Elias Ibrahim, CISSP-CCSP

Cybersecurity Solutions Architect / Consultant

Ottawa, Ontario

PROFILE

Security minded professional with significant experience leading teams on corporate security projects and large-scale SIEM implementation for fortune 50 Security Operation Centers, providing security architecture and SIEM subject matter expertise by reviewing or creating new data lake designs.

SKILLS

- Highly collaborative with exceptional coaching, analysis, written, presentation and verbal skills.
- Strong Business Acumen, Project and People Management, and Cross-Functional Leadership.
- Run to Problems, Detail Oriented, Results Driven, Critical Thinker, Creative Problem Solver.
- Specialize in Security Frameworks, Controls, Security Operations and Secure Design principles.

QUALIFICATIONS

- Demonstrated expertise in overseeing the architecture and providing reference documentation for the cybersecurity operations technology landscape at fortune 50 and government sites.
- Significant experience in designing and implementing architectural processes for efficient threat detection, assessment, and response, and in translating complex technical requirements.
- Proficient in architecting scalable systems for real-time data analysis and maintaining frameworks for log aggregation and normalization, to support advanced threat detection and response.

CERTIFICATIONS

- Google Cybersecurity certificate, CCSP, APISec, ICS, PentesterLabs. **2023**
- Active CISSP, Azure, AWS, SnowFlake. **2022**
- Former ITIL + Networking Technology + MSCE (NT4). **1998 - 2022**

EDUCATION

La Cite Collegiale, Ottawa – ***Management Information Systems*** **1994 - 1997**

EXPERIENCE

Shared Services Canada, Ottawa – **Security Design Specialist**

June 2023 – August 2023

- Lead security architect on a Security Attestation & Accreditation national security system.
- Reviewed design documents, documented gaps and tracked the security controls in a matrix.
- Provided constructive feedback after reviewing artifacts, architecture and technical diagrams.
- Prepared and presented an executive summary presentation to project leadership.

Securonix, Ottawa – **Customer Success Manager**

FEBRUARY 2022 - OCTOBER 2022

- Trusted advisor to the SOC lead and Managers in a customer facing role for clients in multiple industries, providing subject matter expertise on the SIEM, Threat Intel and SOAR products.
- Supported the delivery teams for service requests, contract issues, incident management, customer escalations, and areas of service improvement.
- Mentored the implementation team and security staff on information security best practices.

Micro Focus, Ottawa

NOVEMBER 2021 – FEBRUARY 2022 - Senior Integration Test Engineer

- Created environments and payloads to test mitigations for vulnerabilities in ArcSight products.
- Helped develop and test the Log4J mitigation across the ArcSight product suite.
- Identified waste and gaps in processes and devised a plan to improve the end-user experience.
- Performed penetration testing on ArcSight products to validate pre-release security mitigations.

AUGUST 2020 – NOVEMBER 2021 - Technical Lead Customer Success Manager

- Trusted advisor to fortune 100 ArcSight customers, often in difficult and demanding situations, capturing their pain points and translating them into features to satisfy their urgent needs.
- Coordinated internal resources and led cross-functional efforts to resolve customer pain points.
- Assisted Pre-Sales and PS on large deals with architectural expertise with designs for +1M EPS.
- Created technical enablement training with videos, documents and labs on the deployment and integration of the entire ArcSight product suite on the Kubernetes platform.

MARCH 2019 – AUGUST 2020 - Security Presales (ArcSight)

- Project managed customer POC projects and coordinated architecture discovery sessions.
- Generated +$10M in renewals and additional sales by providing "White glove" treatment to strategic accounts at risk for retention, earning me the technical win award at the yearly SKO.
- Peer reviewed solution designs for Sales, PS and CS teams and technical design documents.

MAY 2018 – MARCH 2019 - ArcSight Security Professional Services Consultant

- Led customer architecture discussions in a customer facing role to integrate ArcSight
- Created internal technical content to improve the Kubernetes deployment documentation.

Environment Canada, Gatineau – **Vulnerability Assessment Consultant**

SEPTEMBER 2017- OCTOBER 2017

- Performed a Threat and Vulnerability Assessment on a web application and 3rd party software following OWASP and the ITSG framework for a Protected B security control profile.
- Assessed the infrastructure servers, the access methods used, database model, permissions, installed components, and encryption used to support the operation of the Web Application.

- Assessed the development environment, the 3rd party components used, their integration process, and their technical and business requirement documentation.
- Performed manual and automated vulnerability scans with custom policies and privilege levels.
- Presented a report with remediation steps, recommendations, and re-test instructions.

Environment Canada, Gatineau – **Network Security Analyst**

JANUARY 2017 – MAY 2017

- Led review and evaluation of InfoSec project documentation, facilitating working sessions with stakeholders and developing security processes and standard operating procedures.
- Reviewed the InfoSec project artifacts, architecture and gaps in security controls assignments.
- Assessed the Secure Laptop, Apricorn USB devices and McAfee DLP components; evaluated existing security controls and implemented additional controls to mitigate vulnerabilities;
- Developed a RACI chart outlining the responsibility, accountability, consulting, and information mappings to the roles and associated tasks of the departmental groups.
- Developed policies, security processes and standard operating procedures for custody tracking of physical assets as well as for privileged account and password management.
- Developed the Concept of Operations (ConOps) for the InfoSec project (asset management, support structure, processes, procedures, roles, tools, architecture, lifecycle, disposal, physical security, compliance, audit);
- Coached and mentored junior (CS1) staff on work tasks and security best practices introduced as part of the project.

Bell Canada, Ottawa – **Security Engineer (Icam Team)**

MARCH 2014 - MARCH 2015

- Lead DRA SME in Security Operations to manage and develop the Windows AD domains across all internal security zones in NetIQ DRA on Windows 2012 Servers for Canada.da ETI project.
- Designed and implemented access controls based on least privilege following RBAC methodology; created and documented policies, SOP, and guidelines for security controls.
- Collaborated with cross-functional teams to gather requirements as well as develop the security DRA reports for SSCOPS and their partners.

DOMAINS

SaaS | SOC | InfoSec | Cloud Security | Security Operations | Vulnerability and Risk Management
Security Data Lakes | Big Data | Threat Intel | DevOps | DevSecOps | Detection Engineering | Maturity
Stakeholder Comm | NIST | ITSG | OWASP | CIS | ISO | MITRE | CAPE | PCI-DSS | HIPAA | SA&A

TECHNICAL SKILLS

NgFW | WAF | SIEM | UEBA | SOAR | CI/CD | IPS/IDS | OAUTH | SSO | CASB | Parser Dev | XDR
EDR | Linux | Windows | Solaris | AWS | Azure | GCP | Azure AD | VMware | VirtualBox | IaC
ArcSight Transformation Hub | Securonix | Azure Event Hub/ Sentinel | Chronicle | Splunk | AWS
Kubernetes | Kafka | GitHub | JIRA | SnowFlake | Hadoop | SYSLOG | GROK | Excel | Visio