Rich Greco C.V. Digital Forensics Expert – Atlanta, Georgia

Digital Forensics Investigation Systems Engineer - Assistant Director at Ernst & Young

Ernst & Young

Southwestern Bible College

Greater Atlanta, Georgia

I was the kid who took everything apart to see what was inside. Unlike others I could actually put them back together, albeit there were a few machines that clearly had redundant mechanisms as they worked so much better without that random piece left over after re-assembly.

My path through life from the age of two on up to the present has been an epic adventure of survival and finding new things to learn. I literally died or almost died seven or more times over this period and who knows how many broken bones.

While my professional endeavors are now tame by comparison I am often reflecting on the path of my life and it looks much like the forging of high grade steel. The folding and welding process removes impurities, the layering of steel with different carbon content enhances toughness and more evenly distributes the carbon. Anyone who has seen a Japanese Katana in person will appreciate what a master smith can create with only iron sand.

I currently specialize in finding and providing solutions, more specifically in the area of Digital Forensics, Incident Response, Malware Analysis, Security Assessments, and all the tangential practices that come with it.

I don't see computing environments or the challenges facing them as simply a list of checkboxes and recommendations. I have lived on the pointed end of the spear, I have tackled and actually implemented solutions, and that is what I do.

I embrace a deep love of learning, I provide Solutions, and my personal code of ethics enables me to thrive in all areas.

So... tell me about your problems.

Experience

-

Digital Forensics Investigation Systems Engineer - Assistant Director

Company Name Ernst & Young

Dates Employed Mar 2016 – Present

Employment Duration 1 yr 8 mos

Location Greater Atlanta Area

Essential Functions of the Job:

• Develop process and tools for forensic investigation and incident response including automation

• Manage, update, and maintain documentation to support the forensic and investigation process

• Provide support to the information security forensics laboratory used for processing investigation and forensic efforts

• Assist team members throughout investigations and incident response procedures

• Manage and improve information security documentation as required, within the IRF&I department

• Influence global forensic and investigation standards for the firm

• Support the Incident Response & Investigations Lead by responding during security incidents as required

•

Forensic Investigator - Malware

Company Name Fiserv

Dates Employed Nov 2015 – Feb 2016

Employment Duration 4 mos

Location Greater Atlanta Area

Serves as the primary contact for investigations related to malware, such as bots, worms, and trojans to understand the nature of their threat. Works with internal anti-virus teams and technical teams to validate and remediate the threat. Additional duties include computer content scans, minimal data recovery, and minimal electronic discovery. Plans, coordinates and implements computer information security measures to safeguard information in computer files against accidental or unauthorized modification, destruction or disclosure. Maintain all aspects of Chain of Custody and forensic

inventory. Works with various technical teams, human resources representatives, and management personnel, as well as with attorneys and corporate clients.

Works under the guidance of the Director of Forensic Investigations. Responsibilities include, but are not limited to:

Malware reverse engineering.

Manage all aspects of malware investigations to completion.

Assist in the coordination of changes/modifications/updates in various Anti-virus solutions.

Stay abreast of the threat landscape and notify specific groups of any warnings or potential dangers.

Monitors operations to ensure compliance with all regulatory requirements.

Coordinates implementation of vendor-issued security software updates.

Stays abreast of evolving information systems and data forensics tools.

Protects the company from potential legal litigation and produces accurate results from digital evidence.

Analyzes data and investigative information.

Communicates with co-workers and management regarding case development in confidential manner.

Provides findings reports and recommendations based on investigative findings.

Prepares reports and documents case details, developments and outcomes.

Networks with members of local trade associations and other groups of interest.

Other duties as requested by management.

-

Associate - Security and Privacy

Company Name McGladrey

Dates Employed Sep 2013 – Nov 2015

Employment Duration 2 yrs 3 mos

Location Greater Atlanta Area

Examples of specific assignments include:

DFIR response for Breach Incidents, including identifying the malware, cleaning the network and developing custom code for eradicating the malware.

Analysis of logs and malware samples for incidents that did not quite reach the level of a breach where notifications were legally required.

Analysis of malware through a wide array of static and dynamic methods, familiarity with SIFT3, REMnux, and DAVIX operating systems.

Familiarity with ARM based malware and ARM based malware development, primarily in the context of iOS and Android.

Forensic analysis for network attacks, malicious insiders, IP theft, unauthorized access, and use of company assets for illegal pornographic material.

Perform data collection at various response sights, ensuring Chain of Custody is documented and accurate.

Installing, configuring, and monitoring FireEye Appliances.

Performing and coordinating technical security assessments including, PCI reviews, internal and external vulnerability assessments, attack and penetration testing, and other technical audits, assess security of client networks, system, and applications

Coordinating the testing and analysis of web applications and web services (SOAP, WSDL, UDDI)

Performing security risk assessments and, evaluating and testing general computer controls including access controls, change management, security, backup controls and operation controls, in a wide range of computing environments (e.g., mainframe, mid-range and client/server).
OBJ OBJ
Reviewing, documenting, evaluating and testing application controls, particularly automated controls on a wide range of software application packages for financial reporting.

Identifying internal IT controls, assessing their design and operational effectiveness, determining risk exposures and developing remediation plans.

Determine technical and business impact of identified security issues and provide remediation guidance to clients

-

Sr Networking Consultant

Company Name The Paradies Shops

Dates Employed Feb 2013 – Sep 2013

Employment Duration 8 mos

Nature of Work

Network security, server implementation and maintenance, malware and virus analysis and remediation. Deploying mechanisms to enforce Acceptable Use Policies, maintenance and configuration of various Cisco appliances. General Solutions Engineer from database analysis to software debugging.

Illustrative Examples Of Work
Conducted two Malware response and remediation efforts
Upgraded and maintained Symantic End Point
Installed and Administered Panda Corporate AV
Administered Google Apps for Business
Administered Aerohive Wireless Cloud nation wide
Administered Sonicwall GMS nation wide
Conducted Forensic Investigations of all Director Grade Employees slated for termination
Conducted Forensic Investigations for general concerns like embezzlement and physical security abuses
Advised on various CISO topics

-

Police Officer

Company Name Phoenix Police Department

Dates Employed Jun 2002 – Feb 2013

Employment Duration 10 yrs 9 mos

While working for PPD I provided innovative solutions to real world problems faced by fellow Officers on a daily basis.

Developed Automobile Accident Reporting application using Adobe Acrobat which allowed Officers to quickly and easily create accident reports and produce printed output in the State approved format. For further see MVD project.

While supervising the Emergency Vehicle Operations Center, rewrote large portions of the AZPOST Driver Training Program in conjunction with the other prominent Subject Matter Experts in the state, taking advantage of the most recent data and innovating new teaching modalities that had not existed prior. In addition, continued to develop curriculum, training outlines, and teaching aides that brought the center closer to the current century. For further see EVOC Project.

Played a key role in the largest and farthest reaching technological upgrade the Phoenix Department has ever undertaken, the upgrade of the CAD and MDT software. CAD primarily for 911 call takers and dispatchers, while MDT software was more for officers on the computers in their cars. For further see MDT Project.

-

Detention Officer

Company Name Coconino County Sheriffs Office

Dates Employed Jun 2001 – Jun 2002

Employment Duration 1 yr 1 mo

Location Flagstaff, Arizona Area

Entry level position in the sheriffs office with a focus on facility security, inmate management, hand to hand combat.

-

Production Manager

Company Name Kinkos

Dates Employed Jun 1999 – Jun 2001

Employment Duration 2 yrs 1 mo

Location Flagstaff, Arizona Area

Production management, customer service, sales, imaging, graphic design.

- 

  ### Copy Shop Manager

  Company Name OfficeMax

  Dates Employed Jun 1997 – Jun 1999

  Employment Duration 2 yrs 1 mo

  Location Phoenix, Arizona Area

  Positions in sales, large business furniture sales, and copy shop manager.

Education

- ### Southwestern Bible College

  Field Of Study Youth Ministry and Biblical Studies

  Dates attended or expected graduation 1998 – 2000

- 

  ### Northern Arizona University

  Field Of Study Computer Science and Engineering

  Dates attended or expected graduation 1997 – 2002

-

Coconino High School