Alexander Isoev — SOC Analyst at CYDEO Security

📍 Dec 2024 – Aug 2025 · 9 months
🛡️ Blue Team · Detection & Response · Threat Investigation

🔹 Role Summary

As a SOC Analyst at CYDEO Security, I worked on real-world incident simulations focused on phishing, malware, and PowerShell-based intrusions.
My role involved proactive monitoring, log correlation, and endpoint investigation to strengthen detection logic and improve response efficiency across the SOC.

🔹 Core Responsibilities

- Monitored and analyzed alerts in Splunk, IBM QRadar, and Elastic SIEM to detect suspicious activity and anomalies.
- Performed endpoint triage with CrowdStrike Falcon, focusing on process injection (T1055) and PowerShell abuse (T1059.001).
- Conducted phishing and malware investigations — decoded malicious URLs, extracted payloads, and enriched IOCs using threat-intel tools.
- Created detailed incident documentation and JIRA tickets with ATT&CK mapping, containment steps, and supporting evidence.
- Assisted in detection rule tuning to reduce false positives and improve signal-to-noise ratio.
- Collaborated with senior analysts during shift handovers and cross-tool investigations.

🔹 Results & Highlights:

• Optimized QRadar rules (−20% false positives), mapped 12+ MITRE techniques, authored SOC playbooks, identified PowerShell injection chains.

🔹 Tools & Technologies

💻 SIEM: Splunk · IBM QRadar · Elastic SIEM
🛡️ EDR: CrowdStrike Falcon
🌐 Network: Suricata · Wireshark · AbuseIPDB · Shodan · GreyNoise · Censys · VirusTotal
🐛 Malware Analysis: Any.Run · Hybrid Analysis · EchoTrail
📘 Frameworks: MITRE ATT&CK · NIST Incident Response
📋 Ticketing & Reporting: JIRA · Confluence
⚙️ Scripting: PowerShell · Regex · Python (basic for log parsing)