CONTACT

+355696838553
adrianolleshi1@gmail.com
https://www.linkedin.com/in/adrianolleshi/
Tirana, Albania

EDUCATION

Master's Degree Information and Communication Technology University of Tirana
2018-2020

Bachelor's Degree Information and Communication Technology
University of Tirana
2015-2018

LANGUAGES

English B2/C1
Italian A2

CERTIFICATIONS

- EC-Council Certified Incident Handler (ECIH)
- Computer Hacking Forensic Investigator (CHFI) - EC-Council (ECC3601745982)
- CompTIA Security+ ce (COMP00122143091)
- Threat Hunter OSTH – OffSec (139732112)
- ISO/IEC 27001 Lead Auditor – PECB (ISLA1123395-2024-02)
- Ethical Hacking Essentials (EHE)- EC-Council
- Digital Forensics Essentials (DFE) - EC-Council (3683264273596)
- Industrial Control System ICS Cybersecurity Lab 301L - Cybersecurity and Infrastructure Security Agency

ADRIANO LLESHI

Cybersecurity professional with extensive expertise in incident response, malware analysis, and digital forensics. Vast experience in overseeing advanced Threat Intelligence initiatives, Purple Team adversary simulation exercises, and investigations in the dark web. Certified in ISO 27001 Lead Auditor, Threat hunting, and Ethical hacking, along with practical knowledge in SIEM, OSINT, and ICS security.

WORK EXPERIENCE

Cyber Security Consultant
Axiom Breach June 2024- Present

Responsible for adversary simulation, penetration testing, advanced TTPs, threat intelligence, threat hunting, and incident response to assess and enhance organizational security posture.

Head of Cyber Security Analysis
National Authority for Cyber Security
Tirana, Albania July 2024- Present

- Conducted advanced malware analysis and forensics to strengthen security.
- Directed Threat Intelligence operations and coordinated NATO cyber exercises.
- Implemented the National Security Operations Center (NSOC) and CSIRT Albania, integrating both open-source tools (ELK, Security Onion, Wazuh, MISP) and commercial technologies (Microsoft Azure, Microsoft Sentinel) to provide a unified national cybersecurity monitoring and response platform.
- Integrated open-source tools into Albania's Cyber Simulation Lab, enhancing defense training. *Trainer of the trainers* on these trainings for all Western Ballkans Critical Infrastructure Operators.

Head of Malware analysis and Digital Forencisc (Purple Team)
National Authority Cyber Security

Tirana, Albania April 2023- July 2024

- Investigated national-level cyber incidents, identifying sources, methods, and preventing future attacks.
- Led Purple Team exercises with adversary simulation to test and improve defense capabilities.
- Conducted malware analysis and digital forensics to track attackers and strengthen security.

Cybersecurity Trainer
Protik | CyberTiranaAL3 Program Sep 2023 – June 2024

Delivered hands-on trainings, CTFs, and cyber drills in Red Team vs. Blue Team scenarios, covering a full range of cybersecurity topics including: *Linux for Hackers, Cyber Attack Process, Security Bypass Methods, OSINT & Social Engineering, Cyberdefensive Monitoring (SIEM, IDS/IPS, EDR), Advanced Pentesting & Privilege Escalation, Infrastructure & Web Application Pentesting (Projects 2–4), and practical labs on TryHackMe.*

Incident Response Specialist
National Authority for Cyber Security

Tirana, Albania July 2019-April 2023

- Monitored, analyzed, and responded to cyber threats and incidents.
- Conducted audits in CII- ensuring compliance with ISO/IEC 27001.
- Provided expertise to CII in mitigating vulnerabilities and defending against emerging threats.

ACHIEVEMENTS

- **1ST Place in Global Cyber Drill GISEC 2024**
- **1ST Place in the Balkans Live-Fire Cybersecurity**
- **Exercise 2025 1ST Place – Western Balkans Cyber Drill**

SKILLS

Incident Response	Malware Analysis	Penetration Testing	Microsoft Defender for Endpoint
Information Security Management	Digital Forensics	Microsoft Sentinel, MDE	Dark Web Investigation, Bitcoin tracking
Vulnerability Assessment	Open-Source Intelligence (OSINT) techniques	Reverse Engineering	Threat Intelligence – SocRadar, Recorded Future, Luminar, ReSecurity

Incident Reports

- https://aksk.gov.al/wp-content/uploads/2024/04/File-analysis-of-cyber-attacks.pdf
- https://aksk.gov.al/wp-content/uploads/2024/04/Analysis-of-Homeland-Justice-Attack-Files-That-Impacted-Infrastructure-in-R.Alb_.pdf
- https://aksk.gov.al/wp-content/uploads/2024/12/Profile-of-Russian-Hacker-Groups.pdf

Prevented Incident Reports

- https://aksk.gov.al/wp-content/uploads/2024/04/Hacker-Groups-impacting-the-Region.pdf
- https://aksk.gov.al/wp-content/uploads/2024/04/Technical-analysis-for-REMCOS-RAT-malicious-file.pdf
- https://aksk.gov.al/wp-content/uploads/2024/04/Spear-Phishing_Malware-analysis-kurs-trajnimi.zip-ScreenConnectWindows.pdf
- https://aksk.gov.al/wp-content/uploads/2024/04/Iranian-Hacker-Groups-Profiles-v1.0_ENG.pdf

Malicious file analysis

- https://aksk.gov.al/wp-content/uploads/2024/05/AgentTesla-Malware-Technical-Analysis-_v1.0.pdf
- https://aksk.gov.al/wp-content/uploads/2024/05/Guloader-Malware-Technical-analysis-_v1.0.pdf
- https://aksk.gov.al/wp-content/uploads/2024/06/Redline-Malware-Technical-Analysis-_v1.0.pdf
- https://aksk.gov.al/wp-content/uploads/2024/09/CrowdStrike-Phishing-Campaign-Analysis.pdf
- https://aksk.gov.al/wp-content/uploads/2024/07/Email-Phishing-Campaign_Konfirmimi-i-regjistrimit-te-marre-1.pdf
- https://aksk.gov.al/wp-content/uploads/2024/07/Phishing-campaign-by-Muddy-Water-1.pdf
- https://aksk.gov.al/wp-content/uploads/2024/12/Technical-Analysis-of-the-Malicious-File-Gootloader.pdf
- https://aksk.gov.al/wp-content/uploads/2024/09/Technical-analysis-for-the-file-GIBANJ-SHIPMENT-LIST-1.pdf
- https://aksk.gov.al/wp-content/uploads/2025/01/Lockbit-4.0-en-2.pdf
- https://aksk.gov.al/wp-content/uploads/2025/01/Analysis-for-the-Remittance-Advice-file.pdf
- https://aksk.gov.al/wp-content/uploads/2025/03/HIDDEN-IN-THE-STARS-CVE-2017-11882-EN.pdf
- https://aksk.gov.al/wp-content/uploads/2025/04/Technical-analysis-for-the-Remcos-Rat-malicious-file-Spear-Phishing-Attempt.pdf
- https://aksk.gov.al/wp-content/uploads/2025/05/Technical-analysis-for-the-malicious-file.pdf
- https://aksk.gov.al/wp-content/uploads/2025/07/Technical-Analysis-of-the-Malicious-File-Display10.pdf
- https://aksk.gov.al/wp-content/uploads/2025/07/Lumma-Stealer-english.pdf
- https://aksk.gov.al/wp-content/uploads/2025/09/Malware-analysis-and-reverse-engineering-of-Online-Seminar.FM_.gov_.om_.doc.pdf