**[Sa](https://saishsolanki.github.io/index.html)athwick Venkataramalingam**

Guelph, ON | 647-334-8690 | saathwick104@gmail.com | linkedin.com/in/saathwickv

Cybersecurity professional with 2+ years of experience in Security Operations and Incident Response. Resourceful and proactive analyst actively building both offensive and defensive skills to become a well-rounded cybersecurity practitioner. Demonstrated expertise in reducing false positives, investigating complex threats, and collaborating cross-functionally to improve detection and response outcomes.

**Work Experience**

**Security Operations Analyst** Jul 2022 – Mar 2024

Deloitte USI, India

* Monitored and triaged over 600 security alerts monthly across Microsoft Sentinel SIEM/SOAR, Microsoft Defender 365, and Abnormal Security.
* Investigated and responded to security incidents by following incident response procedures to contain and mitigate the impact of security breaches.
* Prepared over 20 detailed incident reports and drafted Standard Operating Procedures (SOPs).
* Used Kusto Query Language (KQL) to optimize SIEM analytics rules in collaboration with the SIEM/SOAR team, reducing false-positive alerts by 11%, approximately 200 alerts per quarter.
* Worked with the Threat Intelligence team to analyze emerging cybersecurity threats and updated Indicators of Compromise (IOCs) in SIEM and EDR platforms.

**Security Automation Engineer (Intern)** Feb 2022 – Jun 2022

Deloitte USI, India

* Developed custom Python and C# scripts to automate configuration of around 30 Azure Policy definitions via REST API, enforcing security standards across resource groups.
* Deployed these policies across multiple Azure subscriptions and resources using Terraform modules.
* Built automated security workflows using Cortex XSOAR to enrich incoming alerts with threat intel, asset metadata, and EDR insights, streamlining triage and response.

**PROJECTS**

**Scalable APT Malware Classification**

* Collected 4,630 APT-linked executables; used headless Ghidra in Podman and Python scripts to decompile and extract opcode sequences.
* Converted opcodes into 1‑gram/2‑gram feature sets with variance filtering; trained SVM, KNN, Decision Tree and GPU-accelerated CNN models for precise APT‑group and malware‑type attribution.

**Network and Web application Penetration Testing**

* Completed 50+ OffSec Proving Grounds and HackTheBox labs on Windows and Linux targets, building proficiency in reconnaissance, exploit chaining and privilege escalation techniques.
* Simulated end‑to‑end assessments in isolated Active Directory labs, gaining Domain Admin via Kerberoasting, NTLM relay, GPO abuse and credential exposure and drafted comprehensive reports detailing exploit chains, impact analysis and prioritized remediation steps.
* Conducted black‑box and white‑box tests on web applications, chaining SQL injection, arbitrary‑file uploads and business‑logic flaws to achieve authenticated RCE and exfiltrate sensitive data.

**Cloud Penetration Testing & Forensics**

* Simulated 4 CloudGoat attack scenarios—EC2 metadata abuse, IAM policy rollback, S3 SSRF, Cognito identity compromise—mapping and extracting key forensic artifacts for each vector.
* Injected CloudTrail logs into Elastic SIEM, built custom queries and dashboards, and analyzed over 10,000 log events to uncover anomalous API behaviors and privilege misuse.

**EDUCATION**

* **Masters in Cybersecurity and Threat Intelligence** Jan 2025 - Present

University of Guelph, CA

* **Post-Graduate Certificate in Offensive Cybersecurity** May 2024 - Dec 2024

York University School of Continuing Studies, CA

* **Bachelor of Technology in Information and Communication Technology** Jul 2018 - Jun 2022

SASTRA Deemed University, India

**CERTIFICATIONS**

* OSCP + – OffSec Certified Professional Plus | OffSec | 2025 – 2028
* OSWP – OffSec Wireless Professional | OffSec | 2025
* SC-200 – Security Operations Analyst | Microsoft | 2023 - 2024
* AZ-500 – Azure Security Engineer | Microsoft | 2022 -2024
* AZ-900 – Microsoft Azure Fundamentals | Microsoft | 2022

**PUBLICATIONS**

* “Scalable APT Malware Classification via Parallel Feature Extraction and GPU-Accelerated Learning” Available at arxiv: <https://arxiv.org/abs/2504.15497>
* "Malware Analysis and Reverse Engineering: Unraveling the Digital Threat Landscape"

Available at SSRN: <http://dx.doi.org/10.2139/ssrn.4649754>

**HONORS & AWARDS**

* Spot Award | Deloitte | January 2024

“Recognized for exceptional dedication, hard work, and consistently meeting client expectations” in the previous quarter.