Armend Salihu, MSc

To Whom It May Concern,

It is my distinct pleasure to provide this letter of recommendation for Bujar Nolji, born on 19 Sep. 2006, who has successfully completed our intensive Cybersecurity Training Program. This comprehensive course consisted of 40 structured sessions (totaling 120 Academic Hours) and was rigorously designed to align with the **CompTIA Security+ (SY0-701)** certification framework.

Bujar, has demonstrated exceptional dedication in mastering a curriculum that blends theoretical depth with high-impact practical application. By mirroring the SY0-701 objectives, the student has acquired a modern, industry-standard understanding of the current threat landscape and security architecture.

Core Competencies & SY0-701 Alignment
Throughout the program, Mr. Nolji established a robust foundation in the General Security Concepts domain. They demonstrated a strong command of the CIA triad, Risk Management, and Governance, Risk, and Compliance (GRC). The training emphasized modern architectural principles, including Zero Trust and Secure by Design, while ensuring familiarity with internationally recognized frameworks such as NIST and ISO/IEC 27001.
Technical Proficiency & Tooling
The student's technical skillset is broad and practical, covering both defensive (Blue Team) and assessment operations. They have demonstrated proficiency in:

- **Security Operations:** Leveraging SIEM platforms, IDS/IPS, and EDR/XDR solutions (including **Wazuh**) for continuous monitoring and threat detection.
- **Vulnerability & Threat Analysis:** Utilizing tools like **Nmap (NSE), Nikto,** and **Maltego CE** to identify and assess risks.
- **Adversarial Tactics:** Analyzing attack vectors and the Cyber Kill Chain through simulated scenarios using **Metasploit, SQLMap,** and **Ettercap**.
- **Forensics & Investigation:** Conducting digital forensics and memory analysis using **Volatility** and **Autopsy**.

Operational Readiness
Beyond technical skills, the curriculum focused on the "Security Program Management" domain of the SY0-701 exam. Bujar Nolji was trained in incident response planning, disaster recovery, business continuity, and professional reporting. They have shown professional maturity in stakeholder communication, breach notification procedures, and technical interview readiness.
Based on the discipline, technical aptitude, and comprehensive knowledge demonstrated throughout this program, I confidently recommend mr. Nolji for entry-level cybersecurity roles, IT Support, or further advanced professional development in the field.

Sincerely

□LETËR REKOMANDIMI

Të nderuar,

Kam kënaqësinë e veçantë të ofroj këtë letër rekomandimi për Bujar Nolji, I lindur me 19.02.2006, ka përfunduar me sukses Programin tonë intensiv të Trajnimit në Siguri Kibernetike. Ky kurs gjithëpërfshirës përbëhej nga 40 sesione të strukturuara (në total 120 orë akademike) dhe ishte dizajnuar me rigorozitet për t'u harmonizuar me kornizën e certifikimit **CompTIA Security+ (SY0-701)**.

Përgjatë trajnimit, Bujari dëshmoi një përkushtim të jashtëzakonshëm në përvetësimin e kurrikulës, e cila gërsheton thellësinë teorike me aplikimin praktik të nivelit të lartë. Duke ndjekur objektivat e SY0-701, Bujari ka fituar një kuptim modern dhe të standardizuar sipas kërkesave të industrisë mbi peizazhin aktual të kërcënimeve kibernetike.

Kompetencat Kryesore dhe Baza Teorike Gjatë programit, z. Nolji ndërtoi një themel të fortë në konceptet thelbësore të sigurisë, duke përfshirë triadën CIA, Menaxhimin e Riskut dhe Qeverisjen (GRC). Trajnimi theksoi rëndësinë e arkitekturave **Zero Trust** dhe parimeve **Secure by Design**, duke siguruar gjithashtu njohuri mbi kornizat e njohura ndërkombëtare si NIST dhe ISO/IEC 27001.

Aftësitë Teknike dhe Përdorimi i Veglave Aftësitë teknike të studentit janë të gjera dhe praktike. Ai ka demonstruar kompetencë në përdorimin e veglave standarde të industrisë,

duke përfshirë:

- **Operacionet e Sigurisë (Blue Team):** Përdorimi i platformave SIEM, sistemeve IDS/IPS dhe zgjidhjeve EDR/XDR për monitorim të vazhdueshëm.
- **Analiza e Cenueshmërisë dhe Kërcënimeve:** Përdorimi i veglave si **Wazuh, Nmap (NSE), Nikto** dhe **Maltego CE** për identifikimin dhe vlerësimin e rreziqeve.
- **Taktikat Sulmuese (Simulim):** Kuptimi i vektorëve të sulmit dhe "Cyber Kill Chain" përmes skenarëve të simuluar duke përdorur **Metasploit, SQLMap** dhe **Ettercap**.
- **Forenzika dhe Reagimi:** Kryerja e forenzikës digjitale dhe analizës së memories duke përdorur **Volatility** dhe **Autopsy**.

Gatishmëria Operacionale Përtej aftësive teknike, kurrikula u fokusua edhe në fushat e sigurisë operacionale, duke përfshirë planifikimin e reagimit ndaj incidenteve (Incident Response), rikuperimin nga fatkeqësitë (Disaster Recovery) dhe vazhdimësinë e biznesit. Bujari tregoi pjekuri profesionale në komunikimin me palët e interesuara dhe në përgatitjen e raporteve teknike.

Bazuar në njohuritë, aftësitë praktike dhe disiplinën e treguar gjatë këtij programi, unë rekomandoj me besim të plotë Bujar Nolji, për role fillestare (entry-level) në siguri kibernetike, IT Suport, praktika profesionale (internships), ose për zhvillim të mëtejshëm akademik e profesional në këtë fushë.

Me respekt

LinkedIn: www.linkedin.com/in/asalihu mail: armend.salihu@outlook.com tel: +383 45 504 255 +1 202 570 4072