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

DARIUSZ SOCHA

born 1985

ADDRESS
There's no place like 127.0.0.1
Wrocław, Poland

CONTACT
mobile: +48 **515 490 505**
dariusz@socha.pl| www.**socha.pl**
www.linkedin.com/in/sochadariusz/

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

CURRICULUM VITAE

10 years of experience in cybersecurity, check my **YouTube** channel

34 years in IT (hardware -> web development -> networks -> cybersecurity)

Dariusz represented Poland in a project to build a cybersecurity shield for the European Union at an international workshop in Brussels. His proposal to establish a network of Security Operations Centers (SOCs) was met with approval by all of EU member states.

05.2025- Current
Senior Cybersecurity Architect (High and Low Level Design)
- Kyndryl ; Poland (Canada), Wroclaw // full time, remote

12.2023- 04.2025
Senior Cybersecurity Consultant (XDR/SIEM/SOAR + AI)
- SOC.HA ; Poland, Wroclaw // B2B, remote

10.2022- 11.2023
Senior SOC Solutions Architect (SOC/SIEM Expert)
- NASK PiB ; Poland, Warsaw // full time, remote

05.2017- 09.2022
Senior Cybersecurity Specialist - SOC SIEM L2 Analyst
- IBM ; Poland (USA), Wrocław // full time, hybrid

04.2016- 04.2017
IT Security Specialist - SOC SIEM L1 Analyst (Forensic)
- IBM ; Poland (USA), Wroclaw // full time, hybrid

03.2015- 03.2016
Senior Frontend Developer & UX Designer
- Britenet ; Poland, Lublin // B2B, hybrid

Education

2005-2011 **The College of Enterprise and Administration**
In Lublin, Poland *(www.wspa.pl)*.
Specialization: **IT / Computer Networks**

2000-2005 Technical School in Świdnik, Poland
- title of „technician-mechanic"

Brief / *#CybersecurityExpert*

1. **Diverse Cybersecurity Background:** Leverage my hands-on experience across roles (analyst, threat hunter, administrator, and architect) to safeguard your organization comprehensively.
2. **End-to-End SOC Expertise:** Whether optimizing your existing Security Operations Center or building a new one from the ground up, I'll ensure every step is effective.
3. **Holistic Security Approach:** Security starts with physical safeguards and extends through clear, understandable processes. I'll guide you through each phase, making complex cybersecurity simple.

Core expertise

- **SOC design & optimisation:** maturity assessments, 24 × 7 follow-the-sun models, MITRE ATT&CK-aligned use-case development, purple-team.
- **SIEM architecture:** Microsoft Sentinel in Azure Cloud; log onboarding at terabyte scale, parsing, correlation, UEBA, SOAR playbooks.
- **Endpoint Detection & Response:** CrowdStrike Falcon, Microsoft Defender; policy tuning, behavioural analytics, automated containment.
- **Network Detection & Response:** Darktrace; encrypted-traffic analytics, lateral-movement detection, sensor placement & KPI design.
- **GRC:** NIST CSF, ISO/IEC 27001, SOC2, NIS2, DORA; control mapping, risk-register management, audit readiness, board-level reporting.

General skills:

- **English** - advanced (C1)
- **Polish** - native speaker
- **Creativity** (YouTube, Website)
- **Excellent soft skills**

Network Intrusion Detection and Protection (**NIDS, NIPS**), Full Packet Capture (**FPC**), Online Computer Forensics (**OCF**), Cyber Operations Management Service (**COMS**), Standalone Computer Forensics (**SCF**) / Cyber Defence Situational Awareness (**CDSA**).

Cybersecurity **experience details** 2016-2025

greatest achievement

SOC SIEM
Analyst L1
2016-2017
IBM

- **Mentorship & Insight:** Guided by an exceptional mentor, I discovered that an analyst's job is akin to reviewing logs as if they were books, capturing the key points succinctly while ensuring clarity.
- **Data-Driven Triage:** With no crystal ball, relying on logs and clear instructions became my core method, leading me into the world of triage, where accurate, concise summaries are paramount.

***Technology**: SIEM, NDR | **Tools**: QRadar, ArcSight*

In just six months, I optimized log analysis and triage for over 500 incidents, reducing resolution time by 30% through concise, data-driven summaries.

Senior SOC SIEM
Analyst L2
2017-2019
IBM

- **Conducted in-depth forensic investigations**, correlation rule analysis, and root-cause assessments to pinpoint security threats while ensuring proactive remediation.
- **Efficiently identified, analyzed, and reported** vulnerabilities using SIEM and EDR, resolving issues to protect the organization's infrastructure.

***Technology**: SIEM, NDR, NIST | **Tools**: QRadar, Sentinel*

Successfully conducted 250+ forensic investigations and identified over 1000 vulnerabilities with a 98% resolution rate.

Senior SOC SIEM
Dedicated Analyst
2019-2022
IBM

- **Provide advanced threat hunting** and L3-level analysis to proactively safeguard client environments.
- **Identify and address detection gaps by reviewing AV logs daily**, ensuring no infection goes unnoticed.

***Technology**: SIEM, NDR, EDR | **Tools**: QRadar, Sentinel, CrowdStrike*

Detected and contained a ransomware threat through proactive L3 threat hunting and daily AV log reviews, preventing an estimated $500K in business losses.

Principle SOC
Mentor
2016-2022
IBM

- **Successfully mentored 20 multinational analysts** (including non-IT talent) over 7 years, with outstanding results and top recognition.
- **Recognized by managers as IBM Poland's best mentor**, often stepping in as the "special weapon" to resolve training challenges.

***Technology**: SIEM, NDR, EDR | **Tools**: QRadar, Sentinel, CrowdStrike*

Saving approx. $100,000 by eliminating the need for external trainers.

Splunk

Architect

2022-2023

NASK

National Research Institute

- **Led SIEM Deployment & Architecture:** Selected and licensed Splunk as the optimal SIEM, engineered a tailored on-premise architecture, and managed hardware resources to ensure high performance and security.
- **Implemented Distributed Splunk Environment**: Established a resilient, scalable distributed architecture, fine-tuned data collection, and executed core Splunk configurations, boosting incident response capabilities.

***Technology**: SIEM, GRC, PAM | **Tools**: Splunk*

Successfully deployed a high-performance Splunk-based SIEM in just three months under intense time pressure.

SOC Solutions

Architect

2023

NASK

National Research Institute

- **Embracing the SOC Vision:** Building a Security Operations Center (SOC) from the ground up has been my passion since my very first SIEM Analyst role. I thrive on creating a robust cyber defense ecosystem tailored to organizational needs, turning vision into reality.
- **Aligning with International Standards:** My expertise lies in designing SOC frameworks that comply with the European NIS2 directive, ISO 27001, and SOC2.

***Technology**: SOC, NOC, RACI, ISO27001, PAM | **Tools**: ServiceNow*

Successfully negotiated with the ServiceNow provider to integrate a fully compliant SOC framework (NIS2, ISO 27001, SOC2) with a newly established NOC.

Senior

Cybersecurity

Consultant

2023

SOC.HA

for B2B Network

- **Provided comprehensive SIEM training** for new analysts, demonstrating expertise and leadership.
- **Led a SOC creation project,** comparing top SIEM solutions, negotiating with vendors, a successful PoC.

***Technology**: SIEM, GRC, NIS2 | **Tools**: QRadar, Splunk, Sentinel*

Prepared multiple budget-based SOC variants with phased development steps, ensuring scalability.

Senior Cybersecurity **Consultant**

2024

SOC.HA

for Cloudware

- **Built a new SOC** and IT department from the ground up, leveraging IBM QRadar for security architecture.
- **Delivered comprehensive training content** on becoming a SIEM analyst, boosting team expertise.

***Technology**: SIEM, SOAR, GRC, IAM | **Tools**: QRadar*

Delivered a customized SIEM analyst training program and audits on client offerings that boosted contract acceptance rates by 20%.

Senior Cybersecurity **Consultant**

2024

SOC.HA

for Smart Tech (in Malta)

- **Led the strategic design of a new SOC,** implemented ISO 27001, and developed robust DDoS protections in Malta's largest IT corporation.
- **Conducted comprehensive assessments of NIS 2 and DORA requirements,** enhancing security posture with Darktrace's XDR solution.

***Technology**: SOC, SIEM, SOAR, XDR, CDN | **Tools**: DarkTrace, CloudFlare*

Spearheaded the new SOC design for Malta's largest IT firm. Additionally, completed NIS 2 and DORA assessents.

Associate Director, Senior Cybersecurity **Architect**

2025

Kyndryl

(in Canada)

- **Security Architecture & Standards:** Develop and implement security frameworks, policies and best practices in diverse system environments.
- **Security Consulting & Risk Mitigation:** Advise business and IT teams on security risks, recommend security tools and proper implementation.
- **Threat & Vulnerability Management:** Identify, assess and address high-risk security threats, particularly in cloud environments.
- **Incident Response & Risk Reduction:** Provide recommendations and action plans to mitigate security risks and respond to security incidents.

***Technology**: SOC, SIEM, SOAR | **Tools**: Azure Defender XDR and Sentinel*

Designed, developed, and implemented an authorial SIEM migration system to Microsoft Sentinel in cloud.

Quick but honest **Motivation Letter**

I approach cybersecurity with an ecosystem mindset, much like building with Lego: every piece has a purpose and needs to fit seamlessly. I believe if documentation is seen as unnecessary, it's just not well-crafted and must be improved. I also recognize that not all clients can invest in fully professional solutions, so I focus on meeting regulations first while highlighting the potential for further enhancements. Cybersecurity is an ongoing journey, I'll guide you from start to finish. Let's connect and build a safer digital world together.

C1 level of English Metropolitan School Certificate

METROPOLITAN
SZKOŁA • TŁUMACZENIA

Metropolitan School Certificate

as a proof of language level

Here's to cerify that

Dariusz Socha

DOB : 13.08.1985

is on the C1 level of English.

METROPOLITAN SCHOOL
Aneta Chodorowska
45-057 Opole, ul. Ozimska 4/7 II p.
tel. 796 48 48 01, NIP: 6541995860
info@metropolitanschool.pl

Opole, 15.01.2024

A. Grużewska
Agnieszka Grużewska
Director and teacher of English

#CyberSecurityJobs #InfoSec #ThreatIntelligence #IncidentResponse #PenTesting

#DataProtection #CloudSecurity #SecurityOperations #NetworkSecurity #ITGovernance