

Mattijs Roozeboom

Security /platform / SRE Engineer

CONTACT

Address

Area of Eindhoven

Email

jobs@mattijs.sh

LinkedIn

<https://www.linkedin.com/in/mattijs-r-95140516/>

Languages

Dutch: Native, English: IELTS 9/10

EDUCATION

Avans Hogeschool of Applied Sciences (HBO), Breda

OSCP, OSED, CKA, CKAD, AZ-900, AZ-500, AZ-204, AZ-400, Amazon Cloud Partitioner, AWS Developer Associate, AWS Sysops Administrator Associate, Amazon DevOps Engineer Professional, AWS Security Speciality

Red Team Ops II – Zero Point Security

WWHF Offensive Development
Getting taught how to evade about every AV/EDR solution on the planet

Defcon 22 and 25

Kaspersky, Targeted Malware Reverse Engineering

Sektor7 – Malware development Essentials, Intermediate, Advanced and Advanced 2

Sektor7 – Red Team Operator Windows evasion course

Sektor7 – Privilege Escalation in Windows

Sektor7 – Windows Persistence Course

PROFILE

As an engineer with an intrinsic interest in ethical hacking and reverse engineering I aim to find and solve the more esoteric problems, so the team doesn't have to.

The Dev(Sec)Ops way of working is considered standard operating procedure, yet I strive to improve upon that way of working every day.

I function best in a technical leading and/or pioneering role within a highly technical context.

But I don't shy away from communicating pragmatically with people from other disciplines or departments.

Summarized: Give me the problem no-one else can solve.

IDEAL ASSIGNMENT

I flourish in an environment where I'm not a permanent member of the team but can still help and support the team. If the only reason to go to the office is to strengthen the team spirit, I'm not the right guy.

All I'm looking for is a proper challenge, which we'll discuss before we start the assignment.

**Bright Cubes: Sr platform engineer
ASML**

10/2024 – 5/2025

Hired to develop a platform that automates most of the Azure cloud in such a way, to have the desired infrastructure in a couple of clicks instead of needing a lot of technical knowledge.

Worked with: Terraform, Azure, ArgoCD, Git, Powershell

Bright Cubes 12/2023 – 9/2024

Internal project in Bright Cubes

**Bright Cubes: Sr platform engineer
Enexis**

12/2022 – 12/2023

Hired for my Kubernetes, security, CI/CD and networking knowledge as a Platform Engineer, reduced the steps required to accommodate the automation to Argo CD. In combination with running Kubernetes on 2 separate physical locations, including all hardware, software and networking related challenges that encompass it.

Worked with: Ansible, Kubernetes, Azure Pipelines, Docker, ARM Templates, Artifactory, Git, DevOps, Prometheus, Powershell, RabbitMQ, Grafana, Active Directory, AlmaLinux & Hardening

**Bright Cubes: Sr. platform engineer
SSC ICT**

7/2022 – 11/2022

In charge of converting specialized IBM software in a docker-compose, to a Kubernetes cluster. In my first 2 weeks, onboarded and got the application's status page working in an infrastructure and platform that was setup with policies which invited creative solutions.

Worked with: Openshift, Helm, Kubernetes, Gitlab, Harbor, Gitlab Runners, Docker, CI/CD, Git, Nexus.

**Bright Cubes: Sr Platform Engineer
De Volksbank**

11/2021 – 6/2022

We were a small number of external consultants who innovated the way of working. We were very far ahead of the rest of the company, and we provided the blueprints and were the tech leads of this innovation strain.

Worked with: Terraform, Ansible, Jira/confluence/bitbucket, Kubernetes, Grafana, Docker, Python scripting, Git, Artifactory, AWS, Git Flow (& alternatives), Groovy, NodeJS, Helm, ArgoCD, Jenkins2, XLDeploy, XLRelease, Route53, IAM, Kustomize, Amazon EC2, Container Service, Amazon RDS, Amazon Cloudfront, IaC

ACC ICT: Sr. DevOps Engineer

8/2020 – 7/2021

A position where I solved highly technical and specialized problems. This was during the corona lockdown. Used my development knowledge to solve problems of colleagues more quickly. These were co-engineers out of other specializations such as networking, firewalls or storage.

After 6 months, the CEO wanted me as tech-lead.

Being on call for periods of time was a part of this position.

Worked with: Terraform, Ansible, Azure Devops, Bitbucket pipelines, Kubernetes, VMWare, Graylog, Prometheus, Grafana, Metallb, NFS, Docker, Spring Boot, Bash/perl scripting, Jenkins, Git, FortiGate, File/journalbeat. Atlassian products, AWS, Gitlab, ARM Templates (IaC), Go, Bash.

Linprofs: Engineer

5/2020 - 7/2020

To quickly add more value in this lateral move I used my Scrum/Agile knowledge and experience to structure the company's processes to increase predictability of the company. This was done by coaching both management and engineers in the methodologies of this process.

SIEM, CentOS, Ubuntu, IDS, APT's (Advanced Persistent Threats), Graylog, Grafana, Prometheus, threat identification sourcing, ELK stack, webhosting, Jira, Ansible, Terraform (IaC)

Opinity: Java Developer
11/2019 - 4/2020

Created a proof of concept in Google Cloud with Kubernetes, that moved a .NET project into that new landscape. This removed the need for 3 FTE's of technicians.

Worked with: Google Cloud, VueJS, Kubernetes, Azure DevOps, .NET, Docker, Powershell, Bash.

PharmaPartners: Java Developer / DevOps engineer
3/2019 - 10/2019

Java backend development, part of the security group and made 2 proof of concepts: dockerized COBOL, and a proof of concept which translated COBOL to native JVM. This removed the need for 5 out of 15 technicians.

Worked with: Gradle, Artifactory, Spring Boot, Maven, RPM Building, OWASP Checker, Pitest, Java 8+, Jenkins 1, Jenkins 2 pipelines, SonarQube, Jacoco, RTC, Git, Ant, Docker, Protobuf, SOAP, COBOL

Madlogic B.V.: Sr. Java developer / Sr. DevOps engineer
8/2016 – 2/2019

Responsible for planning and road mapping in collaboration with the product owner / tech lead within a start-up.

My responsibilities were the back end system, architecture and infrastructure and translating this to management. This laid the groundwork for the entire company and sped up internal processes and made sure SLA's were met and exceeded for the next 5 years.

Worked with: Vaadin, Spring Boot, Jenkins, SonarQube, Keycloak, IDS, Azure, Amazon EC2, Python, Java, Git, MySQL, Gradle, Docker, OAuth, Nexus, ADF
Matomo, Java EE, NoSQL, IntelliJ, RabbitMQ, PKI, Firebase, Amazon SNS. Ansible, ARM Templates (IaC)

Docdata: PHP developer / DevOps engineer
2/2014 – 7/2016

Solved business critical security issues on production systems. Vastly improved the core functionality of the platform by using a solution that was 350% easier to automate. Introduced the CI/CD concepts and offered my linux knowledge to colleagues. This ranged from simple questions to production issues, and everything in between. After 2.5 years, I removed the need for 10 out of 20 technicians working there.

Made a proof of concept in ANTLR to show we could standardize/leverage existing techniques instead of building our own small language for specific ESB routing needs. This removed the need for 1 out of the 2 Java employees working there.

Worked with: ELK Stack, PHP, Jenkins, Git, SonarQube, MySQL, Symfony2, Twig, PHPUnit, LaTeX, XML, Java EE, JSON, IntelliJ, Eclipse, PHPStorm, SOAP, XSD, Centos & Ubuntu, Memcached, Redis. PKI, Camel, Started with IaC

Personal Java compiler
2014-2015

Pascal code translation to native JVM code. A precursor to the ANTLR project in the Docdata project above.

Various websites 2008-2014

Made 15+ websites with all known frameworks mentioned below in the technical knowledge page, 10+ of them had CMS's as well.

TECHNICAL KNOWLEDGE

Automation

Jenkins, Jenkins2, Bamboo, Ansible, Terraform, Artifactory, Nexus, Helm, Camel, RabbitMQ, Harbor, kind, XLSRelease, XLSDeploy, Argo CD, Kustomize, IaC (Infrastructure as Code), Pitest, Jacoco, SonarQube, Quarkus.io, ActiveMQ, DTQ, Apache Kafka,

Programming languages

PHP, Java, Go, Perl, Basic C/C++, COBOL, Assembly, Ruby, Python, PowerShell, R, Bash, Groovy, NodeJS, Spring Boot, lex, yacc, Jess, VueJS, reverse engineering and more.

Can teach myself a new programming language in a week or two. Or create one with ANTLR.

Standards

JSON, XSD, LaTeX, Git, Active Directory, Windows Internals (how the operating system functions at the most basic level), MacOS and related, Git flow, NFS, Ant, Vaadin, Protobuf, SOAP, NoSQL, OAuth, ADFS, Swagger.io, FastAPI

Monitoring

ELK Stack, Prometheus, Graylog, Journalbeat, Filebeat, matomo, New Relic, Datadog, Zabbix, Nagios, Splunk

Documentation

If there's no documentation of it, it does not exist.

Cloud related

Kubernetes, OpenShift, OpenStack, Docker, Gitlab, Gitlab Runners, Bitbucket, most minor clouds, Jira, confluence, Metallb, Istio, Kubespray, Kops, Rancher, On-premises clouds

Azure, GCP, Amazon

ARM Templates, Microsoft Sentinel, Azure Key vault, Azure blob storage, Microsoft EntraID, Network Security Groups, Azure VPN Gateway, Web application firewall, Azure Load balancer, Azure ExpressRoute, Azure Traffic Manager, Azure DDoS protection, Azure Bastion, Route53, Amazon RDS, Amazon CloudFront, Amazon SNS, Amazon Cloudwatch, and basically the entire cloud service.

Linux

Most distributions including Alma Linux, CentOS, Ubuntu, Arch. Alpine Linux, Gentoo, LFS and keeping it all as light as possible is the goal.

Databases

MySQL, PostgreSQL, Oracle, SQLite, Microsoft SQL Server, Amazon RDS, CouchDB, MongoDB, Azure Cosmos DB, Neo4j, memgraph, Elastic, Solr, Redis, Memcached, Amazon DynamoDB, Apache Cassandra, GraphQL, Hibernate

Security related

Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS's), ASLR evasion, IAM, Exploit Development, Malware development, SIEM, RPM Building OWASP Checker, Lynis, KeyCloak, PKI, Advanced Persistent Threat's (APT's), Memory Forensics, Linux forensics, Binary analysis, Device Driver development.

Windows development

Windows Kernel development, Advanced Windows Debugging, Malware analysis, Shellcode development, Windows Forensics, Compiler Development, Windows Forensics

Virtual machines

VirtualBox, VMWare, Hyper-V, Qemu, KVM, ESXi, Proxmox, Unraid

Networking

FortiGate, Ubiquity, BGP, Metallb, Istio, Calico and others.

Storage

ZFS, Ceph, IPFS, all cloud storage solutions, ext4, ext3, fat32, NTFS, DAS, NAS, RAID configurations, OrientDB

PHP and Python frameworks

CodeIgniter, WordPress, Drupal, Zend Framework, PHPUnit, Twig, Symfony2, CakePHP, Laravel, FuelPHP, OWASP Scanners, Lynis, Joomla, Silverstripe CMS, Yii Framework, Flask, Django

Java frameworks

Hadoop, Kafka, Solr, , Spark, Storm, , Struts, Tomcat, (Camel), Zookeeper, EclipseLink, Gson, Mockito, Netty, Weblogic, Play, Quarkus.io, Selenium, Thymeleaf

Mobile

Basic android development can teach myself iPhone development in a couple of weeks.