24/09/2024

**Curriculum Vitae**

Gert Nelen

August Van Doorslaerlaan 55

1860 Meise

+32 474 86 19 44

gert.nelen@g3rt.be

https://www.g3rt.be

**Opleiding**

1999-2002: Toegepaste Informatica – Rega-instituut KHL

1997-1999: Psychologie – Katholieke Universiteit Leuven

1991-1997: Latijn Wetenschappen – College van het Eucharistisch Hart (Essen)

**Cursussen**

ISC² Member ID: 784520

2024: Brucon Spring Advanced Incident Response in the MS Cloud, Brucon Autumn A quick, efficient, yet not entirely sane, primer on Cyber Deception

2023: SANS SEC699: Advanced Purple Teaming - Adversary Emulation & Detection Engineering, Brucon 2023 IoT Security Bootcamp

2022: GDAT certification – GIAC Defending Advanced Threats, SANS SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses, Brucon 2022 Linux Forensics Inspection and Incident Response at scale

2021: CCSP certification – Certified Cloud Security Professional, Brucon 2021 Operational Threat Intelligence

2020: CISSP certification – Certified Information Systems Security Professional

2013-2019: Brucon 2019– Full Stack Exploitation, Brucon 2018- Network Data Exfiltration Techniques-Post Exploitation, SANS SEC560 Network Penetration Testing and Ethical Hacking, SANS SEC660 Advanced Penetration Testing, Exploit Writing and Ethical Hacking, SANS SEC575 Mobile Device Security and Ethical Hacking, SANS SEC760 Advanced Exploit Development for Penetration Testers, Suricata Intrusion Detection Training, SANS SEC511 Continuous Monitoring and Security Operations

Ik ben ook regelmatig bezoeker van LEA (Law Enforcement Agency) of andere security-beurzen/seminaries (ICCS, ISS world, Black Hat, Brucon,...) om bij te blijven met de laatste ontwikkelingen.

2009-2013: Ethical Hacking (tailormade) by John Cordier Academy, Fortinet Professional by Exclusive Networks, Fortinet Specialist by Fortinet, Juniper JNCP, VMWare ESXi 5.5 configure and install, Powershell (hogeschool), SANS FOR500 Windows Forensics Analysis, SANS FOR508 Advanced Digital Forensics, Incident Response and Threat Hunting, SANS FOR572 Advanced Network Forensics and Analysis, SANS SEC503 Intrusion Detection In-Depth

2007-2009: Stageopleiding VS/SE waaronder bronbehandeling, onderzoekstechnieken, veiligheidsprincipes, wapenmanipulatie, (inter)nationaal recht, ...

2002-2007: Systeembeheer Active Directory, Exchange mail server, Linux (beginner/advanced), Extreme Networks management, VMWare

**Werkervaring**

3/2018 - heden: Security Consultant voor g3rt – Langetermijn opdrachten:

1/3/2018 – 31/8/2019 @ BNP-Paribas-Fortis – SOC opstart project, Threat Management Capability, Incident Response Tier 3, Threat Hunting

5/8/2019 – 12/2020 @ PWC incident team – Asco industries– Businessnoden vertalen tot een strategie om zo snel mogelijk tot een beveiligde situatie te komen na het incident.

3/1/2021 – 12/2024 @ Colruytgroup – Security Operations Team Coach- Colruytgroup bijstaan vanuit operationeel standpunt in hun evolutie met het oog op integratie van security in alle lagen van de organisatie en professionaliseren werking SOC.

10/2007-3/2018: Veiligheid van de Staat als inspecteur in de Operationele IT-afdeling.

8/2002-10/2007: CIBG, fulltime uitgezonden naar Vlaamse Gemeenschapscommissie als netwerk-en systeembeheerder.

1/2002-5/2002: stage bij Vlaams Parlement – java programmeur dynamische Oracle databank

**Talenkennis/Extra**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Begrijpen** | **Spreken** | **Schrijven** |
| Nederlands | Moedertaal | Moedertaal | Moedertaal |
| Engels | Uitstekend | Vloeiend | Uitstekend |
| Frans | Heel goed | Vloeiend | Goed |

Ook begrip en beheersing van juridische taal en technische taal in zowel engels als nederlands.

**Relaas Ervaring/Skills/Projecten**

2021-2024:

In januari 2021 begin ik als teamcoach en senior analyst bij de Security Operations afdeling van Colruygroup. Het hoofddoel van de opdracht is de SOC werking te professionaliseren en Colruyt te adviseren en begeleiden bij hun evolutie naar een meer systemisch beveiligde en verdedigbare omgeving. Uitbouwen van incident response, detection engineering en threat intel capabilities met een schuivend rollensysteem, aangepast aan de eigenheden van het team, adviseren over security controls en kennis uitbouwen en overdragen binnen het team rond forenische acquisities, onderzoeksmethoden, playbook en rule development, purple teaming, threat reporting,...

2020:

Vanaf begin 2020 wordt ik rechtstreeks ingehuurd door Asco om de continuïteit van de begeleiding naar G2G (go to green) te verzekeren. De projecten worden geleidelijk afgerond en de verantwoordelijkheden overgedragen aan Asco.

2019-2020:

Naar aanleiding van een belangrijk incident bij Asco en door een acuut gebrek aan ervaren security/incident/netwerk profielen binnen PWC word ik ingehuurd om het internationale team van PWC te versterken. Ik krijg de leiding van het team met de verantwoordelijkheid om de netwerkbeveiliging (en daarmee ook het netwerkdesign van de industriereus) in te richten tijdens de nasleep en heropbouw van dit grote cyberincident. De greenfield methode wordt toegepast en in een recordtijd wordt een goed beveiligd, beheersbaar en duidelijk-netwerkdesign, met een verregaande integratie van de verschillende systeem, network, iot en ot componenten uitgebouwd, waarbij de scheiding tussen Green, Amber, Red en Black ook word doorgetrokken op alle beveiligingslagen om menselijke fouten zo veel mogelijk uit te sluiten en te voorkomen dat een incident met dergelijke impact opnieuw kan gebeuren.

2018-2019:

Eind 2018 verschuif ik binnen het SOC team naar Incident Response nav de noden van BNPPF. Mijn taken hier zijn voornamelijk Tier 3 incidenten behandelen en Threat Hunting wanneer er geen incidenten te behandelen zijn. Hiervoor maar ik gebruik van de verschillende beveiligings-technologieën van de bank (F5 reverse proxies, McAfee & Bluecoat Proxy, Cisco Netwerk producten, Fortinet en Palo-alto Firewalls, Infoblox, IDS, Qualys, ArcSight, Splunk, Archer, EagleEye ...) . Ook forensische analyse van zowel systemen als netwerken behoren terug tot mijn takenpakket.

2018:

Ik ben als security consultant ingezet door BNP Paribas Fortis om te assisteren bij de opstart van een volledig functionele SOC (Security Operations Center). Specifiek focus ik mij op de ‘threat management capability’ binnen het team om mee de processen en procedures te stroomlijnen rond de cyber-verdediging van deze grote bank. We zetten threat-informatie om in concrete indicators die direct kunnen worden ingezet in de verschillende lagen van beveiliging in de infrastructuur. Dagelijks worden nieuwe dreigingen en hun implicaties tav de concrete verdediging en detectie geanalyseerd, de bevindingen geraporteerd aan de betrokken partijen en de geplaatste maatregelen getest tegen zowel oude als nieuwe TTP’s (Tools Techniques and Procedures).

2010-2018:

*Vanaf 2010 begint een herorganisatie van de IT-dienst(en) op basis van de wet op de Bijzondere Inlichtingen Methoden (BIM). Dit vormt een wettelijk kader dat onze dienst in staat stelt om onder specifieke voorwaarden en binnen een streng gecontroleerd kader uitzonderingen op (algemenere) wetten te bekomen om bepaalde inlichtingen te verwerven. Gezien mijn uitgebreide netwerkkennis word ik ingedeeld bij de Operationele Tak.*

* In 2010 een nieuw netwerk en diens beveiliging voor onze dienst ontworpen. We proberen de veelheid aan vendoren in te perken en alles homogeen rond enkele producten en technologieën te bouwen. De belangrijkste hoekstenen hierin vormen de producten van Fortinet, Juniper, Cisco en Barracuda.
* Regelmatig forensisch onderzoek op zowel computersystemen als netwerkinfrastructuur, zowel bij derden als diensteigen materiaal.
* De verdere verdieping en uitbreiding van de verbonden netwerken en vooral het toegankelijk maken zonder in te boeten aan security zijn de grootste uitdagingen.
* Design en installatie voor de vervanging van het blackberry systeem door een Knox-oplossing van Samsung. Nauwe internationale samenwerking met Samsung SDS/Electronics om dit te verwezenlijken. Sterk beveiligde dialup-IPSEC tunnels vanuit android-toestellen geven enkel binnen een gecrypteerde container toegang tot het bedrijfsnetwerk en de nodige operationele diensten en programma’s.
* Verdere uitbouw van Red Team die als belangrijkste kerntaak penetratie vanop afstand van computersystemen en het schrijven van exploits om de toegang te blijven verzekeren heeft. We gebruiken hiervoor vooral script- en programmeertalen (o.a. powershell, python, c#, perl, wmi). Er ontstaat een nauwe samenwerking met bevriende buitenlandse diensten om elkaars expertise versneld aan te scherpen. Uitgebreide ervaring met frameworks en tools zoals metasploit, cobalt strike, empire, dnscat2, burp, scapy,...
* De expertise en know-how vanuit het Red Team worden gebruikt om vanaf 2016 het nieuwe netwerk en de beveiliging te hertekenen. Door de veelheid aan diverse verbindingen en externe relaties moet alles meticuleus worden gesegmenteerd met een complex netwerkdesign als resultaat. Verschillende lagen beveiliging in verschillende functionele segmenten vormen de kern waardoor zowel de beveiliging, de logica als de beheersbaarheid worden vergroot. Een 30-tal (al dan niet virtuele) firewalls en andere security componenten filteren en monitoren op alle lagen van het OSI-model.

2007-2010:

* Stage-opleiding bij veiligheid van de staat. Ik leer veel zaken die niet rechtstreeks verband houden met IT, maar wel kaderen in het grotere security-plaatje, zoals wetgeving, problematiek, veiligheidsprincipes, internationale (samen)werking, ...
* Na 1 jaar (inspecteurs)opleiding word ik ingedeeld als stagiair bij de IT-sectie en ondersteun ik mee de werking van de dienst; meer specifiek de vele verbindingen met andere overheidsdiensten en inlichtingendiensten van andere landen. De veelheid aan verschillende databanken, beveiligingsnormen en technieken vormt een goede leerschool. Nog 1 jaar later slaag ik in de eindproeven voor de stage en word ik ingedeeld als inspecteur bij de IT-dienst.
* Set-up van beveiligde mobiele verbindingen met Blackberry, installatie en configuratie van bijhorende AD en Exchange set-up.
* Internet-toegangen professionaliseren, beveiligen en uitrollen naar alle werkposten.

2002-2007:

* Oud Token Ring netwerk omvormen naar nieuw Ethernet-based netwerk met Switches en routers (merk Extreme).
* Opzet en beheer sendmail mailserver die alle mailadressen voor alle nederlandstalige instellingen in Brussel bevat en een bind dns-server voor de publieke adressen.
* Beveiligde verbindingen met alle externe (nederlandstalige) entiteiten in Brussel (scholen, gemeenschapscentra, administratiehuizen, ...). Introductie van functioneel gesegmenteerd netwerk, beveiligd met iptables en snort.
* Opzet, beveiliging en beheer nieuwe Apache webserver voor de Nederlandse scholen in Brussel.
* Design, Opzet en beheer Active Directory en Exchange voor alle administratiehuizen.
* Vanaf 2005 werd de open source firewall vervangen door een Firewall Cluster van Vasco.

**Over mezelf**

Hobbies: muziek maken/luisteren, een goede film meepikken of een avontuurlijke reis maken kunnen mij een uitlaatklep bieden. Ik ben een fervent skiër en geniet van de rust bij het diepzeeduiken in tropische zeeën. Ik maak regelmatig tijd voor een privé-projectje waarbij ik fijn handwerk moet verrichten, zoals het ineenknutselen (en programmeren) van robots, het bouwen en inrichten van een terrarium of het automatiseren van een aquarium met raspberry pi. Ik ben geïnteresseerd in nieuwe technologische ontwikkelingen en snufjes en word in mijn vriendenkring dan ook soms ‘Mr. Gadget’ genoemd.

Ik ben gedreven en gemotiveerd en kan complexe problemen en situaties omvatten en zeer diep in een specifiek probleem duiken zonder het overzicht of de finale doelstelling uit het oog te verliezen. Ik geef niet (snel) op voordat het gewenste resultaat is bereikt. Als keerzijde heeft dit tot gevolg dat ik soms moeilijk kan loslaten en problemen mee naar huis neem. Ik kan om met werkdruk hoewel ik af en toe een uitlaatklep nodig heb, die ik dan in mijn hobbies wel kan vinden. Ook regelmatig tijd doorbrengen met mijn gezin vind ik belangrijk.

Ik kan repetitieve en minder uitdagende taken aan, zolang er een toekomstperspectief is.

Ik kan goed werken in teamverband, hoewel soms ik (te) weinig geduld heb met incompetentie of vooral gebrek aan inzet bij mijn teamleden. Ook met het aansturen van mensen met andere vaardigheden en het totaalpakket van projectbeheer heb ik ervaring. Ik kan duidelijk communiceren, zeker op technisch vlak (hoewel ik niet het talent bezit om boeiende presentaties te geven).

Ik bezit een analytische geest en een goed geheugen waardoor ik over een groot probleemoplossend vermogen beschik. Gecombineerd met mijn diepgaande kennis van computernetwerken en ip-pakketten zijn er zelden mysteries in een netwerk die onverklaard of onopgelost blijven. Daarnast heb ik een brede kennis van vele aanvallende technieken en methodes waarvan ik gebruik maak om gerichte verdedigende security aanpassingen door te voeren en desgewenst de doelmatighed ervan te verhogen door te testen en te tweaken (purple-team testing).

Mijn vele jaren ervaring in verscheidene lagen en vormen van beveiliging, het uitvoeren van onderzoeken en operaties, meedraaien in allerhande incidenten, complexe netwerken beveiligen en het werken in een SOC hebben me een unieke skill-set gegeven die u mogelijk kan interesseren. Indien ik uw organisatie of team van dienst kan zijn, hoor ik dat graag.