REZA AHMAD NUGROHO

rezaahmadnugroho@gmail.com • (+62) 822 2984 3105 • no0g.github.io • South Jakarta, Indonesia • Indonesian

SOC Lead and Security Analyst with certifications for both Blue Teaming and Red Teaming. Experienced with SIEM, Security Operations, Penetration Testing engagement, Incident Handling, Security Policy and IT security in general.

EXPERIENCE

L2 Security Analyst/SOC Team Lead, Protergo **Apr 2022 – Present**

- Perform Deep Analysis with SIEM and other supporting tools (WireShark, SOCradar, VirusTotal)
- Oversees up to 20+ clients SIEMs and T1 analysts
- Maintaining up to 90% asset/network visibility by making sure SIEM is in good health
- Making sure SIEM is up to date with the latest detection signature for IDS and vulnerability detection for Vulnerability Assesment
- Provide support, technical problem solving and analysis for Enterprise XDR and Firewall solution
- Managing Resources Maintain SOC Analyst KPI based on SLA
- Plan and Develop SOC-related products and processes

Security Analyst, Protergo **Sep 2021 – Apr 2022**

- Perform security monitoring and reporting of clients' network
- Utilized AlienVault USM SIEM technology
- Deliver possible solutions and mitigations against existing threats to client

SOC Tier 1 Analyst, Asia Pacific University **Mar 2020 – Jul 2020**

A hands-on program as SOC analyst. Was part of APU Cyber Security Undergraduate program.

- Perform security monitoring and reporting of APU network
- Utilized MSSGARD as NextGen SIEM

PROFESSIONAL CERTIFICATION

(eJPT) eLearnSecurity Junior Penetration Tester, eLearnSecurity **7593150**

(NSE 3) Network Security Expert Level 3: Certified Associate, Fortinet **ohn1Y8lc73**

EDUCATION

Asia Pacific University | Staffordshire University, BSc (Hons) Cyber Security **CGPA 3.7, First Class**

Final Year Project: APU H4CKVERSITY, Hacking learning platform for universities – **GPA 4,0**

SKILLS

- Offensive Security: Network, and Web App Penetration Testing, Vulnerability Assesment, Basic Exploit Development
- Digital Forensics: Malware Analysis, Reverse Engineering, and Data Recovery
- Cybersecurity Consulting: Analysis on Cybersecurity Control implementation and Cybersecurity Gaps based on Existing Infrastructure
- Security Operations: SIEM, Threat Intelligence and Hunting, Detection Engineering, SOC Resource Management, Incident Handling and Response
- Scripting, Programming & Tools: C, Python3, Bash, SQL, Javascript (NodeJS), PHP, OpenVPN, Virtualization (VMware, VirtualBox), Git

ACHIEVEMENTS

Gold Medalist and Best Video Award Virtual Innovation Competition 2021, UiTM Kelantan, Malaysia **2021**

First Place APU Internal CTF 2021, APU Forensics and Security Research Center Student Section, Malaysia **2021**

Runner-up Regional Cyber Challenge 2019, Cyber8Labs and Silensec, Australia **2019**