Sagnik Das

sagnikdaswork@protonmail.com

EDUCATION

The University of Texas at Dallas

M.S. Information Technology and Management, Major: Cybersecurity, Information Systems

Certifications:

- CompTIA Security+, Nozomi Networks Certified Engineer, IAEP certificate, UTD Cybersecurity certificate, Google Cybersecurity dual credential, IBM automation and application security certificate. Credly: https://www.credly.com/users/sagnik-das.65db49fb

Skills: Microsoft Office, IDEA analytics, AuditBoard, Masergy, PaloAlto, SecureEnds, Rapid7InsightVM, Python, SQL, Snyk, Qualys, ServiceNow, Tableau, AWS Cloud Security, PCI-DSS, NIST 800-53, COBIT, Automation (Selenium, Ansible, Puppet, Custom Scripts), Operational Technology, Purdue Model Networking, Django, Node.js, Flask, Unity, Pygame, Google Cloud Console, Kubernetes, AWS, OSINT, Firebase, Unity, Unreal Engine, C#

iTrustXForce, South Lake, Texas (Current) May 2023 – Present

Senior CyberSecurity Specialist and Customer Success Manager Jan 2024 – Present

- Leads the management of US-based and international client accounts for DigitalXForce platform
- Delivers TVM automation and Appsec labs services, (TVM Automaation and Pentest Automation services developed in house) to multiple clients with extensive business history
- Reduced the TVM process cost by automating it by 60% using python and FastAPIs automation scripts developed in house
- Developed the TPRM and CRLI module for the DigitalXForce platform
- Developed the Security connectors for Rapid 7, Snyk, Qualys and Ivanti and Enterprise connectors for AWS, Slack, Okta, Salesforce, Microsoft Azure to gather real time security metrics and perform analysis to realize the security posture
- Worked on mapping NIST 800-53, ISO-27001, PCI-DSS, and SOC 2 frameworks to add value to the real time security assessment of major US state clients and their domain of operations over the internet.

CyberSecurity Consultant and Developer May 2023 – Jan 2024

- Implemented automated cybersecurity processes to minimize manual workloads for OT and Application Security
- Identifying, assessing, and managing threats and vulnerabilities in the organization's network and systems
- Automating the process of evaluating the security of operational technology across multiple sites, which involves assessing physical systems like control systems, SCADA systems, and other industrial processes
- Conducting security evaluations of websites to identify potential vulnerabilities and threats
- Automating the preparation for SOC2 (Service Organization Control 2) compliance, focusing on security, availability, processing integrity, confidentiality, and privacy of a system
- Creating and maintaining labs that focus on application security, providing a controlled environment for testing and research
- Offering expert advice on setting up and running labs that focus on operational technology security, that include the integration of physical and digital security practices

Bread Financial, Columbus, Ohio August 2022 – May 2023

Information Technology Auditor SOX

- Improved audit efficiency and accuracy by 20% by testing critical business processes, such as payment, security, and change management, testing security policies and procedures against MITTRE and Cyber Kill Chain
- Resolved critical control deficiencies and enhanced compliance with SOX, PCI-DSS, and ISO 27001 by analyzing ITGCs using MS Excel and Python Jupyter (created a private database using pandas for automated testing using NLP)
- Reduced risk exposure by 15% by performing risk analysis for critical systems and recommending control improvements
- Enhanced security posture and compliance by identifying and remediating control gaps in SDLC and Network Security
- Detected and responded to identity-based attacks by using Red Canary for IAM threat hunting

Independent Financial, McKinney, Texas May 2022 – August 2022

Internal Audit Intern

- Implemented Auditboard system for 73 audit entities, migrating environment and data from Archer with a 2-person team
- Audited IT User Access Management, IT Incident Response, and IT Network Security using a top-down risk-based approach with a 3-person team
- Used IDEA analytics to review appraisals and loan operations policies and procedures, improving auditing accuracy and efficiency
- Presented Thematic Findings 2022 to the Audit Committee, using IDEA analytics and Excel for preliminary data analysis, receiving positive feedback and appraisal
- Analyzed risks and controls for IT Asset Management, Service, and Licensing Audit, enhancing risk mitigation strategies
- Tested Auditboard system for security vulnerabilities and compliance issues, using OWASP ZAP reporting any findings

Global Payments Incorporation, Plano, Texas March 2022 – May 2022

Information Technology Audit Intern

- Conducted Global Payments Inc. acquisition audit in compliance with GP's IT control standards
- Collaborated with diverse professionals to comprehend business processes, assess risks, and enhance the Risk Control Matrix (RCM)
- Identified discrepancies in two processes, resulting in recommended improvements in Identity and Access Management (IAM) during the audit

The University of Texas at Dallas, Richardson, Texas January 2022 – May 2022

Graduate Teaching Assistant

- Provided administrative support to four instructors teaching undergraduate and graduate courses on Cybersecurity Fundamentals, Network and Information Security, and Cybersecurity in Cloud Computing
- Enhanced students' understanding of various cybersecurity concepts such as cryptography using a Windows application I developed using Python, and network security tools such as Wireshark, Nmap and Metasploit in the Kali Linux OS
- Guided and motivated students to pursue COMPTIA security+ or other cybersecurity certifications as part of their career development
- Demonstrated the fundamentals of cybersecurity forensics using open source tools such as Autopsy**,** Wireshark**,** and PowerForensics

Indian Institute of Engineering Science and Technology, Shibpur, India July 2020 – July 2021

Project Engineer

- Designed and developed medical device for fungal infected skin treatment using argon gas plasma jet with 90% efficacy with a five-member team
- Implemented Confidentiality and Integrity of sample collection process of initial application of test apparatus for 10 patients
- Developed gravitational acceleration measurement apparatus using laser beams with 99.97% accuracy
- Analyzed the test data and performed regression analysis to filter out deviations and check the environment in which the apparatus was used to understand the reasons for deviations

Indian Statistical Institute, Kolkata, India March 2020 – May 2020

Artificial Intelligence Engineer

- Developed base clustering modules for pollution analysis using machine learning on Jupyter, optimizing them to reduce performance time by 30%
- Conducted Regression Analysis to analyze test data for errors and reported on error analysis
- Created a concise unsupervised clustering program for test data, consisting of only 60 lines, meeting the demand for a shorter, efficient program (including visualization codes)
- Established a Hadoop environment for Big Data across three computer systems using the Apache stack and VMware.
- Ensured Data Safety for cleaned set of proprietary experimental project data by encrypting devices using VeraCrypt

UGC-DAE Consortium for Scientific Research, Indore, India September 2019 – July 2020

Post Graduate Trainee

- Optimized input gas pressure in helium plant using proprietary software, increasing helium gas production rate by 10%
- Managed demand and supply of liquid helium and nitrogen for 200+ researchers at research center by creating a new database on the facility's cloud server
- Streamlined gas usage by converting researchers' applications from paper-based to digital forms

Mitsui O.S.K Lines, Tokyo, Japan September 2018 – August 2019

Marine Engineer V (OT Security)

- Spearheaded an OT security incident response team, successfully managing and mitigating a critical cybersecurity incident with zero downtime for ship operations
- Enhanced the ship's cybersecurity posture by integrating a state-of-the-art security information and event management (SIEM) system, increasing threat detection speed by 40%
- Collaborated with international maritime cybersecurity experts to revise and update the vessel's OT security policies, aligning with the latest industry standards and best practices