DMYTRO CHMYR

PERSONAL

d.chmyr.sec [at] gmail.com

+49 ••• ••• ••• (on request)

linkedin.com/in/dimachmyr

Mannheim, Germany

LANGUAGES

German - fluent

English – fluent

Ukrainian – native

Russian – native

INTERESTS

OSINT & CTFs

Strength training

PROFESSIONAL SUMMARY

Cybersecurity Professional with a background in IT solutions and specialization in Detection, Incident Response and Security Engineering. After completing further education (BTL1, EuroTech), extensive practical experience in SIEM, malware analysis, vulnerability assessment and network forensics. Versatile in the area of SOC, Security Engineering or technical support for security solutions.

SKILLS

SIEM & DETECTION ENGINEERING
Splunk, Sentinel, Sigma, Sysmon, KQL, Rule Tuning

DIGITAL FORENSICS & MALWARE ANALYSIS
Volatility, FTK Imager, KAPE, Autopsy, CyberChef

INCIDENT RESPONSE & ALERT HANDLING
MITRE ATT&CK, IOC Analysis, Case Documentation, Playbook Development

NETWORK ANALYSIS & TRAFFIC MONITORING
Zeek, Suricata, Wireshark, PCAP-Analysis

THREAT INTELLIGENCE & USE CASE DESIGN
MISP, TheHive, OSINT, TTP Mapping, Detection Development

SOFT SKILLS

Analytical Thinking | Structured Problem Solving |
Communication | Resilience

EDUCATION

Cybersecurity Engineering Training,
EuroTech Study GmbH, Frankfurt 12/2023 – 12/2024
Final grade: 96/100

CERTIFICATIONS

- ▣ Security Blue Team Level 1 (BTL1)
- ▣ CompTIA Security+
- ▣ Junior Penetration Tester (PT1)
- ▣ CompTIA PenTest+
- ▣ Splunk Core Certified User
- ▣ Fortinet FortiGate 7.4 Administrator (FCP)
- ▣ TÜV Information Security Officer

DMYTRO CHMYR

PROFESSIONAL EXPERIENCE / PRACTICAL EXPERIENCE

2024 Cybersecurity Analyst (Internship), TechNS GmbH, Oberursel (Taunus), Germany

- Analysis & escalation of alerts (Splunk), rule optimization, IOC correlation
- Creation of technical reports, vulnerability assessments, web pentesting (SQLi, XSS)
- Co-development of use cases, runbooks & playbooks
- Reduced false positive rate by improving Splunk alert logic
- Documented key detection use cases later used in onboarding

2023–2024 Cybersecurity Engineer, EuroTech Study GmbH, Frankfurt, Germany

- Focus on Incident Response, Malware Analysis, APT Tracking, Security Automation, Cloud Security (AWS/GCP) Final grade: 96/100

2019–2022 Consultant It Security, iIT Trading, Kyiv, Ukraine

- Advised on Endpoint Protection, Backup & Network Segmentation, Conducting Awareness Trainings, Support in Technical Customer Issues and Security-Related Project Management

2007–2019 Senior Sales Manager, Comtrading, Kyiv, Ukraine

- B2B Sales, Technical Customer Consulting, IT Infrastructure Projects, including Security Components

2004–2007 System Administrator, LeaseIT, Kyiv, Ukraine

- Windows and Network Administration, AD, Server Operations, Troubleshooting
- User onboarding, system maintenance, backup configuration

TECHNICAL PROJECT EXPERIENCE & LABS

BTL1 & Blue Team Labs (BTLO, CyberDefenders)

• Practical DFIR and detection labs focused on SIEM, forensics, Sigma rule creation, MITRE ATT&CK, and Zeek.

LetsDefend – SOC Analyst Path

• Completed 20+ realistic alerts including log analysis and incident response using Splunk, Sigma, TheHive, and MISP.

Splunk Alert Rule Tuning (Self-Initiated Tests)

• Evaluated rule logic, identified false positives, performed field extractions and threshold tuning.

Virtual Cybersecurity Case Studies (Forage: PwC & TCS)

• Performed risk assessments, security analysis, and IAM strategy development with international project presentation.

Mannheim , Germany