JEEVA KUMARADAS

Cybersecurity Analyst

14 Nicks Street, Bowmanville, ON L1C 5P3 | jeeva_richardon@yahoo.com | +1 647 774 4190
linkedin.com/in/jeeva-kumaradas | https://www.securewithjeeva.ca

SUMMARY

Cybersecurity Analyst with hands-on experience in SIEM (IBM QRadar), endpoint detection, vulnerability management, log analysis, and network forensics. Completed a cybersecurity internship at DDSB with real-world exposure to QRadar, SentinelOne, and threat monitoring. Cross-trained with the networking team to gain insights into server and storage infrastructure. Familiar with creating offense rules in a lab setting and supporting phishing simulations, vulnerability assessments, and system hardening efforts. Strong foundational knowledge backed by labs, certifications, and a passion for continuous learning.

SKILLS

- **SIEM & Detection:** IBM QRadar, Splunk (basic), Custom Offense Rules, Log Analysis
- **Vulnerability Management:** Nessus, OpenVAS, Patch Management, CVSS Scoring
- **Incident Response:** Root Cause Analysis, NIST 800-61, Evidence Collection, Phishing Playbooks
- **Endpoint & Network Security:** SentinelOne, Wireshark, DNS Log Analysis, Packet Capture
- **GRC & Documentation:** Risk Assessments, Security Awareness, Training Reports, TAP Systems
- **OS & Platforms:** Windows Server 2019, Windows 10, Ubuntu, pfSense, VMware Workstation

SELECT HOME LABS & PRACTICAL EXPERIENCE

Demonstrated hands-on skills aligned with real-world cybersecurity operations**:**

- **DNS Log Analysis Lab**

  Enabled detailed DNS logging to investigate Indicators of Compromise (IoCs), simulate beaconing behavior, and correlate logs with potential malware activity.

- **Wireshark Network Traffic Analysis**

  Captured live network traffic and used protocol filters to identify abnormal behaviors and reconstruct TCP sessions, simulating network forensics scenarios.
- **SIEM Offense Creation with IBM QRadar**

  Created custom offense rules to detect simulated brute force and lateral movement attacks. Tuned offenses to improve detection accuracy and reduce false positives.
- **Nessus Vulnerability Scanning Lab**

  Executed authenticated scans, identified critical CVEs, and prioritized remediation based on CVSS scores and business risk impact.
- **Threat Hunting Basics**

  Used MITRE ATT&CK as a framework to develop hunting hypotheses, analyze Windows event logs, and detect signs of privilege escalation and lateral movement.
- **Malware Behavior Analysis Lab**

  Executed malware in a controlled lab to analyze DNS beaconing, persistence mechanisms, and registry changes, simulating a malware triage workflow.
- **Incident Response Playbook (Phishing)**

  Created a step-by-step phishing response guide following NIST 800-61, incorporating detection, containment, eradication, and recovery phases along with communication protocols.
- **SOC Home Lab Deployment with IBM QRadar CE**

  Successfully built and interconnected a full SOC lab using VMware Workstation. Configured pfSense (firewall/router), IBM QRadar CE (SIEM), Windows 10 (Workstation), Windows Server 2019 (Domain Controller), and Ubuntu Linux (Syslog/source). Demonstrated inter-VM communication, log forwarding, rule creation, and asset monitoring in a simulated enterprise environment.

PROFESSIONAL EXPERIENCE

CYBERSECURITY ANALYST INTERN

Durham District School Board – Whitby, ON | 05/2024 – 08/2024

- Monitored and analyzed security alerts using QRadar SIEM and SentinelOne XDR.
- Conducted root cause analysis for multiple threat events and documented findings.

- Supported phishing simulation campaigns and reported results to senior analysts.
- Participated in patch management and asset hardening exercises.
- Assisted in internal vulnerability assessments and remediation tracking.
- Cross-trained with the Networking team to understand server and storage infrastructure, including backups, file systems, and directory services.

FACILITY SERVICES WORKER

Durham District School Board – Whitby, ON | 09/2020 – Present

- Performed daily inspections and maintained physical security across school facilities to ensure compliance with DDSB safety protocols.
- Monitored access control systems, documented incidents, and escalated security concerns to relevant departments.
- Supported emergency procedures by coordinating with internal staff and external responders during drills and real events.
- Ensured timely reporting and resolution of facility issues through digital logs and maintenance platforms.

NUTRITION AIDE

Toronto Western Hospital – Toronto, ON | 02/2013 – 02/2021

- Maintained dietary compliance records and simplified data entry processes for audit readiness.
- Supported communication between nursing staff and dietary team, ensuring accurate delivery of meal plans and documentation.
- Used Microsoft Office tools for recordkeeping and handled confidential patient dietary data.

OPERATIONS MANAGER

Jairo Group of Hotels – Chennai, India | 03/2008 – 07/2011

- Led cross-functional teams, managed crisis communications, and ensured business continuity during peak disruptions.
- Developed SOPs and training material for customer service and operational processes.
- Supported internal audits, compliance documentation, and risk reviews.

GUEST SERVICES SUPERVISOR

Jairo Group of Hotels – India | 06/2005 – 02/2008

- Handled guest escalations, led front desk operations, and managed VIP protocol coordination.
- Staff training and reporting infrastructure maintenance issues.

EDUCATION

- Network Security and Architecture – Fanshawe College (Grad: 12/2024), Ontario
- Complete Python Developer – Zero to Mastery Academy (06/2024 – 07/2024)
- Bachelor's Equivalent in Hotel Management – EMPEE Institute, India (Credential Evaluation Available Upon Request)
- Post Grad Diploma – Computer Applications – IIC India (2002 – 2003)

CERTIFICATIONS

- CompTIA CySA+ (Credential ID: COMP001020000800563, Expires Apr 2028)
- ISC2 Certified in Cybersecurity (CC) – ID: 844264, Issued Apr 2024
- Cloud Security Fundamentals – Palo Alto
- EC-Council Intro to Dark Web, Anonymity, & Cryptocurrency
- TryHackMe: Jr Penetration Tester
- Palo Alto Cloud Security Fundamentals
- AWS Security Labs (CloudWatch, GuardDuty, IAM)

LANGUAGES

English – Advanced | Tamil – Fluent