Allan van Leeuwen

SOC TEAMLEADER

Personalia

Gerard Reijnststraat 64A
2593ED, Den Haag
0628026870
wateraxe@gmail.com

Links

LinkedIn

SecutiryTalks Podcast

Vaardigheden

People Management

Coaching

SIEM

Vulnerability Management

Pentesting

Malware Analysis

Forensic investigations

Windows Operating System

Linux Operating System

Profiel

Sterke people manager die structuur en team verband kan aanbrengen of verbeteren. Het begeleiden, motiveren, coachen en stimuleren van werknemers is waar ik energie uit haal. Met een lange achtergrond in de security sector breng ik de kennis en ervaring die nodig is om een SOC naar het volgende niveau van volwassenheid te brengen.

Werkervaring

Teamlead SOC, KPN B.V., Nederland

FEBRUARI 2024 — HEDEN

Door het implementeren van het SOC-CMM framework heb ik een strategische roadmap ontwikkeld die leidde tot meetbare groei in security maturity. Ik transformeerde de afdeling tot een hecht en effectief team dat proactief inspeelde op veranderende dreigingen. Op basis van klantfeedback heb ik gerichte verbeteringen aan de dienstverlening doorgevoerd, wat resulteerde in verhoogde klanttevredenheid en een versterkte marktpositie voor KPN's security-oplossingen. Ook heb ik innovatieve educatieve tools specifiek gericht op red teaming ontwikkeld, die binnen de organisatie breed zijn toegepast.

SOC Manager, Nomios, Zoeterwoude

DECEMBER 2022 — DECEMBER 2024

Groeide het SOC-team van 3 naar 6 professionals voor betere servicedekking en efficiëntie. Verzorgde klant-onboarding met maatwerk beveiligingsoplossingen. Ontwikkelde en verkocht nieuwe Vulnerability Management diensten, wat bijdroeg aan omzetgroei. Stuurde dagelijkse SOC-operaties aan inclusief incidentrespons en dreigingsanalyse. Implementeerde trainingen en evaluaties ter bevordering van continue professionele ontwikkeling in het team.

Teamlead SOC, Motiv ICT Security, IJsselstein

NOVEMBER 2017 — NOVEMBER 2022

Transformeerde het Security Operations Center van 5 naar 50 medewerkers in 5 jaar tijd als eindverantwoordelijke voor operations en personeel. Optimaliseerde alert management door structurele implementatie van MAGMA en SOC-CMM frameworks en methodieken. Begeleidde teamleden in hun vakinhoudelijke training en persoonlijke ontwikkeling. Onderhield nauwe contacten met klanten en leveranciers om de security monitoring dienstverlening continu te verbeteren en af te stemmen op nieuwe dreigingen en technologische ontwikkelingen.

Security Officer, ABN-AMRO, Amsterdam

JANUARI 2017 — SEPTEMBER 2017

Leidde als SCRUM master het use case development team binnen het SOC van ABN-AMRO. Stuurde de ontwikkeling van geavanceerde use cases voor ArcSight en Q-Radar platformen aan. Coördineerde een deels extern development team in India voor effectieve oplevering. Ontwikkelde specialistische IDS signatures voor Sourcefire ter ondersteuning van Tiber red team exercities, wat bijdroeg aan verbeterde detectie van gesimuleerde aanvallen en verhoogde weerbaarheid.

Security Analist, Aramco, Den Haag

JULI 2013 — DECEMBER 2016

Verantwoordelijk voor de continue monitoring van Aramco's wereldwijde netwerk. Taken omvatten proxy server- en antivirusbeheer, implementatie van SIEM-platforms, ontwikkeling van relevante use cases, verwerking van threat intelligence en uitvoering van threat hunting activiteiten. Ontwikkelde daarnaast eigen security tools en oplossingen voor effectieve malware-analyse en forensische onderzoeken, wat bijdroeg aan de versterking van het beveiligingslandschap.

Technical Security Specialist, T-Mobile Nederland, Den Haag

APRIL 2003 — JUNI 2013

Verantwoordelijk voor algehele informatie beveiliging T-Mobile Nederland. Project risico beoordelingen, vulnerability management, implementatie PKI infrastructuur, 2g/3g/4g security, internal investigations (forensische onderzoeken), malware analyse en preventie.

Systeembeheerder & 3e lijns support, Orange Nederland, Den Haag

APRIL 2001 — APRIL 2003

Verantwoordelijk voor het beheer van Active Directory en 3e lijns escalatie punt. Controle op beveiligings dreigingen / notificaties en ontwikkeling van security tools.

Intranet Server Beheerder, AEGON Nederland, Den Haag

JULI 2000 — MEI 2019

Ondersteunen van web ontwikkelaars op 200+ intranet websites. Installatie en onderhoud van web servers, backups en beschikbaarheids monitoring.

Internet server beheerder, HBG, Rijswijk

OKTOBER 1999 — JUNI 2000

Technische implementatie en beheer van nieuwe E-commerce web servers. Beheer en monitoring van (interne en externe) DNS en firewall configuraties.

Systeem beheerder, KPN Telecom, Den Haag

JULI 1998 — SEPTEMBER 1999

Opleiding

Excellent Leiderschap, Nyenrode Business University, Breukelen

JANUARI 2025 — JUNI 2025

Leidinggeven aan professionals, Schouten Nelissen, Remote

DECEMBER 2021 — JANUARI 2022

MCSA Windows 2012 r2, Firebrand

2015

Practical Malware Analysis, Brucon training, Gent

2014

Bluecoat administration, Global Knowledge, Zoetermeer

2013

Splunk 5, SMT, Zoetermeer

2012

Certfied Ethical Hacker, EC Council

2012

CISSP, ISC2

2010

Qualysguard certified specialist, Qualys, Zoetermeer

2009

SANS508 Digital forensics, SANS, Praag

2008

MCSE Windows 2000, Global Knowledge

2004

MCSE NT4 + Internet, Global Knowledge, Zoetermeer

1999

ITIL essentials, EXIN, Den Haag

1998

Medewerker Beheer Informatiesystemen, ROC Voorburg, Voorburg

1995