ook een "stiltecultuur" in een organisatie een mogelijke bedreiging.

Definitie en Impact van Stiltecultuur in Cybersecurity

Stiltecultuur als Risico binnen het Domein van Cybersecurity

Verhoogde Risico's

Stilteculturen kunnen leiden tot een toename van cyberdreigingen doordat medewerkers zich niet vrij voelen om verdachte activiteiten of kwetsbaarheden te melden.

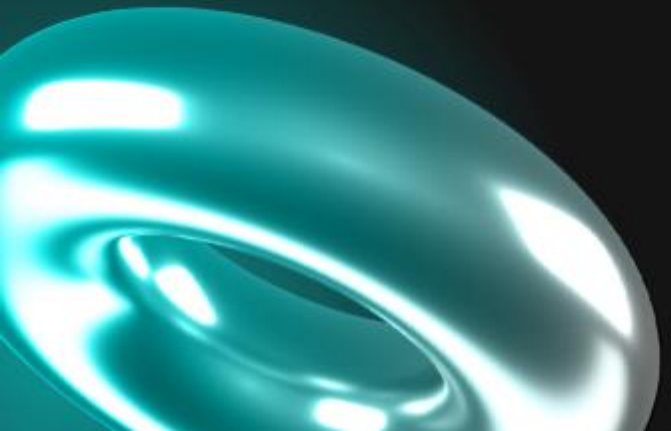
Onvoldoende Incidentrespons

Het ontbreken van open communicatie kan de snelheid en effectiviteit van incidentbeheer verminderen, waardoor aanvallen langer onopgemerkt blijven.

ANNACON
0X7E8

De APT en de Insider Threat Case: AD Compromittering

Stilte voor de storm...



Stap 1: Insider Verschaft Toegang

Hoe insiders helpen bij APT-aanvallen op Active Directory

01 **AD-referenties**

De insider biedt toegang tot domein administrator of IT admin accounts, cruciaal voor de APT.

02 **Netwerktopologie**

Informatie over netwerkstructuren en belangrijke systemen, waardoor de APT effectief kan opereren.

03 **Beveiligingscontroles**

Details over bestaande beveiligingsmaatregelen, zoals EDR en firewalls, helpen de APT om deze te omzeilen.

04 **Uitschakeling van interne verdedigingen**

De insider helpt om de beveiliging te verzwakken, waardoor de APT onopgemerkt kan blijven.

ANNACON
0X7E8

Stap 2: APT Verkrijgt Persistentie

De rol van insider-gegevens bij het opzetten van backdoors

Insider-gegevens benutten

De APT gebruikt de door insiders geleverde AD-gegevens om zich binnen het netwerk te verplaatsen.

Legitieme Windows-diensten

Technieken zoals PowerShell en WMI worden gebruikt voor onopgemerkte uitvoering van opdrachten.

Instellen van backdoors

Malicious GPO's en andere methoden zorgen voor blijvende toegang tot de AD-infrastructuur.

Behouden van persistentie

Door het opzetten van backdoors kan de APT zijn toegang handhaven, zelfs na detectiepogingen.

Stap 3: Gericht op Belangrijke AD-objecten

Aanvallen op domeincontrollers en serviceaccounts met geavanceerde technieken.

01

Aanvallen op Domeincontrollers

De APT richt zich op domeincontrollers om volledige controle over het netwerk te verkrijgen.

02

Gebruik van Kerberoasting

Kerberoasting wordt gebruikt om hashes van serviceaccount-inloggegevens te stelen uit de AD-omgeving.

03

Pass-the-Hash Techniek

Met Pass-the-Hash kan de APT zich voordoen als hooggeplaatste gebruikers zonder detectie.

04

Informatie van de Insider

De insider biedt cruciale kennis over AD-structuren, wat de APT helpt bij gerichte aanvallen.

05

Verhoogde Privileges

Door het gebruik van deze technieken kan de APT zijn privileges binnen de AD-omgeving verhogen.

Stap 4: Insider Vermindert Detectiekansen

Manipulatie van AD-logs en beveiligingscontroles om detectie te voorkomen.

Voorkomen van systeemupdates

Door updates op kritieke systemen te blokkeren, worden bekende kwetsbaarheden toegankelijk voor de APT.

Beveiligingscontroles aanpassen

Veranderingen aan beveiligingsinstellingen maken het moeilijker voor SOC-teams om aanvallen te detecteren.

Manipulatie van AD-logs

Insider wijzigt loginstellingen om detectie van verdachte activiteiten te minimaliseren.

Stap	Actie	Technieken	Detectie	Impact
1. Insider biedt toegang BYPASS!	De insider deelt AD-credentials	Credential Access TA0006 Privileged Access TA0004	Event ID 4624	Initiële toegang tot AD
2. APT verwerft persistentie	Gebruik van legitieme Windows-diensten	Living off the Land - TA0003 Network Logon Script - T1037.003	Endpoint Detectie Logs	Continuïteit in toegang
3. Doelgerichte aanvallen op AD-objecten	Kerberoasting, Pass-the-Ticket	T1558.001	Ongebruikelijke Kerberos tickets	Verkrijgen van extra toegang
4. Vermijden van detectie	Manipuleren van AD-logs	T1003	Altereren logging beleid	Minimaliseren van detectierisico's
5. Volledige AD-overname	Data-exfiltratie via stealthy kanalen	T1087.002	Ongebruikelijke uitgaande verkeer	Volledige controle over het netwerk

DE TOEKOMST VAN AI-GEDREVEN DREIGINGSDETECTIE IN SOC'S (2024-2029)

AI als ruggengraat voor dreigingsdetectie en anomaliedetectie

- **(Semi)-Autonome analyse van datasets**

  AI zal in staat zijn om enorme hoeveelheden gegevens zelfstandig te verwerken en te analyseren.

- **Real-time detectie van anomalieën**

  Detectie van verdachte activiteiten zal onmiddellijk plaatsvinden, waardoor snelle reacties mogelijk zijn.

- **Inhoudelijke invulling van de rol van de analyst verandert**

  Het gebruik van AI verandert hoe de analist in het werk staat

- **Verbetering van UEBA-systemen**

  AI zal gedetailleerde baselines van normaal gedrag opbouwen en continu leren van nieuwe gegevens.

- **Detectie van 'stille' bedreigingen**

  AI zal in staat zijn om geavanceerde persistente bedreigingen en insider threats te identificeren.

ANNACON
0X7E8

Deze partners hebben een ❤️ voor ANNACON 0x7E8.

ANNACON
0X7E8

easi
NEUVIK
astrea
UPRIGHT
INFOSENTRY
TSF
pwc
Business
exabeam
REFRACTED
JARVISS
FOX IT
SentinelOne
sweepatic
Beltug
ISACA
Belgium Chapter
SAI