Aarsh Patel

TRIAGE SECURITY ANALYST (GCS)

Email: aarshpatel.infosec@gmail.com | Phone: +1 (778) 855-1071 | LinkedIn | Vancouver, BC, CA

November 18th 2024

Hiring Manager
RBC
1055 Georgia St W
Vancouver, BC, V6E 0B6

Sub: Triage Security Analyst (GCS)

Dear Hiring Manager,

As a Cybersecurity professional my passion for addressing evolving threat landscapes through proactive monitoring and defense strategies deeply resonates with RBCâs commitment to innovation and resilience in cybersecurity. As a cybersecurity professional with over two years of experience in SOC operations, incident response, and security analysis, I am eager to bring my technical expertise to protect and enhance the security of your enterprise systems. I am excited to apply for the Security Analyst, Triage position at RBC.

In Riskstifle, as a Cybersecurity Analyst, I attained competency in incident response by running back-to-back, in-depth investigations of security incidents using the Splunk SIEM, EDR, and NDR platforms. Applying such frameworks as MITRE ATT&CK and NIST 800-53, I am confident to state that the security posture for the organization was enhanced by at least 30%. I have been instrumental in the protection of enterprise systems by being able to identify root causes and develop mitigations through IDS/IPS tuning and malware analysis. Working with different teams, active threat intelligence with a workflow of optimized responses was developed to mitigate risks efficiently.

In addition to my technical skills, my experience with scripting languages like Python, PowerShell, and Bash has allowed me to automate repetitive tasks, improving operational efficiency. Past colleagues have praised my analytical mindset and collaborative approach to problem-solving. The opportunity to contribute to RBCâs Intelligence-led Security and Resilient Services objectives aligns with my professional values of teamwork, precision, and adaptability in high-pressure environments.

I am especially honored to join the team in its mission of defense of critical assets and in support of the global environment of CNB. Thank you for considering my application. I look forward to discussing how my qualifications and experiences meet your requirements.

Sincerely,
Aarsh Patel

Aarsh Patel

TRIAGE SECURITY ANALYST (GCS)

Email: aarshpatel.infosec@gmail.com I Phone: +1 (778) 855-1071 I LinkedIn I Vancouver, BC, CA

SUMMARY

CEH I Security Analyst I SIEM I Incident Response & Management I Cloud Security I Security Operations I NIST

A Dynamic highly motivated and result-driven professional with 2+ years of experience in Information Security and having Masterôs in Cybersecurity. Seeking an opportunity to excel in a Cybersecurity role and aiming to apply analytical skills and data-driven insights to fortify cybersecurity measures and mitigate potential risks.

Tech-savvy with strong analytical and reasoning skills, who is persistent, detail-oriented and a capable problem solver. Demonstrable understanding of security frameworks, SOC analysis, threat landscape and security controls. Possess a very fine knowledge in analyzing network traffic, malware analysis and network attacks.

Excellent with tools such as Wireshark, Burp Suite, Nmap, Tenable Nessus, OWASP ZAP. Strong conceptual understanding of various industry standards such as NIST-800-53, ISO 27001.

PROFESSIONAL EXPERIENCE

Cyber Security Analyst
Riskstifle, Canada I June 2023 - Present

- Enhanced security posture by 30% through comprehensive monitoring, incident response, and vulnerability management using tools like Tenable SC, Nessus, Nmap, and Wireshark.
- Collaborated with the Security Operations Center (SOC) to identify, investigate, and respond to security incidents, conducting comprehensive root-cause analyses with advanced network traffic and threat analysis.
- Drafted and implemented information security policies aligned with MITRE ATT&CK, NIST 800-53 standards, Cyber Kill Chain.
- Triaged and investigated high-risk security incidents using Splunk SIEM, improving incident response efficiency by 30%.
- Utilized EDR and NDR tools for enhanced threat visibility and rapid incident response, while customizing IDS/IPS rules to mitigate diverse network attacks, incorporating TCP/IP packet analysis for in-depth threat investigation.
- Detected and removed malware in Unix/Linux Operating Systems causing CPU and memory exhaustion, restoring server performance and preventing future slowdowns.
- Improved security compliance by 25% by handling Active Directory access control, audit logging, administration, and implementing MFA, SSO, security policies, and hardening servers and operating systems.

Cloud Security Engineer
Hrimtech PVT LTD, India I September 2020 - August 2021

- Triaged security alerts and prioritized incidents for response based on severity and impact, ensuring timely remediation.
- Assessed cloud security architectures and recommended controls in line with zero-trust strategies.
- Enhanced cloud security by implementing IDS/IPS controls, achieving a 20% reduction in intrusion risks.
- Automated firewall updates and alert management using Python and PowerShell, reducing manual effort by 30%.
- Conducted deep security testing to identify vulnerabilities in cloud environments, ensuring a robust security posture.

IT Support Intern
Lark Info Way, India I August 2019 - July 2020

- Setting up cPanel and WHM hosting environments: DNS, e-mail service, and security settings configuration.
- Ensured high availability by automating backup and security updates through scripting.
- Enhanced the security of the website with SSL certificates/firewall rules for secure web hosting environment.
- Technical support for web-hosted environments to maintain user access and configuration of domains.
- Supported the archival configuration of various systems include Microsoft Teams, Web Host Manager Complete Solution (WHMCS).

Aarsh Patel

TRIAGE SECURITY ANALYST (GCS)

Email: aarshpatel.infosec@gmail.com | Phone: +1 (778) 855-1071 | LinkedIn | Vancouver, BC, CA

FUNCTIONAL EXPERTISE

Compliance Framework:	SOC2, ISO27001, NIST 800-53, GDPR, HIPAA, CCPA, PIPEDA, OWASP
Risk Management:	Risk Assessment, Third-Party Vendor Assessment, Security Audits
Security Tools:	Nessus, Burp Suite, Nmap, Wireshark, Splunk
Network Firewalls:	Firewalls (Palo Alto, AWS Cloud Firewall), IDS/IPS, VPN, Snort, Iptables, GRE Tunnel
Enterprise Application:	ServiceNow, Office 365, Microsoft Teams, Zenput, Zendesk
IAM & PAM	Active Directory
Cloud Platforms:	AWS, Azure, Oracle, Digital Ocean, OVH, Linode
Data Analysis:	Excel dashboards, Tableau, Power Bi
Project Management:	Agile, Kanban, MS-Project.

EDUCATION

Master of Science in Cybersecurity
New York Institute of Technology, Vancouver, BC, Canada | September 2021 - December 2022
B.Tech in Information Technology
Silver Oak College of Engineering and Technology - GTU, India | September 2016 - August 2020

CERTIFICATIONS

- EC-Council Certified Ethical Hacker **Master** (CEH Master) (ECC0756941832)
- (ISC)¿ Certified in Cybersecurity (CC)
- Fortinet Network Security Expert- 1,2,3.
- NIST SP-800-53 Fundamentals and Control Families - EC-Council
- Offensive Bug Bounty Hunting & API Hunting - Hackersera
- Python 3 for Offensive Pen Testing - Udemy
- ISO/IES 27001 Information Security Management - Udemy

PROJECTS

Cybersecurity Mentorship Program (May 2023 - Present)

- Hands-on experience in DevOps practices, threat risk assessment, threat modeling, and cloud infrastructure security.
- Risk assessment of network, applications, and technical environment
- Penetration testing of different websites.
- Secure the cloud environment for a client
- Managed projects with Agile methodologies
- Tuned the PAM environment with the CyberArk tool
- Implement the NIST 800-53 controls for compliance with the NIST framework

Implementing IDS/IPS to Prevent UDP DDOS Attacks on Multiplayer Game Servers (Aug 2022 - Dec 2022)

- Developed a GRE Tunnel between servers using Iptables routing to conceal the main serverˆs IP.
- Implemented IDS rules to prevent DDoS attacks from reaching the main server, leveraging AWS and Oracle Cloud Firewall APIs, shell scripting, and bandwidth monitoring.
- Utilized scripting languages including Bash, Python, and PowerShell to automate Firewall rules update, Packets Logging, Bandwidth Monitoring.
- Automated logging and inspection of packets, enabling the creation of signature-based firewall rules for enhanced security.