Elias Ibrahim, CISSP-CCSP-SECRET

Fully Bilingual SIEM and SOC Solutions Architect

Ottawa, Ontario

PROFILE

Customer focused and security minded professional with deep technical expertise and a strong business acumen. Strategic and tactful with a track record of customer delight, Elias has managed and led project teams on Government security projects and on SIEMs deployments for Fortune 50 SOCs.

SKILLS

- Highly collaborative with exceptional coaching, analysis, written, presentation and verbal skills.
- Strong Business Acumen, Cross-Functional Leadership, and Project and People Management.
- 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 deploying, configuring, data/log source onboarding, custom parsing, use case development and tuning SIEMs working closely with Fortune 50 SOC Staff and their partners.
- Significant experience in designing and implementing SOAR 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.

DOMAINS

SaaS | SOC | Security Operations | Security Architecture | Risk Management | Network Administration
Security Data Lakes | Big Data | Threat Intel | DevOps | Data Source Onboarding | Program Maturity
Stakeholder Comm | NIST | ITSG | OWASP | CIS | ISO | MITRE | CAPE | PCI-DSS | HIPAA

TECHNICAL SKILLS

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

EXPERIENCE

Shared Services Canada, Ottawa – **Security Design Specialist (Splunk SIEM)**

June 2023 – August 2023

- Lead Security Architect on a Security Attestation & Accreditation for a national security system.
- Reviewed detailed design documents, documented gaps and tracked the security controls using a traceability matrix; presented developers with findings using constructive feedback.
- Reported on gaps in events missing critical fields being sent to the Splunk SIEM as part of the classified national security system and advised on improvements to address SIEM related gaps.
- Managed, directed, inspired and coached the work and capability of the team often engaging with a much wider audience of 50+ virtual team members of senior managers, technical, subject matter experts and business managers.

Securonix, Ottawa – **Customer Success Manager (SIEM / UEBA / SOAR)**

FEBRUARY 2022 - OCTOBER 2022

- Trusted advisor to the SOC lead and Manager in a customer facing role for clients in multiple industries, providing subject matter expertise on the SIEM, Threat Intel and SOAR products.
- Managed several SaaS onboarding journeys to meet the business needs for strategic accounts.
- Helped onboard new log sources to strategically increase MITRE ATT&CK coverage, configured mappings and developed custom for security use cases with correlation / identity attribution.
- Supported the delivery teams on service requests, contract issues, incident management, customer escalations, and areas of service improvement.
- Prepared and presented, plans, QBRs and EBRs to executive and director-level management.

Micro Focus, Ottawa (ArcSight SIEM, SOAR, Kubernetes and ML Global Expert)

NOVEMBER 2021 – FEBRUARY 2022 - Senior Integration Test Engineer

- Moved to the engineering side to improve processes as well as the code base, provided Level 3 SIEM escalation support on customer P1s, and architecture expertise for strategic projects.
- Engineered a simulated Windows and Linux network to generate test events for a clean ML dataset, and performance testing/monitoring ArcSight Logger with Grafana and Telegraf.

AUGUST 2020 – NOVEMBER 2021 - Technical Lead Customer Success Manager (ArcSight)

- Customer facing role responsible for the adoption, value realization and product success of ArcSight security solutions in assigned fortune 100 and strategic accounts.
- 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 SIEM POC projects in a customer facing role for strategic accounts and coordinated architecture discovery-level sessions to meet their security goals.

- Provided "White glove" treatment to at risk accounts, generating over +$10M in renewals and additional sales, earning me the technical win award from the VP of Sales at the SKO.
- Helped strategic accounts onboard new log sources to meet strategic goals and augment their MITRE coverage. Identified correlation opportunities, enriched and configured field mappings, and developed custom parsing to meet the objectives of the security use case.
- Peer reviewed solution designs for Sales, PS and CS teams and technical design documents.
- Created and presented content for training, demos, and support for customer-facing teams.

MAY 2018 – MARCH 2019 - ArcSight Security Professional Services Consultant

- Led customer architecture discussions to deploy and integrate the ArcSight SIEM solution.
- Contributed to the development of the implementation team's methodology and templates.
- Led the development and documentation of architectural templates and solution designs for use in solutions, offering my expert consulting and coaching skills to project teams.

Environment Canada, Gatineau – Vulnerability Assessment Consultant (AppSec)

SEPTEMBER 2017- OCTOBER 2017

- Performed a Threat and Vulnerability Assessment on a .NET webapp and 3rd party libraries for vulnerabilities following OWASP and documented the ITSG frameworks security control profile.
- Collaborated with cross-functional teams to align Secure SDLC architecture with business goals, and led initiatives to integrate security tools and technologies.

Environment Canada, Gatineau – Network Security Analyst (Security Program)

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.
- Collaborated with cross-functional teams to align the InfoSec architecture with business goals, and led initiatives to integrate security tools and technologies.
- Evaluated new security technologies and processes, conducted architectural reviews, and proposed enhancements for system scalability and performance.

Bell Canada, Ottawa – Security Engineer (Icam Team on Canada.ca ETI project)

MARCH 2014 - MARCH 2015

- Lead DRA SME in Security Operations in building and managing the Windows AD domains across all internal security zones in NetIQ DRA on Windows 2012 Servers for Canada.da ETI project.

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**