PERSONAL INFORMATION

Adriano Lleshi

Papa Gjon Pali II, Floor II

adrianolleshi1@gmail.com

+355 69 6838 553

Sex Male | **Date of birth** 06/08/1996 | **Nationality** Albanian

PROFESSIONAL SUMMARY

Expert in cyber incident management with deep experience at Albania's National Cyber Security Incident Response Team. Specialized in the identification, assessment, and resolution of cyber incidents, along with malware analysis and digital forensics. Demonstrated abilities in responding to high-stress incidents, ensuring the implementation of best practices and quick solutions to protect national critical infrastructure.

With a strategic and analytical approach, I have contributed to strengthening cyber defense and increasing awareness of cyber security importance. Dedicated to continuous improvement of security processes and practices, staying at the forefront of new technologies and methodologies in cyber security.

EDUCATION

15/10/2018–17/07/2020	**Master degree in Information and Communication Technology (ICT)** Faculty of natural Sciences, University of Tirana - Tirana (Albania)
22/10/2015–19/07/2018	**Bachelor degree in Information and Communication Technology (ICT)** Faculty of natural Sciences, University of Tirana - Tirana (Albania)

WORK EXPERIENCE

16.02.2024– Present	**Director – Directorate of Cyber Security Analysis | National Authority on Electronic Certification and Cyber Security, Prime Minister Office** ● Incident Response Coordination: Lead the incident response team in identifying, investigating, and handling cybersecurity incidents. Ensure all incidents are reported and managed effectively and in accordance with response protocols. Malware Analysis and Digital Forensics: Direct in-depth technical investigations to analyze malware and conduct digital forensic analyses to identify the sources and methods of attacks, as well as to reconstruct the activities of cyber-attacks happened on Critical and Important Infrastructures in Albania. ● Procedure Development and Improvement: Create, review, and continuously improve security procedures and practices to ensure an effective and coordinated response to security incidents. ● Reporting and Analysis: Prepare and present analytical reports and incident summaries to inform and guide the strategic decision-making of stakeholders and senior management. ● Stakeholder Education and Training: Develop and implement training

programs to raise cybersecurity awareness and improve incident response capabilities across the organization.

Team Management: Recruit, train, and develop a dedicated team of security professionals, including mentoring and supporting the professional development of team members.

● Inter-organizational Collaboration: Build and maintain relationships with other organizations, governmental institutions, and third parties for the exchange of information and best practices in the field of cybersecurity. Contribute to the preparation of legal and by-laws in the field of security cyber, as well as within the scope of AKCESK's activity.

Monitors the work of dependent employees and ensures the qualification of employees, for enabled the highest level of professionalism that the implementation requires NATO standards in the field of cyber security.

Apr 2023 – 16.02.2024	**Head of Malware analysis and Digital Forensics (Purple Team) | Cyber Security Incident response Team at National Authority on Electronic Certification and Cyber Security, Prime Minister Office**
(Full-time)	● Analyze cyber incidents occurring at the national level and help identify the sources, goals, and methods of attacks. Develop advanced strategies and policies to prevent cyber-attacks and protect the country's cyber infrastructure. Coordinate the necessary actions to investigate and handle cyber incidents efficiently.

● Auditing the CI and CII for implementation and regulation on the content and method of documenting security measures ISO 27001. Conduct audits of the Information Security Management Systems (ISMS) for *over **30 Critical and Important Infrastructures in Albania** (**More than 600 hours**)*, adhering to the provisions outlined in Albania Law Nr. 02/2017:
(https://cesk.gov.al/wp-content/uploads/2023/07/ligj-2017-01-26-2.pdf) and the Regulatory Framework for Security Measures:
(*https://cesk.gov.al/wp-content/uploads/2023/09/Rregullore-e-masave-te-sigurise-1.pdf*). This regulatory framework is aligned with ISO/IEC 27001 and incorporates best practices recommended by ENISA. Defend incidents that could occur, the latest vulnerabilities, recommended security measures that Critical and Important Information Infrastructures will provide. Assistance in recommendations, cyber security measures, incident response for the latest vulnerabilities that happened.
● Part of many Cyber Ranges and tabletop exercises where their purpose was the aspect of cyber security and the methods to be implemented to ensure, catch the flag, etc.

02/07/2019 – April 2023	**Expert | Cyber Security Incident response Team at National Authority on Electronic Certification and Cyber Security, Prime Minister Office**
(Full-time)	● Defend incidents that could occur, the latest vulnerabilities, recommended security measures that Critical and Important Information Infrastructures will provide. Assistance in recommendations, cyber security measures, incident response for the latest vulnerabilities that happened.

Auditing the CI and CII for implementation and regulation on the content and method of documenting security measures ISO 27001. Have been for 3 years those audits.
● Part of many Cyber Ranges and tabletop exercises where their purpose was the aspect of cyber security and the methods to be implemented to ensure,

catch the flag, etc.

01/02/2022 – 01/04/2022
(Part-time)

Web developer mentor at From0ToHero - Albania

● Tutoring university students subjects like mastering WordPress site.
Teaching ftp connections, phpMyAdmin, managing and configuration of domains, SSL configurations, SEO - their explanation, tricks through keywords to be displayed in the first rank in google, cloud hosting, security for webpages and methods of protection against attacks that are most present across WordPress pages.

01/02/2019 – 02/05/2019
(Internship)

Software Developer Internship at ALBtelecom Sh.a – Tirana (Albania)

● Have individual projects which are located on the website, touch, design in C#, as well as the database for the data specified in SQL Server. The tasks performed during the teaching practice are as follows:

-Microsoft C# 4.5 -Web Application Development with MVC, C# and .Net 4.5

-Web Service Development with C# and .Net 4.5 Basics

-Database Design

PROJECTS

09/2019 – 02/2020 Transnational Threats Department Cyber/ICT Security OSCE. Successfully completed the OSCE e-learning course on OSCE Cyber/ICT security Confidence-Building Measures

10/07/2022 – 15/07/2022

Regional Cybercrime Exercise on a Ransomware Attack.

I increase the knowledge on investigating Ransomware attacks and secure electronic evidence; Digital Forensics; Knowledge on effective and balanced access to data, search, seize and confiscate cybercrime proceed, prevent money laundering on the Internet. Investigate Ransomware with digital forensics, analyzing pay page and identify ransomware steps. OSINT for suspects. Find exploits about pay page, negotiate with hackers. Cryptocurrencies, Production Orders and blockchain investigations with blockchain explorer like: graphsense.info, blockchain.com, etherscan.io, chainanalysis.com, elliptic.co, scorechain.com, ciphertrace.com. Seize bitcoin address after investigating it and follow the flow of the money where they go, procedure with Interpol for crypto exchanges platforms and identify the hacker.

04/07/2022 – 08/07/2022

Interagency and international cooperation on Cyber-attacks. 04 July 2022 – 08 July 2022. I developed 1) professional skills to detect and investigate cybercrime, while using online investigation methods and 2) techniques, to enhance co-operation with cyber-crime experts. Learn for Cybercrime Threat Landscape, Cyber Attacks, Investigative techniques, search & seizures, criminal procedure, cryptocurrencies, Tracing blockchain transactions, OSINT tools techniques and methods, Basics of Malware Analysis, Deep and dark web investigation, Ransomware example that have completed successfully with the findings and the recommendations, Advanced OSINT tools, Cyber Attacks relation to deep and dark web. Certified in successfully participated in this course.

09/2019 – 02/2020 Build a lot of websites, e-commerce's: artmadeofficial.com, desa.al, movimento.al, blagflowers.com, focusarchitecture.al, biocare.al, duamakine.com. Also take care of the security of these sites to be safe from cyber attacks

04/2019 – 07/2019 Developed ransomware attack example, implementing it with a backdoor malware that was generated with a phishing attack from the business mail account. After that also are explain the recommendation security measures against those attacks.

05/2018 – 07/2018 Developed a job seeker portal on a web platform which helps users to find a job easily and helps companies to post a job position. Inspired by Glassdoor.

01/2018 – 04/2018 Developed a desktop app which facilitates the way how busy people and businesses maintain their schedule.

02/2017 – 08/2017 Developed many informative websites such as personal website, media, educational, portfolio and a few other websites for local businesses.

SKILLS

• **Incident Response** (Information security analyst, cybersecurity on Cloud Computing, network security, vulnerability assessment, IT audit consultant, Junior Pen Tester, Security Awareness, Social Engineering)

• **Web Development** (Visual Design, Brand Design, UI design, Web design, Php WordPress and Laravel)

• **Programming** (Html, JavaScript, CSS, C# WinForms & Asp.Net, MVC)

• **Databases** (SQL Server, Oracle, MySQL)

• **APIs** (REST APIs, Postman)

• **Modern Development Tools** (Gitlab, GitHub)

• **Software Development Methodologies** (Agile, Scrum, Waterfall)

• **Operating Systems** (Kalilinux, windows, CentOS, Ubuntu, LinuxOS)

- **IDEs** (VS Code, Sublime, Visual Studio)
- **Documentation** (Draw.io, UML Diagrams, Prezi, MS Office, Google package)
- **Digital Image Processing** (Photoshop CC, Canva)
- **Social Marketing** (Marketing strategy, SEO strategy, Facebook / Instagram Ads)
- **Soft Skills** (Communication, quick learning, problem solving, logical thinking, critical thinking, leadership, adaptability, teamwork, work ethic)

LINGUISTIC PROFICIENCY

	Listening	**Reading**	**Speaking**	**Writing**
Albanian	Native	Native	Native	Native
English	C1	B2	B2	B2
French	A2	A2	A2	B1
Italian	A2	A2	A2	A2