Gerard Vince I. Lillo

+639192313175 | gerardvince.lillo@gmail.com |
https://www.linkedin.com/in/gerard-vince-lillo | https://gerardvincelillo.com

PROFESSIONAL SUMMARY

A results-driven cybersecurity professional with expertise in cloud security, DevSecOps, and penetration testing. Proven track record of automating security processes, securing cloud infrastructure on AWS, and enhancing threat detection. A certified eJPT holder passionate about applying development skills to build resilient and secure systems.

EXPERIENCE

Cloud Ready Technologies Corp.
Full-time | 2 years 3 months

- **Security Engineer |** May 2025 - Present
  - Built a CI/CD security pipeline using Bitbucket, Python, and Trivy to automate vulnerability scanning and Jira ticket creation.
  - Deployed Trend Micro File Storage Security (FSS) in AWS via CloudFormation, implementing an automated S3 malware scanning workflow (Scan, Clean, Quarantine buckets).
  - Administer Bitdefender GravityZone across 400+ endpoints, managing security policies, whitelisting/blacklisting, and delivering periodic security audit and MDR reports to clients.
  - Conducted cloud security posture assessments using Plerion and Prowler to scan AWS accounts, analyze vulnerabilities, and develop remediation strategies.
- **Security Analyst** | July 2024 - April 2025
  - Monitored, triaged, and responded to security alerts from multiple client environments using Vision One and Splunk, analyzing Indicators of Compromise (IoCs) to neutralize threats.
  - Authored weekly security health reports for clients, detailing malware detections, endpoint agent status, and compliance with security policies.
  - Provided actionable security recommendations to clients, including system upgrade advisories, policy enforcement, and threat mitigation plans.
- **Software Engineer** | January 2024 - July 2024
  - Developed Python-based log parsers to automate the processing of security alerts and integrate them with Jira, improving SOC analyst efficiency.
  - Utilized AWS services (Lambda, S3, SQS, EC2) to build and host serverless automation tools for security operations.
  - Configured and secured Wazuh and Graylog log management instances on EC2, restricting access via VPCs and security groups.

EDUCATION

University of Nueva Caceres
Bachelor of Science in Information Technology | 2019 - 2023

- Relevant coursework: Cybersecurity, Networking, Programming, Virtualization

TECHNICAL SKILLS

- **Cloud:** AWS (CloudFormation, Lambda, S3, EC2, CloudWatch, SQS, VPC)
- **Security Tools:** Splunk, Plerion, CrowdStrike, Trivy, Wazuh, Graylog, Burp Suite, Metasploit, Nmap, Bitdefender, Vision One
- **Languages:** Python
- **DevOps & Version Control:** Bitbucket, Git
- **Operating Systems:** Linux, Kali Linux

CERTIFICATIONS

- eJPT (eLearnSecurity Junior Penetration Tester)
- ICSI CNSS Certified Network Security Specialist
- IBM Cybersecurity Analyst
- GravityZone Cloud MSP Security Technical Specialist