

Jeremy J. Willingham

Garner, NC

PHONE (855) 932 6623

E-MAIL jeremy@lightstormsecurity.com

Summary

I have over 25 years of experience as a trainer, operator, and analyst in various cybersecurity roles and I specialize in the analysis of network data, digital data, forensic data, and threat artifacts. I have a proven track record of expertise in **Computers, Cell Phones** and other **Mobile Devices, Forensics, Network Communication** and the **Internet**.

Employment Experience

President: Determine areas of opportunity in the field of cybersecurity, especially relating to training and education. Develop unique capabilities in the industry. Identify and develop relationships with potential customers. Coordinate with customers to administer delivery of a capability that produces the highest possible impact and value. Be involved in the INFOSEC community to ensure relevancy of capabilities.

LightStorm Security LLC, Raleigh, NC

Oct 2017 – Pres

Director of Training: Identify and rectify gaps in the capability of delivering high quality training to customers. Train and mentor new instructors to ensure quality delivery. Coordinate with customers to ensure an effective and customized delivery option. Stay abreast of the industry to ensure training capability is relevant and cutting-edge. Developed custom training package for DHS conference. Developed new Hunt operation course. Delivered training in networking, packet analysis, Windows, Linux, Exploitation, and Tactical Forensics.

root9B, Colorado Springs, CO

Jan 2017 – Sep 2017

Services Enablement Architect: Develop, deliver and maintain Optiv U courses to Optiv employees and select partners. Work with practice areas throughout Optiv to identify training needs for current employees. Represent Optiv at recruiting events to identify candidates for hire. Mentor Associate Consultants during their training regimen.

Optiv Security, Denver, CO

Sep 2014 – Jan 2017

Director Advanced Cyber Training: Develop, deliver, maintain, and integrate Art of Exploitation training suite to customers. Identify subject areas where development of new training would have an impact in the mission. Identify and acquire personnel capable of delivering training while maintaining the program's high standards. Assist in the acquisition of programs/contracts related to the AoE mission. Responsible for mentoring and managing all cyber training personnel in the company, regardless of assigned project.

TCS Cyber Intelligence Group, Hanover, MD

Jul 2007-Sep 2014

JFCC NW CNO Planner: While assigned to the Joint Functional Component Command Network Warfare, provide support in the development and review of Concept of Operations (CONOPs), Intelligence Needs (INs), Request for Information (RFI), and Evaluation Request Messages (EReqMs) to support COCOMs requirements. Develop and validate measures of effectiveness and provide network analysis. Provide government counterpart CNO coordination and de-confliction in support of real world

events. Provide support in the development of Courses of Action (COAs) in support of COCOMs and JFCC NW partner organizations.

Northrop Grumman IT TASC, Annapolis Junction, MD

Sep 2005-Jun 2007

Remote Operations Center Operator: Plan, lead, and conduct Computer Network Operations (CNO). Develop and test new tools for CNO. Conduct research on both hardware and software that may lead to new procedures and techniques for CNO. Train military and civilian personnel on CNO tactics. Also a subject matter expert (SME) for development of policy and procedure for the Marine Corps CNO effort.

Company L, Marine Cryptologic Support Battalion, Ft Meade, MD, USMC

Sep 2004-Sep 2005

Company L Operations Chief: Responsible for Marine integration into the National Security Agency's (NSA) Computer Network Operations. Serve as a liaison with other Service CNO work centers and the Intelligence Community. Identify training requirements to develop and maintain proficiency for computer network operators within the Company. Developed reach-back capability with various NSA offices to improve the support to deployed CNO assets in regard to analysis and reporting.

Company L, Marine Cryptologic Support Battalion, Ft Meade, MD, USMC

Jun 2004-Sep 2004

NSA/DIO Red Team Operator: Responsible for identifying information security vulnerabilities and improving the security readiness posture of the Defense Information Infrastructure. Duties included: testing vulnerabilities with DIO Red Team tools, installing backdoors on remote systems, utilizing root kits to gain information about a system, maneuvering from network to network, data-mining a target network to obtain proof-of-concept information. Responsible for creating reports on success or failure of operation and presenting those reports to senior customer personnel, and assigned as a Red Team 101 instructor.

Company L, Marine Cryptologic Support Battalion, Suitland, MD, USMC

Jun 2001-May 2004

Network Security Vulnerability Assessment Team Leader: Led a team of network vulnerability specialists. Coordinated with partner organizations during operations, exercises, and training events. Researched new technologies in the network and telecommunications fields. Performed vulnerability assessments of network nodes to include: CISCO routers/switches, Windows 9x/NT, Linux, Sun Solaris, various Web Servers, and Mail Servers. Designed and implemented a training network. Provided input regarding national policy on information assurance. Responsible for recruiting and training new team members and briefing various military and government officials.

1st Radio Battalion, USMC

Feb 2000-Jun 2001

System Administrator and LAN Technician: Responsible for server, client, and network assistance to an infrastructure sustaining over 200 users on a Banyan Vines network. I was responsible for backup procedures, helpdesk management, and onsite troubleshooting. Installed and configured Windows NT servers, Cisco routers, Windows 98 and NT clients, and network printers.

1st Radio Battalion, USMC

Jul 1997-Feb 2000

Education

Strayer University:

- Bachelor's in Computer Information Systems – Internetworking Technologies.

Learning Tree International:

- Introduction to Cisco Routers.
- Advanced Cisco Routers.
- Virtual Private Networks.

SANS Institute:

- Track 8, System Forensics, Investigation, and Response.

BlackBag Technologies:

- iOS Forensics with Blacklight.

National Cryptologic School (NCS):

- COMP2160, Introduction to Programming
- COMP1119, Introduction to Unix
- COMP1129, Sun Usage
- MP369, Solaris 2.x Administration
- EDUC1160, Basic ISD Process
- IAEC2205, Systems Approach to Threat
- IS232, Information Operations Awareness
- OIAC1170, Introduction to Computer Security

Art of Exploitation:

- Penetration Testing Boot Camp Edition
- Wireless Analysis Edition
- Wiretap Edition: Fundamentals of Packet Analysis
- LAN/WAN Fundamentals: Understanding Data Communications
- x86 Assembly Programming Language

Certifications

Project Management Institute:

- Project Management Professional (PMP)