Shane Pusz
New York, NY | shane@shanepusz.com

EXPERIENCE

Appalachian Information Security, LLC | New York, NY
Independent Consultant, Owner November 2023 - Present

- Identified source of and public infrastructure involved with healthcare company ransomware attack. Collaborated with client and local FBI field office to reverse encryption and restore business functionality.
- Leveraged self-hosted security infrastructure, including Splunk SIEM and Python scripts, in order to quickly understand and remediate client infrastructure in post-breach environments.
- Responded to spear phishing incidents, including security event impact analysis, external threat actor research, and internal communications.
- Initialized security programs for various small businesses by creating incident response playbooks, performing cloud infrastructure security posture management, and leading security maturity assessments.

Aetion | New York, NY
Staff Security Engineer October 2022 - August 2023

- Initiated and led Product Security function by collaborating with engineering teams to identify, track, and remediate 12,000 dependency based vulnerabilities across microservice architecture.
- Consolidated data from multiple vulnerability reporting sources and automated remediation verification workflows by creating a custom vulnerability management pipeline with Python and Jira, reducing product vulnerabilities by 98%
- Created Python based custom tooling for cloud native forensics, allowing analysis of AWS S3 based logs on the order of 30 million records per hour.

Flatiron Health | New York, NY
Security Engineering Manager, Staff Engineer March 2020 - September 2022

- Designed and deployed an automated host deployment pipeline that uses Terraform, Ansible, Vault, and Jenkins CI/CD, to create, maintain, and monitor Linux and Windows cloud infrastructure, reducing deployment time and manual inputs by 70%, increasing reliability and ability for engineers to more safely deploy and experiment with infrastructure as code.
- Created and productionized custom company-wide digital asset inventory system to track cloud and physical infrastructure, allowing operational teams to track assets, metadata, and tooling health from one central SIEM (Splunk).
- Onboarded 2 junior developers during pandemic, while increasing team project output and task completion by 50%.

Senior Security Engineer, Technical Team Lead August 2019 - March 2020

- Added structure and direction to new security team vertical by building out initial project plans, agile ceremonies, overall team structure, roadmaps, and core process documentation.
- Reduced fleet wide upgrade time for agent based critical monitoring solution from several hours to minutes by leveraging modular Ansible solution.
- Led a team of three engineers to identify, architect, and deploy industry leading tooling and applications to automate day-to-day security team operations and long term goals, consolidating technical processes while reducing costs.

Senior Security Engineer, Incident Response June 2017-August 2019

- Led incident response efforts across engineering and the rest of the organization to respond to, mitigate against, and resolve critical security threats, risks, and other incidents.
- Subject matter expert for Splunk SIEM product, including administration of on-prem instance, technical lead for cloud migration, and resource for effective usage across engineering departments.
- Collaborated closely with IT on operational process improvements, including firewall configurations, appliance and fleet observability, and incident response playbook automations.
- Subject Matter Expert to Privacy and Legal teams for successful incident response programs and

sensitive internal investigations.

Metlife | Cary, NC
IT Risk & Security Analyst January 2015-May 2017

- Engineered vulnerability management platform that leverages vendor APIs in Python code to sort through international vulnerability data to distribute automated actionable reports and metrics on a global scale.
- Automated Infrastructure Security team metrics program, eliminating data entry errors and increasing department visibility into international vulnerability management, saving 20 hours in operational workloads
- Collaborated with several engineering teams and the vendor Tanium to leverage the Tanium API for automated global reporting of software versioning, patch statuses, and additional security information.

Education

University of North Carolina at Chapel Hill | Bachelor of Science in Information Science May 2014
Data Structures | Numerical Analysis | Usability Testing and Evaluation | Text Mining | Classical Mechanics