

VINCE ADRIAN DE MESA

CYBER SECURITY PROFESSIONAL

CONTACT

Calamba Laguna Philippines
(+63)9959234327
dvinceadrian.17@gmail.com

EDUCATION

**BACHELOR OF SCIENCE IN
COMPUTER ENGINEERING •**
JUNE 2015-JUNE 2020

Lyceum of the Philippines University

CERTIFICATION

Certified Ethical Hacker •
November 2022 • ECC0521768934

Qualys Certified Specialist •
May 2022

**AWS Certified Cloud Practitioner
(CLF-C01) •**
December 2022 •
E9WFGPJ1SE1QQ1G2

KEY SKILLS

Vulnerability Management
Risk Assessment
Malware Analysis
Security Awareness Training
Penetration Testing
Mitigation Strategies

PROFILE

Dedicated professional experienced in performing vulnerability and risk assessments to ensure the security of new and existing technologies. Also, a security professional that continues to develop skills to adapt to the new and evolving threats that will exist.

EXPERIENCE

**VULNERABILITY AND PATCH MANAGEMENT
ENGINEER • SEPTEMBER 2023 - PRESENT**

Alumni Inc.

Roles and Responsibility:

- Plan, develop, configure, and executes vulnerability scans using Qualys toolset on a wide range of information systems both on-premises and cloud based.
- Collects and aggregates information and provides reports to customers.
- Effectively collaborates and communicates with Compliance, Internal Audit the Business teams and others to identify analyze and communicate risk and provides support around vulnerability management within their business requirements.
- Identifies, develops, and implements mechanisms to detect vulnerabilities and how they may lead to corporate incidents to enhance compliance with and support of security standards and procedures.
- Responds to tickets and incidents in a proactive manner.

Skills and Abilities:

- Performs Vulnerability Assessment, Security Awareness Trainings, and Penetration Testing.
- Use tools such as Qualys, Knowbe4, and NodeZero.

SOLUTIONS HANDLED

Qualys
Knowbe4
NodeZero
Acunetix
Burpsuite
OwaspZAP

SECURITY SOLUTIONS ENGINEER • MAY 2022 –
SEPTEMBER 2023

Next Generation Technologies Global Inc.

Contributions:

1. Security Team Lead for Blue Team

- Primary Contact for Blue Team Qualys Projects.
- Primary responsible for overseeing and evaluating the team members.
- Identify performance improvements in existing workflows and recommend enhancements.

Roles and Responsibility:

- Conduct product/solution presentation or demo for clients. Executes Proof of Concept (POC) and provides Scope of Work (SOW) based on the recommended solutions.
- Works directly with the Clients, Account Teams and Solutions Architects to help plan and design optimal solutions.
- Conducting Implementation with client's environment for the chosen security solutions.
- Providing technical support for Qualys Modules.

Skills and Abilities:

- In-depth technical knowledge with Qualys Solution.
- Solid understanding of cybersecurity principles, standards, and protocols (OWASP Top 10, CIS Benchmarks, NIST, etc.).
- Experience with Security Assessment tools (NMAP, Metasploit, Burp Suite, etc.).
- Familiar with MITRE ATTACK Framework, Cyber Kill chain, and Common Vulnerability Databases like CVE.
- Risk assessment to identify critical flaws in application and systems that cyber attackers could exploit.
- Good understanding of networking – TCP/IP, routing, switching, firewalls
- Knowledge of EDR and SIEM Technologies.

CLOUD SECURITY ENGINEER • FEBRUARY 2021 –
APRIL 2022

Trend Micro Philippines

Contributions:

1. Case Management Specialist

- Primary responsible for overseeing and evaluating the team members' open cases.
- Identify performance improvements in existing workflows and recommend enhancements.
- Provide regular reporting to team leader.

Roles and Responsibility:

- Provides frontline technical assistance of Trend Micro Home products through Phone, Email, and Chat for customers.

-
- Identifies product issues and proactively reports it for escalation to Product Development Team.
 - Identify and address the customer success gaps when using Trend Micro solutions.
 - Meet business objectives defined by the balanced scorecards of the team.

Skills and Abilities:

- Experience with Endpoint Security Monitoring tools (Sysinternals, Windows Event Logs, Sysmon, etc.).
- Background on Malware & Threat Related Cases.
- Good working knowledge in troubleshooting endpoints (Windows, ChromeOS, and Mac OS.).
- Adept familiarity with the Trend Micro Product, Technology, and Framework.
- Knowledge in Data Privacy Handling.
- Knowledge of phishing and social engineering techniques.
- Provides Security Awareness to clients.