centric
connect.engage.succeed.

NFIR
IT FORENSICS & INCIDENT RESPONSE

DE CYBER SECURITY PARTNER VAN CENTRIC

Strategische Conferentie |Figi - Zeist | 30-11-2023

Samenwerking Centric - NFIR

- Centric kan op dit moment geen passend portfolio aanbieden in de lokale overheidsmarkt m.b.t. “Managed Detection & Response (MDR) en Forensics.
- NFIR beschikt wél over een passend diensten portfolio dat voldoet aan de gestelde eisen en heeft een uitstekende reputatie.
- Er is sprake van een ‘cultural fit’ tussen Centric en NFIR.
- Door een samenwerking aan te gaan met NFIR kan Centric zijn klanten toch een volledig dienstenpakket op het gebied van Security Monitoring, Forensics en Incident Response aanbieden, inclusief pentesten en consultancy diensten.

Strategische overwegingen

- Door een samenwerking aan te gaan:
  - wordt een tijdrovende en kostbare eigen ontwikkeling vermeden
  - is er met onmiddellijke ingang een concreet en samenhangend aanbod van specialistische diensten die zich al hebben bewezen in de markt en wordt Centric ook op het gebied van security een relevante gesprekspartner voor lokale overheden
  - wordt belangen-tegenstelling voorkomen (“slager keurt eigen vlees”)
  - kan i.g.v. security incidenten meteen gecorrelleerd worden met onze SaaS diensten (‘hotline’)

<Introductie NFIR/>

ONZE DRIJFVEREN

Organisatie ondersteunen om zo **weerbaar mogelijk te zijn tegen de gevaren en risico's** van de digitale wereld.

Met onze **motivatie** en **ervaring** kunnen wij helpen bij het vergroten van de digitale weerbaarheid om de kans en impact van een Security-Incident te verkleinen.

Onze **passie voor IT-Security** en de drang om opdrachtgevers zo goed mogelijk te helpen is bijzonder groot!

HOE WIJ WERKEN

Wij bieden ca 60 **IT-Security specialisten**, die niet alleen heel **vakkundig** en **creatief** zijn, maar ook **snel** kunnen handelen, **procedureel werken en in begrijpelijke taal communiceren** met onze opdrachtgevers.

WAT WIJ KLANTEN VAN CENTRIC BIEDEN

Onze ervaren medewerkers staan **24/7 /365** paraat om opdrachtgevers te helpen bij **cyber security incidenten. Daarnaast** voeren wij **Digitaal Forensische Onderzoeken** uit, **monitoren** real-time de IT en OT infrastructuur van onze klanten en sporen onze ethisch hackers kwetsbaarheden op door het uitvoeren van **Pentesten** en **Social Engineering** opdrachten. Tot slot helpen onze **Security Consultants** opdrachtgevers met het verhogen van de IT-Security volwassenheid.

Reactieve diensten

Incident Response

Digitaal Forensisch Onderzoek

Incident Response Retainer Contract

Preventieve diensten

Pentesten

Security Monitoring

CIS Controls Consultancy

Social Engineering

Dossier Monitoring

Incident Response Plan

WAAR NFIR TROTS OP IS

Werken volgens Incident Response procedures NIST en SANS

Computer Emergency Response Teams (CERT)

Alle medewerkers hebben Korpschef toestemming en voeren periodiek integriteit gesprekken

Particulier Opsporingsbureau met POB-vergunning van Ministerie van Justitie en Veiligheid en gediplomeerde Particulier Onderzoekers

Zeer tevreden klanten uit diverse private en publieke sectoren

Korte lijnen met het NCSC, IBD, AP, Politie (High Tech crime), het Openbaar Ministerie en privacy juristen

ISO27001:2022 & 9001
CCV pentest keurmerk

bsi ISO 9001 Quality Management Systems CERTIFIED ISO/IEC 27001 Information Security Management CERTIFIED

Onafhankelijke Nederlandse organisatie


<korte toelichting op diensten/>

INCIDENT RESPONSE (NFIR CERT)

Hulp bij onverwachte gebeurtenissen in uw IT omgeving

- Geen toegang meer tot werkplekken, applicaties en servers
- Ongeautoriseerde toegang tot onderdelen van het netwerk
- Geen toegang meer tot data door ransomware
- Mogelijk datalek

Het NFIR Computer Emergency Response Team

- 24/7/365 binnen 3 uur NFIR CERT op locatie of binnen 30 min. op afstand
  - Incident Response Retainer Contract garandeert deze SLA
- Impact en schade van het Security Incident tot een minimum beperken
- De continuïteit van de primaire processen zsm terug op orde brengen
- Digitaal Forensisch Onderzoek naar de Root Cause en impact van het incident

INCIDENT RESPONSE RETAINER CONTRACT

NFIR CERT 24/7/365 binnen 3 uur op locatie of direct op afstand in actie

Een vaste en ervaren Cyber security partner aan uw zijde

Kennis van de technologie (IT&OT)

Relatie opbouwen met uw crisis team

Inzicht in alle beschikbare logfiles

Inzicht in uw crisis plannen en processen (IR plan / BCP)

DIGITAAL FORENSISCH ONDERZOEKEN

Computers en laptops

Mobiele telefoons

Fraude en diefstal

Afpersing

Datalekken

OSINT (Open Bronnen Onderzoek)

Grensover-schrijdend gedrag

Onderzoek op professionele en procedureel juiste wijze

In bezit van geavanceerde forensische apparatuur

Bevoegd om onderzoek te verrichten naar personen

Alle bevindingen zijn bruikbaar voor gerechtelijke procedures.

BPOB

MANAGED DETECTION & RESPONSE

Waarom monitoren?

- Inzicht krijgen in Digitale dreigingen op het netwerk en schending van privacy
- Snel acteren bij malafide activiteiten of mogelijke schending van privacy
- Monitoren is een passende maatregel om te voldoen aan de AVG

NFIR biedt geautomatiseerde monitoring oplossingen

- Geschikt voor diverse logbronnen van het IT/OT netwerk en applicaties
- Direct op de hoogte van verdachte activiteiten
- Helder en eenvoudig te interpreteren rapportages

SECURITY MONITORING

DOSSIER MONITORING

SECURITY MONITORING

1 centrale monitoring ipv verschillende dashboards

Volledig geautomatiseerde SIEM/SOC oplossing

loganalyse: rule based (use cases) & machine learning

Geen logbronnen zelf interpreteren

Heldere output & direct op de hoogte van verdachte activiteiten

Geen mensen achter scherm, 80/20 regel, UEBA, TI

Schaalbare oplossingen met maatwerk mogelijkheden

Indien noodzakelijk rekenen op directe ondersteuning CERT

Operationele Technologie (OT)

DOSSIER MONITORING

Waarom Dossier Monitoring?

- Regie op privacy, sturen op gedrag, bewustzijn en maatregelen met relevante inzichten
- Conform wet- en regelgeving (o.a. NVZ, AVG, NEN7510)
- Zicht hebben en houden op onrechtmatigheden en gedrag binnen de organisatie
- Geen onverwachte schending van privacy die kunnen leiden tot boetes

Wat biedt Dossier Monitoring?

- Gereedschap voor het monitoren van dossier inzagen tbv (bijzondere) persoonsgegevens
- Data analisten voor het leveren van maatwerk bovenop generieke modules
- Informeren over onregelmatigheden inclusief context via diverse kanalen
- Maandelijks optimaliseren van usecases om nog betere inzichten te krijgen
- Nauwe samenwerking met opdrachtgevers tijdens het implementatie traject en doorontwikkeling van de dienst

SECURITY CONSULTANCY

Incident Response Plan

CIS Security Controls v8 advies en implementaties

PENTESTEN

Penetratietesten en code reviews zijn noodzakelijk om de technische weerbaarheid en de effectieve werking van de beveiliging aan te tonen.

Web applicaties , IT-infrastructuren, websites, koppelingen (API's), DigiD, MedMij, Mobiele applicaties en Operationele Techniek.

Pentesten op maat

- Samen de scope bepalen
- Samen de aanvalsscenario's bepalen
- De ethisch hackers beschikken over veel ervaring, creativiteit en certificeringen
- Uitvoering volgens internationale standaarden
- Heldere, complete en zeer bruikbare rapportages
- Uitvoering volgens het CCV pentest kwaliteit keurmerk

SOCIAL ENGINEERING DIENSTEN

Mysterie Guest bezoeken

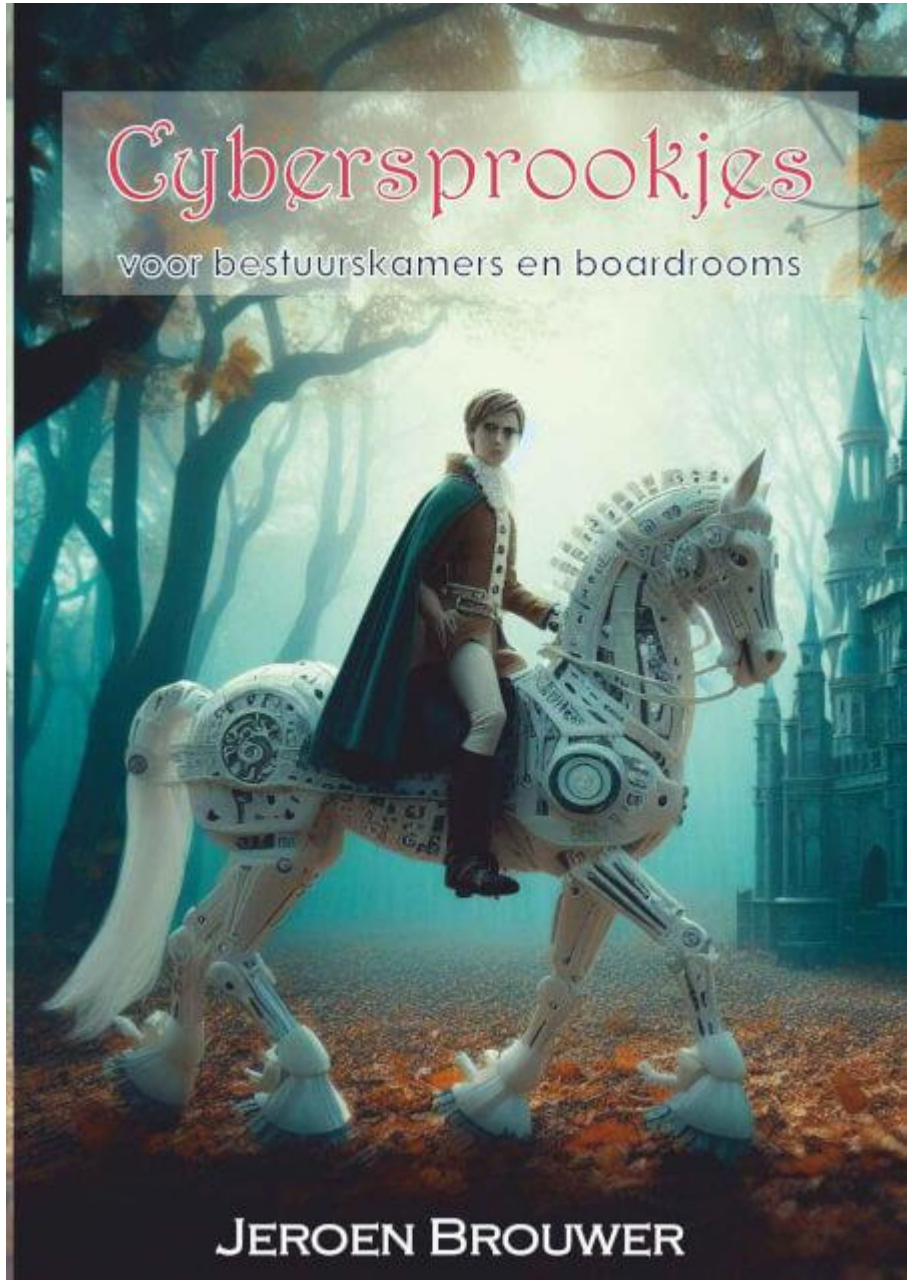
USB Dropping

Mail phishing

Voice phishing

Smishing

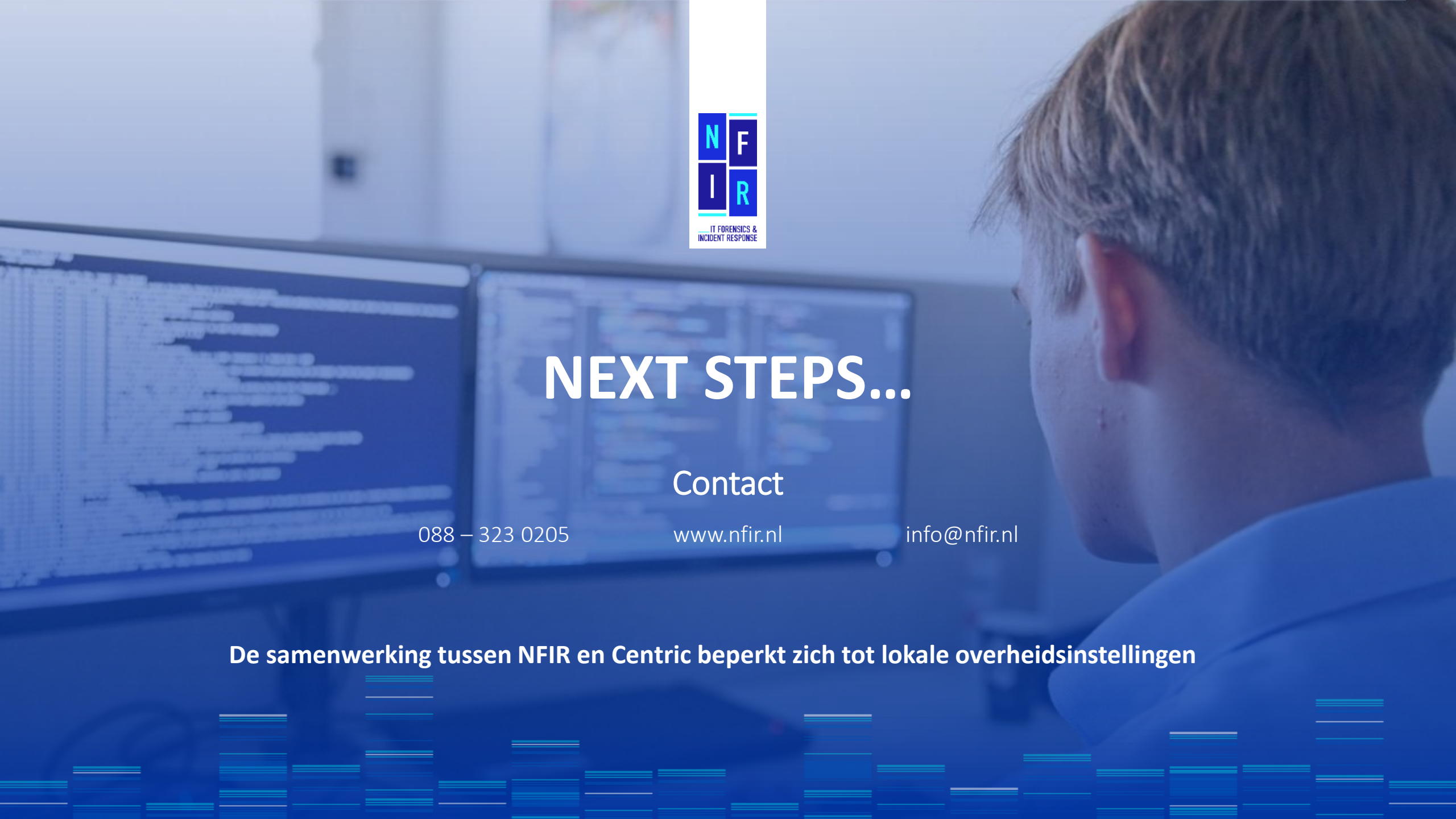
Social Media Phishing



TIP VOOR ONDER DE BOOM

Dit boek is een hulpmiddel met een knipoog, bedoeld om cybersecurity vanuit een wat minder traditionele invalshoek te adresseren.

Aan de hand van een aantal sprookjes wordt de complexe cyberwereld teruggebracht tot de strategische essentie: het beschermen van belangen. Mogelijk kan dit bijdragen om in bestuurskamer of boardroom van cybersprookjes tot cybersecuritystrategie te komen.



NEXT STEPS…

Contact

088 – 323 0205 www.nfir.nl info@nfir.nl

De samenwerking tussen NFIR en Centric beperkt zich tot lokale overheidsinstellingen