Kemba Willette

Cyber Information Assurance Analyst - Northrop Grumman Corporation
Laurel, MD 20724
Kemba.Willette@gmail.com
240-501-6642

Work Experience

Penetration Tester

Confidential
August 2015 to Present

· Support the Cyber team with cyber security consulting across multiple programs, through Penetration Testing and Incident Response
· Help support Incident Response Process by Identifing, seizing, and analyzing digital evidence related to online activities encountered during investigations to determine impact on government network
· Perform penetration testing on network , web application, wireless and user awareness testing
· Perform testing on security standards and access controls sucha s ISO27001/2 and PCI DSS
· Work with system owners and software developers to inspect Source code , compiled applications and source installation files for security flaws and vulnerabilities
· Support Bug Bounty program by verify vulnerabilities listed in web server and application technologies (IIS/Apache/Tomcat/ColdFusion) according to OWASP Top 10
· Produce advisory reports regarding 0-day exploits, CVE vulnerabilities, current network
· Conduct briefings with business leadership to validate scope(s), objective(s) and desired results.
· Build internal scripts, tools and methodologies to enhance our capabilities

Cyber Intelligence Analyst(Contractor)

Confidential
September 2013 to August 2015

Performed Digital Forensics, Incident Response and Threat Hunting to ensure security of Corporate network
Wrote detailed incident reports to include Timeline, PCAP, Malware analysis and remediation
Produced threat reports and blog posts related to research and lessons learned for Cyber Incident Response Team Members
Participated in cross-organizational security and quality initiatives
Advised incident responders in the steps to take to investigate and resolve computer security incidents.
Helped implement phishing program which helped reduced email phishing attacks. Phishing program involved training and phishing exercises for employees
Seized, imaged, deconstructed, and analyzed digital media for evidence from varying device types, utilizing digital forensic tools currently preferred by federal, state, and local law enforcement agencies.

Conducted hands-on forensic searches to identify intrusion methods into network from devices such as laptops, tablets, smartphones, and more.

Penetration Tester

July 2011 to September 2013

Conducted Web Application Penetration Tests using Automated and Manual Methods
Created Reports on vulnerabilities and mitigation recommendations

Network Security Analyst

July 2009 to July 2011

• Performed IDS monitoring and analysis, network traffic and log analysis, prioritization and differentiation between potential intrusion attempts, determination of false alarms, insider threat and APT detection, and malware analysis/forensics.
• Created and tracked investigations to resolution.
• Composed security alert notifications.

Web Application Penetration Tester

Pragmatic Solutions
December 2008 to July 2009

Conducted network and web-based application penetration tests
Conducted Web Services security testing, Database Penetration Testing+
Simulatef sophisticated cyberattacks to identify vulnerabilities for clients worldwide
Conducted source code reviews for security vulnerabilities

User Support Specialist

CHF International
November 2007 to December 2008

• Provided Level 2 service help desk support to assist 150+ end -users in a Windows and Macintosh environment
• Responded to phone and email request to assist off-site field program
• Installed, configured, troubleshoot and resolved hardware, software, blackberries, server, network issues and request on site.

Systems Technician

Affiliated Computer Services
August 2005 to November 2007

• Research, analyze, diagnose and resolve issues with customer systems including computer hardware & software, peripheral equipment, and networks using documented processes where available and best practices where not.
• Perform computer imaging including software & hardware validation and pre-delivery testing. Work on primarily Microsoft Windows and Macintosh

Education

B.B.A. in Computer Information Science

Howard University - Washington, DC
August 2005

Skills

CEH, Penetration Testing, Ethical, Forensic

Additional Information

- 11 years Insider threat and APT detection, and malware analysis/forensics, Network Monitoring, CERT, SOC, Penetration Testing, Intrusion Forensics, Timeline Analysis, RED Team/Blue Team, Hunting, Adversary & Anti-Forensics Detection, System log analysis, TCP/IP, Incident Response
- Bachelor's Degree in Computer Information Systems
- Active Secret, Top Secret Clearance
- Certificaitons: CompTIA Security+CE, CEH, GCED, OSCP