Paradise, Canada A1L 1G8 | +1 709 315-4480 | keepdsn@icloud.com |
WWW: https://www.linkedin.com/in/davniyson/ | **WWW:** https://github.com/keepdsn/cybersecurity-labs

ANTON IVANOV

PROFESSIONAL SUMMARY

Technically skilled IT professional transitioning into cybersecurity with 10+ years of experience in systems administration and technical support.
Hands-on practice in SOC monitoring, log analysis, incident response, and malware forensics. Adept in using tools like Splunk, Wireshark, Volatility, and Redline.
Fast learner with strong scripting (Python, Bash) and troubleshooting skills, seeking to contribute in an entry-level SOC Analyst role.

TECHNICAL SKILLS

- **Networking & Systems:** Windows Server (Active Directory, Group Policy), Windows 10/11 administration; network setup (TCP/IP, DNS, DHCP, VPN); basic Linux CLI; remote troubleshooting and support.
- **Tools:** Hands-on experience with security tools including SIEM (Splunk), Wireshark, Volatility, Redline, CyberChef, and OleVBA; working understanding of IDS/IPS systems and alerts.
- **Virtualization:** Experience with virtualization platforms (VirtualBox, VMware) for testing and sandboxing environments.
- **Cybersecurity:** Knowledge of SOC operations, security monitoring, log analysis, incident response, malware analysis basics, phishing detection, and OSINT techniques.
- **Programming & Scripting:** Python (automation scripts and data analysis), Bash, PowerShell; version control with Git/GitHub.

PROFESSIONAL EXPERIENCE

SYSTEM ADMINISTRATOR & TECHNICAL SUPPORT SPECIALIS 01/2012 to 09/2022
Private IT Business, Kerch, Ukraine

- Administered Windows-based IT infrastructure for small business clients, including user support, troubleshooting, data backups, and software installations, ensuring minimal downtime.
- Designed and implemented local networks (TCP/IP configuration, DNS/DHCP setup, router and switch configuration) to meet client requirements for connectivity and reliability.
- Provided timely technical assistance and resolved hardware/software issues to maintain smooth daily operations for end-users.
- Implemented cybersecurity measures such as antivirus deployment, regular patch management, and user access controls to protect client systems and data.

EDUCATION

:

- **TryHackMe:** Completed "Cybersecurity 101" and "SOC Level 1" learning paths, gaining hands-on experience in analyzing logs, investigating incidents, and using common SOC tools.
- **Blue Team Labs Online:** Ongoing practice with blue team challenges and incident response scenarios to enhance threat detection and analysis skills.
- **HackTheBox:** Solved multiple penetration testing and defense challenges to strengthen understanding of attacker techniques and system hardening methods.
- **Yandex Data Science & Python Bootcamp (400 hours):** Completed a 400-hour intensive training program focused on Python programming and data analysis
- **Cybersecurity Labs Repository:** Maintains a GitHub repository ("cybersecurity-labs") showcasing projects, scripts, and write-ups.

LANGUAGES

English
Professional Working

Ukrainian, Russian
Native or Bilingual