OLEKSII HLUSHKOV

Security Analyst

Education

2014-2019

NTUU KPI
Master in Cyber Security

Certifications

- CEH
- ECIH
- CySA+
- CHFI

Work Experience

SCPC SSSCIP | 2019-2022
SOC Engineer

- SIEM Splunk
- Data ingesting & normalization
- Incidents triage & investigation
- Logs analysis & correlation

Contact Me

- oleksii.hlushkov@gmail.com
- linkedin.com/in/oleksii-hlushkov-46a3a919a

About Me

I have been involved in cybersecurity for 4 years with 2 years of industry experience as a SOC Analyst. SIEM - is my best friend.
I have a good understanding of Linux and Windows environments, networking, and security principles. Familiar with network forensics, intrusion detection, and anomaly monitoring. I have also conducted cybersecurity training as my hobby since graduate school.
I am continuously improving my skills by participating in CTF competitions.

Expertise Skill

- SIEM (Splunk preferred)
- Splunk Enterprise Security
- Threat Intelligence
- Threat Hunting
- Network Forensics
- Windows Forensics

Standards

- MITRE ATT&CK
- MITRE DEF3ND
- SIGMA
- NIST CSF
- CIS 20

Language Skill

- Ukrainian
- English
- Russian