Matthew Aubert

Active DoD Clearance
www.linkedin.com/in/aubsec
matt@theauberts.net
586-306-2638
507 Kings Crest Drive, Stafford VA, 22554

PROFESSIONAL PROFILE

PRAGMATIC MALWARE AND CYBER FORENSIC ANALYST

Pursuing MS in Digital Forensic Science with Champlain College.

Recently completed BS in Information System Security college program with a 4.0 GPA.

DoD Cleared and experienced IT professional with over thirteen years experience. Multiple professional certifications to include the GREM, GCFA, CISSP, CEH, and ITIL. DoD IAT III and IAM III compliant.

Strong leader with praise from subordinates and superiors for unique effective leadership style.

Nine year combat veteran of the United States Marine Corps. Served overseas in four deployments.

AREAS OF EXPERTISE

- Malware Analysis
- Systems Administration
- Digital Forensics
- Thinking outside the dodecahedron
- Technical Leadership
- Network Architecture
- Reverse Engineering of Binaries
- Incident Response
- Cyber Security Operations
- Innovative Problem Solving

CAREER SYNOPSIS

Information Security Senior

2016 - Present, Freddie Mac, Herndon Virginia

Responsibilities:

- Respond to cyber security incidents identified in the Splunk SIEM
- Proactivly hunt indicators of compromise utilizing available tools such as the FireEye HX and Splunk SIEM.
- Ingest threat intelligence to create YARA and OpenIOC rules based on the unique identifiable indicators discovered. Leverage available tools to deploy signatures and look to emerging tools to improve host based security.
- Perform analysis of Malware in direct support of Incident Response utilizing both surface, runtime, and reverse engineering analysis techniques.

Cyber Forensic Analyst

2014 – 2016, Northrop Grumman Corporation, Quantico Virginia

Responsibilities:

- Extraction of indicators of compromise, through a combination of digital artifact examination, static code analysis and reverse engineering, runtime malware execution, and simulation techniques.
- Perform analysis of Malware in direct support of Incident Response utilizing both basic static and dynamic analysis techniques along with disassembly and debugging of suspicious files.
- Develop strong host based indicators to identify enterprise wide impact. Create YARA rules based on the unique identifiable indicators discovered. Leverage available tools to deploy signatures and look to emerging tools to improve host based security.
- Maintain a Malware Analysis lab environment in order to provide effective results. Major tools to include VMWare Workstation and ESX, FireEye Malware Analysis System, Cuckoo sandbox, REMnux GNU/Linux distribution, Xubuntu GNU/Linux, Microsoft Windows, OllyDbg, IDAPro, Python, INetSim, EnCase, and various other tools as required to support the mission.
- Engage in research to find solutions to Incident Response problems. Such as the improvement of deployable Incident Response tool, implementation of YARA rules into the Malware Analysis processes, development of in-house Malware Analysis course, and other research as required.

Key Projects:

- Deployment of a Cuckoo automated malware analysis system. This system allows for the Incident Responders to perform quick analysis of suspicious files. By capturing artifacts from the properties of the suspicious file and the dynamic execution of the file, the Incident Responders can quickly develop indicators. The systems also utilizes Yara signatures written by the Malware Analysts to identify previously reversed samples.

CAREER SYNOPSIS CONTINUED

Information Systems Security Officer

2013 – 2014, Smartronix Inc., Quantico Virginia

Responsibilities:

- Assist the Information System Security Managers (ISSMs) in meeting their duties and responsibilities.
- Implement and enforce all Department of Defense (DoD) Information System (IS) cybersecurity policies and procedures, as defined by cybersecurity related documentation.
- Ensure that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS under their purview before being granted access to those systems.
- In coordination with the ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered and ensure that a process is in place for authorized users to report all cybersecurity related events and potential threats and vulnerabilities to the ISSO.

Key Projects:

- Successfully prepared the systems within the area of operation for the command cyber readiness inspection and computer network defense service provider inspection.

Public Key Infrastructure Chief (Supervisory)

2010 – 2013, United States Marine Corps, Quantico Virginia

Responsibilities:

- Direct, Organize, and Support the deployment of Public Key Infrastructure in tactical environments.
- Lead Public Key Infrastructure Instructor, responsible for directing the update of training materials and providing on site training for Marine Corps units preparing for deployment.
- Manage Certificate Validation Infrastructure using Tumbleweed Enterprise Validation Authority and Desktop Validator throughout the Marine Corps.
- Manage Microsoft Root and Subordinate Certificate Authorities for the Marine Corps Enterprise Network and the Navy and Marine Corps Intranet.
- Certified National Security System (NSS) and Department of Defense (DoD) Local Registration Authority (LRA), Registration Authority (RA), and Key Recovery Agent (KRA).

Key Projects:

- Configured Tumbleweed Validation Authority Responders and Repeaters for II MEF deployed to Camp Leatherneck, Afghanistan.
- Validated Security Technical Implementation Guide adherence of all Layer 2 and Layer 3 Cisco network devices on Camp Leatherneck, Afghanistan.

Cyber Systems Chief and Platoon Sergeant (Supervisory)

2005 – 2010, United States Marine Corps, World-Wide

Responsibilities:

- Managed the welfare (which includes food, sleep, exercise, etc.) of 30 Communication Marines while directing the day-to-day operation of managing shipboard and shore networks.
- Engineered Unclassified and Classified networks, with two Active Directory Domain Controllers and one Exchange 2003 server on each network of the two networks, to support 250 users with a total of 110 computer assets, located between two geographical locations.
- Managed Network Infrastructure using Cisco devices to include various models of both Routers and Catalyst switches.
- Configured and managed a Support Wide Area Network (SWAN) satellite system for remote Unclassified and Classified connectivity.

Key Projects:

- Completed three deployments. One eight month tour in Southern Afghanistan and two shipboard deployments on board the USS Nashville and USS Mesa Verde.

PREVIOUS EXPERIENCE

Network Engineer
2003 – 2004, Whitlam Label Company, Michigan

Network Engineer
2002 – 2003, Certinet Professionals, Michigan

Intern Help-Desk Technician
Summers 2000 and 2001, Macomb Oakland Regional Center, Michigan

EDUCATION

Pursuing Master of Digital Forensic Science
Champlain College
Projected 2018

Bachelor of Science in Information Systems Security
American Public University System
August 2015

Associate of Science in Computer Applications
American Public University System
August 2013

CERTIFICATIONS

GREM - GIAC Reverse Engineering Malware
2015 – GIAC - License 4185

GCFA – GIAC Certified Forensic Analyst
2015 – GIAC - License 11141

CISSP-ISSMP - Certified Information Systems Security Professional – Information Systems Security Management Professional
2012 – $(ISC)^2$ - License 424038

C|EH - Certified Ethical Hacker
2012 – EC-Council - License ECC972334

ITILv3 - Information Technology Infrastructure Library version 3 Foundation
2012 – EXIN - License EXN4418096

TECHNICAL EXPERTISE

Operating Systems	Microsoft Windows 2000, XP, 7, 8, 10 Microsoft Windows Server 2000, 2003, 2008, 2012 Debian GNU/Linux, Ubuntu Mac OS X Cisco IOS
Malware Analysis Tools	REMnux Workstation INetSim IDAPro OllyDbg ProcDOT Cuckoo Sandbox
Cyber Forensics Tools	SIFT Workstation Encase 7 The Sleuth Kit Volatility
Incident Response	Mandiant Redline Microsoft SysInternals McAfee Host Based Security System (HBSS) McAfee Enterprise Security Manager (ESM) McAfee Network Security Manager (NSM) BlueCoat Proxy