Aniket Agarwal

Toronto, ON | aniketagarwal57@gmail.com | +1 (438) 924-4321 | LinkedIn | GitHub | Medium Blog

PROFILE

SC-200 Certified Cybersecurity Analyst with 1 year of hands-on experience hardening hybrid environments using **Microsoft Sentinel**, **Splunk**, and **Defender for Endpoint**. Specializes in engineering **Python** and **SOAR** automation to slash incident response times and optimize detection logic. Brings operational expertise in proactive threat hunting, vulnerability mitigation, and NIST-compliant incident handling to deliver immediate value in high-tempo security operations.

CERTIFICATIONS

Microsoft Certified: Security Operations Analyst Associate (SC-200) | CompTIA Security+ (SY0-701) | ISC² Certified in Cybersecurity (CC)

TECHNICAL SKILLS

- **SIEM & Log Analysis:** Microsoft Sentinel, Splunk Enterprise, KQL, SPL, Azure Log Analytics.
- **Security Operations:** Defender for Endpoint (MDE), Threat Hunting, Alert Triage, Incident Response (IR).
- **Vulnerability Management:** Tenable Cloud, Nessus, DISA STIGs, Patch Management, Risk Mitigation.
- **Automation & Scripting:** Python (Pandas/Requests), PowerShell, Bash, n8n (SOAR), Azure Logic Apps.
- **Infrastructure & Governance:** Active Directory, Linux (Ubuntu/Kali), TCP/IP, NIST 800-61, MITRE ATT&CK.

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst (Intern) | Log(N) Pacific *Aug 2025 - Dec 2025*

- **Analyzed** high-volume log sources in **Microsoft Sentinel** using custom **KQL** queries, successfully filtering noise to reduce false positive rates by **30%** during daily triage.
- **Prioritized** the remediation of critical **Tenable** vulnerabilities based on risk severity, coordinating with IT teams to enforce **DISA STIG** benchmarks and achieve **100% SLA compliance**.
- **Executed** incident containment efforts via **Defender for Endpoint (MDE)** to isolate compromised hosts, while utilizing **PowerShell** scripts to detect and block lateral movement during live attack simulations.

PROJECTS

***Automated Incident Response & Threat Hunting* |** *Python, Azure Sentinel, OpenAI* *Oct 2025 – Dec 2025*

- Enhanced threat hunting capabilities by integrating Azure Sentinel with OpenAI, accelerating complex query formulation by **90%** for faster investigation cycles.
- Accelerated incident response times by implementing SOAR workflows that trigger instant VM isolation, slashing Mean Time to Respond (**MTTR**) to less than **60 seconds**.
- Standardized threat reporting by mapping **100%** of analyzed alerts to **MITRE ATT&CK** tactics, ensuring consistent documentation and validation of attack vectors.

***Enterprise SOAR & Active Directory Security* |** *Splunk, n8n, Active Directory* *Nov 2025 – Jan 2026*

- Established visibility into identity-based attacks (Kerberoasting, Brute Force) by ingesting **Windows/AD logs** into **Splunk**, enabling real-time monitoring of user behavior.
- Streamlined alert triage by configuring an **n8n** pipeline to enrich Splunk alerts with Threat Intelligence (AbuseIPDB), reducing manual analysis time by **40%**.
- Validated detection logic by simulating live **lateral movement** (workstation to **Domain Controller**), refining alert rules to ensure high-fidelity detection of privilege escalation.

EDUCATION

Master of Engineering – Information Systems Security | Concordia University, Montreal, QC *Sept 2023 – May 2025*

Bachelor of Technology – Computer Science & Engineering | SRMIST, Chennai, IN *June 2019 – May 2023*

VOLUNTEERING AND LEADERSHIP

- **CTF Designer (AtHack):** Engineered vulnerability challenges for **400+ participants** and mentored students.
- **Technical Writer (Medium):** Author technical guides on **SOC automation** for the open-source community.