Robin Breggeman

Cyber Security Professional

Personalia

Goudsmid 13,
3162XJ, Rhoon

06-18708568

robin@itdutchie.com

08-01-1983

Nederlands

linkedin.com/in/robinbreggeman

Language

NL	●●●●●
EN	●●●●○

Skills

Analyses	●●●●○
Incident Response	●●●●○
Threat hunting	●●●○○
Forensics	●●●●○
SOC processes	●●●●○
Reports	●●●●○
Security Management	●●●○○

Hobby's

- Familie
- Duur sporten
- Vakantie
- BBQ

Werkervaring

Justitiële ICT Organisatie (JIO)

Bedrijf | 2022 – heden

- Analysing alerts and security incidents (2 line)
- Writing rules / use cases / fine tuning in in the SIEM (elastic)
- Writing processes and workflows for the SOC analists 1, 2 and 3 line.
- Writing Incident response for in the SOC
- Writing processes and procedures for vulnerability management and coordinate in the organisation for operation
- Support by audits
- Building basic asset management
- Building reports for Management / Customers / Operations
- Advising improvements inside the SOC

Dienst Justitiele Inrichtingen (DJI)

Bedrijf | 2021 – 2021

- Managing ArcSight environment
- Writing Use Cases and implement them in the SIEM
- Monitoring alerts generated by the SIEM
- Incident response
- Forensisch research on tablets
- Building Use Case management
- Building dashboards for more insight in the environment
- Advising improvements inside the SOC

Dienst ICT Uitvoering (DICTU)

Bedrijf | 2014 – 2020

- Complex SSL offloading project: Termination SSL negotiation for digikoppelingen (Communicatie method between governments) on an F5.
- Complex werkplace program: From Networking and Security side point of contact and executive project member for a new private Cloud workplace inside Dictu (EZ). Consulting and review netwerksecurity implementations. Including implementation of proxy environment, firewalls and F5 loadbalancing virtual system with SSL offloading. Solving routing challenges inside datacenter.
- Cyberdefense project: Technical consultant, for the installation off McAfee cyberdefense solution. (OpenDXL oplossing met ATD en TIE functionalitie).
- Small and medium projects: Writing and implementing LLD n.a.v. HLD. HLD reviewen. Aanspreek punt op gebied van network (security), adviseren op gebied van security vraagstukken bij projecten.
- Administrator: Point of contact, 3e line administrator for the Firewall (CheckPoint) proxy (McAfee) environments, troubleshooting issues

Competence

- Eager to learn
- Communicative
- Driven
- Analytical
- Flexibel
- Integrity
- Respectful
- Social
- Enterprising

Tools

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

Knowledge areas

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

Werkervaring

FortyTwo (van Oord)

Bedrijf | 2014 – 2015

- Project, executed alone, upgrading the CheckPoint firewall environment for Van Oord. Locations worldwide, replacing the hardware and upgrading the software remote or onside.
- Implementating F5 loadbalancer SSL VPN with MFA, OTP server.
- Sharing knowledge about CheckPoint to the administrators

Qi ICT

Bedrijf | 2011 – 2014

- Troubleshooting, medium to large networks, network related issues, performance, routing issues, firewall issues etc;
- Customer contact: Rapportage besprekingen;
- Suppliers contact: Solving incidents with supplier support;
- Administration security devices;
- Worldwide customer contact: conference calls, troubleshooting, migrations, performing changes in the production environment;
- Installations;

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
1996	**2001**	HAVO, Bahurium (Brielle) & Jacob van Liesveld (Hellevoetsluis)	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
2021	Certified Information Security Manager (CISM)	Studie
2020	Computer Hacking Forensic Investigator (CHFI) - EC Council	Certificaat
2020	Certified Cloud System Professional (CCSP) - ISC2	Studie
2018	Certified Ethical Hacker (CEH) - EC Council	Certificaat