JEEVA KUMARADAS

CYBERSECURITY ANALYST

CONTACT

☎ 647-774-4190

✉ jeeva_richardon@yahoo.com

📍 Bowmanville, Ontario

🌐 https://www.securewithjeeva.ca

in www.linkedin.com/in/jeeva-kumaradas-info-shield

EDUCATION

2022 - 2024
FANSHAWE COLLEGE

- Network Security & Architecture
- GPA - 3.2

2002 - 2005
EMPEE INSTITUTE

- Bachelor's Equivalent - Hotel Management

SKILLS

- SIEM & Detection
- Endpoint & Network Security
- Vulnerability Management
- Incident Response & Analysis
- Cloud Security
- Reporting & Documentation

PROFILE

Cybersecurity Analyst with hands-on experience in SIEM monitoring, endpoint security, vulnerability assessment, and incident response. Built and managed SOC lab environments and contributed to phishing simulations and detection workflows. Currently pursuing ISO 27001 Lead Implementer certification.

TECHNICAL SKILLS & GOVERNANCE

- Governance & Compliance: ISO 27001, ISO 31000, NIST 800-53
- SIEM & Detection: Splunk, IBM QRadar, Log Analysis, Alert Tuning
- Endpoint & Network Security: Defender, SentinelOne, pfSense, Wireshark
- Vulnerability Management: Nessus, Rapid7, CVSS, Remediation
- Cloud & Systems: AWS (EC2, IAM), Windows Server, Ubuntu, VMware

SELECT HOME LABS & PRACTICAL EXPERIENCE

- SOC Lab Build: Deployed pfSense, Splunk, Windows Server, and Ubuntu lab with centralized log forwarding, detection rule creation, and firewall traffic analysis in AD-integrated scenarios.
- AWS EC2 & IAM: Configured EC2 instances, SSH, Security Groups, IAM roles/policies, CLI access, and MFA implementation.
- Network & Log Analysis: Simulated DNS beaconing, analyzed Windows Event Logs, conducted packet capture and session analysis using Wireshark, and performed Nmap asset discovery with OS fingerprinting.
- Vulnerability Management: Executed Nessus scans for CVE identification, CVSS scoring, and remediation reporting.
- Phishing Simulation & Incident Response: Deployed GoPhish campaigns, developed NIST 800-61–aligned IR playbooks, and documented IOCs and escalation workflows.
- System Hardening & SOC Operations: Applied endpoint hardening baselines, configured NTP for SIEM accuracy, optimized DNS resolution, and authored Tier 1 SOC SOPs (alert triage, false positives, escalation procedures).

CERTIFICATIONS

- CompTIA CySA+ (Expires 2028)
- ISC2 Certified in Cybersecurity (CC)
- ISO/IEC 27001 Lead Implementer (Exam Expected Q2 2026)

ADDITIONAL LEARNING

- AWS Security Labs (CloudWatch, GuardDuty, IAM)
- Palo Alto Cloud Security,
- TryHackMe Jr Pen Tester Path

LANGUAGES

- English (Fluent)
- Tamil (Fluent)

WORK EXPERIENCE

Durham District School Board **05/2024 – 08/2024**
CYBERSECURITY ANALYST INTERN

- Triaged and investigated security alerts in IBM QRadar and SentinelOne; escalated validated incidents according to SOC playbooks and escalation procedures.
- Analyzed phishing emails and associated IOCs; documented findings and recommended containment actions.
- Conducted vulnerability scans using Rapid7 and Nessus; reported CVEs, assessed CVSS severity ratings, and tracked remediation efforts.
- Reviewed Microsoft Defender for Endpoint alerts; identified and flagged likely false positives to reduce alert noise.
- Supported SaaS security reviews through TAP due diligence assessments.
- Assisted with network configuration tasks including AP swaps, port changes, and Aruba Central uploads; gained exposure to Fortinet firewall workflows and VMware vSphere environments.
- Maintained detailed ticket documentation and updated SOPs to ensure accurate incident tracking and clean operational handoffs.
- Shadowed Fortinet stack (FortiGate, FortiManager, FortiAnalyzer, FortiSandbox, FortiAuthenticator) and documented firewall policy and logging observations.

Durham District School Board **09/2020 – Present**
Educational Assistant

- Supported students in structured learning environments while maintaining strict confidentiality of student records and sensitive information in accordance with board policies.
- Monitored classroom and common areas to ensure a safe environment, identifying and reporting behavioral or safety concerns in a timely manner.
- Documented incidents accurately and provided detailed reports to teachers and administration, ensuring proper escalation and follow-up.
- Assisted in implementing individualized support plans, following established procedures and compliance guidelines.
- Collaborated with multidisciplinary teams to manage risk, address emerging concerns, and maintain a secure and inclusive learning environment.
- Applied conflict resolution and de-escalation techniques to manage high-stress situations effectively.