Evan Ahmed

(732) 599-4915 | evan2580@gmail.com | Miami, FL 33101 | Portfolio: https://evan2580.github.io/evans-resume/

Santander Bank, N.A. **August 2021-Present**
Sr. Associate, Information Security

- Contribute to the definition, development, and oversight of a global network and endpoint security threat management strategy and framework on a team of 7.
- Responsible for management of the overall team(s) providing both leadership and guidance.
- Guided optimization & performance improvements across on-prem Splunk environment utilizing best practices
- Automated upgrades across Splunk and syslog servers using ansible by creating custom scripts across 50+ hosts.
- Built & maintained architectural diagrams for the flow of data from offsite to internal systems globally.
- Successfully orchestrated migration of 3000+ hosts to AWS Cloud utilizing custom built pipelines in Cribl
- Developed comprehensive architecture diagrams outlining security controls & procedures for internal systems, ensuring clarity and alignment with security best practices.
- Monitored, Developed and Maintained critical business dashboards for business critical applications across mobile, online, and branch banking.
- Controlled cost across business units by implementing custom alerts for log ingestion, incidents in ES, SOAR playbooks, missing data sources and overall health of the instance.
- Lead the team when Auditors needed to see our Disaster Recovery & Business Continuity plan ensuring it aligns with banking industry standards and compliance requirements.

University of Miami Continuing Education - Cyber Security **April 2020-Present**
Adjunct Professor

- Helping students learn the basics of becoming a well rounded cyber security analyst, also mentoring them in my free time to help them get certifications Sec+, Net+, Splunk, Cribl.
- Foster a collaborative and interactive learning environment
- Encourage student participation and hands-on practice with Virtual Box and multiple VM's, Kali, Windows, Ubuntu.
- Effectively convey complex cybersecurity concepts in a clear and concise manner.
- Actively seek feedback from students and peers to improve teaching methods and using pedagogical methodologies.

Tekstream Solutions **August 2020-August 2021**
Sr. Splunk Consultant

- Multiple Splunk Consulting engagements CVS pharmacy data quality analysis and optimization 100+ indexers, Search Head Cluster, Cluster Master, Deployer, Deployment Server, Multiple sites.
- Quantum Research standing up a full installation of Splunk Core with SSL certificates 4 indexers, 3 SH's, multiple forwarders.
- Implementation of Splunk CMMC for compliance with DFARS & NIST protocols of all Practice Libraries.
- Argo AI configuration and full installation of Splunk Enterprise Security of all best practices and standards, helping onboard all assets and identities and create use cases for alerts.
- Splunk Admin On Demand answering all troubleshooting calls with customers and fixing issues answering their questions, creating dashboards, onboarding data and all admin tasks that were needed to satisfy the customer.
- Owning all technical aspects of splunk build and dashboard development. Performing hands-on architecture, design, and development of systems
- Manage and maintain multiple clusters in multiple sites for FedEx ensuring uptime & reliability for team.

Santander Bank N.A, Miami, FL **July 2019-July 2020**
Splunk Administrator

- Splunk ES admin developing correlation searches across data sources based on specific threats.
- Validated all new data coming into Splunk ensuring it was CIM compliant for specific Data Model mappings.
- Managed both the production and dev environments for all upgrades globally.
- Wrote powershell scripts to automate all repetitive tasks for ingesting data into splunk.
- Optimized searches based on requirements, converting them into Accelerated datamodels
- Pulled daily alerts from IBM Resilient performing incident response & analysis across P2,P3 incidents escalating them to the global SOC.
- Wrote Python scripts to ingest data into splunk via the HEC from API calls within virustotal and phishme.
- Some of the other technologies that I use on a sporadic basis are Crowdstrike, Cyberark, Mcafee EPO, Threatmetrix, Oracle DB, Ironport, Demisto, Phantom, SOAR and Checkpoint firewall.

Tire Barn, North Brunswick, NJ **January 2003 – July 2019**
Network Administrator/Pen Tester

- Use Burpsuite to intercept traffic to send to repeater for further inspection, Wireshark to monitor network traffic and help secure the LAN by analyzing packets coming in to e-commerce and wholesale tire websites. Test the sites with Burpsuite for XSS, Sql Injection and OS to check if the site is vulnerable to those types of attacks.
- Gained hands on experience in conducting Web Application Security scan, Network Penetration Testing and Ethical Hacking using commercial and non-commercial applications and methodologies such as OWASP Top 10, Burp Suite, Firefox Add-ons XSS Me, SQL InjectMe, and others. Used these tools to determine the security of a given web application developed in Javascript, J2EE, AJAX, PHP and many others.
- Writing Javascript, Ajax, Json, Jquery, Node.js for everyday full stack development to learn how everything works on the web and keep up with current technologies and doing self research if I do not understand something.
- Keep the Network up and running, ensuring it doesn't go down by utilizing Splunk to analyze data coming into the network, check for unusual activity, and create pivot tables for upper management. Analyze the Splunk data for anomalies.
- Knowledge of the FS-ISAC traffic light procedures in the FinTech industry and understand the value of sharing information for cybersecurity issues and how important it is.

Education

- Bachelor of Science – Computer Science Rutgers University

Certifications and Training

- **Splunk** - User, Admin, Architect, Core Certified Consultant, Enterprise Security.
- **Cribl** - fundamentals 1, Data Collection and Replay, Managing Data with Gitops
- **Certified Ethical Hacker** - EC - Council, Passed October 2018
- **Rutgers Continuing Education**: Javascript, JSON, AJAX, MongoDB, React, Angular, Express, Node.js
- Microsoft Azure Security Solutions, Edx Analyzing Data with Python
- AWS Cloud Practitioner

Skills

- Good knowledge of web development with strong front-end skills in JavaScript, JQuery and HTML
- **Foreign Language**: Conversational Spanish and Portuguese
- **Computer**: C++, PERL, Python, Java, Cyber Security, Networking Technologies, MS Office, Metasploit, Nessus, Nmap, Netcat, Wireshark, Burp, John the Ripper, Kali Linux