Maciej Drobniuch

XSOAR Subject Matter Expert & XSIAM | Palo Alto Networks

maciej@drobniuch.pl linkedin.com/in/maciej-drobniuch-4985175a drobniuch.pl Szczecin, Poland

11+	4	16+	1,000+
YEARS IN CYBERSECURITY	MARKETPLACE INTEGRATIONS	XSOAR SERVERS MANAGED	INCIDENTS/DAY AUTOMATED

SUMMARY

Cortex XSOAR Subject Matter Expert at Palo Alto Networks with 11+ years of cybersecurity experience. Focused on enterprise XSOAR 8 migrations and XSIAM integration. Track record in large-scale SOAR deployments, advanced playbook optimization, marketplace integration development, threat intelligence management, and CI/CD pipeline engineering for content automation.

EXPERIENCE

XSOAR SME

Feb 2025 - Present

Palo Alto Networks

- Led strategic migrations for enterprise customers from legacy systems to Cortex XSOAR 8
- Facilitated technical onboarding of customers onto Cortex XSIAM
- Provided high-level SME expertise to resolve complex deployment blockers

XSOAR 8 | XSIAM | Migration | Enterprise

XSOAR Content Development

Feb 2024 - Jan 2025

Kyndryl

- Architected XSOAR 8 On-prem solutions integrated with ElasticSearch clusters
- Engineered CI/CD pipelines for standardized content development
- Designed Threat Intel Management (TIM) strategies for indicator lifecycle automation
- Led XSOAR capability "ramping" into business units

CI/CD | ElasticSearch | TIM | DevSecOps

XSOAR CyberSOC Automation Expert

Sep 2021 - Feb 2024

Orange Cyberdefense

- Managed 16+ XSOAR servers, processing 1,000+ incidents/day with auto-remediation
- Published 4 official integrations to XSOAR Marketplace: EdgeScan, PAN-OS Policy Optimizer, OpenCV, UnifiNVR
- Developed custom Prometheus XSOAR integration for system diagnostics
- Spearheaded Global CSOC conversion to XSOAR-centric operational paradigm

Marketplace | Prometheus | Scale | CSOC

Senior PS Consultant / PS Consultant

May 2019 - Aug 2021

Palo Alto Networks

- Delivered end-to-end SOC automation strategies using Cortex XSOAR
- Automated firewall migrations and pioneered IaC for cloud firewall deployments
- Implemented container security measures for compliance and threat protection

SOC | IaC | Cloud Security | Containers

Senior Network Security Engineer

Jul 2016 - Feb 2019

Collective Sense

- Spearheaded anomaly detection for security incidents using ML models
- Trained ML models on malicious traffic data for improved detection
- Reverse engineering of application and network layer attacks
- Utilized Metasploit and offensive tools for R&D

ML | Anomaly Detection | Reverse Engineering

Security Solutions Architect

Oct 2014 - Jul 2016

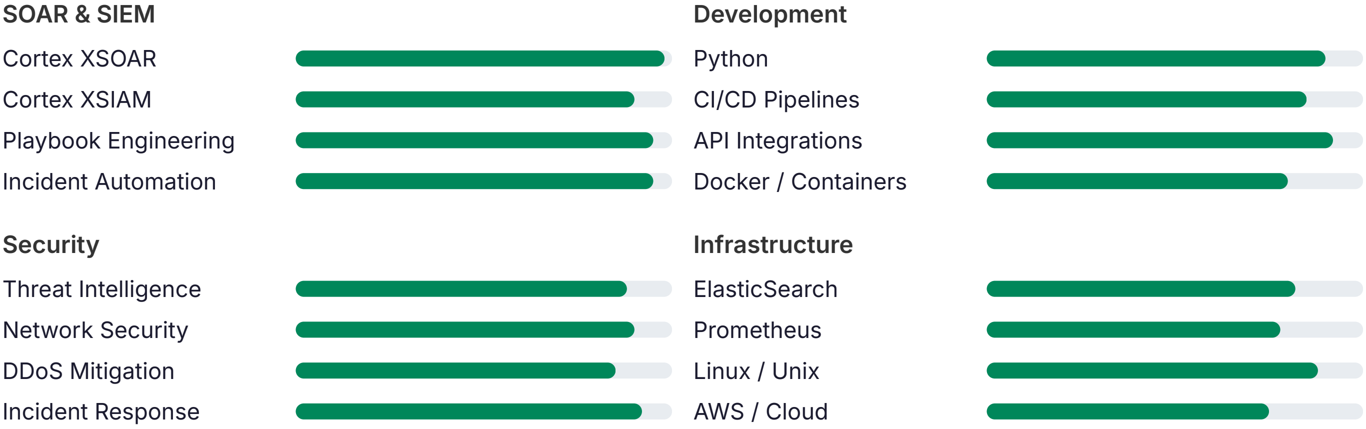
Akamai Technologies

- Implemented emergency integrations during active DDoS attacks with SOC team
- Managed BGP/GRE configuration and troubleshooting
- Integrated anti-DDoS products into customer network infrastructures

DDoS | BGP | Anti-DDoS | CDN

Earlier Career (2010-2014): IT Infrastructure Consultant at Capgemini | Technical Specialist at brightONE | Test Engineer at Tieto | Network Technician at Stream Global Services

SKILLS



SOAR & SIEM

Cortex XSOAR

Cortex XSIAM

Playbook Engineering

Incident Automation

Development

Python

CI/CD Pipelines

API Integrations

Docker / Containers

Security

Threat Intelligence

Network Security

DDoS Mitigation

Incident Response

Infrastructure

ElasticSearch

Prometheus

Linux / Unix

AWS / Cloud

MARKETPLACE INTEGRATIONS & PROJECTS

XSOAR MARKETPLACE

PAN-OS Policy Optimizer

Official integration for optimizing PAN-OS firewall security policies. Automates policy analysis and rule optimization.

XSOAR MARKETPLACE

EdgeScan

Integration for EdgeScan vulnerability management. Automated vulnerability ingestion and remediation workflows.

XSOAR MARKETPLACE

OpenCV Integration

Bridging computer vision with security operations for image analysis in automated workflows.

XSOAR MARKETPLACE

UnifiNVR

Ubiquiti UniFi NVR integration for security camera management and alerting within SOAR.

CUSTOM

Prometheus XSOAR

Custom integration exposing XSOAR system diagnostics and health metrics to Prometheus for observability.

ARCHITECTURE

Global CSOC Transformation

Led Orange Cyberdefense's Global CSOC conversion to XSOAR-centric paradigm. 400 concurrent incidents, zero degradation.

LANGUAGES

English (Professional) | German (Professional) | Polish (Native)