Resumes

* 1. Resume – Eric R. Smith

eric r. smith

Proposed Labor Category: Security ANALYST

Summary of Qualifications

Eric Smith is an accomplished Software Engineer with strong domain knowledge in Cybersecurity. An NSA approved “Information Systems Security Professionals” and CISSP, Eric has a unique combination of academic qualifications and industry experience. His expertise and familiarity with various cybersecurity tools and applications such as FireEye, Splunk and WireShark along with his experience working on cloud platforms gives him a distinct edge to see through the vulnerabilities of an organization and recommend the security measures to strengthen their security posture. He has been supporting the five pillars of Zero Trust for multiple customers.

Eric brings strong technical knowledge of object-oriented programming, web development technologies, and security applications. Eric is a self-driven professional, always eager to learn new technologies and is known as a committed team player. His expertise includes the implementation and the configuration of MS O365 E3/E5, MS Azure, AWS, and Cloud Application Security Brokers (CASB).

Education

**Bachelor of Science**, Computer Science

Minor: Computer Information System  
*James Madison University*, Harrisonburg, VA May’18

Security Clearance

IRS Cleared, public trust, MBI

Certifications and Training

Certificates

* NSA approved “Information Systems Security Professionals”, NSTISSI No. 4011 certification
* CISSP

Tools/Frameworks

* FireEye Security Products, IDA Pro, Kali, Splunk, Docker, VMWare, Wireshark, Elasticsearch, MS O365, SharePoint, OneDrive

Relevant Experience

Technuf LLC*, Rockville, MD*

**Security Analyst (IRS Contractor)** Oct’18–Present

* Intimately familiar with the IRS cybersecurity environment, infrastructure, policies and processes
* Supported on-prem, on-cloud and hybrid cloud initiatives
* Have collaborated with multiple IRS stakeholders including EOPS, UNS and various BU’s to successfully deploy FireEye/Trelix agents on approximately eleven thousand Wintel and Linux servers
* Currently supporting Operation and Maintenance of the HIDS-EDR program with close collaboration of CSIRC security analysts
* Supporting the IRS with event process optimization with data integration with Splunk and Robotic Process Automation framework, Phantom
* Served as a subject matter expert for FireEye’s Endpoint Security system (FireEye HX) within the IRS for their Computer Security Incident Response Center (CSIRC).
* Setup FireEye HX appliances in multiple environments for high availability/disaster recovery and performed functional and performance testing within the test environment.
* Prepared architectural diagrams and documentation for the endpoint detection and response system which the IRS uses monitor 130,000+ endpoints.
* Integrated the security appliance with Splunk and created dashboards for easy digestion of data and events.
* Created Indicators of Compromise (IOCs) based on the Mitre ATT&CK framework.
* Performed threat hunting activities in relation to the SolarWinds SUNBURST supply chain attack.
* Collaborated with the Criminal Investigation unit in the IRS to stand up their Endpoint Detection and Response environment.

**Penetration Tester** Dec’20– Present

* Performed initial enumeration scanning to map out client’s environments.
* Used various tools and scripts to perform vulnerability scanning of servers.
* Utilized BloodHound to analyze Active Directory environments and recommend ways to secure attack paths.
* Created reports for clients outlining risks of security weaknesses and ways to mitigate them.

**Test Automation Engineer** Dec’19 – Oct’20

* Led effort to deploy Selenium Grid testing framework for test automation.
* Configured Selenium hub and node architecture for mobile and desktops
* Wrote Selenium WebDriver test cases and TestNG test suites for a NodeJS web application.

Plus3 IT Systems, *Reston, VA***Cloud Development Intern** Jun’18–Aug’18

* Utilized ServiceNow cloud software to implement and automate a company-wide training reimbursement form.
* Led team through Agile methodologies to plan sprints and manage requirements.
* Teamed with skilled company professionals in maturing project deliverables.

Coursework and Relevant Interests

* Interests: Malware Analysis, Endpoint Security, Penetration Testing, Network Security, Incident Response
* Relevant Coursework: Technical Writing, Cyber Defense and Security, Computer Systems

Skills

**Programming/Scripting Languages:**

Java, JavaScript, C, C++, Python, Bash, PowerShell