

# Oybek Turaev

[LinkedIn](#) | [Github](#) | [oybekturaev.cs@gmail.com](mailto: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, 18+ 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

<b>MSc in Cybersecurity (Erasmus-Mundus Joint Master Program)</b>	European Union
<i>CYBERUS-Joint Masters, University of Southern Brittany, University of Luxembourg, and TalTech Sep 2024 – Present</i>	
<b>BSc in Software Engineering</b>	Bishkek, KG
<i>American University of Central Asia, Full-Ride Scholarship, GPA - 3.86/4.0</i>	<i>Sep 2020 – Jun 2024</i>

## 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

<b>Cybersecurity Teaching Assistant</b>	Sep 2024 – Present
<i>Amazon Cybersecurity Program, Correlation One</i>	<i>Remote, Part-Time (Based in U.S.)</i>
<ul style="list-style-type: none"><li>Delivered sessions on Endpoint Security, SIEM (Splunk), Incident Response to 40+ learners.</li><li>Conducted practical labs on Network Forensics, Discovery: Wireshark, Snort(IPS/IDS), Nmap</li><li>Assisted participants to work with security standards (ISO 27001, NIST, GDPR).</li></ul>	
<b>SOC Research Intern</b>	Jun 2025 - August 2025
<i>University of Southern Brittany</i>	<i>Lorient, France</i>
<ul style="list-style-type: none"><li>Completed 175+ HTB Academy challenges, 18+ Hack The Box machines, 25 Bash script challenges, building SOC, Threat Hunting, Incident Response and Scripting skills.</li><li>Analyzed Windows Logs with Sysmon/ETW for DLL Hijacking, Powershell Injection, .NET assembly loading</li><li>Conducted 5 Splunk BOTS APT hunts, Solved 5+ HTB Sherlocks (ongoing), applying SIEM&amp;Adversary techniques.</li></ul>	
<b>QA Analyst Intern</b>	Jun 2022 – Sep 2022
<i>Eurosoft Company</i>	<i>Tashkent, UZB</i>
<ul style="list-style-type: none"><li>Contributed to implement OWASP &amp; MASVS compliance standards for 4 web applications: <i>Avlo Shop, etc</i></li><li>Implemented Dynamic Testing using JUnit for Java-based projects and DOCTEST for C++ projects using Docker</li><li>Conducted security hardening on Linux-based systems.</li></ul>	
<b>Cyber Security Analyst Intern</b>	Jun 2021 - Sep 2021
<i>Verzeo Company</i>	<i>Remote, India</i>
<ul style="list-style-type: none"><li>Assisted in 7+ security testings and threat assessments, contributing to vulnerability identification and mitigation</li><li>Utilized Wireshark, Nessus, and Splunk for anomaly detection and investigation, reducing phishing threats.</li><li>Contributed to the implementation of ISO 27001, NIST CSF for network security compliance in multi-cloud env</li></ul>	

## 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