# Allan van Leeuwen

SOC TEAMLEAD

## 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

Strong people manager who can establish or improve structure and team cohesion. Guiding, motivating, coaching, and encouraging employees is what energizes me. With an extensive background in the security sector, I bring the knowledge and experience needed to take a SOC (Security Operations Center) to the next level of maturity.

## Werkervaring

### Teamlead SOC, KPN B.V., Nederland

FEBRUARI 2024 — HEDEN

By implementing the SOC-CMM framework, I developed a strategic roadmap that led to measurable growth in security maturity. I transformed the department into a cohesive and effective team that proactively responded to evolving threats. Based on customer feedback, I implemented targeted improvements to service delivery, resulting in increased customer satisfaction and a strengthened market position for KPN's security solutions. I also developed innovative educational tools specifically focused on red teaming, which have been widely applied throughout the organization.

### SOC Manager, Nomios, Zoeterwoude

DECEMBER 2022 — DECEMBER 2023

Grew the SOC team from 3 to 6 professionals to improve service coverage and efficiency. Managed customer onboarding with customized security solutions. Developed and sold new Vulnerability Management services, contributing to revenue growth. Directed daily SOC operations including incident response and threat analysis. Implemented training and evaluations to promote continuous professional development within the team.

### Teamlead SOC, Motiv ICT Security, IJsselstein

NOVEMBER 2017 — NOVEMBER 2022

Transformed the Security Operations Center from 5 to 50 employees over a 5-year period as the final responsible party for operations and personnel. Optimized alert management through structural implementation of MAGMA and SOC-CMM frameworks and methodologies. Guided team members in their professional training and personal development. Maintained close contacts with customers and suppliers to continuously improve security monitoring services and adapt to new threats and technological developments.

### Security Officer, ABN-AMRO, Amsterdam

JANUARI 2017 — SEPTEMBER 2017

Led the use case development team within ABN-AMRO's SOC as SCRUM master. Directed the development of advanced use cases for ArcSight and Q-Radar platforms. Coordinated a partially external development team in India for effective delivery. Developed specialized IDS signatures for Sourcefire to support Tiber red team exercises, which contributed to improved detection of simulated attacks and increased resilience.

### Security Analist, Aramco, Den Haag

JULI 2013 — DECEMBER 2016

Responsible for the continuous monitoring of Aramco's global network. Duties included proxy server and antivirus management, implementation of SIEM platforms, development of relevant use cases, processing of threat intelligence, and execution of threat hunting activities. Additionally developed custom security tools and solutions for effective malware analysis and forensic investigations, which contributed to strengthening the security landscape.

### Technical Security Specialist, T-Mobile Nederland, Den Haag

APRIL 2003 — JUNI 2013

Responsible for overall information security at T-Mobile Netherlands. Managed project risk assessments and vulnerability management processes across the organization. Implemented and maintained PKI infrastructure to enable secure communications. Oversaw security for 2G/3G/4G telecommunications networks, protecting critical infrastructure and customer data. Conducted internal investigations using forensic techniques to identify and resolve security incidents. Performed detailed malware analysis and developed custom tools for this purpose.

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

APRIL 2001 — APRIL 2003

Responsible for Active Directory management and 3rd line escalation point. Monitored security threat feeds and developed forensic security tools.

### Intranet Server Beheerder, AEGON Nederland, Den Haag

JULI 2000 — MEI 2019

Supporting web developers on 200+ intranet websites. Installation and maintenance of web servers, backups and availability monitoring.

### Internet server beheerder, HBG, Rijswijk

OKTOBER 1999 — JUNI 2000

Technical implementation and management of new E-commerce web servers. Management and monitoring of (internal and external) DNS and firewall configurations.

### 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