Matthew Riedle
Senior Information Security Analyst at Castlight Health
Email: riedlem@gmail.com
Cell: 980-263-4707
www.linkedin.com/in/matthewriedle/ https://github.com/riedlem

Objective

Primary interests lie in computer security along with the detection and prevention of cybercrimes. Looking to gain additional hands-on experience in a SOC and help build out security architectures and programs. Experience in customer management, project management, information security analysis, and SOC management.

Experience

Senior Information Security Analyst at Castlight Health
August 2018 - Present

- Developed and implemented security controls, such as SPF, DKIM, DMARC, MFA, and Anti-Malware to secure corporate mail from phishing threats
- Analyzed possible security infrastructure gaps and oversaw deployment, signal tuning, quality assurance, documentation, and maintenance of detection and prevention tools
- Led cross-functional teams on several occasions in an effort to enhance Castlight's security posture. This led to other teams approaching Security for advice and input prior to implementation
- Presented new security technologies across the organization, including to C-Level members, in order to get buy-in for implementation
- Documented procedures to make handling of security incidents more efficient and effective
- Participated in and passed audits, including presenting evidence to auditors
- Analyzed malicious traffic patterns in order to write custom WAF rules for blocking credential stuffing attacks
- Led investigations into possible fraudulent activity on user accounts, including credential stuffing and fraudulent account registrations

Information Security Analyst at Castlight Health
July 2016 – August 2018

- Cleared massive backlog of security tickets and established procedures for better handling of incoming tickets
- Monitored and acted on alerts from security tools such as DLP, IDS, WAF, Anti-Bot, Database Monitoring, and Anti-Virus
- Tested application vulnerabilities to ensure older vulnerabilities were patched
- Wrote bash and python scripts for automating some security testing to ensure that tools were properly blocking attacks
- Monitored current security events to stay on top of threats, such as ensuring organization was protected against WannaCry and writing a blog entry to inform the business

Malware Analyst at RSA, The Security Division of EMC
August 2014 – June 2016

- Dynamic analysis of common Trojan Malware families to identify triggers and C&C server credentials as they relate to the AFCC's customers.
- Wrote reports for advanced Malware Families for RSA's Trojan Reports

Engagement Manager at RSA, The Security Division of EMC
January 2014 – January 2016

- In charge of 8 customers in the Middle East (including Kuwait, Lebanon, Qatar, and Saudi Arabia), as well as 17 customers in the United States
- Work with Sales on a regular basis on contacting new potential customers and promoting Fraud Action sales (demos, presentations, etc.)
- Proactive account management - Establishing and maintaining clear channels of communication, lead meetings with customer, collect requirements, manage timelines and provide service deliverables.
- Manage and coordinate day-to-day relations between RSA and its international clients – escalation/crisis management, handling tickets, inquiries, client's notifications and maintaining customer's satisfaction and loyalty.
- Customization management - Identify and define customer needs and requirements, identify needed internal resources, manage client expectations.
- Work with other teams within RSA to ensure the clients' needs are understood and addressed in a timely manner.

Anti-Fraud Command Center Team Leader / Site Manager at RSA, The Security Division of EMC
January 2013 – February 2016

- Managed a cybercrime response team of 17 fraud analysts.
- Conducted training for all new analysts, ensuring they were ready to begin the tasks of an anti-fraud analyst.
- Full responsibility for the professional qualification (and continued education) of new analysts from the first steps in the OTMS through the certified analyst.
- Managed the department recruiting evaluation center, conducting personal and technical interviews.
- Advanced analysis of variant threads escalated from the AFCC, obfuscation, encoding, decoding, forensics investigations and credentials recovery.
- Managed the daily logistics of a fully-functioning office site (including addressing maintenance, IT, and upkeep needs).
- Assisted in growing the site from inception with 11 anti-fraud analysts to a profitable anti-fraud site with over 45 analysts performing advanced roles including Shift Managers, Follow Up, and Trojan investigators.
- Developed, maintained, and executed emergency contingency plans to ensure minimal downtime in 24x7 site capabilities.

Anti-Fraud Command Center Analyst at RSA, The Security Division of EMC
October 2012 – January 2013

- Responsible for detecting and analyzing cyber-crimes (Phishing, Malware, Pharming, Brand Abuse, Fraudulent Emails, etc.)
- Taking prevention steps, terminating online frauds and performing computer forensic analysis.
- Comprehensive knowledge of website structures and related authorities (ISP's, Webhosting, Registrar, etc.)

Education

Purdue University
Master's Degree, Cyber Forensics, 2013 - 2015

Purdue University
Bachelor's Degree, Computer and Information Technology with a focus in Network Security, 2008 - 2013

Skills and Expertise

Network Security	Digital Forensics	Malware Debugging
Information Security	Cyber Fraud	IDA Pro / OllyDbg
Computer Security	Phishing	Sandboxing
Intrusion Detection	Pharming	VMmare
Wireless Networking	Trojans	VirtualBox
Network Traffic Analysis	Malware Dynamic/Static Analysis	Windows

Mac OS X	HTML	Managing Client Relationships
Linux / Unix	Team Management	SIEM
SQL	Leadership	Anti-Bot
C#	Conducting Interviews	

Honors, Awards, and Scholarships

- AccessData Certified Examiner (ACE)
- Purdue Presidential Scholarship
- Elected to National Honor Society

Extracurricular Activities and Positions Held

- Member of the CERIAS Student Organization
- Member of Purdue Cyber Forensics Club
- Volunteer and serve at Camp Living Waters
- Tutor for National Honor Society, 2007 - 2008

International Experience

- Missionary activities, 2005-2007
    - Training in Palmer Lake, Colorado
    - 10 months in Massy, France
    - 6 months in N'Djamena, Chad