# SANJANA FARIAL OISHEE

**CYBERSECURITY ANALYST | SECURITY OPERATIONS | INCIDENT RESPONSE**

Montreal, QC | +1 514-224-6469 | s.farial.oishee@gmail.com
linkedin.com/in/sanjana-farial | github.com/SanjanaFarial

## PROFESSIONAL SUMMARY

Cybersecurity professional with a Master of Engineering in Information Systems Security and more than four years of experience across software engineering, network operations, technical support, and regulated customer operations. Hands-on security practice includes Microsoft Sentinel, Wazuh, Azure, KQL threat hunting and detection rules, vulnerability assessment, secure application development, and controlled attack-defense labs. Skilled in alert triage, log correlation, incident investigation, root-cause analysis, technical documentation, escalation, and cross-functional problem solving.

## CORE TECHNICAL SKILLS

**Security Operations and Incident Response (lab/project):** Microsoft Sentinel, Wazuh, SIEM monitoring, alert triage, incident scoping, IOC and TTP analysis, evidence collection, containment, eradication, recovery, post-incident review, playbooks

**Detection and Threat Analysis:** KQL detection-rule development, threat hunting, log correlation, Windows/Linux telemetry, EDR/XDR concepts, MITRE ATT&CK, Cyber Kill Chain, malware triage, ransomware investigation

**Vulnerability and Application Security:** Trivy, Grype, Snyk, vulnerability prioritization, Docker, secure coding, OWASP awareness, authentication, RBAC, input validation, REST API testing

**Network Identity and Cloud:** Microsoft 365, Azure, Log Analytics, NSGs, Windows Server, Linux, Active Directory (lab), TCP/IP, DNS, VPN, routing, firewall and infrastructure management, Nmap, Wireshark, Zabbix, Cisco Packet Tracer

**Automation and Engineering:** Python, PowerShell, Bash, SQL, PostgreSQL, MySQL, GitHub, GitLab, CI/CD, Jenkins, Jira, technical workflow automation

**Governance and Communication:** NIST CSF, ISO/IEC 27001, PCI DSS, GDPR, PIPEDA, incident reports, procedures, technical documentation, stakeholder presentations

## PROFESSIONAL EXPERIENCE

**Financial Care Recovery Representative | Alorica | Montreal, QC | Jul 2025 - May 2026**

- Managed sensitive accounts and transactions for a U.S. banking client under PCI DSS-aligned procedures; verified identities, investigated discrepancies, and maintained accurate case records in a regulated financial environment.
- Triaged anomalies and escalated suspected fraud, privacy concerns, security issues, and policy exceptions with clear supporting documentation.
- Applied structured problem solving and de-escalation, contributing to a 15% improvement in client satisfaction.

**Software Engineer | Mir Info Systems Ltd. | Dhaka, Bangladesh | Jan 2021 - Aug 2023**

- Investigated production incidents across Django and Odoo applications, REST APIs, and PostgreSQL workflows by reproducing issues, correlating logs with database records, documenting findings, and implementing or escalating resolutions.
- Performed root-cause analysis and delivered corrective actions that improved application stability and reduced recurring defects across development, test, and production environments.
- Applied secure coding, input validation, authentication, and role-based access controls; supported vulnerability remediation, CI/CD pipelines, API testing, and secure deployments.
- Supported production web-server installation and administration for Django and Odoo services, monitored service health, coordinated releases and rollback activities, and performed backup checks and recovery preparation.
- Translated technical findings for international users and stakeholders through product walkthroughs and live webinars, contributing to 30% business growth.

**IT Delivery Support Executive - Network Operations and Security | Banglalink | Dhaka, Bangladesh | Jul 2019 - Jul 2020**

- Monitored enterprise systems and networks with Zabbix; triaged alerts, collected diagnostics, maintained incident records, and escalated complex issues, improving incident-response workflow efficiency by 20%.
- Configured and troubleshot VPN tunnels, TCP/IP connectivity, routing, firewall access, and supporting infrastructure for secure remote access, helping maintain 99% service uptime.
- Coordinated access-control and infrastructure changes, validated network paths, documented operational risks, and prepared weekly service reports for technical and business stakeholders.
- Used Microsoft 365 to document incidents, service impact, dependencies, troubleshooting steps, and follow-up actions across technical teams.
- Built Python and Django tools that automated infrastructure tracking and operational reporting for network operations and IT delivery teams.

**Intern - Infrastructure and Service Management | Banglalink | Dhaka, Bangladesh | May 2019 - Aug 2019**

- Built a Python/Django/MySQL application to centralize nationwide network-site records and support service management.

## CYBERSECURITY PROJECTS

**Microsoft Sentinel Cloud SOC and Honeypot Lab** | Azure, Sentinel, Log Analytics, AMA, Windows Server, KQL

- Built an isolated Azure SOC lab with Microsoft Sentinel, Log Analytics, Azure Monitor Agent, Data Collection Rules, and a Windows Server VM acting as a controlled honeypot.
- Hunted across Windows and Azure telemetry with KQL to investigate failed RDP authentication, source-IP activity, geographic patterns, and indicators of compromise; documented findings and incident timelines.
- Developed KQL detection rules, analytics queries, and Sentinel workbooks to improve alert visibility and make investigations repeatable.
- Mapped observed activity to MITRE ATT&CK and Cyber Kill Chain stages and followed a formal incident-response workflow covering preparation, detection, containment, eradication, recovery, and post-incident review.

**Enterprise Attack-Defense Homelab - ProjectX** | Active Directory, Wazuh, Kali Linux, Windows, Ubuntu

- Built a multi-VM enterprise environment with Active Directory, Windows and Linux endpoints, email services, centralized SIEM/XDR monitoring, and an isolated attack host.
- Executed controlled scenarios covering reconnaissance, phishing, credential access, lateral movement, privilege escalation, persistence, and data exfiltration; analyzed IOCs and TTPs and mapped activity to MITRE ATT&CK.
- Performed lab-based malware triage and ransomware investigation using process, authentication, file-system, endpoint, and network telemetry; documented scope, containment, recovery, and lessons learned.
- Collected and correlated evidence across hosts, identified affected systems, and documented escalation paths and remediation recommendations for each controlled scenario.

**Container Security and Vulnerability Assessment** | Docker, Kali Linux, Python, Trivy, Grype, Snyk

- Scanned container images with Trivy, Grype, and Snyk; compared findings, assessed risk, prioritized remediation, and documented image-hardening recommendations.
- Reviewed container and application logs after controlled attacks and tracked corrective actions to reduce recurring vulnerability exposure.

**Network and Firewall Configuration Practice** | Cisco Packet Tracer, TCP/IP, routing, segmentation, access controls

- Modelled network topologies and practised device configuration, routing, connectivity troubleshooting, segmentation, firewall rules, and network access-control concepts in a simulated environment.
- Tested traffic paths and access rules while documenting configuration changes and troubleshooting steps for repeatable network support and security review.

**DefenX360 Cybersecurity Platform Proposal for SMEs** | NIST CSF, ISO/IEC 27001, PIPEDA - Co-developed a security platform concept aligning monitoring, incident-response workflows, risk visibility, compliance automation, and policy requirements with NIST CSF, ISO/IEC 27001, and PIPEDA. Defined practical capabilities for security reporting, policy management, and response coordination for SMEs.

## SECURE APPLICATION PROJECTS

**Secure eLearning Platform - BYLCx** | Python, Odoo, PostgreSQL, RBAC, JavaScript

- Built a scalable learning platform with role-based access control, real-time chat, analytics, and secure backend workflows for user, content, and course administration.
- Implemented permission boundaries and administrative workflows to separate user roles and protect sensitive application functions.

**ERP System Development for Mir Group of Companies** | Python, Odoo, ERP, HTML, Kanban

- Developed integrated ERP workflows for HR, payroll, accounting, sales, CRM, invoicing, and multi-location inventory; automated processes and built KPI dashboards to improve accuracy and operational visibility.
- Supported controlled access, data validation, workflow testing, and issue resolution across interconnected business modules.

## EDUCATION AND CREDENTIALS

**Master of Engineering - Information Systems Security** | Concordia University, Montreal, QC | 2025

Advanced study and applied projects in information systems security, network defense, risk analysis, privacy, and secure systems.

**Bachelor of Science - Computer Science and Engineering** | Ahsanullah University of Science and Technology, Dhaka | 2019

Foundation in software development, databases, operating systems, computer networks, algorithms, and systems analysis.

**Credentials:** Red Hat Certified System Administrator (RHCSA) | CompTIA Security+ exam preparation in progress

**Professional Development:** HackCTF Cybersecurity Hackathon participant (2024-2025)

## ADDITIONAL QUALIFICATIONS

**Published Research:** "An Improved Method for Facial Expression Recognition Based on Extended Local Binary Pattern and Differential Features," IEEE ICCIT, 2019 | DOI: 10.1109/ICCIT48885.2019.9038395

**Leadership:** Director, Graduate Student Association, Concordia University

**Languages:** English (Fluent) | French (B1 - Intermediate)

**Security Focus:** SOC operations, incident response, detection engineering, threat hunting, vulnerability management, cloud security, and secure software development