Robin Breggeman

Cyber Security Professional

Personalia

Goudsmid 13,
3162XJ, Rhoon

06-18708568

robin@itdutchie.com

08-01-1983

Nederlands

linkedin.com/in/robinbreggeman

Talen

NL	●●●●●
EN	●●●●○

Vaardigheden

Analyses	●●●●○
Incident Response	●●●●○
Threat hunting	●●●○○
Forensics	●●●●○
SOC processen	●●●●○
Rapportages	●●●●○
Security Management	●●●○○

Hobby's

- Familie
- Duur sporten
- Vakantie
- BBQ

Werkervaring

Security Analist

JIO | 2022 – heden

- Diepgaande analyse van security-incidenten op basis van het MITRE ATT&CK-framework.
- Ervaring met diverse securitytools, waaronder SIEM (Sentinel, Elastic), EDR/XDR (Elastic, Carbon Black, Defender for Endpoint), IPS/IDS en proxy logging etc.
- Functioneel beheer Elastic SIEM
- Inrichten en optimaliseren security monitoring, inclusief coaching van SOC-analisten.
- Opzetten en uitvoeren van Incident Response (IR)-processen.
- Implementeren en beheren van kwetsbaarhedenmanagement in de organisatie (Vulnerability management).
- Opstellen van Use Cases op basis van Red Team-bevindingen, Pen Tests en eigen onderzoek naar ontbrekende detectieregels.
- Ondersteuning bij audits en naleving van compliance-richtlijnen.
- Opzetten van assetmanagement binnen het SOC.
- Opstellen van rapportages voor management, operationele teams en klanten.
- Adviseren over SOC-verbeteringen in processen, technologie en strategie.

Senior Security Analist

Dienst Justitiële Inrichtingen (DJI) | 2021 – 2021

- Beheer van de ArcSight-omgeving en optimalisatie van functionaliteiten.
- Opstellen en implementeren van Use Cases binnen het SIEM.
- Monitoren en analyseren van SIEM-alerts voor dreigingsdetectie.
- Incident Response (IR) uitvoeren op gedetecteerde alerts.
- Forensisch onderzoek op tablets bij security-incidenten.
- Opzetten en beheren van Use Case-management binnen het SOC.
- Ontwikkelen van dashboards voor verbeterd inzicht in securitydata.
- Adviseren over SOC-verbeteringen in processen, detectie en responscapaciteit.

Senior Netwerk Security Specialist

Dienst ICT Uitvoering (DICTU) | 2014 – 2020

- Complex SSL Offloading-project: Implementatie van SSL-terminatie voor Digikoppelingen op een F5-apparaat binnen een overheidsomgeving.
- Werkplekprogramma: Netwerk- en securityaanspreekpunt voor de implementatie van een private cloud-werkplek binnen Dictu (EZ), inclusief proxy- en firewallomgeving, F5 load balancing, SSL offloading en routinguitdagingen binnen het datacenter.
- Cyberdefense-project: Technisch aanspreekpunt bij de implementatie van McAfee Cyber Defense-oplossingen, waaronder OpenDXL, ATD en TIE-functionaliteit.
- Kleine/middelgrote projecten: Opstellen en implementeren van LLD's op basis van HLD's, inclusief HLD-reviews op netwerksecurity en fungeren als aanspreekpunt voor network security.
- Beheer en ondersteuning: 3e-lijns aanspreekpunt voor Check Point- en proxy-omgevingen, inclusief troubleshooting en ondersteuning bij complexe issues.

Competenties

- Leergierig
- Communicatief
- Gedreven
- Analytisch
- Flexibel
- Integriteit
- Respectvol
- Sociaal
- Ondernemend

Tools

Elastic SIEM	●●●●○
Elastic Defender	●●●●○
MS Sentinel	●●●○○
MS Defender XDR	●●●○○
Outpost24	●●●○○
Trellix	●●●○○
MS Azure security	●●●○○

Kennisgebieden

- NIS2
- BIO
- NIST
- SOC-CMM
- Mittre Att&ck
- Use Cases
- Preventie technieken
- Detectie technieken
- Cloud (Azure)

Werkervaring

Senior Firewall Specialist

FortyTwo (van Oord)| 2014 – 2015

- Check Point Upgrade & Vervangingsproject: Zelfstandig uitgevoerd project voor de vervanging en upgrade van de wereldwijde Check Point-omgeving binnen Van Oord, zowel remote als op locatie.
- Implementatie van F5 Load Balancer & SSL VPN: Opzetten van een F5-oplossing met SSL VPN, MFA en OTP-server voor veilige toegang.
- Kennisoverdracht Check Point: Training en begeleiding op het gebied van Check Point-producten voor interne teams.

Monitoring Network Security Engineer

Qi ICT | 2011 – 2014

- Troubleshooting in middelgrote tot grote netwerken, inclusief netwerkgerelateerde issues, performanceproblemen, routing- en firewallproblemen.
- Klantcontact: Bespreken van rapportages en bevindingen met klanten.
- Leverancierscontact: Samenwerken met leveranciers bij het oplossen van incidenten en storingen.
- Beheer van security devices, inclusief implementatie van RFC's en incidentoplossing.
- Wereldwijd klantcontact: Conference calls, troubleshooting, migraties en doorvoeren van wijzigingen.

Opleiding

2019	**2019**	Certified Information System Security Professional (CISSP) – ISC2	Certificaat
2001	**2009**	HRO University, Rotterdam Higher Informatics (Bachelor of Information Communication Technologie (B-ICT)	Diploma

Certificering

2025	Kaspersky: Targeted Malware Reverse Engineering	Studie
2025	Kaspersky: Reverse Engineering 101	Certificaat
2024	Micorosft SC-200: Security Operations Analyst Associate	Certificaat
2024	Security Bleu Team BTL1 & BTL2 training en Praktijk examen	Certificaat BTL1 Certificaat BTL2
2023	Elastic Certified Engineer	Certificaat
2023	Elastic Certified Analist	Certificaat
2021	ArcSight ESM 73 Administrator and Analyst Certified Professional	Certificaat
2021	Certified SOC Analyst (CSA) – EC Council	Certificaat
2020	Computer Hacking Forensic Investigator (CHFI) - EC Council	Certificaat
2020	Certified Cloud System Professional (CCSP) - ISC2	Studie
2018	Check Point – CCSA – CCSE R80.10	Certificaat CCSA Certificaat CCSE
2018	Certified Ethical Hacker (CEH) - EC Council	Certificaat