

Shrit Shah

SOC Technical Lead

📍 Toronto, Ontario, Canada 📞 +1 (519) 731-8020 ✉ i.am@shrit.xyz 🌐 www.shrit.xyz

🌐 www.linkedin.com/in/shrit-shah/ 📄 github.com/Shrit-Shah/ 🏆 www.credly.com/users/shrit-shah

📁 WORK EXPERIENCE

GlassHouse Systems Inc. [🔗](#)

SOC L1 Technical Coordinator

Feb 2026 – Present | North York, ON, Canada

- Led a **24x7 Security Operations Center (SOC)** team of 11 analysts across 3 shifts, ensuring continuous monitoring, incident triage, and SLA adherence in a high-volume environment
- Acted as **primary technical escalation point** for L1 analysts, guiding investigations involving **SIEM (e.g., Splunk, QRadar)** and **EDR (Defender, CrowdStrike)**
- Developed SOC runbooks and **SOAR playbooks aligned with MITRE ATT&CK**, improving response consistency and MTTR
- Identified alert fatigue and operational gaps; drove **process improvements and use-case tuning**, increasing detection efficiency and reducing noise
- Tracked and reported **SOC KPIs (MTTD, MTTR, SLA compliance, escalation rates)**, enabling data-driven operational improvements
- Conducted QA reviews and mentored analysts, improving **incident accuracy, escalation quality, and team capability**
- Collaborated with cross-functional teams (Threat Intelligence, IT, IR, Platform) to enhance **threat visibility** across **hybrid cloud environments (AWS, Azure)** and improve security posture

SOC Analyst I

Dec 2024 – Feb 2026 | North York, ON, Canada

- Monitored, triaged, and investigated security events across **20+ environments** using SIEM (Splunk, QRadar, Elastic, Google SecOps) and EDR (CrowdStrike, Defender), including phishing and account compromise analysis
- Collaborated with Tier-2 and Incident Response teams for **incident escalation, RCA, and mitigation of high-fidelity alerts**
- Developed a **scalable AI-powered Threat Intelligence automation solution** to generate customer-specific security advisories for 20+ clients, enriching IOCs to support threat hunting and detection engineering
- Designed and implemented **SOAR playbooks** to automate incident triage and investigation workflows, improving SOC efficiency and reducing manual analysis effort by 30%

Difenda Inc., *Threat Intelligence Analyst (Co-op)* [🔗](#)

May 2024 – Aug 2024 | Oakville, ON, Canada

- Produced **MITRE ATT&CK-aligned CTI reports** using Azure AI Studio and Microsoft Security Copilot, improving analytical depth and reporting consistency
- Automated CTI workflows using **PowerShell, Azure Logic Apps, and Azure DevOps**, reducing manual effort and improving response efficiency by 70%
- Utilized Threat Intelligence Platforms including **Anomali ThreatStream, Defender TI, and VirusTotal** for threat enrichment and analysis

elInfochips (An ARROW Company), *IT Security Analyst* [🔗](#)

Feb 2022 – Jul 2023

- Performed vulnerability assessments and remediated **5000+ risks**, ensuring compliance with **ISO 27000, CIS, and NIST standards**.
- Automated key IT operations with **Bash and PowerShell**, cutting manual workload by 25%.
- Deployed enterprise-wide **EDR solutions** and delivered **security training**, improving detection capability and team readiness

🧠 SKILLS

— **SOC Operations** | **Incident Response** | **SIEM** (Splunk, QRadar, Elastic, Google SecOps, FortiSIEM, Datadog) | **EDR/XDR** (CrowdStrike, Microsoft Defender) | **Threat Intelligence** (MITRE ATT&CK, IOC Enrichment, Threat Hunting) | **Automation** (PowerShell, Bash, SOAR, Generative AI) | **Cloud** (AWS, Azure, GCP) | **Vulnerability Management** (Tenable, Nessus) | **Network Analysis** (Wireshark) | **Linux** | **Active Directory** | **Documentation & Runbooks**

🎓 EDUCATION

Master of Cyber Security & Threat Intelligence, *University of Guelph* [🔗](#)

Sep 2023 – Aug 2024

Guelph, ON, Canada

- GPA: 93.5 | ISA Cybersecurity Scholarship Recipient [🔗](#)

Bachelor of Engineering, Computer Engineering, *LDRP-ITR, KSV University* [🔗](#)

2018 – 2022

- GPA: 8.55/10

📄 PUBLICATIONS

AI-Driven Cyber Threat Intelligence Automation [🔗](#)

Developed an **AI-driven Cyber Threat Intelligence framework** leveraging GPT-4 and Microsoft security tools to automate CTI workflows, enhancing threat detection, hunting, and TTP analysis while significantly reducing manual effort

📄 CERTIFICATIONS

- (ISC)2 Certified in Cybersecurity (CC) [🔗](#)
- Microsoft Security, Compliance and Identity Fundamentals (SC-900) [🔗](#)
- Red Hat Certified System Administrator (RHCSA) [🔗](#)
- Microsoft Azure Fundamentals (AZ-900) [🔗](#)