Summary

A Cyber Security Engineer and Architect who openly shares expertise in Information Systems Security with the team to build confidence, capabilities, and commitment. Safeguards company assets, privacy, sensitive data, and critical business systems by providing security prevention, detection, and remediation services. Responds to the top cybersecurity challenges that businesses face — preventing downtime, identifying, mitigating security risks, and protecting and maintaining a critical security infrastructure.

Skilled in Security Architectures, Security Designs, Security Requirements, Application Security, Forensics, Penetration Testing, Security Automation, Security Frameworks.

Professional Experience

Senior Cyber Security Engineer / Cyber Security Architect, Company Name 2013 – Present

Architected and built a sustainable cybersecurity program with a comprehensive approach that includes standardization, strong user authentication and encryption, automated security controls, and balanced access controls. Rapidly grew the program, assuming expanded roles to meet the needs of a fast-paced environment: Cyber Security Administrator, Security Architect Engineer, Security Analyst, Vulnerability Assessor, and Intrusion Detection Specialist.

- **Security Products** – Conducted an in-depth evaluation of existing products, as well as a comparison evaluation on other vendors and products. Established a process and evaluation standard that was adopted by the entire IT department and is now required before purchasing any new products.
    - Connected cloud, mobile, and web-based security products and GDPR compliance products within our environment.
- **NOC Support** – Provided extensive support, applying excellent understanding of networking topologies, internetworking concepts, access lists, direction structures, and account management.
- **Streamlined Data Capture** – Reviewed all data sources to identify opportunities to reduce redundant and legacy data loaded into our data analytics tool, by more than 700GBs daily.
    - Identified the biggest ingest within our Linux audit logs which accounted for 50%+ of our entire log ingestion - our anti-malware solution was writing its agent logs to the audit file. Reconfigured the agent and successfully reduced the log ingest by 45%.
- **Endpoint Protection** – Evaluated products against a mathematical rating model and in my research, discovered a startup company that fit our security needs; the company has since become a market leader.
    - Fully migrated to a next generation vendor. Implemented standards and policy for maintaining 100% coverage to comply with Security Insurance standards.
    - Integrated with vendor to become a development partner and part of the development board.
- **Cyber Security Operations (SOC)** – Performed ongoing analysis and created a new incident management process and standards. Constructed stop loss and highlighted large gaps within our security posture.
    - Investigated security related events and potential sensitive information leaks; as an example, led security team to respond to a CapitalOne incident, with work that included reviewing the AWS environment and looking at access management and AWS S3 bucket data.
- **Active Directory** – Through strong stakeholder communications and ongoing team coordination met a short deadline for the complete redesign and architecture of Active Directory. Provided documentation and how to guides to ensure appropriate training.
    - Implemented new administrative accounts and transferred permissions. Segmented OU groups so restricted accounts, workstations, and servers were migrated to a more controlled OU section.

- **SIEM Architect** – Architected, integrated, and fully operationalized a log collector product, Sumo Logic, and established as our Cyber Security SIEM; configured SIEM with every log source.
    - Developed detection criteria and created searches to alert against criteria. Developed a training path for users and analysts.
    - Segmented and limited access to critical data to the least privilege.
- **AWS Security** – Implemented a micro segmentation AWS environment and deployed strict AWS Security group standards and policies that were auditable.
- **O365 Security and Compliance** – Configured all O365 security tools, including Data Classification, DLP/Encryption, Threat Management policies, malware detection, email phish and spam protection, impersonation detection, and reporting.

Education

University of Houston, TX
MBA, Major - Information Security, 2016
Bachelor's Degree, Computer Science, 2013