Karan Tank

Security Engineer | Advanced Security Response Team (ASRT)

6472989129 | karantank.csi@gmail.com | linkedin.com/in/karan-tank |credly.com/users/karan-tank/badges

Security Engineer with proven expertise in **advanced threat analysis, incident response**, and cutting-edge **cybersecurity measures**. Demonstrated leadership in spearheading **application security** initiatives, **DDoS protection**, and effective **bot management**. Holds certifications including S**ANS GCIH and CompTIA Security+**. **Senior Security Analyst** with a track record of **mitigating malicious activities** and providing mentorship. Additional skills include user support excellence, device management, and PowerShell automation for enhanced workflow efficiency.

Certifications 🏅

- **TCMSecurity**: Practical Web Application Security and Testing — **Oct 2023**
- **TryHackMe:** Junior Penetration Tester (THM JPT) — **Jul 2023**
- **SANS GCIH:** GIAC Certified Incident Handler (SEC 504) — **Jan 2023**
- **SANS GSEC:** GIAC Certified Security Essentials Certification (SEC 401) — **Oct 2022**
- **SANS GFACT:** GIAC Foundational Cybersecurity Technologies (SEC 275) — **Aug 2022**
- **CompTIA Security+** — **Apr 2022**
- **Ec-Council CHFI:** Certified Computer Hacking Forensic Investigator — **Jan 2022**

Work Experience 💼

Thales - **Security Engineer - Advanced Security Response Team (ASRT)** — **Jul 2024 - Present**

- ➔ Spearheaded comprehensive application security initiatives, integrating cutting-edge measures such as **Web Application Firewall (WAF)** and **advanced bot protection** to fortify against evolving cyber threats.
- ➔ Led Distributed **Denial of Service (DDoS)** protection efforts, establishing protocols and measures to mitigate the impact of malicious attacks on organizational assets.
- ➔ Utilized **Tableau** for **traffic analysis** and created rules to mitigate bot traffic in customer environments, ensuring enhanced operational security.

Imperva - **SOC Engineer** — **Jan 2024 - July 2024**

- ➔ Implemented effective strategies for **bots detection and management**, specializing in advanced bot protection and **account takeover prevention** to safeguard critical systems and data.
- ➔ Conducted thorough analysis and reviews of **Common Vulnerabilities and Exposures (CVE)**, facilitating timely updates and patches to enhance system resilience.
- ➔ Analyzed **network traffic patterns**, utilizing advanced techniques to identify and respond to potential security incidents, contributing to a secure operational environment.
- ➔ Provided services across **OSI model layers 3/4 and layer 7,** delivering comprehensive security solutions and ensuring a resilient defense against threats at different network layers.

SecureOps - **Senior Security Analyst (SOC) II** — **May 2023 - Dec 2023**

- ➔ Conducted **advanced analysis and triage** tasks across diverse IT infrastructure, including endpoints, servers, and

network components.

- ➔ **Led proactive security investigations** and comprehensive searches within client environments to swiftly detect and respond to malicious activities.
- ➔ Coordinated and executed **incident investigations** with in-depth analysis to identify and respond to detected threats promptly.
- ➔ Demonstrated a comprehensive grasp of the **MITRE ATT&CK framework,** effectively mapping client use cases to relevant tactics and techniques for enhanced security.
- ➔ Formulated professional opinions and pragmatic recommendations, all in accordance with established standards, rules and guidelines.
- ➔ Acted as an **expert resource** in the analysis and resolution of security incidents.
- ➔ Scoped customer security incidents to precisely understand their magnitude and potential impact.

SecureOps - Security Analyst (SOC) I **May 2022 - April 2023**

- ➔ Proactively engaged in **Threat Hunting activities** on client networks to detect, isolate, and offer strategic recommendations to mitigate threats effectively and Assessed logs and model threats.
- ➔ Skillfully identified and understood **indicators of attack and compromise** within alerts by meticulous data analysis and thorough review of investigation notes.
- ➔ Conducted thorough analysis, review, and provided raw log data to gain deeper insights into **security escalations** through SIEM.
- ➔ Demonstrated **strong communication skills,** both orally and in writing, for clear and efficient collaboration with system and network administrators, systems users, and managers.
- ➔ Maintained a deep understanding of the evolving threat landscape to stay proactive in security measures

Vox Mobile - Technical Support Specialist **Jan 2021 – Nov 2021**

- ➔ **End-User Support Excellence**: Delivered comprehensive technical and mobility support through calls and emails, utilizing a range of tools including ServiceNow, vFire, Citrix Workspace and Vox Mobile's knowledge base support center tools.
- ➔ **Device Management and Procurement**: Efficiently managed devices on BlackBerry UEM, VMware Workspace ONE, and Microsoft Intune MDM servers, while overseeing user procurement requests via Vox Mobile's dedicated channel and Telus IQ portal.

Internship👩‍💻

Corporation of City of Brampton - Information Security Analyst **Jan 2020 – April 2020**

- ➔ **Enhanced Workflow Efficiency:** Implemented PowerShell automation to streamline workflow processes, optimizing operational efficiency.
- ➔ **Effective User Management:** Managed user onboarding and offboarding procedures, ensuring security and data protection through Active Directory oversight and assessments.

Education and Training 🎓

Toronto Metropolitan University - Bootcamp: CyberSecurity Training Program **Jul 2022 – Jan 2023**

NPower Canada - Bootcamp: Junior QA and Security Analyst Program **Jan 2022 – Apr 2022**

Fleming College - Advanced Diploma: Computer Security and Investigations **Jan 2018 – Apr 2020**