Shrit Shah

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

SOC Analyst I, *GlassHouse Systems*

Dec 2024 – present | North York, ON, Canada

- Monitored, triaged, and escalated security incidents across multi-tenant environments using IBM QRadar, FortiSIEM, Google SecOps, and Elastic Security.
- Investigated endpoint threats using Microsoft Defender; supported compromised user and phishing analysis.
- Collaborated with Tier-2 and threat intelligence teams for escalation, RCA, and mitigation of high-fidelity alerts.
- Actively contributed to daily Threat Intelligence Advisories by tracking emerging threats, CVEs, and TTPs; developing a parallel automation project using OpenAI and scripting to scale CTI operations.

Threat Intelligence Analyst (Co-op), *Difenda Inc.*

May 2024 – Aug 2024 | Oakville, ON, Canada

- Leveraged Generative AI (Azure AI Studio, MS Security Copilot) to generate CTI reports aligned with MITRE ATT&CK, enhancing analytical accuracy and reporting quality.
- Automated CTI workflows with PowerShell, Logic Apps, and Azure DevOps, reducing manual tasks and accelerating SIEM response by 70%.
- Gained hands-on experience with TIPs and tools including Anomali ThreatStream, Defender for Threat Intelligence, and VirusTotal.

IT Security Analyst, *eInfochips (An ARROW Company)*

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 EDR agents enterprise-wide to enhance threat detection and response.
- Led cybersecurity training for new hires, improving team readiness and efficiency.

EDUCATION

Master of Cyber Security & Threat Intelligence,
University of Guelph

Sep 2023 – Aug 2024 | Guelph, ON, Canada

- GPA: 93.50/100
- **Awarded $5000 ISA Cybersecurity Inc. *Scholarship*** for academic excellence, recognized as the top achiever within the cohort.

PUBLICATIONS

AI-Driven Cyber Threat Intelligence Automation

Developed an AI-powered framework leveraging GPT-4 and Microsoft tools to automate Cyber Threat Intelligence (CTI) processes. The research focused on enhancing threat detection, hunting and TTP analysis while reducing manual effort. Demonstrated the effectiveness of AI in improving CTI reporting speed, accuracy, and operational efficiency.

SKILLS

SOC | **SIEM** | **Log Analysis** | **EDR & XDR** | **Cyber Threat Intelligence (CTI)** | **Virus Total** | **MITRE ATT&CK** | **Vulnerability Assessment** | **Incident Handling** | **Tenable Nessus** | **Security Event Correlation** | **Threat Analysis** | **Wireshark PCAP Analysis** | **PowerShell** | **Automation** | **Bash Scripting** | **Linux Admin** | **Gen-AI** | **Active Directory** | **Documentation** | **Cloud** (AWS, Azure, Google Cloud)

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)

Demystifying Networking - NPTEL IIT-Bombay
Ranked among the top 5% of candidates across the nation.

PROJECTS

Linux OS Hardening using CIS Benchmarks, *Bash*

Automated shell script for hardening Ubuntu Linux 22.04 LTS according to CIS Benchmarks v8. Features a user-friendly menu interface, allowing users to easily navigate and customize hardening configurations to meet their specific requirements.*(Video Link)*

NAS Storage Automation, *Bash*

A tool to automate the configuration of Network Attached Storage between Linux systems and automate periodic backups with an easy Menu-based User-Interface.

VOLUNTEERING

Co-Founder & Technical Head, *Team Cache*

During the pandemic, we formed a student community titled "Cache" to bring out the extracurricular skills of our college students through online workshops.