MATTHEW WESTFALL
disloops@gmail.com

SUMMARY

I am an information security professional with fifteen years of experience that includes cloud security, penetration testing, network assessment, threat intelligence, and team leadership.

CERTIFICATIONS

Amazon Web Services Solutions Architect
GREM – GIAC Reverse Engineering Malware
Metasploit Pro Certified Specialist

EXPERIENCE

Salesforce
Senior Security Engineer
May 2022 – Present

- Conducting secure architecture review of full stack cloud applications
- Authoring risk assessments and remediation guidance for developers and stakeholders
- Performing manual penetration testing and source code review for a variety of technologies
- Developing security tooling for the detection and prevention of security threats

nVisium
Principal Application Security Consultant
June 2020 – May 2022

- Led security assessments for web applications, networks, and cloud-hosted assets
- Defined and developed core capabilities in our application and cloud security service offerings
- Authored and reviewed technical documentation including proposals, reports, and deliverables
- Created remediation guidance and engineering solutions for product teams and senior leadership

MindPoint Group, LLC
Team Lead
July 2016 – June 2020

Acted as the operational lead for a cross-functional security team. Provided security services to a government agency leveraging a cloud environment powered by Amazon Web Services (AWS):

- Conducted full-scoped penetration testing of cloud-hosted applications
- Provided guidance on network architecture and application security
- Performed OSINT research to provide actionable threat intelligence

Created and released “CloudFrunt” – an open-source AWS CloudFront exploitation tool:

- Performed private research into exploitable issues in core CloudFront functionality
- Created “CloudFrunt” tool to automate the process of discovering and hijacking domains
- Squatted roughly 2,000 domains over a five-day period, which were turned over to AWS Security
- Nine vulnerable federal domains were reported to US-CERT at NCCIC
- Research covered by Bleeping Computer, NJCCIC, Threatpost: disloops.com/cloudfront-hijacking

ENSCO, Inc.
Software and Security Engineer
May 2015 – June 2016

- Provided secure research and network capabilities to full-spectrum cyber operations personnel
- Created mission-critical web applications for federal customers using RESTful API, Java, and C#

MindPoint Group, LLC
Security Consultant
April 2013 – April 2015

Provided security services to a government agency migrating to a cloud environment powered by Amazon Web Services (AWS). Acted as the lead security contact for applications being deployed or updated. Responsibilities included:

- Conducting targeted penetration testing of network and web applications
- Performing static code reviews in a variety of languages
- Creating reports to describe existing vulnerabilities and steps for remediation
- Responding to emerging threats that affected the security of client applications
- Performed platform hardening, monitoring, and compliance tasks as required

Performed an assessment of a sensitive production network in support of a legislative government agency:

- Enumerated active devices using a variety of network mapping tools
- Performed physical verification of devices, cabling, and air gaps
- Conducted vulnerability scans using a proprietary security platform
- Verified tool-driven results using manual testing where necessary
- Documented network discrepancies and created remediation guidance

Authored an original Application Security policy for a financial institution:

- Created a charter document to describe best practices in Application Security
- Performed a gap analysis of development activities and developer proficiency
- Created a training plan and a solution for delivering security requirements
- Established attack surface analysis and threat modeling within the software design phase

CACI, Inc.
Systems Programmer
February 2007 – March 2013

- Participated in the full Software Development Life Cycle (SDLC) of a web interface for personnel stationed at Eastern Naval Warfare Centers deployed on the Navy Marine Corps Intranet (NMCI)

- Acted as lead developer in creating an Emergency Muster system for Naval Sea Systems Command (NAVSEA) and an automated system for identifying inactive phone lines and circuits

EDUCATION

Bachelor of Science, Computer Science – University of Mary Washington