

Joshua Smith
Email: smithjk@infosecworx.com | [LinkedIn](#)
Twitter: [@n0hats](#)

- Summary -

Highly accomplished Information Security leader with 15+ years of experience delivering robust solutions across all domains. Proven track record in proactive threat mitigation and staying ahead of security trends. Passionate about fostering junior colleagues' professional development through collaboration and mentoring. Eager to leverage experience to empower others and cultivate a culture of continuous learning. Maintained top-secret clearance with polygraph, accessing exclusive training opportunities in social engineering and tradecraft for evasion.

Specialties: Splunk, Devo, MITRE ATT&CK (Attack), NipperStudio, BurpSuite Pro, Metasploit Framework, PowerShell, Open Web Application Security Project (OWASP), IDA Pro, Ghidra

- Professional Experience -

Devo Technology, Inc.

Senior Detection Engineer

Sept 2020 - Jan 2024

- Led development of a Flask-based Python app to streamline detection creation, automating input and output for Devo ingestion, significantly enhancing efficiency.
- Implemented training regimen for junior team members' understanding of detection engineering and avoidance utilizing the MITRE ATT&CK framework.
- Managed exploit research, collected logs, and identified signatures to generate SIEM alert content, boosting OOB detections and strengthening Devo's client utilization.
- Built PowerShell scripts that executed atomic tests individually or collectively, enhancing the organization's capabilities.
- Developed an extensive array of detections for various CVEs, showcasing proficiency in identifying and mitigating vulnerabilities.
- Researched and validated potential vulnerabilities to identify exploit signatures and improve overall detection coverage.

Syntasa Corporation

Senior Security Advisor

Dec 2019 - Mar 2020

- Enhanced security posture across diverse locations through thorough risk assessments and targeted measures, boosting the client's cybersecurity resilience strategy.
- Implemented process improvement that achieved compliance with Agency regulations, leading to significant operational efficiency.
- Delivered daily security briefings to senior leadership, analyzing and presenting critical security metrics with actionable insights that enable proactive risk mitigation.
- Designed and implemented collaborative remediation plans addressing potential site vulnerabilities and improving the overall security posture.

Joshua Smith

Email: smithjk@infosecworx.com | [LinkedIn](#)

Ingenium Consulting, LLC

Container Engineer

Sept 2019 - Dec 2019

- Deployed Docker containers enterprise-wide, bolstering cyber resiliency strategies and fortifying the organization's defenses.
- Championed a collaborative, security-first approach, cross-functional coordination to minimize deployment risks, and optimized implementation of Docker solutions.
- Directed the requirements gathering and workflows for an enterprise Docker solution, aligning with organizational goals for a secure and sustainable strategy.
- Facilitated stakeholder meetings, proactively addressing Docker deployment concerns, ensuring transparent communication, and aligning with strategic security goals.

Pathoras / Proaptiv Corporation

Senior Penetration Tester

Mar 2016 - Sept 2019

- Administered multiple blue team penetration tests on AWS instances, identified inherited vulnerabilities, and delivered mitigation strategies.
- Executed penetration tests on client's VoIP system, uncovering vulnerabilities and fortifying security measures.
- Mentored junior staff, offering training and career guidance to foster professional development.

ManTech International

Senior Cyber Defense Specialist

Aug 2011 - Sept 2019

- Managed Blue Team defensive operations which improved the overall security posture of Agency systems.
- Coordinated with multiple USG components to perform offensive technical operations that were responsible for capturing several high-value targets.

BAE Systems, Inc

Lead Cyber Forensics Specialist

Jul 2009 - Aug 2011

- Utilized forensic analysis of various media using FTK and EnCase, offering insights into nation-state actors' TTPs.

Perot Systems Government Services

Information Systems Security Officer

Nov 2005 - Jul 2009

- Led the review process to ensure each SSP was complete and in compliance, thereby ensuring the security of Agency systems.

- Education -

George Mason University, B.S. Information Technology - 2008

Certified Ethical Hacker (CEH), Certification Number: ECC60361231296, Apr 2018 – Apr 2021

AWS Certified Cloud Practitioner, Validation Number: ZCWE1TQ2FJVE18WD, Nov 2019 - Nov 2022