Aung Thu Aye

+959-448-034647 | aungthuaye.ygn@gmail.com
Yangon, Myanmar
Linked In, Personal Collection

SUMMARY OF QUALIFICATIONS

Information technology and security professional with experience in penetration testing, endpoint security, network security, cloud security, web application security and incident response. Dedicated to continual learning through training and certification courses, as well as daily practice in a home lab. Exceptional communication and prioritization skills. Active member of OWASP, Myanmar Computer Professional Association, Myanmar Security Forum (MSF) and KAY Red Team (monthly MeetUp focused on learning penetration testing techniques, security soft skills, Hack the Box, and Capture the Flag activities).

AREAS OF EXPERTISE

Security Best Practices, Policies, & Tools
Multi Factor Authentication (Okta/OAuth/SAML)
Scripting (PowerShell, Python)
Penetration Testing
Network Security Tools & Practices

Incident Response
PCI & ISO Compliance
Vulnerability Management
GRC Management
Cloud Security

Security Breach Mitigation
Endpoint Protection/Logging
Researching Vulnerability and Exploit
Ticket Queue Management
Secure Messaging/Communication

SECURITY EDUCATION & PROFESSIONAL TRAINING

University of the People	Bachelor of Science (expected 2028)
John Academy	IT and Cyber Security Diploma
The SecOps Group	**Certified** Application Practitioner (CAP), **Certified** AppSec Pentester CAPen (Mock)
Security Blue Team	Blue Team Junior Analyst
International Cyber Security Institute	**Certified** Network Security Specialist

PROFESSIONAL EXPERIENCE

ONOW, Myanmar September 2023- Present

Cyber Security Analyst (2023 – Present)

- Conducted security assessments on cloud-based infrastructure and services to identify vulnerabilities and weaknesses.
- Assessed the security of web applications to discover and address potential vulnerabilities and threats.
- Educated employees and users about security best practices, potential threats, and how to avoid falling victim to social engineering attacks.
- Simulated phishing attacks to test the susceptibility of users and evaluated adherence to security best practices.
- Designed and implemented a secure architecture for an organization's IT infrastructure.
- Analyzed and documented the root causes of security incidents to understand and address underlying issues.
- Created and maintained documentation that outlines standard operating procedures for security processes.
- Implemented and enforced security policies and procedures within an organization.
- Documented and communicated the results of security assessments, including identified vulnerabilities and recommendations for improvement.
- Provided comprehensive reports detailing the outcomes of penetration tests, including successful exploits and suggested remediation steps.
- Continuously monitored for weaknesses and potential attacks, including the use of threat intelligence.
- Created detailed reports that explain discovered vulnerabilities, the methods used for exploitation, and recommended measures for remediation.
- Knowledgeable on NIST Cybersecurity Framework and how the Identify, Protect, Detect, Respond, and Recover categories comprise and facilitate an information security program.

CYBER SECURITY PROJECTS

Web Application Technologies and Cyber Security

- Skilled in database design, implementation, and management using SQL (MySQL, PostgreSQL) and NoSQL (MongoDB) databases, ensuring data integrity and security.
- Experienced in utilizing frameworks such as Django, Flask, React.js, and Angular.js to develop robust and secure web applications.
- Proficient in server-side technologies such as Node.js and Express.js for building scalable and efficient web applications.
- Familiar with a range of cybersecurity tools such as Burp Suite, Wireshark, Nmap, Metasploit, and Snort, leveraging these tools to enhance the security posture of web applications and networks.
- Experienced in conducting thorough VAPT assessments to identify and remediate security vulnerabilities in web applications, networks, and systems.
- Implement secure coding practices to mitigate common vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection, and Cross-Site Request Forgery (CSRF), ensuring the integrity and confidentiality of web applications.
- Proficient in incident response procedures, including incident detection, containment, eradication, and recovery, to minimize the impact of security breaches on web applications and systems.
- Experienced in utilizing security scanning tools such as SonarQube, OWASP ZAP, and Snyk for static code analysis, dynamic application security testing (DAST), and dependency scanning.

Governance, Risk and Compliance

- Experienced in analyzing and prioritizing security risks identified through SimpleRisk assessments, collaborating with stakeholders to develop and implement risk mitigation plans tailored to organizational needs.
- Familiar with automating risk management processes and workflows in SimpleRisk, streamlining risk assessments, issue tracking, and reporting tasks for improved efficiency and accuracy.
- Experienced in conducting risk assessments using SimpleRisk, identifying and evaluating potential threats and vulnerabilities to organizational assets, and implementing risk mitigation strategies.