Sebastian Fischer

+45 29 22 91 75
sebastianfischerdk@outlook.com
sefischery
sebastian-fischer

Work experience

Present **Cybersecurity Consultant (DART)**, ***Microsoft***, part of the "Detection And Response Team" operating in both reactive and proactive settings. Threat hunting and Incident response operations using a data science based approach with "KQL", in relation to hunting for threat actors in an environment (cloud/on-prem), while combining proactive services. This entails operating in highly stressed environments, needing to be operate quickly and handle people in crisis. Additionally, was responsible for helping with on-boarding of new employees acting as a buddy and guider..

2021-2022 **Security Customer Engineer**, ***Microsoft***, advising, guiding and implementing with customer security teams with defending their infrastructure and securing their organization through Microsoft technologies both on-prem, multi-cloud, and Azure native. Focus on building, structuring and architecting PoCs and coordinating with teams to implement and create working solutions within multiple security domains, examples including IAM, Azure security components, DevOps, containers, threat, and vulnerability management, GRC, EDR/AV deployments, SIEM etc. Also focus on presentations, stakeholder management and presenting to higher level stakeholders to illustrate value.

2020-2021 **Software Developer**, ***Lars Thrane***, engaged with an agile team of developers, building various tools in relation to maritime global emergency systems, thereby being exposed to a wide set of tools, techniques, and experiences. Directly involved with the development of multiple automation tools, with the major objective of decreasing and optimizing production flow thereby increasing output performance. This was done in order to remove a large set of tasks that were typically done manually and physically by dedicated FTEs. Assisted in the further growth and maturing of varying unit tests with the main purpose of ensuring code coverage and proper function of software as well as physical hardware (Device under testing, etc.) Also developed scripts to automate encryption and protection of production code on custom linux distros. Mainly programmed in Python and C, in combination Docker, Jenkins and similar tools .

2018-2020 **Jr. Consultant**, ***Deloitte***, *Cyber Secure*.
Tasks include running and maintaining an external scanning server for audits of clients' security (webapps, firewalls, etc.) and writing reports in regards to vulnerabilities present as well as writing various scripts to confirm these vulnerabilities with Python, metasploit, Kali Linux related tools, Nessus etc.

Education

- **MSc. Computer Science & Engineering**, *Technical University of Denmark*.
- **BSc. Network Technologies and IT**, *Technical University of Denmark*.

Research & Projects

2021 **IoT end-to-end security**, *MSc. Thesis*, developed an entire setup of end-to-end PoC solutions with IoT devices employing various protocols (NB-IoT, Sigfox, WiFi, BLE, MQTT) to communicate with a custom-built server hosted on an Azure VM. This was with the objective of using high-performance authenticated encryption algorithms to provide E2E confidentiality of the transmitted payload (data). Furthermore, a performance evaluation was done in order to conclude which cryptographic algorithm was most fitting in terms of processing power of the microcontrollers' CPU.

2020 **Occupancy Counting System For Auditoriums Using IoT based WiFi Sniffer**, *DTU*, Implemented a WiFi frame sniffer in C, able to scan 2.4GHz/5GHz spectrum and extract MAC addresses from frames to attach MAC addresses originating from devices to keep count of people in a room/auditorium. The source code was implemented on embedded systems which meant major complexity in regards to a single core needing to both observe frames and interpret.

2020 **Gate Counter - Raspberry Pi**, *Roskilde Festival & DTU*, project where we developed a Raspberry Pi solution with a camera which is able to count people going in and out of a gate based on recognizing people with machine learning. Sadly, cancelled due to COVID.

2019 **Security Aspects of IoT**, *BSc. Thesis*, implemented a C version of a hybrid cryptosystem using AES and RSA in Arduino based platforms in regards to power management, CPU usage, etc. Furthermore, a Deauthentication attack was implemented in Python to test its effect on WiFi IoT based solutions and its effectiveness as well as various forms of DoS attacks (TCP SYN, ICMP, UDP floods).

General Technical Skills

Programming

Python	3 Years of Exp.
C	2 Years of Exp.
KQL	1 Year of Exp.
PowerShell	1 Year of Exp.
Java	1 Year of Exp.

Technical Experience

TCP,UDP,IP,802.11,etc.
Docker, Virtualization
IAM
ISO, CVSS, NIST
CI/CD pipelines
Agile Methodologies
IoT, embedded SW
M365, Azure, Azure AD
Defender for Cloud
Defender for Endpoint
Defender for Office
Defender for Identity
Microsoft Sentinel
Azure operations, VMs, Docker, etc.

Certifications

Microsoft Azure Administrator (AZ-104), Azure Security Engineer (AZ-500), Security Operations Analyst Associate (SC-200), AZ-900, SC-900, MS-900, AI-900