VIACHESLAV ANTONYUK

Moscow, Russia ♦ viacheslavantonyuk@gmail.com ♦ +79152201219

PROFESSIONAL SUMMARY

Confident and highly organized cybersecurity specialist with 5-year experience in a company with highly-loaded infrastructure as a member of SOC CIRT. Knowledge and usage of a variety of technologies to protect infrastructure and prevent cyber threats. Team management and collaboration with adjacent divisions to address identified challenges. Optimizing processes and procedures to ensure the best efficiency in operational activity. Balanced and integrated approach to achieve objectives.
Open to relocation on a global level.

SKILLS

- Incident analysis and response management
- Incident response plan and procedures development
- Working with host-based and network security tools
- Provide situational awareness for CIRT
- Analysis and improvement of response processes
- Coaching and supervising team members
- PowerShell automation [Intermediate]
- Coordinating incident response actions

EXPERIENCE

10/2019-NOW
Moscow, Russia

Cyber Security Expert

PJSC Sberbank

- Developed, controlled, and modified core SOC processes related to ensure incident response and situational awareness.
- Handled cybersecurity incidents and coordinated response actions between teams
- Developed and implemented various automation tools to reduce time-to-response.
- Communicated with the team to determine and develop key requirements for reports to measure SOC efficiency.
- Created and updated incident response plans to keep up-to-date.
- Mentored and coached the SOC staff. Organized inner training for more than 40 analysts.
- Created and updated onboarding guides and checklist to make the process more convenient and clearer.
- Validated 300+ playbooks and procedures required to process and response alerts from correlation rules.
- Created comprehensive dashboard presets to control security posture of the organization based on the current situation. Issued the book with the description of all dashboards and possible reactions based on the metrics from them.
- Organized and developed the coordination between IT-support and Cybersecurity support to ensure that information about incidents reach SOC as quickly as possible from the employees.
- Prepared and participated in organizing 10+ mass malware infection tabletop exercises to improve situation awareness of the employees and provide business continuity.
- Adapted existing response processes to regulatory requirements.

10/2017-10/2019
Moscow, Russia

Cyber Security Analyst

PJSC Sberbank

- Worked as a Tier 1-3 SOC analyst to handle cybersecurity incidents with the experience to work with various technologies (SIEM, SOAR, NGFW, NBA, EDR, AVS).
- Participated in the creation of the comprehensive situational awareness product for SOC to reduce MTTR for different types of incidents and controlling organization’s security posture.
- Analyzed and proposed improvements for existed UseCase scenarios to decrease false positive rate.

- Conducted department’s inner quality assessment to identify and address problems with procedures, knowledge, and technologies. Identified areas that can be automated to decrease manual work based on the results of the assessment.

EDUCATION

2012-2018
Moscow, Russia

Specialists degree: Automated Systems Information Security
U.S. Equivalency summary (WES evaluation): Master’s degree
Bauman Moscow State Technical University

2018
Moscow, Russia

System Center Configuration Manager: Concepts and Administration Advanced
Microsoft Premier Support

2019
Moscow, Russia

Interconnecting Cisco Networking Devices 3.0. Part 1 & 2
Microtest

2019
Moscow, Russia

Certified Ethical Hacker (CEH)
HackerU

2020
Moscow, Russia

ITIL v4 Foundation
IT Expert

CERTIFICATIONS

10/2019-10/2025
CompTIA

CompTIA Security+
T9T643H34LRE10CC

LANGUAGE

Russian	Native
English	Advanced (C1 IELTS)