Elias Ibrahim, CISSP-CCSP

Security Solutions Architect / Consultant

Ottawa, Ontario

SKILLS / QUALIFICATIONS

- Customer Focus, Run to Problems, Detail Oriented, Critical Thinking, Creative Problem Solving.
- Analysis, Business Acumen, Project and People Management, Cross-Functional Leadership.
- Highly Collaborative with strong mentoring, written, presentation and verbal skills.
- Experienced with Security Frameworks, Controls and Secure Design/Development principles.
- Proven success implementing security controls and coaching security to Development/QA teams.

DOMAINS

Information Security | Cyber Security | Cloud Security | SOC | Vulnerability Assessment + Mgmt.

Architecture | Application Security | DevOps | DevSecOps | Penetration Testing | Product Mgmt.

NIST | ITSG | OWASP | CIS | ISO | MITRE | CAPE | PCI-DSS | HIPAA | SA&A | ITIL | Threat model

TECHNICAL SKILLS

NgFW | WAF | SIEM | UEBA | SOAR | CI/CD | IPS/IDS | OAUTH | SSO | SAML | Gitlab | GitHub

Linux | Windows | Solaris | AWS | Azure | GCP | AD | Azure AD | VMware | VirtualBox | IaC

IAM | PAM | SQL | Python | JS | Bash | PS | API | PKI | SYSLOG | GROK | Excel | Visio | Jenkins

Docker | Tigera | RDBMS | Kubernetes | Kafka | GitHub | JIRA | McAfee | OKTA | Burpsuite

CERTIFICATIONS

- CISSP, CCSP, Google Cybersecurity certificate, APISec, ICS, PentesterLabs badges.
- Azure, AWS (Not active), SnowFlake.
- Formerly: ITIL, MSCE (NT4).
- Certification and Badge verification: https://www.credly.com/users/elias-ibrahim

EDUCATION / PROJECTS

Present - Developing an Electron(js) QR Code and URL security desktop application with a backend Python API hosted on GCP using Firebase, VM, Load balancers, App hosting, containers and MySQL.

2024 – PentesterLabs Code Review challenges, PortSwigger LLM and Web Sec labs

2023 - ICS Penetration Testing | CI/CD Goat | Security Risks in AI and Machine Learning: Categorizing Attacks and Failure Modes | Automate Cybersecurity tasks / Python | GitHub actions for CI/CD | Jenkins labs

2022 - Learning Secure Payments and PCI | Six Sigma White Belt

1998 - Networking Technology (MCSE program) @ Praxis Training Institute, Ottawa

1997 - Management Information Systems @ La Cite Collegiale, Ottawa

EXPERIENCE

WEIR Minerals – Naval Engineering, Ottawa - Senior IS Security Analyst

May 2024 – Present

- Review, comment and advise on security related SA&A project artifacts guided by NIST (53, 160, 161, 170, 171, 218), ITSG(22, 33), CSE Cyber center and the CS RMP methodology.
- Bridge the communication gap by providing constructive feedback on security in a relatable manner.

Employment and Social Development Canada, Ottawa - Security Design Specialist

February 2024 – May 2024

- Practitioner on a Dynamics 365/PowerApps SA&A I worked with the customer, development, IT, security and product teams in helping them meet their security control objectives.
- Developed a Security Concept of Operations and worked with multiple IT and Security teams in the enterprise to implement Security Controls.
- Designed processes, procedures and solutions to meet Security Control requirements and documented the evidence as part of the SCTM submission package.
- Security champion and coach providing guidance to the development and IT teams.

Health Canada, Ottawa - Vulnerability Assessment Specialist

February 2024 – May 2024

- Worked with many development teams in performing application vulnerability assessments following HTRA and OWASP guidelines using assessment tools and manual methods.
- Assessed system and application configurations for misconfigurations, as well as secrets handling.
- Performed RBAC and Access Control analysis, documented and reported findings, recommended mitigations for found issues and coached developers on secure development practices.
- Coached development teams and helping them understand findings and how to mitigate.
- Improved the Vulnerability Assessment program in place by going beyond scans and seeding the development teams with the benefits of DevSecOps when SAST is part of their workflow.

Shared Services Canada, Ottawa – Security Design Specialist

June 2023 – August 2023

- Practitioner on a Security Attestation & Accreditation for a Secure Mobile phone project.
- 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

- Managed SaaS onboarding journeys for several strategic accounts concurrently.
- 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.

Micro Focus, Ottawa

NOVEMBER 2021 – FEBRUARY 2022 - Senior Integration Test Engineer

- Advised product management and development using constructive feedback on security best practices, vulnerabilities and mitigations for the ArcSight product suite comprised of monolith and Kubernetes platforms including container security.
- Improved processes in quality management across the ArcSight ecosystem and reported findings to cross-departmental executive and director level management.
- Reviewed and updated designs for private and public SaaS ArcSight offerings
- Engineered a simulated network for event generation to identify and capture cyber-attacks.
- Developed and validated the Log4J mitigation for ArcSight products.
- World expert on Kubernetes and Kafka, helped improve support costs by reducing complexity.
- Developed and validated ANSIBLE scripts for Kubernetes and docker deployment automation.
- Reverse-engineered functionality and documented it for live customers.
- Performed penetration testing on ArcSight products to validate pre-release security mitigations.
- Engineered performance and metric capturing systems for security and IT systems.
- Created lab setups and crafted payloads for QA to test and validate mitigations for vulnerabilities in ArcSight products.

AUGUST 2020 – NOVEMBER 2021 - Technical Lead Customer Success Manager

- Led and project-managed the adoption of ArcSight and Interset SaaS security solutions for dozens of strategic clients, and acted as their trusted security advisor pre/post onboarding.
- Reviewed and validated +1Million EPS high level architectural designs for Pre-Sales and PS.
- Reviewed bare metal, AWS, Azure, GCP and Oracle Cloud Kubernetes solution architecture designs for Sales, Professional Services and Customer Success teams.
- Engineered a POC for a new product to help customers manage PKI and endpoint certificates.
- Created technical enablement training with videos, documents and labs on the deployment and integration of the entire ArcSight product suite on the Kubernetes platform.
- Contributed and led discussions with product management and development to ensure proper alignment of the product roadmap to meet customers' security needs.
- Contributed and tested IaC (Infrastructure as Code) yaml templates using Ansible and terraform in the cloud as well as on premise.
- Created knowledge base and how-to articles for support staff in troubleshooting customer P1 relating to their Kubernetes and how to resolve most of them in under 5 minutes.

MARCH 2019 – AUGUST 2020 - Security Presales (ArcSight)

- Project managed customer POC projects and coordinated architecture discovery-level sessions to understand their policies, traffic, and security event types to prove that customer needs are met.

- Supported Sales, PS and CS team during statements of work (SOW) development. Peer reviewed solution designs and configuration documents to ensure alignment with customer requirements.
- Created technical content for training, demos, and support processes for customer-facing teams.
- Initiated and completed a performance testing project to showcase the benefits of using SSDs in appliances and suggested blade architecture to reduce the barrier of entry for the next generation.
- Created custom Grafana dashboards with performance metrics agents for data-driven decisions.

MAY 2018 – MARCH 2019 - ArcSight Security Professional Services Consultant

- Led solution design and deployments, utilizing analytical skills to meet customer needs.
- Mentored colleagues and led the establishment of best security practices using templates.
- Improved Kubernetes deployment documentation and updated vendor parsers for ArcSight.
- Engineered performance and metric capturing systems for security and IT systems.

Environment Canada, Gatineau – Vulnerability Assessment Consultant

SEPTEMBER 2017- OCTOBER 2017

- Conducted a Threat and Vulnerability Assessment on a .NET Web application using OWASP Top 10 and HTRA methodology following ITSG-33 guidelines, and delivered a report with all artifacts.
- Assessed the development environment and performed a Software Composition Analysis (SCA) of 3rd party components used, their integration process, and their technical and business requirements.
- Performed manual and automated vulnerability scans using IBM AppScan custom policies.
- Assessed the development environment, the 3rd party components used, their integration process, and their technical and business requirement documentation.
- Mentored developers on secure software development best practices.
- Presented a final report of the findings with remediation steps, recommendations, and re-test instructions.

Environment Canada, Gatineau – Network Security Analyst

JANUARY 2017 – MAY 2017

- Led the review and evaluation of InfoSec project documentation, facilitating working sessions with stakeholders and developing security processes and standard operating procedures.
- Performed vulnerability assessments for the Secure Laptop, Apricorn USB devices and McAfee DLP; evaluated existing security controls and implemented additional controls to mitigate vulnerabilities;
- Provided training and knowledge transfer to service desk agents in preparation to In-Service operation; 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) / DevOps / DevSecOps

MARCH 2014 - MARCH 2015

- Lead SME for the NetIQ DRA Identity Automation product suite of the Canada.ca Email System.
- Coordinated version control and deployment of fixes/patches, managed Windows AD domains, contributed to cross-functional teams, and designed RBAC access controls based on least privilege.
- Managed the custom code in the Identity Control Access Management system, validated static code reviews/analysis (SAST) status for deployment, and triaged and prioritized defects from start to live.
- Developed custom SRSS usage and billing reports, check-in in custom code in to secure repository.