Syarique Syahrizal

syarique.syahrizal5@gmail.com | +1 (289) 879-4824 | linkedin.com/in/syariques | github.com/syarique31 | syarique-syahrizal-portfolio

EDUCATION

Queen's University *Expected Graduation: May 2027, Kingston, ON*
Bachelor of Computer Science (Honours) — Cybersecurity

- Dean's Honor List | GPA: 3.70/4.3
- Relevant Coursework: System Level Programming (Linux, Bash), Data Structures (Java, Python), Software Specifications (C, C++), Operating Systems

Google Cybersecurity Certificate *January 2025*

- Developed core skills in network security, threat management, incident response, and risk mitigation.

Ethical Hacking Essentials (EHE) *August 2025*

- Built foundational skills in ethical hacking, penetration testing, and system security.

St. Andrew's College *Graduated: June 2023, Aurora, ON*

EXPERIENCE

SIME *May 2025 – August 2025*
Cybersecurity Analyst Intern Petaling Jaya, Malaysia

- Triaged **150+** security alerts in **Microsoft Sentinel** (SIEM), responding to **service tickets** from internal users to validate activity, reduce false positives, and lower incident volume by **30%**.
- Supported **incident response** by investigating **identity-based threats** across **Active Directory** and **cloud environments**, analyzing sign-in logs to validate incidents and support containment and remediation.
- Supported the execution of organization-wide cybersecurity awareness training via **KnowBe4**, overseeing training coordination, progress tracking, and user support for **600+** employees across numerous branches.
- Managed identity records for **200+** users in **Microsoft Entra ID**, supporting **IAM** operations; maintained Sime's **Security Scorecard** profile and coordinated security escalations with DxC and Logicalis GSOC.

Queen's Startup Summit *April 2025 – Present*
Director of Technology Kingston, Ontario

- Oversaw technical operations during the summit, ensuring infrastructure reliability.
- Maintained and enhanced the QSS website using React.js.
- Collaborated cross-functionally to support ongoing development.

Rogers Cybersecure Catalyst *October 2024 – March 2025*
Cybersecurity Practitioner Remote

- Gained hands-on experience in SOC operations, threat intelligence, and vulnerability scanning via TryHackMe.
- Practiced **DFIR** and **network traffic analysis** for cyber threat mitigation.
- Built foundational skills in Linux CLI, scripting, SIEMs, and encryption.

ACT Technology Solutions *July 2024 – Aug 2024*
Database Engineer Intern Klang, Malaysia

- Assisted with **Oracle Database** optimization and learned Linux, SQL.
- Supported schema development and dataset organization.
- Integrated data and improved performance alongside senior developers.

PROJECTS

Risk-Driven Cyber Threat Prioritization Engine *December 2025*

- Developed an **end-to-end Python-based cyber risk prioritization pipeline** that generates, normalizes, and scores security incidents to support risk-based SOC triage and decision-making.
- Designed a **quantitative risk scoring model** incorporating likelihood, impact, exploitability, external exposure, business criticality, control coverage, detection gaps, and confidence weighting.
- Applied **NIST Cybersecurity Framework (CSF)** principles and **MITRE ATT&CK** attack categories to align technical detections with organizational risk and produce remediation-ready, prioritized risk reports.

Web Application Exploitation Lab *November 2025*

- Built an isolated penetration-testing lab using Docker with a **Kali** attacker container and DVWA vulnerable web server.
- Conducted service discovery with **Nmap** and exploited DVWA's Command Injection flaw to run system commands remotely.
- Executed a custom reverse-shell payload, gaining interactive access to the target and performing post-exploitation enumeration.

Cybersecurity Portfolio *August 2025 - Present*

- Built a React and Tailwind CSS portfolio showcasing cybersecurity projects, CTF write-ups, and technical research.

Security Analysis Dashboard *July 2025 - Present*

- Built an interactive **Splunk dashboard** using the BOTS v3 dataset to visualize security events, anomalies, and high-risk sources.
- Developed optimized SPL queries to categorize alerts, track event severity, and identify top alerting hosts.
- Incorporated statistical and visual analysis to support threat detection and incident investigation workflows.

TECHNICAL SKILLS

Security Tools: SIEM (Microsoft Sentinel, Splunk), Offensive Tools (Metasploit, Nmap, Kali Linux, DVWA, TryHackMe), Network Analysis (Wireshark), Identity & Access (Delinea PAM, Microsoft Entra ID), Infrastructure (VMware, VirtualBox), Risk (Security Scorecard), Ticketing (Jira)
Security Domains: Vulnerability Assessment, Incident Response, Penetration Testing, Network Security, IAM, Threat Hunting
Frameworks: NIST CSF, ISO 27001, MITRE ATT&CK, OWASP Top 10
OS: Windows, Linux (Ubuntu), macOS
Languages & Scripting: Python, SPL, SQL, C, C++, PowerShell, Bash