SECURITY ANALYST 🧑‍💻

Serhii Tsybulnyk

- tsserg@protonmail.com 📨
- +38(096)038-01-55 📞

I have 2 year of entry experience as a SOC analyst. I have a strong understanding and experience with incident handling, log analysis and threat hunting. I have been involved in a full incident management lifecycle. My main domain is blue teaming, especially SIEM, but I am also familiar with penetration testing and have a basic experience as a manual QA.

🗣️ Languages 🗣️

- Ukrainian native
- English

🏢 Job experience 🏢

- CERT-UA SOC analyst - 2 year

> (Jul 2021 - Present)

🚨 Responsibilities 🚨

- Incident triage handling
- Detection rules implementing
- Incident report creating
- Communications with customers
- SIEM engineering (logs ingestion, normalization etc.)

🎓 Common skills 👨‍🎓

- Windows (Familiar with active directory, windows advanced audit)
- Linux (Installing and configuring services such as Apache, Bind, Nginx, etc.)

- TCP/IP stack
- Virtualization, Containerization (VMware, VirtualBox, Docker)

💻 Security systems 💻

- Firewall (iptables)
- IDS/IPS (Snort, Suricata, Security Onion, Zeek, Wazuh)
- Honeypot
- Sandbox (Trend micro, Any Run)
- SIEM (ELK, Splunk, QRadar, Logrhythm)
- Cisco network security (Firepower, Stealthwatch)
- EDR (Cisco AMP)

🕸️ Frameworks, utilities, and services 🕸️

- OSINT (Amass, Maltego, Foca, OSINT Framework, etc.)
- Forensic (Hayabusa, Chainsaw, Sigma, Volatility, BloodHound)
- Pentest (Nmap, Metasploit, Wireshark, Burp suit, etc.)
- Vulnerabilities scanners (Infection monkey, Core impact, Netsparker, rEngine, Nessus)
- Red Team (Atomic red team, Caldera, Empire, Unicorn, Metasploit, etc.)
- Online analysis services (VirusTotal, AnyRun, Shodan, DomainTools, ZoomEye, etc.)

📖 Cybersecurity standards (basic understanding) 📖

- ISO/IEC 2700X
- NIST SP 800

🧘 Other skills 🧘

- Programming languages (Python, C/C++)
- Scripting (PowerShell, Bash)
- QA manual testing

⚔️ Cybersecurity events ⚔️

- CTFs (“Fresh Blood», “OWASP CTF Kyiv”, etc.)
- Offline competition (“SANS netwars”, “INT20H”, “Cybexer blue team competition”, etc.)
- Online competition (“Splunk Boss Of the SOC”, “Tatanka 2022”, etc.)

🌠 Certificates and courses 🌠

- I-CSO
- CSA - EC-Council
- QA base / advance - ITEA
- Security analyst - Dubex
- Splunk Enterprise Security - Splunk
- GIAC Certified Detection Analyst (GCDA) SEC-555GIAC - SANS

🪀 Personal qualities 🪀

- Purposeful
- Humorous
- Responsible
- Able to learn quickly
- Friendly
- Punctual

🔗 Social networks 🔗

- LinkedIn