

„There are 10 types of people in the world  
- those who understand binary, and those who don't.”



# DARIUSZ SOCHA

## MY COMPANY

SOCHA.mt LTD  
Buforowa 99a/13  
52-131 Wrocław, Poland

## CONTACT

Malta: +356 99 068 505  
Poland: +48 515 490 505  
dariusz@socha.mt ; www.socha.mt



I consent to the processing of all personal data required for recruitment purposes.

## CURRICULUM VITAE

BORN 1985

### it experience (just a brief - details on 2nd page)

- |                     |   |
|---------------------|---|
| 12.2023-<br>current | <b>SOC SIEM Expert</b> - full remote preferred from UE<br>- Cyber Security Consulting SOCHA.mt LTD                                    |
| 10.2022-<br>11.2023 | <b>Senior SIEM Splunk Architect / SOC Solution Architect</b><br>- National Research Institute (NASK PiB) Poland,<br>Warsaw.           |
| 05.2017-<br>09.2022 | <b>Senior IT Security Specialist - SOC SIEM Expert<br/>Dedicated Analyst / L2 and Principle SIEM Mentor</b><br>- IBM Poland, Wrocław. |
| 04.2016-<br>04.2017 | <b>IT Security Specialist - SOC SIEM L1 Analyst</b><br>- IBM GSDC, Wrocław.   |
| 03.2015-<br>03.2016 | <b>Senior Frontend Developer / UX Designer</b><br>- Britenet, Lublin.   |
| 01.2012-<br>02.2015 | <b>Founder of Software House - Frontend Developer</b><br>- SochaCreate.com, Swidnik.  |
| 06.2011-<br>12.2011 | <b>IT Service Desk 2<sup>nd</sup> line / SharePoint Administrator</b><br>- IT department „Polkomtel S.A.”, Warsaw.                    |

### Education

- |           |   |
|-----------|---|
| 2005-2011 | <b>The College of Enterprise and Administration</b><br>In Lublin, Poland ( <a href="http://www.wspa.pl">www.wspa.pl</a> ).<br><br>Specialization: <b>IT / computer networks</b> |
| 2000-2005 | <b>Technical School in Świdnik, Poland</b><br>- title of „technician-mechanic”  |

### SOC SIEM Expert

I have spent 2016-2022 as a Senior SIEM Analyst (Qradar) working for IBM X-Force Command Cyber Tactical Operations Center, analyzing network traffic and detecting potential attacks on the customer's infrastructure, mainly to biggest corporation and banks from the USA and Canada - being at the same time the best trainer of SIEM Analysts in IBM Poland. Recently, from the end of 2022 I was working for the National Research Institute (NASK PiB), implementing IT security projects and creating a new SOC (Security Operation Center) for government as a Senior Cybersecurity Solution Architect. Currently, I work as a B2B contractor in the SOC/SIEM area as part of my company SOCHA.mt LTD. (EU-NIP PL8992982765).

### Skills

(c) Dariusz Socha. All Rights Reserved (not apply to the recruitment process).

- SIEM tools** - IBM QRadar, Splunk, Service Now, CMDB + Qualys.
- EDR tools** - CrowdStrike, Symantec, McAfee, Kaspersky.
- Cyber Security** - IoT, IoC, CVE, Mitre Att&ck, SOAR, AI, SIEM, EDR.
- Networks (courses)** - Cisco CCNA, CompTIA Security+ & Network+.
- Others (cyber)** - Network Intrusion Detection and Protection (**NIDS**, **NIPS**), Full Packet Capture (**FPC**), Online Computer Forensics (**OCF**), Cyber Operations Management Service (**COMS**), Standalone Computer Forensics (**SCF**) / Forensic Evidence Management Service (**FEMS**), Cyber Defence Situational Awareness (**CDSA**).

### General skills:

- **Polish** - native speaker
- **English** - fluent (C1)
- **Creativity**
- **Excellent soft skills**

By conducting training, I show how simple the topic is, instead of how smart I am - much better approach. I am an enthusiast of a human approach and treating people with respect (*especially if they are in lower positions*).

## SOC SIEM experience details

<p>SIEM Analyst L1 2016-2017</p> <p>IBM</p>	<p>I had a great mentor thanks to whom I understood that an analyst is like a book reviewer, but instead of a book, we have logs that we have to summarize in a short form as a ticket. We also don't have a crystal ball, so we have to rely only on logs plus special instructions and this is where my adventure with triage begins. BTW this should be a melody for AI (SOAR), programmable playbooks + human checkers.</p>
<p>Senior SIEM Analyst L2 2017-2019</p> <p>IBM</p>	<p>Deep dive into forensic and understanding correlation rules. Performing multiple assigned technical tasks including monitoring and performing event analysis. Tracking and analyzing malware attacks, network scans and intrusion attempts. Performing root cause of security events. Reporting findings to customer for resolution using SIEM and EDR as well, fixing the vulnerabilities and protecting the organization. Experience in creating and fixing procedures. Also I see here place for AI (Integration CMDB + Qualys).</p>
<p>Senior SIEM Dedicated Analyst 2019-2022</p> <p>IBM</p>	<p>Sometimes called L3 or Threat Hunter. It's not just weekly conversations with the client. When you check the AV logs in the morning and see the not removed infection without any sign of an alert into console it means that the correlation rule has gaps and this is only one of multiple job for a dedicated analyst which means conscious as much as possible.</p>
<p>Principle SIEM Mentor (2016-2022)</p> <p>IBM</p>	<p>I trained 20 analysts of different nationalities over 7 years - sometimes they were people from outside the IT world at all and they did great. My students achieved the best results, which made me the best mentor of IBM Poland (according to findings of my two managers). Often in the case of problems with the analyst, I served as a special weapon, i.e. if everything failed, additional training with me had to help and always did. I understood that the way I teach is much more important than what I teach, so during the course I show you calmly how simple it is instead of how smart I am.</p>
<p>SIEM SPLUNK Architect 2022-2023</p> <p>NASK</p>	<p>Project (documentation) and execution of implemented Splunk from the scratch to an existing S46 government project (described in the Act on the National Cybersecurity System of Poland), starting with the selection of SIEM, licensing, Splunk on premise architecture, planning hardware resources, ending with the installation in a distributed architecture and initial configuration of Splunk.</p>
<p>SOC Solution Architect 2023</p> <p>NASK</p>	<p>Building a SOC from scratch was my dream since I started my first role in SOC like a SIEM Analyst. I am very grateful to NASK PiB for the opportunity to design SOC according to the European NIS2 directive in accordance with ISO 27001 and SOC2 as a new solution. In short - people, processes, tools. I also had the pleasure of helping in the process of creating NOC as the foundation of each SOC.</p>

This is my 8th year working at CyberSecurity. Each different role introduces something new, so I don't want to limit myself to my previous experience. I know that I consistently want to further develop towards CyberSecurity, especially SOC and SIEM.

# Quick but honest **Motivation Letter**

Hi! At the beginning of 2024, I decided to realize my dream and live „on vacation”, so that's why I am in the process of moving from Poland to Malta right now, to sunny paradise where it is warm all year round so I can ride all over the island in shorts on a scooter which is just awesome! 😊 Work? Remotely, occasionally flying out to meet client and to the office - a flight from Malta to Poland takes just under 3 hours, similar to other EU countries, while also running the polish company SOCHA.mt LTD. I prefer fully remote work for UE countries, but I'm also open to hybrid approach within Malta. Generally, I'm looking for a B2B contract (tax optimization) in the Cyber Security area, especially SOC/SIEM, due to my last 8 years of experience like an SIEM Analyst and SOC Architect.



## **C1 level of English** Metropolitan School Certificate




## TESTIMONIALS from three of my recent students at IBM



**Samela Bajraktari** · 1st

IT Security Consultant at TWINSOFT GmbH & Co. KG

January 31, 2021, Samela worked with  Dariusz on the same team

 All LinkedIn members

It has been a big pleasure for me to have had Dariusz as my mentor at IBM to introduce me to the role of SIEM analyst. Except from always having a very professional attitude, he is a very motivating person who tries to bring out the best in people. Dariusz has very good communication skills, which avoid the pressure of being a newcomer. He is very dedicated to work and always looking for solution in every problem. What I mostly appreciate is his human sense in treating others and also in cyber analysis. It was a privilege starting this new job being mentored by him.



**Ramkishore Ramakrishnan** · 1st

XFTM Investigation Analyst - IBM

September 29, 2021, Ramkishore worked with  Dariusz on the same team

 All LinkedIn members

It is my pleasure & honor that I know Dariusz Socha and have worked with him. Throughout his time with our team, Dariusz proved himself to be a hard-working, motivated, ambitious, and reliable employee. He always understands the importance of what he does and his technical skills from both a Cybersecurity and Business perspective are sharp and effective. His honesty, dependability, confidence, and excellent communication skills helped him to achieve in his career growth. It's my great pleasure to recommend Dariusz Socha and I wish him both personal and professional success in all of his future endeavors. If you have any questions or need further information, please do not hesitate to contact me.



**Karolina Szyszka** · 1st

Threat Monitoring Security Analyst at IBM Poland

October 6, 2021,  Dariusz was senior to Karolina but didn't manage Karolina directly

 All LinkedIn members

Dariusz was my mentor at IBM and I consider it be a huge privilege of mine. His great communication skills, patience and true devotion to help new employees are inexchangable. Not only that, but also his vast knowledge about the IT security and the pure eagerness to develop in the field make him an exceptional addition to the team. He is not afraid to propose new ideas and express his point of view, but is also very open to opinions different from his. He is an excellent professional who always does his job to the best to his abilities and who helps his co-workers achieve the same thing. Dariusz has my highest recommendation as a terrific security analyst and a wonderful team player.

Thanks for your time! 

