JEEVA KUMARADAS

Toronto, ON L1C 5P3 | jeevarichardon@gmail.com | +1 647 774 4190 |
www.linkedin.com/in/jeeva-kumaradas-info-shield | Certifications: CompTIA CySA+, ISC2 CC
|https://www.securewithjeeva.ca

PROFESSIONAL SUMMARY

Cybersecurity Analyst with hands-on experience in SIEM platforms (QRadar, Splunk), endpoint protection, vulnerability scanning, and incident response. Completed a cybersecurity internship with DDSB supporting security monitoring and phishing simulations. Developed and managed a custom SOC lab for practical training in threat detection, log analysis, and cloud security. Passionate about security operations, eager to contribute to a fast-paced SOC environment, and continually improving technical skill sets through real-world labs and training.

Cybersecurity Experience & Projects

Technical Skills

- **SIEM & Detection:** IBM QRadar, Splunk, Event Correlation, Log & Alert Analysis
- **Endpoint & Network Security:** Microsoft Defender for Endpoint, SentinelOne, pfSense, Wireshark, DNS Monitoring, Cisco Security Concepts
- **Vulnerability Management:** Rapid7 InsightVM, Nessus, OpenVAS, CVSS Scoring
- **Incident Response & Analysis:** NIST 800-61, Root Cause Analysis, Evidence Preservation
- **Cloud Security:** AWS IAM, EC2, VPC/Subnets, GuardDuty, CloudShell, AWS CLI
- **Platforms & Tools:** Windows Server 2022, Windows 10, Ubuntu, VMware Workstation
- **Reporting & Documentation:** SOPs, Phishing Reports, Vulnerability Summaries, Risk Logs

SELECT HOME LABS & PRACTICAL EXPERIENCE

Full Lab Portfolio: securewithjeeva.ca/labs

- **SOC Lab Build**: pfSense, Splunk, Windows Server, Ubuntu – log forwarding and detection rules.
- **AWS EC2 & IAM Labs**: Configured SSH, Security Groups, IAM roles/policies, CLI, MFA.
- **DNS Analysis**: Simulated DNS beaconing and investigated logs via Event Viewer.
- **Phishing Playbook**: Designed IR workflow for phishing attacks based on NIST 800-61.
- **Wireshark Packet Capture**: Identified malicious traffic, session analysis.
- **Nessus Scanning**: CVE identification, CVSS scoring, reporting.
- **Nmap Asset Discovery**: Network scanning, OS fingerprinting.
- **Time Synchronization**: Configured NTP on Kali & Windows for SIEM accuracy.
- **System Hardening**: Applied rules, hosts file config, and DNS resolution testing.

- **Firewall & Packet Review:** Used pfSense and Wireshark to analyze firewall rules and captured traffic, focusing on AD-integrated network scenarios.
- **GoPhish Simulation:** Deployed phishing simulation campaigns and trained mock users on phishing red flags and email security hygiene.
- **SOC SOP Development:** Authored step-by-step playbooks for Tier 1 tasks like alert triage, false positive handling, IOC documentation, and escalation procedures.
- **System Hardening & Audit Readiness:** Applied hardening baselines across lab endpoints, reviewed security configurations, and created audit-aligned documentation.

PROFESSIONAL EXPERIENCE

CYBERSECURITY ANALYST INTERN

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

- Monitored alerts and performed triage using QRadar SIEM and SentinelOne EDR.
- Investigated phishing emails, analyzed IOCs, and escalated suspicious activity.
- Performed vulnerability scans using Nessus and Rapid7 InsightVM, tracked remediation, and documented CVSS risk levels.
- Reviewed Microsoft Defender for Endpoint alerts, identified false positives, and coordinated response with IT.
- Assessed SaaS application security through DDSB's Third-Party Approval Process (TAP).
- Collaborated with Cisco network team to review firewall rules, packet captures, and AD-integrated security policies.
- Created phishing simulation reports using GoPhish and trained staff on phishing indicators.
- Participated in system hardening checklists, baseline image reviews, and audit preparation documentation.
- Documented SOPs for SOC Tier 1 tasks, improving onboarding efficiency.

Technical Support (Cybersecurity & IT)

Various Lab & Internship Projects | 2022 – 2024

- Provided technical support for simulated and real-world issues in a SOC lab and internship, including troubleshooting endpoint, network, and cloud security problems.
- Diagnosed and resolved configuration errors, connectivity issues, and software conflicts in Windows Server, Windows 10, and Ubuntu Linux systems.
- Utilized Microsoft 365 Security Center and Defender for Endpoint to investigate phishing emails, analyze headers, check user activity, and review quarantine reports.
- Configured and tested Microsoft Defender policies, including Safe Links, Safe Attachments, device control, and attack surface reduction rules, across test endpoints.
- Performed endpoint and network vulnerability scans using Rapid7 InsightVM, identified risk levels using CVSS scores, and tracked remediation steps.
- Practiced Cisco security concepts such as VLAN segmentation, ACLs, port security, and monitored packet activity using Wireshark and pfSense logs.

- Responded to simulated SOC alerts in QRadar and Splunk, categorized severity, and initiated test triage playbooks.
- Delivered user support by explaining phishing alerts, assisting with MFA setup, and walking through email security best practices.
- Documented technical steps, false positives, resolution timelines, and built reusable troubleshooting SOPs.

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.

EDUCATION & CERTIFICATIONS

- **Post-Grad Certificate** – Network Security & Architecture, Fanshawe College
- **CompTIA CySA+** (Expires 2028) | **ISC2 Certified in Cybersecurity** (CC)

ADDITIONAL LEARNING

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