Oybek Turaev

[LinkedIn](#) | [Github](#) | oybekturaev.cs@gmail.com

SUMMARY

Cybersecurity MSc Student (Erasmus Mundus CYBERUS) with a background in Software Engineering and certifications CompTIA CySA+, Security+, and Hack The Box CDSA (Exam completed, results pending). Hands-on in SOC operations, Threat Hunting, and Incident Response, with 175+ HTB Academy challenges, 21+ Hack The Box machines, 5 Splunk BOTS APT hunts, and ongoing HTB Sherlocks (GitHub). Skilled in SIEMs (Splunk, ELK), Network Security, Digital Forensics, MITRE ATT&CK and Automation (Python, Bash, PowerShell). Currently seeking internship opportunities in SOC, Threat Hunting, or Incident Response.

EDUCATION

MSc in Cybersecurity (Erasmus-Mundus Joint Master Program) — European Union
CYBERUS–Joint Masters, University of Southern Brittany, University of Luxembourg, and TalTech — *Sep 2024 – Present*

BSc in Software Engineering — Bishkek, KG
American University of Central Asia, Full-Ride Scholarship, GPA - 3.86/4.0 — *Sep 2020 – Jun 2024*

PROFESSIONAL CERTIFICATES

CompTIA CySA+ (*ID: S2WFPY1Q6B4Q1WKK*)
CompTIA Security+ (*ID: LG84WV3RKEF11597*)
HTB (Hack The Box) Certified Defensive Security Analyst (CDSA) (*Exam Completed, results pending*)

PROFESSIONAL EXPERIENCE

Cybersecurity Teaching Assistant — Sep 2024 – Present
Amazon Cybersecurity Program, Correlation One — *Remote, Part-Time (Based in U.S.)*
- Delivered sessions on Endpoint Security, SIEM (Splunk), Incident Response to 40+ learners.
- Conducted practical labs on Network Forensics, Discovery: Wireshark, Snort(IPS/IDS), Nmap
- Assisted participants to work with security standards (ISO 27001, NIST, GDPR).

SOC Research Intern — Jun 2025 - August 2025
University of Southern Britanny — *Lorient, France*
- Completed 175+ HTB Academy challenges, 21+ Hack The Box machines, 25 Bash script challenges, building SOC, Threat Hunting, Incident Response and Scripting skills.
- Analyzed Windows Logs with Sysmon/ETW for DLL Hijacking, Powershell Injection, .NET assembly loading
- Conducted 5 Splunk BOTS APT hunts, Solved 6+ HTB Sherlocks (ongoing), applying SIEM&Adversary techniques.

QA Analyst Intern — Jun 2022 – Sep 2022
Eurosoft Company — *Tashkent, UZB*
- Contributed to implement OWASP & MASVS compliance standards for 4 web applications: *Avlo Shop, etc*
- Implemented Dynamic Testing using JUnit for Java-based projects and DOCTEST for C++ projects using Docker
- Conducted security hardening on Linux-based systems.

Cyber Security Analyst Intern — Jun 2021 - Sep 2021
Verzeo Company — *Remote, India*
- Assisted in 7+ security testings and threat assessments, contributing to vulnerability identification and mitigation
- Utilized Wireshark, Nessus, and Splunk for anomaly detection and investigation, reducing phishing threats.
- Contributed to the implementation of ISO 27001, NIST CSF for network security compliance in multi-cloud env

TECHNICAL SKILLS

Threat Detection & SIEM: Splunk, ELK Stack, Wireshark, Suricata, Zeek
Frameworks & Standards: MITRE ATT&CK, ISO 27001, GDPR, NIST
Tools: Docker, Snort, Nessus, Nmap, Git
Scripting & Programming: Bash, PowerShell, Python, Java, C++

PROJECTS & ACHIEVEMENTS

Best Graduate 2024: Steven F. Shea Excellence Award, U.S.-CAEF Program
Research Project: Enhancing SOC Threat Detection Through Simulated Incidents (documented in GitHub)
Competitive Programming: 350+ coding problems (Java/C++) on UVA/LeetCode; 25+ Bash scripts on Exercism.
Cybersecurity Project Leader: U.S. Embassy–funded awareness initiative ($4.7K).

LANGUAGE SKILLS

English: C1-Advanced **Russian**: C1-Advanced **French**: B2-Independent