Mateusz Filipczak

+48 605 050 155 | mateusz.filipczak@outlook.com

Warsaw, Poland

SUMMARY OF QUALIFICATIONS

IT Security Professional with 8+ years of progressive experience in cybersecurity operations, security automation, data engineering, and identity governance. Skilled in building and managing SOAR platforms, developing automated workflows for threat detection and response, and integrating with SIEM, EDR/XDR platforms, vulnerability management solutions, and threat intelligence feeds. Currently supporting a global Cyber Defense Center in the renewable energy sector, delivering end-to-end orchestration and automation solutions.

Experienced across diverse industries including finance, media, and telecommunications. Customer-centric and solution-oriented, with a strong focus on understanding business needs and delivering tailored security solutions. Adept at building trust and maintaining clear communication with both technical teams and non-technical stakeholders. Collaborative team player, working closely with SOC teams and cross-functional partners to develop and automate security use cases. Committed to continuous learning, service excellence, and strengthening enterprise security resilience through proactive support and process optimization.

CORE COMPTENCES

Category	Skills & Tools
Security Operations	SOC, Splunk, Sumo Logic, CrowdStrike, Cortex XDR, OpenCTI, MITRE ATT&CK, DLP
Threat Detection & Response	Alert triage, playbooks, incident handling, containment, forensics
Security Automation	Python, XSOAR, Graph API, REST API, Bash, PowerShell, Git, CI/CD pipelines (Azure DevOps)
IAM & Governance	SailPoint, AD / Entra ID, RBAC, provisioning, access reviews
Vulnerability Management	Tenable, Qualys, patch validation, risk prioritization
Network & Endpoint Security	Firewalls, IDS/IPS, baselines, hardening
Cloud & Data Engineering	SQL DB design, Azure provisioning, secure architecture
Threat Hunting & Log Analysis	Anomaly detection, log correlation, custom queries, use cases
Collaboration & ITSM Tools	Jira, ServiceNow, Confluence

PROFESSIONAL EXPERIENCE

Senior Security Automation Analyst / Security Automation Analyst

Ørsted Polska – Warsaw, Poland | 03/2021 – Present

- Established and grew the Security Automation & Reporting team, onboarding all team members and leading a five-person team of analysts.
- Designed, implemented, and currently maintain the enterprise SOAR platform (XSOAR), leading end-to-end deployment including POC, vendor comparison, requirement documentation, onboarding plan, and installation.
- Maintained the platform both on-premises and through successful migration to the cloud-based SaaS solution, ensuring continuity and improved scalability.
- Developed and continuously refined playbooks, custom integrations, and scripts to automate threat detection and incident response across key domains including SIEM, IAM, case management, data enrichment, threat intelligence, databases, email gateways, endpoint protection, network security, and utility services.
- Collaborated with SOC and other security teams to identify and prioritize automation opportunities, driving operational efficiency and reducing manual workload.
- Provisioned Azure subscription and supporting infrastructure (landing zone) to host SQL databases and Power BI reporting pipelines.
- Designed and delivered end-to-end security reporting in Power BI and Splunk: onboarding and normalizing data, defining KPIs, and maintaining reports for key stakeholders.
- Provided ongoing administration of the SOAR platform, ensured continuous improvement of workflows, and acted as a mentor by training junior automation analysts.

Senior Information Security Analyst / Security Information Analyst

VIMN Poland (currently Paramount Network Polska) – Warsaw, Poland | 01/2019 – 03/2021

- Managed the full vulnerability lifecycle, including assessment, prioritization, remediation tracking and patching process.
- Designed and implemented automated alert handling workflows in the SOAR platform to enhance SOC efficiency.
- Deployed and maintained deception technology components to improve threat detection capabilities.
- Executed IDS migration from on-premises infrastructure to cloud environments, ensuring uninterrupted monitoring.
- Monitored network traffic, intrusion detection, and prevention systems to identify and mitigate threats.
- Conducted thorough investigation of security alerts and performed incident response activities.
- Developed automation scripts using VBA, Bash, and PowerShell to streamline security operations.
- Researched emerging cybersecurity threats and recommended mitigation strategies.
- Reviewed and analyzed network and endpoint security configurations to enforce robust policies.
- Owned threat detection and data loss prevention platforms, handling upgrades, alert tuning, and vendor collaboration.
- Performed proactive threat hunting to detect advanced persistent threats and anomalies.

Senior IT Security Analyst / IT Security Analyst

Accenture – Warsaw, Poland | 09/2016 – 12/2018

Project: Digital Banking Transformation – French Bank

- Collected and analyzed security requirements for integrating internal and external applications with the banking platform.
- Planned and coordinated security testing activities, including vulnerability assessments and remediation tracking.
- Acted as the single point of contact (SPOC) for all security-related topics, including preparation of project security status reports.
- Conducted incident management and response coordination during the project lifecycle.
- Reviewed systems for compliance with OWASP best practices and GDPR requirements.
- Performed web server security hardening by removing sensitive headers and configuring X-Frame-Options and X-Content-Type-Options.
- Implemented Content Security Policy (CSP 2.0) and anti-CSRF mechanisms in an ASP.NET MVC web application.
- Developed and delivered a comprehensive Security & Quality Improvement Plan for the project.

Project: Identity & Access Management Framework – Scandinavian Bank

- Designed and developed automated reporting tools in Visual Basic to support IAM metrics and compliance tracking.
- Defined the onboarding strategy and technical requirements for integrating infrastructure assets with SailPoint IdentityIQ.
- Administered SharePoint environment used for documentation, access governance, and project collaboration.
- Created executive-level dashboards and visual reports for the client's Architecture Board.
- Designed a prototype database schema to support scalable and efficient onboarding of infrastructure components.
- Collected and normalized application access data from diverse systems including Active Directory, SAP, RACF, HP NonStop, and local authentication methods.
- Developed PowerShell scripts for data extraction and transformation across IAM systems.

IT Support Associate / Intern

Accenture Services – Warsaw, Poland | 05/2015 – 08/2016

- Delivered first-line support for hardware and software issues across PCs, MacBooks, mobile devices, printers, and accessories for global users.
- Managed Active Directory accounts, IT asset inventory, and coordinated hardware orders and vendor communication.
- Escalated complex issues to L2 support and contributed to documentation, policy improvement, and service quality enhancement.
- Created user manuals, supported internal tools, and transitioned from intern to full analyst through active involvement in IT support operations.

EDUCATION

Master of Arts in Information Technology

European University — Warsaw, Poland | 10/2016 – 06/2018

Thesis: *"Proper Identity and Access Management in organization improves business administration and offloads the network administrators"*

Bachelor of Arts in Information Technology

European University — Warsaw, Poland | 10/2011 – 06/2015

Thesis: *"Photo editor embedded in a responsive website"*

CERTIFICATIONS

- CompTIA Security+ ce Certification – 2019
- Certified SAFe® 5 Practitioner – 2021
- Microsoft Certified: Azure Fundamentals – 2023
- GIAC Python Coder (GPYC) - 2024

ADDITIONAL INFORMATION

Interests (Outside Security): Home lab innovations, world travel (30+ countries), smart home automation, and video editing.

I hereby consent to the processing of my personal data included in this CV for the purposes of recruitment, in accordance with the EU General Data Protection Regulation (GDPR).