Valerii Serkin

Security Operations & Engineering Leader

Málaga, Spain +34 667 297 354 val.serkin@gmail.com linkedin.com/in/valeriy-serkin

Education

National Research Nuclear University (former Moscow Engineering Physics Institute) Moscow

Specialist, Integrated Information Security of Automated Systems *2007 – 2012*

Work Experience

Senior Manager, Security Engineering Sep 2025 – Present

TradingView *Málaga, Spain*

- Lead the internal Security Operations Center, delivering continuous, organization-wide security monitoring, incident response, and proactive threat hunting across the TradingView environment.
- Established the SOC from the ground up, standing up monitoring, detection, and response capabilities and embedding a Threat Intelligence function to drive intelligence-led operations.
- Architected and deployed SOAR automation and cross-tool integrations, unifying the security stack into a single workflow and significantly reducing mean time to detect and respond.
- Tuned and optimized EDR for maximum detection coverage and performance, strengthening endpoint visibility and containment across the fleet.
- Designed and operationalized Data Loss Prevention (DLP) controls to safeguard sensitive and regulated data across endpoints and corporate channels.
- Built and ran continuous phishing simulation campaigns and security-awareness training, measurably improving the organization's resilience to social engineering.
- Pioneered methods and internal tooling to detect and prevent "shadow AI" usage, mitigating data-exposure and compliance risks from unsanctioned AI services.

Head of Cyber Defense Center Jan 2024 – Sep 2025

Malcrove *Dubai, UAE*

- Lead a team of 20+ SOC analysts, overseeing daily security operations, incident response, and threat detection across diverse environments.
- Direct Digital Forensics and Incident Response (DFIR) efforts across client environments, ensuring swift containment, investigation, and remediation of security incidents.
- Perform comprehensive compromise assessments, identifying breaches, evaluating incident scope, and providing expert recommendations for remediation and prevention.
- Drive continuous improvement of SOC processes and workflows, optimizing tools such as SIEM platforms (Elasticsearch, Splunk, QRadar), IDS/IPS, and threat intelligence systems.
- Mentor SOC analysts in incident handling, DFIR, and forensic investigations, promoting knowledge-sharing and professional growth.
- Collaborate with clients and internal teams to align security operations with business requirements.

Head of Detection Engineering and Threat Hunting Oct 2022 – Jan 2024

Malcrove *Dubai, UAE*

- Led a team developing and optimizing detection engineering and threat hunting across multiple clients, leveraging advanced analytics and security tools.
- Designed and deployed customized detection rules using the SIGMA framework.
- Spearheaded threat hunting across on-premise, AWS, and Azure infrastructures, identifying hidden threats and potential attack vectors.
- Implemented and maintained automated detection workflows using custom Python scripts and tools to improve response efficiency and accuracy.
- Coordinated with the SOC team to validate detection logic, ensuring rapid identification and response to emerging threats.
- Analyzed adversary tactics, techniques, and procedures (TTPs) to stay ahead of evolving threat landscapes.
- Tailored threat detection strategies to each client's security requirements and risk profile.

Senior Cyber Security Consultant Sep 2021 – Oct 2022

Malcrove *Dubai, UAE*

- Led Threat Hunting and Incident Response engagements for multiple clients, identifying and mitigating advanced cyber threats.
- Developed internal microservices in Python to automate data enrichment, incident triage, and response workflows.
- Conducted in-depth malware analysis, including reverse engineering, to produce actionable threat intelligence.
- Performed compromise assessments and delivered detailed remediation strategies to reduce future risk.
- Provided technical leadership and hands-on support to Tier 1 and Tier 2 SOC analysts during complex investigations.

Senior SOC Analyst — Research & Development Sep 2016 – Sep 2021

Kaspersky *Moscow, Russia*

- Played a key role in building the SOC's core processes and tools from scratch (Elasticsearch, TheHive, Cortex, and other open-source solutions).
- Collaborated with incident responders and threat hunters to strengthen overall client security posture.
- Developed internal microservices in Python, Go, and .NET Core to automate SOC workflows, improving detection accuracy and reducing response times.

Leading Information Security Specialist Jun 2015 – Sep 2016

Credit Bank of Moscow *Moscow, Russia*

- Developed and implemented comprehensive information security policies to protect critical assets and sensitive customer data.
- Managed security assessments and audits, mitigating risks and ensuring regulatory compliance.
- Oversaw deployment of firewalls, intrusion detection systems, and endpoint protection across the bank's infrastructure.
- Conducted incident response and forensic investigations, identifying root causes and implementing corrective measures.

Leading Information Security Engineer Mar 2014 – Jun 2015

Transaero Airlines *Moscow, Russia*

- Led generation of key carriers for the client-bank clearing center, configuring and troubleshooting eToken and RuToken devices.
- Managed information security projects end to end, aligning with company security goals.
- Conducted internal penetration tests and delivered detailed reports and recommendations.
- Investigated security incidents and coordinated mitigation to prevent future breaches.

Information Technology Security Engineer Dec 2011 – Sep 2012

Microtest *Moscow, Russia*

- Conducted pre-sale consultations and identified security solutions matching customer technical and business needs.
- Delivered product demos and comparative analyses to support informed decisions.
- Implemented communication-channel and personal-data protection systems at Kuibyshev Azot JSC and Renaissance Insurance Group, ensuring regulatory compliance.

Technical Skills & Interests

Programming: Python, Go, Rust, .NET Core, C/C++, JavaScript
Operating Systems: Windows, Linux, macOS
Cloud: Azure, AWS, GCP
Cloud Log Sources: AWS CloudTrail/GuardDuty/CloudWatch, Azure AD / Security Center / Activity Log, Google Cloud Audit Logs, Cloud Armor
Detection & Response: SIGMA, TheHive, Velociraptor, MISP, Zeek (Bro), Suricata
Threat Intelligence: STIX/TAXII, MITRE ATT&CK, OpenCTI
IR & Orchestration: Cortex, SOAR
SIEM: Elastic SIEM, Splunk, Azure Sentinel, Security Onion, Wazuh, LogRhythm, Sumo Logic, Rapid7 IDR
EDR & Threat Hunting: OSQuery, Elastic Endpoint Security, QRadar, CrowdStrike, Carbon Black, Microsoft Defender 365
Offensive / Red Team: Caldera, Burp Suite, Atomic Red Team, Kali Linux, Cobalt Strike, Sliver, Metasploit
Vulnerability Management: Nessus, OpenVAS, OWASP ZAP

Languages

Russian: Native, including technical and cybersecurity terminology.
English: Fluent, with command of technical and cybersecurity language.
Spanish: Beginner (A1).