SAUMYA DESAI

+1 519-860-8900 ◇ Toronto, CAD
E-mail ◇ GitHub ◇ Linkedln

OBJECTIVE

Passionate security analyst with a Post-graduate degree in Information Security Management from Fanshawe College and Conestoga College. In my previous role at Showmates, I identified and mitigated over 5000 security risks, created automation scripts, and developed a comprehensive Information Security training program. Always eager to learn, I hold multiple certifications in Information Technology and aim to protect businesses from the latest threats.

EDUCATION

Postgraduate Certificate, Fanshawe College
Information Security Management

Postgraduate Certificate, Conestoga College
Virtualization and Cloud computing

Bachelor of Technology, SAL College of Engineering
Information Technology

SKILLS

Cloud and Security Tools	VMware, AWS, AZURE, SIEM, IDS, Incident Response, Kali Linux, ParrotOS, Wazuh.
Frameworks	NIST, ISO27001, FISMA, COBIT, ITIL, LAMP, KERAS
DevOps and API Tools	IIS, Git, Docker, OpenShift, Kubernetes, Swagger, Postman
Languages	Python, JavaScript, TypeScript, C/C++, SQL, HTML, CSS, Java
Others	Active Directory, Vulnerability Assessment, Agile, SOLID, E-mail, Documentation

EXPERIENCE

Threat Intelligence Analyst [**Showmates**]
London, Canada May 2023 – Present

- Identified and mitigated 5000+ security risks by performing vulnerability assessments and implementing remediation procedures across enterprise infrastructure. Reduced attack surface and ensured that systems were compliant with industry standards. Includes Auditing and ensuring ticket compliance per ITIL and Major Incident Management best practices
- Created automation scripts using Bash and PowerShell to streamline IT operations and reduce manual workload by more than 25. Decreased the risk of errors and increased operational efficiency. Developed and delivered a comprehensive cyber security training program for new joiners and interns, resulting in a 30 increase in team productivity. Contributed to developing and implementing the organization's security policies, procedures, and guidelines by incorporating the latest industry frameworks, standards, and regulations such as ISO 27000, CIS benchmarks, NIST Cybersecurity Framework and SP-800 series.
- Secured network by successfully deploying Endpoint Detection and Response (EDR) agents, across organization assets to detect and prevent any incoming malicious intrusions. Provided comprehensive technical IT support for Linux and Windows Servers, as well as VMware systems. Proficient in working with complex WAN network architectures.
- Produce accurate and thorough Major Incident Reports to be delivered to Customers and Stakeholders. Responsible for initiating and implementing continual improvements for escalation Best Practices in Incident Management workflows and Change Management workflows.

NOC Analyst [**Petro-Canada Fuels**]
London, Canada Jan 2023 – July2023

- Worked with internal and external teams to resolve incidents, communicated status and impact to stakeholders, and prioritized high-priority issues while maintaining SLA commitments. Documented incidents and troubleshooting steps in ITSM/ServiceNow.
- Monitored production infrastructure and applications for deviations, performed in-depth analysis of alerts, and provided support to correct system deviations. Conducted health checks on high-priority servers and notified technical teams.
- Implemented continual improvements for escalation and incident management workflows, automated false alerts, addressed gaps in monitoring tools, and ensured accurate alert redirection.

Software Engineer [**wayRabbit**]
Ahmedabad, IND May 2020 – Nov 2022

- Developed and maintained high-volume data processing and collection systems using Microsoft Azure, including Azure Data Factory, Azure Functions, Logic App, and Azure Data Lake Gen 2. Automated the migration of on-premises infrastructure and applications to cloud environments, and created database design and migration pipelines to transition Oracle Cloud Database to Azure for B2C billing applications.
- Collaborated with cross-functional teams and clients to gather requirements and provide solutions, actively participating in POC building and staying updated on Azure features. Re-architected B2B applications from ASP.NET Classic to C# .NET Core, developed client portals using Sitefinity and .NET Core and demonstrated a strong understanding of the SDLC to ensure seamless project execution.
- Conducted code reviews, unit testing, and maintained code quality standards. Customized features and integrated them with the Sitefinity database using the Entity Framework, developing personalized and conditional access based on user interaction. Proven ability to troubleshoot and resolve complex technical issues, leading to a permanent position as a junior software engineer.

Backend AI/ML Engineer Intern [**Silverwing Technologies PVT LTD**]
Ahmedabad, IND July 2019 – Jan 2020

- Developed API endpoints in Django, enhancing performance with Postgres and task parallelization via Celery.
- Created 'Sammachar Pathshala' in ReactJS, adopted by 27 schools to boost interactive learning.
- Built a Bitbucket CI/CD pipeline, automating deployments to AWS EC2 to streamline updates.

PROJECTS

Emulating and Detecting APT29 with Caldera and ATT&CK Evals Enhanced cybersecurity by simulating APT29 attacks and assessing detection capabilities using Caldera and MITRE ATT&CK frameworks. Developed attack scenarios, configured automated threat emulation, and implemented SIEM detection rules. Identified detection gaps and improved security measures, successfully testing defenses and enhancing threat response.

Hack The Box, Blue Team Labs, TryHackMe Lab Works Successfully solved over 25 complex cybersecurity labs across Hack The Box, Blue Team Labs, and TryHackMe platforms. Engaged in hands-on penetration testing and defensive strategies that reinforced skills in real-world security vulnerability exploitation and mitigation.

Python Malware Lab. Python ransomware prototype using Fernet to demonstrate the ease of creating malicious software, highlighting significant cybersecurity vulnerabilities. Gained practical cybersecurity insights by analyzing a variety of malicious Python scripts within a controlled malware playground, enhancing understanding of potential security threats and defense mechanisms.

Scalable Web App on Kubernetes on AWS. A scalable Node.js application on Amazon EKS using Docker and Kubernetes, which enhanced efficiency through auto-scaling and load balancing. Successfully integrated AWS services, reducing load times by 50% and increasing user engagement by 20%.

x86 Operating System (C++) An enhanced IP-TV system using IP multicasting with UDP and TCP protocols, leveraging multi-threaded sockets for improved performance. I also implemented a GTK-based VLC client in C++ that enables users to subscribe to multicast streams through a user-friendly API, demonstrating my skills in network programming and interface development.

Hybrid and Converged Solutions Enabled secure, private communication between AWS and Azure resources, demonstrating the potential of multi-cloud architecture without public exposure. This project provided a valuable learning experience in implementing robust cross-cloud solutions, enhancing my expertise in cloud interoperability and network security

Security Awareness Training Program Developed and executed a comprehensive security awareness training program for a company with 50 employees. The program included interactive workshops, simulated phishing attacks, and regular security updates, resulting in a 75% reduction in employee susceptibility to phishing and other social engineering attacks within six months

CERTIFICATIONS

- CompTIA Security+
- Google Cybersecurity Professional
- Oracle Cloud
- Red Teaming (TryHackME)
- BurpSuite (PortSwigger)