Emagined Security Penetration Test / Red Team

A CREST Certified company

https://service-selection-platform.crest-approved.org/member_companies/emagined-security-inc/

Main Website: www.emagined.com
Security Blogs: blog.emagined.com

Introduction

Emagined Security, a privately owned and operated company, has been helping organizations with their security needs with an excellent track record of success since 2002. The company is comprised of 45 senior information security professionals in the industry, with an average of 15+ years of experience. Consultants have varied and diverse backgrounds in information and cybersecurity with high levels of knowledge, industry certifications, and practical experience. Various diverse backgrounds include former Fortune 100, C-level, Big Four Accounting firms, strategy consultants, process engineers, etc., with cumulative security experience. Team members are selected based on the respective knowledge, skills and attributes associated with each of the project tasks; however, the project will be managed by the practice leads who follow.

Emagined Security was created to offer corporations a comprehensive array of sophisticated, adaptive security solutions that include both consulting and managed services. In support of this initiative, Emagined Security has built a highly talented organization specializing in information security consulting. Our company focuses on securing business solutions by providing a full complement of proactive, real-time, reactive, executive advisory, license advisory and support security services to global institutions, major corporations, and other smaller organizations, while providing a fully business-driven approach.

Emagined Security is a leading professional services provider for Information Security and Compliance solutions. Emagined Security empowers its clients to help them effectively manage IT risk in today's dynamic business environment. With deep industry and domain expertise, a proven track record, and by employing well known and respected individuals from the Information Security community, Emagined Security can scale quickly and efficiently to provide clients with the rapid response required by best-in-class organizations. Emagined Security’s commercial clients cover a wide range of U.S. and global Fortune 500 organizations, including the financial services, energy, healthcare, high tech, manufacturing, and insurance sectors.

Certifications, Licenses & Memberships

Emagined Security ethical hackers possess a variety of certifications, licenses and memberships including but not limited to:

Penetration Testing / Offensive Security:

- EC-Council Certified Ethical Hacker (C|EH)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Web Expert (OSWE)
- Offensive Security Experienced Pentester (OSEP)
- Offensive Security Kali Linux Certified Professional (KLCP)
- GIAC Penetration Tester (GPEN)
- CREST Registered Tester (CRT)
- Burp Suite Certified Practitioner (BSCP)
- eLearnSecurity Certified Penetration Tester eXtreme (eCPTX)
- eLearnSecurity Certified Professional Penetration Tester (eCPPTv2)
- eLearnSecurity Mobile Application Penetration Tester (eMAPT)
- eLearnSecurity Certified eXploit Developer (eCXD)
- eLearnSecurity Certified Web Application Penetration Tester eXtreme (eWPTXv2)
- ZeroPointSecurity Certified Red Team Operator (CRTO)
- TCM Security Practical Network Penetration Tester Certification (PNTP)
- CompTIA PenTest+
- CJIS Level 4 certification

Cybersecurity (other):

- ISC2 Certified Information Systems Security Professional (CISSP)
- ISC2 Systems Security Certified Professional (SSCP)
- Thales nCSE
- CompTIA A+ Certified
- CompTIA Server+ Certified
- CompTIA Network+ Certified
- CompTIA Project+ Certified
- Certified Computer Examiner
- EnCase Certified Examiner
- Certified Data Recovery Expert (DRE)
- HP Accredited Platform Specialist – Proliant (APS)
- Microsoft Certified Professional Systems Engineer (MCSE)
- EC-Council Certified Cybersecurity Technician (C|CT)
- EC-Council Certified EC-Council Instructor (C|EI)
- Certified in Homeland Security – Level 3 (CHS-III)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Incident Handler (GCIH)
- Cellebrite UFED Certified – Mobile Devices (C00028)

- Cellebrite UFED Physical Certified – Mobile Devices (P00169)
- Securing Solaris – The Gold Standard (GGSC)
- Katana Forensics Lantern iOS First Responder Certification
- Katana Forensics Laboratory iOS/Mac OS X Certification
- GIAC Certified Forensic Analyst (GCFA)
- Cisco Certified Networking Professional Security Specialist 1
- Cisco Certified Networking Professional + Security (CCNP + Security)
- Check Point Certified Security Administrator (CCSA)
- Cisco Certified Networking Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- Microsoft – Microsoft Certified Professional, Systems Engineer, & Trainer
- Novell – Certified Novell Administrator, Engineer, & Instructor
- Project Management Institute – Project Management Professional
- Oracle Certified Professional Java Programmer
- CIW Perl, JavaScript, Database Specialist, and Web Development Professional
- Vontu Certified
- Symantec Endpoint Protection Certified
- PGP Certified
- Brightmail Gateway Certified
- Altiris SE Certified
- SecurityTube Linux Assembly Expert (SLAE)
- SecurityTube Python Scripting Expert (SPSE)
- Palo Alto Networks Certified Network Security Engineer (PCNSE)
- Microsoft Sharepoint Server Certified
- Amazon Web Services(AWS) Cloud Practitioner
- VMware Certified Professional 6.5
- Selenium + Java Certified

Organizations, Affiliations & Memberships

- International Information Systems Security Certification Consortium $(ISC)^2$
- High Technology Crime Investigation Association (H.T.C.I.A.)
- US Secret Service Electronic Crime Task Force (ECTF)
- Federal Bureau of Investigation Infragard
- CREST USA

Additionally, we provide a matrix of our penetration testers skills showcasing the comprehensive nature of our penetration testing experience. In order for a penetration tester to be certified by Emagined Security standards the penetration tester must:

- Be trained by Emagined Security on the methodology and requirements to perform a comprehensive test for that service.
- Have a Senior or Principal Penetration Tester co-pen test the service at a minimum of 6 test.
- Perform over 25 tests in the service category.

- Be certified by the VP of Penetration Testing Training to be able to perform the service to Emagined Security standards.

Below is the matrix of Emagined Security Penetration Test Team and their skills

Consultant	Certifications	Project Management	Engagement Lead	Web Application	Thick Client	Network Pen	API Pen	Mobile Pen	SCADA	Mainframe	Physical	Red Team	Embedded Device	OSINT	Config Reviews	Exploit Dev & Execution	Wireless	Social Engineering (Phishing)	Cloud Pen Testing	Security Architecture
[3]	CISSP, EnCE, CCE, APS, MCSE, SSCP, A+, Server+, OSCP, KLCP, CCT, DRE, GCFW, GSEC, GIAC Gold, CJIS Level 4 UFED Physical and Logical Certified Certified EC-Council Instructor	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
	OSCP, OSWE, GSEC, Security+, Oracle Certified Professional Java Programmer, CIW Perl, JavaScript, Database Specialist, and Web Development Professional, Project+, Network+, A+, CJIS Level 4 SSBI Top Secret Clearance (inactive)	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X
	OSCP, KLCP, OSWE, OSEP, CCT CCNA, CCNA Security (Expired) CompTIA A+, N+, Security+ CREST CRT Accredited	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X
	Certified Ethical Hacker Certified A+ Certification Vontu Certified Symantec Endpoint Protection Certified PGP Certified Brightmail Gateway Certified Altiris SE Certified Currently pursuing CISSP – Certified Information Systems Certified Ethical Hacker Certified	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	GIAC Penetration Tester (GPEN), Burp Suite Certified Practitioner (BSCP), eLearnSecurity Certified Penetration Tester eXtreme (eCPTX), eLearnSecurity Certified Professional Penetration Tester (eCPPTv2), eLearnSecurity Mobile Application Penetration Tester (eMAPT), eLearnSecurity Certified eXploit Developer (eCXD), eLearnSecurity Certified Web Application Penetration Tester eXtreme (eWPTXv2), ZeroPointSecurity Certified Red Team Operator (CRTO), TCM Security Practical Network Penetration Tester Certification (PNTP, Offensive Security Certified Professional (OSCP), Offensive Security Web Expert (OSWE) , Offensive Security Experienced Penetration Tester (OSEP), CompTIA PenTest+, Certified Ethical Hacker (CEH)	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X
	SLAE, SPSE, SJSE, PCNSE, CCNA (R&S),Pentest+, CySA+, Sec+, Net+, A+	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X
	AWS Cloud practitioner VMware Certified Professional 6 5 CCNA, CCNA Security (Expired) CompTIA A+, N+, Security+	X				X								X	X		X	X	X	
	Certified Ethical Hacker (CEH) Nessus Proficiency Splunk Fundamentals Splunk Sales Rep I	X	X	X	X	X	X					X		X	X		X	X	X	
	Certified Ethical Hacker (CEH) Certified in Selenium + Java			X			X							X	X		X	X		
	CompTIA Network + CompTIA Security +	X	X	X		X	X							X	X		X	X	X	
	Certified Cybersecurity Technician (CCT) CompTIA Security+ (expired)					X								X	X		X	X	X	
	Certified Ethical Hacker (CEH) CompTIA A+ Certification Microsoft Windows SharePoint Services 3.0, New Horizons, 2008 Microsoft Office Share Point Server 2007, New Horizons, 2008 Windows SharePoint Services Installation, New Horizons, 2008 Windows SharePoint Services Administration, New Horizons, 2008	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing / Red Team

Vulnerability Management

Vulnerability Assessments

Digital Forensics

Fraud Detection / Prevention / Control

Network Architecture Analysis / Design

Security / Risk Assessment

Process Development / Instantiation

Network, Application and Perimeter Security

Problem Solving – Concrete & Abstract

Analytics and Research

Program Creation, Management and Development

Documentation

Converged Environments / Cloud

Social Engineering

Law Enforcement Relations and Collaboration

[3], *Executive Consultant*

[3] is an executive security consultant with Emagined Security, and the Chief Training Officer of the Penetration Testing team, providing expertise in the fields of Ethical Hacking/Penetration Testing, Digital Forensics and Risk/Fraud Protection. Prior to joining Emagined Security, Mr. [3] served in both technical and managerial capacities at Visa Inc., Fairchild Semiconductor and KHQ-TV. Mr. [3] is a versatile communicator and innovator, with demonstrated ability to translate complex security issues and challenges into proven, viable security control measures/results as implemented throughout all levels of an organization. Given Mr. [3] diverse background and experience in enterprise environments, he is uniquely positioned to blend security and business advocacy into cohesive enterprise solutions with a high level of efficacy.

Penetration testing accomplishments:

- Lead tester and trainer on hundreds of penetration testing engagements, including a social engineering exercise complete with pivot and advancement protocols and behavioral pattern analysis, as well as coordinator and program lead for annual global security assessment efforts which conducted network penetration testing at a macro-level on both external and internal enterprise assets totaling in excess of 6500 systems and applications.
- Highly skilled technical lead with demonstrated expertise in web application, thick client, API, websocket, mainframe, and embedded applications as well as networks and critical infrastructure, including ICS/SCADA. Mr. [3] has performed during his 25+ years in cybersecurity over:
  - **500+ network penetration tests,**
  - **500+ web application penetration tests,**
  - **300+ API penetration tests**
  - **150+ thick client penetration tests**
  - **100+ ICS/SCADA penetration tests**
  - **50+ Mainframe and specialized penetration tests**
- Industry certified instructor (EC-Council) for penetration testing and cybersecurity.

Other key accomplishments:

- Author of over twenty keystone policy and procedural documents including an incident response and computer security team handbook, a perimeter security handbook, and a computer forensics procedural guidelines document.

EMAGINED SECURITY

Certifications

CISSP, EnCE, CCE, APS, MCSE, SSCP, A+, Server+, OSCP, KLCP, CCT, DRE, GCFW, GSEC, GIAC Gold, CJIS Level 4

UFED Physical and Logical Certified

Certified EC-Council Instructor

Affiliations

HTCIA

N-TEC

NCFTA

InfraGard

Education

Eastern Washington University (MFA)

University of Maine at Farmington (BA)

- Lead assessor for more than seventy-five (75) security assessments that required documented risk analysis, mitigation and containment research and controls evaluation and recommendation. [3] worked across all facets of the organization to ensure security controls were understood, documented and implemented properly in accordance to recommendation and compliance.
- Selected by the CISO of a Fortune 500 company to create, develop, socialize, and lead a next-generation perimeter security program with core focus on the extensible perimeter, including cloud, converged and mobile platforms.
- [3] oversaw the procurement, deployment, and operations turn-over effort for a Fortune 500 company's web application firewall adoption.
- [3] was the innovator and early adopter of a Fortune 500 company's cyber security program. [3] established controls and programs to protect the organization from phishing, fraud, malware, and similar nefarious activities as well as secured key partnerships with service leaders and innovators. The work undertaken by [3] in this space is still being advanced today.
- [3] has been the lead investigator or lead forensics consultant on over seventy-five investigations, some of them extremely high-profile and newsworthy. [3] has contributed directly to these investigations by discovery of evidence and indicators of compromise that have been shared with law enforcement organizations including the United States Secret Service and Federal Bureau of Investigation.
- [3] has been highly praised and lauded for his contributions at each organization where he has worked. [3] continues to bring daily passion, confidence and positivity to his work and ensures that every Emagined Security client leaves more secure and aware than before they engaged Emagined!
- [3] was instrumental in detecting/flagging and communicating an early warning issue in a state agency's information security program that if addressed at the time of reporting would have saved the agency and the state multiple thousands of dollars in fraud.

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing / Red Team

Vulnerability Management

Vulnerability Assessments

Network Architecture Analysis / Design

Security / Risk Assessment

Process Development / Instantiation

Network, Application and Perimeter Security

Secure Software Development

Web Application Programming

Problem Solving – Concrete & Abstract

Analytics and Research

Program Creation, Management and Development

Documentation

Converged Environments / Cloud

Social Engineering

[3], *Principal Consultant*

[3] is a principal security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing, Network Architecture, Software Development, and Program Management. Prior to joining Emagined Security, Mr. **[3]** served in both technical and managerial capacities at Visa Inc. and the United States Navy. Mr **[3]** possesses strong skills in identifying client needs and fostering collaboration with multiple teams to formulate solutions. He has effective written and verbal communication skills in English, Spanish, and Portuguese, with demonstrated ability to bridge the gap between technical and non-technical personnel.

Penetration testing accomplishments:

- Lead tester on over 400 penetration testing engagements, including web application, thick client, API, embedded devices and network and critical infrastructure based.
- Implemented a 3rd party penetration testing program for a Fortune 500 company, including formulating business justification, authoring request for proposals (RFP) and process documentation, performing cost savings analyses, and training personnel.
- Mr. **[3]** has performed during his 20+ year career:
  - **600+ web application penetration tests**
  - **400+ network penetration tests**
  - **300+ API penetration tests**
  - **200+ thick client penetration tests**

Other key accomplishments

- Updated antiquated client processes to meet their respective requirements. The processes included moving from static documentation to database-driven applications to intelligently gather and manipulate data throughout the process lifecycle. Technologies used to implement these solutions included Windows SharePoint Services, OpenText Livelink, and custom programs.
- Developed a security management application to compose, generate, and track vulnerability assessments for a Fortune 500 company, which resulted decreased reporting times, multi-team collaboration, and a cost-savings of over $1.5M to the company. Alongside the application was the implementation of programming best practices, including continuous integration and robust bug tracking for progressive development.
- Lead assessor for more than a hundred security assessments that required documented risk analysis, mitigation and containment research and controls evaluation and

Certifications

OSCP, OSWE, GSEC, Security+, Oracle Certified Professional Java Programmer, CIW Perl, JavaScript, Database Specialist, and Web Development Professional, Project+, Network+, A+, CJIS Level 4

SSBI Top Secret Clearance (inactive)

Education

Western Governors University (BS CIS)

recommendation. Mr. [3] worked across all facets of the organization to ensure security controls were understood, documented and implemented properly in accordance to recommendation and compliance.

- Pioneered the implementation and integration of several technologies for a Fortune 500 company, which resulted in enterprise-wide adoption, including virtualization, full disk encryption, and configuration management. Received several awards in recognition of these achievements.
- Received a Navy and Marine Corps Achievement Medal (NAM) for working aggressively with Fleet Information Warfare Center to identify and eradicate network vulnerabilities, and successfully implement a shipboard information security program continue such practices.

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing / Red Team

Vulnerability Management

Vulnerability Assessments

Network Architecture Analysis / Design

Security / Risk Assessment

Network, Application and Perimeter Security

Systems Administration

Peer Training/Team Mentorship

Technical Expertise

Security Tools

Burp Suite

Hashcat

Metasploit

Nessus

Nikto

Nmap

PowerShell Empire

PowerSploit

SQLMap

Wireshark

Wfuzz

[3] *, Principal Consultant*

[3] is a principal security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing. Prior to joining Emagined Security, **[3]** served in a technical capacity at Nicklaus Children's Hospital as a Systems Administrator. **[3]** comes from a diverse background and experience working with a wide array of technologies and enterprise products including but not limited to VMWare vSphere, Cisco UCS, Microsoft Exchange, Active Directory, Microsoft SCCM, Sophos SafeGuard, and Sophos Endpoint Security and Controls.

Penetration testing accomplishments:

- Lead tester on over 300 penetration testing engagements.
- **[3]** has performed during his 10+ year career:
  - **300+ web application penetration tests**
  - **300+ network penetration tests**
  - **100+ API penetration tests**
  - **70+ thick client penetration tests**
- Mentored/trained team members on penetration testing/ethical hacking methodologies.
- Developed multiple Python scripts to automate repetitive tasks commonly encountered on penetration tests.
- Achieved "Guru" status and ranked in the top 100 in the "Hack The Box" penetration testing labs, which is a well-known educational platform for ethical hacking.

Other key accomplishments:

- Managed and grew a VMWare environment of about 50 hosts to over 300 hosts and 1500 + virtual machines.
- Developed and maintained security hardened baseline/golden images for multiple operating systems distributions of both Windows and Linux.
- Implemented a "light-touch" operating system deployment leveraging Microsoft SCCM.
- Implemented a phased monthly patching process for all workstations and servers with WSUS/SCCM integration.
- Maintained a Microsoft SCCM environment and managed over 5000 servers and workstations, including patch management, OSD, and application delivery.
- Managed a Cisco UCS infrastructure spanning four UCS domains and over 200 blade servers.
- Developed and implemented numerous Active Directory GPO policies and ACLs.
- Led initiatives to automate various Active Directory tasks using PowerShell scripting.

Technical Expertise cont.

Programming Languages

PowerShell

Python

Product Experience

Active Directory

Cisco UCS

Microsoft Exchange

Microsoft SCCM

Sophos

VMWare vCenter

VMWare vSphere

Certifications

OSCP, KLCP, OSWE, OSEP, CCT

CCNA, CCNA Security (Expired)

CompTIA A+, N+, Security+

CREST CRT Accredited

Education

Western Governors University (B.S.)

- Successfully completed a project to implement and maintain hardware encryption using Sophos SafeGuard Encryption.
- Implemented and maintained Sophos Endpoint Security and Control.
- Managed and successfully completed projects to migrate over 3000 workstations to Windows 7 and then again to Windows 10.

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing / Red Team

Mobile Application testing

Threat Modeling for FDA – HIPAA Compliance

Vulnerability Management

Vulnerability Assessments

Digital Forensics

Fraud Detection / Prevention / Control

Network Architecture Analysis / Design

Security / Risk Assessment

Process Development / Instantiation

Network, Application and Perimeter Security

Problem Solving – Concrete & Abstract

Analytics and Research

Program Creation, Management and Development

Documentation

Converged Environments / Cloud

Social Engineering

Certifications

GIAC Certified Incident Handler (GCIH)

[3], *Senior Consultant*

[3] is a senior consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing. [3] is an Offensive Security Engineer with over two decades of experience in Information Technology. He specializes in identifying and exploiting software vulnerabilities and has a proven track record of successfully analyzing software and systems to identify weaknesses. [3] has demonstrated expertise in coordinating the testing and recommendation of security measures for operating systems, user authentication, and applications. Prior to joining Emagined Security, Mr. [3] has supported various within the Navy (NAVAIR, NAWCAD, NAVSUP), Army (ARCYBER, RCCP), Department of Defense (DoD), and other government agencies such as the Census, Department of Homeland Security (DHS) supporting CISA and US-CERT, Customs and Border Protection (CBP), and Threat Systems Management Office (TSMO) and their SOCs since 2003. [3] has provided solutions that preserve compliance, access, and security in rapidly changing environments. He is adept at evaluating risks and threats and adopting adaptive security policies, processes, and technologies.

Penetration testing accomplishments:

- Conducted insider and outsider threat perspective penetration tests on all DHS CISA networks, creating security access reports (SAR) as a weekly deliverable. Expertise in emulating adversarial exploitation techniques against targeted infrastructure, endpoints, and software. Conducted research on internal service and application vulnerabilities to enhance Red Team capabilities. Utilized proof of concept (POC) code to develop working exploits for red team use.
- [3] has performed during his 25+ year career:
    - **2700+ penetration tests, encompassing all facets of network, mobile, and application penetration testing**
- Expertise in conducting vulnerability assessments for networks, applications, and operating systems, identifying critical flaws that could be exploited by cyber attackers.
- Experience conducting penetration testing using standard tools such as Metasploit, Nmap, Nessus, and Burp Suite. Planned, coordinated, and executed penetration testing, application testing, and security assessments at the application, system, and enterprise levels. Conducted manual penetration tests, validated vulnerability scan results, and developed automation/scripts for replicating validation and penetration tests. Performed penetration testing on DHS and CBP commercial off-the-shelf (COTS) and government off-the-shelf (GOTS).

EMAGINED SECURITY

Certifications (cont.)

GIAC Penetration Tester (GPEN), Burp Suite Certified Practitioner (BSCP), eLearnSecurity Certified Penetration Tester eXtreme (eCPTX), eLearnSecurity Certified Professional Penetration Tester (eCPPTv2), eLearnSecurity Mobile Application Penetration Tester (eMAPT), eLearnSecurity Certified eXploit Developer (eCXD), eLearnSecurity Certified Web Application Penetration Tester eXtreme (eWPTXv2), ZeroPointSecurity Certified Red Team Operator (CRTO), TCM Security Practical Network Penetration Tester Certification (PNTP, Offensive Security Certified Professional (OSCP), Offensive Security Web Expert (OSWE) , Offensive Security Experienced Penetration Tester (OSEP), CompTIA PenTest+, Certified Ethical Hacker (CEH)

Education

Strayer University (B.S.)

- Validated findings through manual exploitation to eliminate false positives. Demonstrated ability to recognize, document, and report vulnerabilities and kill chains, describe remediation activities, and effectively communicate results to technical and non-technical audiences within DHS/CISA.

Other key accomplishments:

- Skilled in conducting secure code reviews (SCR) using static code analyzers such as HP Fortify, SonarQube and CheckMarx. Experienced in coordinating with developers to address findings and documenting completed development projects for operational use.
- Proven ability to provide oral briefings to technical and non-technical audiences, including leadership, on assessment results. Skilled in developing and presenting Red Team reports, diagrams, and presentations detailing attack chains, timelines, and compromise metrics.
- Experience in developing and tuning offensive tooling to increase effectiveness and reduce detection. Participated in offensive operations and provided support for rapid capability and tool development.
- Involved in Purple Team exercises, collaborating with DHS/CISA cyber defense teams to influence executive leadership on prioritizing and executing remediation plans. Strong communication skills used to present findings and recommendations to various audiences.
- Conducted regular network security audits and scanning over 400,000 DHS and CBP assets using Tenable Security Center (SC) to pinpoint vulnerabilities and streamline tasks.
- Skilled in developing and modifying custom Python scripts and applications for vulnerability testing and parsing CSV reports produced by Tenable SC and validated report findings manually to minimize false positives.
- Mr. [redacted] has made notable contributions to the MASV (Mobile Application Security Verification Standard) and MASTG (Mobile Application Security Testing Guide) projects of OWASP (Open Web Application Security Project).

EMAGINED SECURITY

[redacted] *Senior Consultant*

[redacted] is a senior consultant and has been working with information technology for over eight years and has shown himself to be a great wealth of information in the information technology and security tools arena. [redacted] is a self-starting individual that takes great pride in understanding as much of information technology as one person can. [redacted] experience encompasses enterprise operations and security management, policies and standards, consulting, assessments, and penetration testing.

[redacted] s the consultant you engage to learn, understand and improve your security tool sets. He has the motivation and energy to perform any task assigned. He has the ability to learn and understand multiple security tools, product and service and harness that knowledge to better serve an enterprise. His understanding of security far outweighs that of many of his peers in time and experience.

Penetration testing accomplishments:

- **Lead penetration tester on over 400 application and network-based penetration tests, including mobile applications and embedded devices as well as web application, thick clients, APIs and network-based/critical infrastructure.**
- Cisco Hacking - Performed an ethical hack on a high value Cisco Router where the client had stated the router failing would alert support. Resulting test changed the scope of how the boundary router security mechanisms were implemented.
- Wireless Hacking - Provided Wireless Penetration supporting clients identifying rogue wireless access points and clients attempting connections to their corporate wireless network.
- Web application testing for customer member bank member interface applications. Providing Ethical hacking on high-net-worth internet sites where customers have access to sensitive marketing and reporting of industry trend reporting.

Other key accomplishments:

- Implementation of Vontu into enterprise network environment including day to day operations guides, product tuning and infrastructure design and roll-out

Areas of Expertise

Ethical Hacking

Information Technology, Security Methodology

Penetration Testing

Security Management

Problem Solving

Project and Program Management

Embedded Controllers

Secure SDLC Development

Software Development (Agile / Waterfall)

Vulnerability Assessments

Microsoft Exchange

TCP/IP Administration

Digital Systems

Technical Expertise

Operating Systems

Windows (all versions), Linux/Unix

Languages

.NET, c#, c/c++, Java, Assembly, RS232/RS485

Protocols & Services

TCP/IP, HTTP(s), (s)FTP, SMTP, POP3, DNS, IMAP, SCP, SSH

EMAGINED SECURITY

Software

Backtrack, Burp Suite, Nessus, Netcat, Nikto, OWASP ZAP, Snort, Wireshark, Web Inspect, Various other tools

Certifications

Certified Ethical Hacker Certified

A+ Certification

Vontu Certified

Symantec Endpoint Protection Certified

PGP Certified

Brightmail Gateway Certified

Altiris SE Certified

Currently pursuing CISSP – Certified Information Systems

Certified Ethical Hacker Certified

Technical Specialties

Penetration Testing

802.11x Wireless

Security Tool Infrastructure Design, Implementation and Operation

- Endpoint Security implementation expert with detailed knowledge of client computer requirements on upgrading to endpoint security products including, AV, FW, Vontu and Altiris.
- Day-to-day security tool operations, enhancements and maintenance of multiple security tool platforms.
- Symantec ESM 6.5, Bindview and Endpoint 12 Integration and Product Management Support. Provide support for product implementation and support including setup, training and identification of areas of use of product deployments.
- Responsible for customer training in various areas including; security, automation management, and programming control.
- Technical Support (SE) for consultant, sales department and upper management.
- Learned all past and present programming software and hardware specifications related to security and automation control systems.

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing / Red Team

Vulnerability Management

Vulnerability Assessments

Digital Forensics

Security / Risk Assessment

Network, Application and Perimeter Security

Problem Solving – Concrete & Abstract

Documentation

Social Engineering

Web Development

Certifications

SLAE, SPSE, SJSE, PCNSE, CCNA (R&S),Pentest+, CySA+, Sec+, Net+, A+

Education

Johnson County Community College

Centriq Training

[3] *Senior Consultant*

[3] is a Senior Security Consultant with Emagined Security with more than 6 years of proven information security experience. After being an integral blue team member in a network operations center, [3] opted for a more offensive role, where he realized a deep passion that lent itself to naturally accelerated growth within the field. [3] devotion to problem-solving and out-of-the-box creativity has helped him identify and report multiple security vulnerabilities to multiple bug bounty programs.

As an active member of Kansas City's longest-running monthly security meetup, [3] often delivers rigorous reports to executives employed by several Fortune 300 companies and leads talks to better inform local cyber security professionals in the group. Additionally [3] actively analyzes consumer devices, such as Roku, Nikon cameras, garage door controllers, and smart entry systems akin to the Amazon Ring, for security weaknesses.

Penetration testing accomplishments:

- Contributed more than a dozen unique vulnerabilities to open-source bug bounty programs and many more unpublished ones that had been discovered by others.
- **[3] has conducted over 200+ application and network-based penetration tests during his 6+ year career.**

Other key accomplishments:

- Architect of modular, responsive, elegant systems for myriad use-cases, including custom Command and Control back-ends, surreal phishing guises with effective results, as well as intricate payload delivery systems that thwarted Top 10 security appliance vendors.
- Effective, driven tester with a proven track record on 200+ penetration testing engagements, including social engineering, physical and perimeter assessments, lock bypass demonstrations, and custom exploitation development for bench-marking security controls at an unparalleled standard with multiple Fortune 500 clients.

EMAGINED SECURITY

Areas of Expertise

Penetration Testing

Cyber Threat Analysis

Vulnerability Management

Vulnerability Assessment

Red Team/ Adaptive Threats

Digital Forensics

Security / Risk Assessment

Process Development

Symantec Endpoint Protection/Two Factor Authentication

SIEM Analysis

Technical Writing

Incident Response

Symantec Backup Exec

Network, Application and Perimeter Security

Problem Solving – Concrete & Abstract

Analytics and Research

Program Creation, Management and Development

Social Engineering

Documentation

Clearance

Secret Clearance (DoD)

[3] *Senior Consultant*

[3] s a senior security consultant with Emagined Security, providing expertise in the fields of Ethical Hacking, Proactive Network Testing, Cyber Security Threat Management Analysis, Security Information and Event Management (SIEM), Vulnerability Management, Incident Response, and Computer and Network Forensics. Prior to joining Emagined Security, [3] served in both technical and supervisory capacities at Aerojet Rocketdyne. [3] possesses strong skills in identifying client needs and fostering collaboration with multiple cross-functional teams to formulate and implement successful security solutions. [3] is an effective communicator who excels at both written and verbal communication skills. [3] has demonstrated ability to bridge the gap between technical and non-technical personnel and brings with him an arsenal of experience working on a myriad of established and cutting-edge security technologies, hardware, and software platforms.

Penetration testing accomplishments:

- **Lead penetration tester on over 400 engagements, including various web application, API, thick client, and network-based penetration tests, including mainframe and ICS/SCADA.**

Other key accomplishments:

- Lead cyber threat and incident management liaison between client and Defense Cyber Crime Center (DC3) / Defense Industrial Base (DIB) that required risk analyses metrics, incident response, containment, mitigation, threat actor analysis, forensic acquisition and analysis, remediation techniques and implementation and collaboration with appointed Department of Security Services (DSS) and Federal Bureau of Investigations (FBI) agents. [3] worked across all aspects of the organization.

- FireEye-MAS/WebMPS/EX appliance administrator, event monitor, and incident response lead. [3] has contributed directly to all FireEye appliances deployed throughout the organization. [3] constantly updated all FireEye appliances with real time threat intelligence from Defense Intelligence Agency (DIA), National Security Agency (NSA), DC3, Department of Homeland Security, Central Intelligence Agency (CIA), US Computer Emergency Response Team (US CERT), Federal Bureau of Investigations (FBI), iDefense Threat Intelligence, and Department Security Services (DSS), ensuring all perimeters of the organization were secure.

EMAGINED SECURITY

Education

Sacramento, California State University, BS – Business Administration

Industry Certifications

Certified Ethical Hacker

CompTIA A+ Certification

Microsoft Windows SharePoint Services 3.0, New Horizons, 2008

Microsoft Office Share Point Server 2007, New Horizons, 2008

Windows SharePoint Services Installation, New Horizons, 2008

Windows SharePoint Services Administration, New Horizons, 2008

- Appointed Cisco Proxy Admin. [3] created and maintained web policies, Custom URL Categories, web reputation and filtering, acceptable use controls, identities, routing and access polices throughout the infrastructure meeting customer's expectations for UAT of new controls and polices, and implementation.
- Forensic acquisition, analysis, and data preservation. [3] utilized Gudiance Software's EnCase for laptops, desktops, tablets, cell phones, storage devices, multiple platform servers and live memory collection and images through physical, logical, and remote acquisitions. [3] irectly aided investigations through discovery of evidence and identification of indicators of compromise (IoCs) that have been shared with law enforcement organizations including DSS, FBI, and Air Force OSI.
- [3] provided technical support, security process and procedures development and maturation, direction, supervision, and leadership to members of the PC support group and IT call centers. [3] contributed numerous knowledge-base articles and remediation guides for deskside support and the IT call center.
- Provided guidance and direction regarding security control elements in policies that included TLS, email encryption, phishing campaigns, Cyber Security awareness campaign, customer data exchange, overseas computing, and incident reporting.
- Technical writer for a Corporate Security Visitor Security Management implementation. [3] was selected to test and configure visitor security management software, peripherals, printers. [3] constructed supporting documentation for deployment and training for corporate security.
- Directed over $500K in infrastructure resources. [3] nstructed and trained peers as well as department employees with developed documentation and training that fosters to all learning altitudes at a technical and non-technical standpoint.

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing / Red Team

Vulnerability Assessments

Network Architecture Analysis / Design

Security / Risk Assessment

Vulnerability Management

Network, Application and Perimeter Security

Systems Administration

Peer Training/Team Mentorship

Hyperconverged Infrastructures

PowerShell

Active Directory

Microsoft Exchange

Microsoft SCCM

Azure

AWS

Sophos

VMWare vCenter

VMWare vSphere

Cisco UCS

[3] *Senior Consultant*

[3] is a senior security consultant with Emagined Security, providing technical and managerial expertise in the fields of Ethical Hacking/Penetration Testing, Virtualization and Converged Environments, and Enterprise Systems Administration. [3] is an IT professional with over 17 years of progressive experience in secure design and implementation, operations, vulnerability management, and data center operations. Prior to joining Emagined Security [3] served in technical and supervisory capacities for CDR Maguire, Royal Caribbean Cruises, and Miami Children's Health System where he oversaw the daily administration, security, and management of multi-million dollar architectures, their critical network infrastructures, and various support teams. [3] diverse background and experience with a variety of IT technologies and enterprise environments, coupled with his bilingual proficiency in Spanish and English allows him to excel in identifying client needs, providing secure and comprehensive security solutions, and with adroitly navigating the rapid and ever-evolving cybersecurity landscape for his clients and their respective organizations.

Penetration testing accomplishments:

- [3] brings over 15+ years of IT experience, customer service, project and engagement management, with focus in large project management.
- [3] **has conducted over 50 network-focused penetration tests, and has lead several OSINT discovery efforts and web application penetration tests.**

Other key accomplishments:

- Managed a multi-state effort to deploy IT infrastructure in COVID-19 testing and vaccination sites for the Florida Division of Emergency Management and FEMA.
- Researched and implemented different technologies to support LTE communications utilizing multicarrier redundancy with Verizon, AT&T, and/or T-Mobile.
- Implemented MDM solutions to manage mobile technologies like Apple IOS, Android, Unitech or Zebra handhelds, as well as Cradlepoint solutions for VPN and network communication.
- Supervised a team of over 100 field technicians, assigned work and activities, conducted performance reviews, and instilled/promoted overall employee engagement within the team.
- Developed procedures and implemented communication channels to support over 100 COVID-19 testing and vaccination sites with over ten thousand user endpoints.

EMAGINED SECURITY

Certifications

AWS Cloud practitioner

VMware Certified Professional 6.5

CCNA, CCNA Security (Expired)

CompTIA A+, N+, Security+

Education

Western Governors University (B.S.)

- Implemented multiple solutions in Microsoft Azure including but not limited to the automation of virtual machines deployments. Setup VPN connectors to provide interoffice connectivity, leveraged Microsoft Intune to support managed mobile iOS devices and unmanaged devices (BYOD).
- Deployed mobile applications from Azure Intune to Apple iOS and implemented multiple workflows in Azure AD.
- Directed, managed, coordinated and completed multiple VMWare ESXi migrations and/or upgrades across multiple ships and shore side data centers.
- Automated the virtual server migration in VMWare using tools such as PowerShell and PowerCli. Also automated repetitive task like server provisioning and the installation of applications like FlexNet, Cylance and others.
- Supported a VMWare infrastructure with over 10,000 mission critical virtual servers.
- Successfully completed the deployment of Cisco Internight to centralize the management of over 30 Cisco UCS domains.
- Full SCCM implementation to automate, package and deploy operating systems and applications.
- Deployed multiple Cisco UCS domains leveraging server profiles, fabric interconnects, chasses, and blades.
- Implementation of WSUS to integrate with SCCM for the management and deployment of Microsoft Windows updates.

EMAGINED SECURITY

[3] *Senior Consultant*

Areas of Expertise

Ethical Hacking / Penetration Testing

Network Penetration Testing

Application Penetration Testing

API Penetration Testing

Vulnerability Management

Project Management

Certifications

Certified Ethical Hacker (CEH)

Nessus Proficiency

Splunk Fundamentals

Splunk Sales Rep I

Education

Western Governor's University - M.S. in Business Management and Administration

[3] is a senior consultant with Emagined Security, providing expertise in Ethical Hacking/Penetration Testing. [3] has been with Emagined Security for 4+ years, with experience on the Security Operations Center (Blue Team) and on the penetration testing team. [3] has excellent technical skills in security and great communication and problem-solving skills in finding solutions to security issues in applications and networks.

Penetration testing accomplishments:

- **[3] has performed over 100 penetration tests on networks, applications, and APIs, delivering detailed vulnerability analyses, related business impact, mitigation techniques, and expertise on overall security posture.**
- In addition to testing, [3] has led numerous engagements and is an excellent technical resource in finding, exploiting, and providing mitigation methods to the most common and widespread security issues in today's landscape.

Other key accomplishments:

- [3] has performed over 100 penetration tests on networks, applications, and APIs, delivering detailed vulnerability analyses, related business impact, mitigation techniques, and expertise on overall security posture.
- [3] has a full vision for information security providing insights to both offensive and defensive postures, with experience as a security operations center (SOC) analyst as well as ongoing experience in penetration testing.
- [3] s heavily involved in the cyber security community, being involved in numerous organizations that focus on staying up-to-date on the latest and most important security issues that we see today.
- Recently, [3] focus has been on engagement management and delivering stellar end-to-end project management and customer satisfaction/experience for Emagined Security clients.

EMAGINED SECURITY

Areas of Expertise

Ethical Hacking / Penetration Testing

Vulnerability Assessment

Vulnerability Reporting

Web Application Security

Automation Testing

Accessibility Testing

Risk Assessment

Agile, SDLC, STLC

Scrum Methodologies

Certifications

Certified Ethical Hacker (CEH)

Certified in Selenium + Java

Education

Master's in computer science from Osmania University in 2007

[3] *Senior Consultant*

[3] has nine (9) years of IT experience with dedication placed on penetration testing, security assessment, and automation testing. [3] s a senior consultant with Emagined Security, providing expertise in the fields of Ethical Hacking/Penetration Testing and Open-Source Intelligence gathering. Before joining Emagined Security [3] served in Health Resources and service administration as an application penetration test engineer [3] has excellent exposure in multiple industries and verticals like Healthcare, Utility, Retail and Pharmaceuticals worked as Lead Automation Test Engineer. [3] is an excellent team player, enthusiastic initiator, who brings with her the ability to implement fundamental security tenets and concepts effectively and efficiently.

Penetration testing accomplishments:

- Lead OSINT investigator for Emagined Security, conducting over seventy-five (75) OSINT discovery efforts.
- **Web application penetration tester who has logged more than 100 web application penetration tests with several thick client and API tests.**
- Excellent working knowledge and practitioner of the OWASP penetration testing methodology, including the various attack vectors, risk assessment and vulnerability reporting.
- Proficient in exploiting application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc.
- Skilled using Burp Suite, OWAP Zap, NMAP, Nessus, SQL Map, and other trade tools for application penetration tests and infrastructure testing.

Other key accomplishments:

- Collaborates on a cross-functional and highly specialized team on cross-product technical issues with a variety of resources including development to documenting software defects to exploitation to customer vulnerability remediation.
- Designed automated test cases using the Selenium WebDriver inside the Eclipse IDE using Java.
- Involved in development of POC for Open-Source testing framework using Selenium IDE/RC, Java, Junit, X path Firebug.

EMAGINED SECURITY

[3] *Security Consultant*

Areas of Expertise

Ethical Hacking / Penetration Testing

Network Penetration Testing

Application Penetration Testing

API Penetration Testing

Vulnerability Management

DevSecops

Microservice Orchestration

Container technologies

Cloud technologies & Security

Image Hardening

Cloud Security

Python

C++

Javascript

Embedded Devices

IoT Security

CI/CD pipelines

Certifications

CompTIA Network +

CompTIA Security +

Education

University of Maryland Global Campus -B.S. in Computer Networks and Cybersecurity

O.A.U Ile-Ife – BA in Law

[3] is a security consultant with Emagined Security, providing expertise in Ethical Hacking/Penetration Testing. He is a veteran who holds a top-secret clearance and has worked in both classified/unclassified environments. He has a broad range of security experience with different technologies including cloud technologies, IoT (Internet of Things) devices, DevSecops, design/development of embedded devices, container orchestration and software development.

Penetration testing accomplishments:

- Performed penetration testing for several systems in pursuit of a FedRamp Authority to Operate (ATO)
- **[3] has performed over 150+ penetration tests on infrastructure and applications during his 6+ years career.**

Other key accomplishments:

- Designed a FedRamp Compliant AWS environment from ground up for a top-secret system for the department of justice
- Developed automation to harden Linux, Windows systems using go-task, ansible, chef inspec, python and GitHub actions resulting in images that achieved up to 80% compliance with CIS benchmarks.
- Developed PowerShell and python scripts to audit user interaction with a top-secret system.
- Developed a Docker image that bundles several security tools to aid performing penetration tests in new environments with minimal setup.
- Discovered and assisted to remediate several critical vulnerabilities in a system that could have exposed millions of PII, and top secret marked information.
- Led a team to achieve SOC2 Compliance for a private organization.

EMAGINED SECURITY

[3] *Security Consultant*

Areas of Expertise

Ethical Hacking / Penetration Testing

Testing

Vulnerability Management

Open-source Intelligence

Container technologies

Cloud technologies

Image Hardening

Cloud Security

Python

C++

Embedded Devices

IoT Security

Certifications

Certified Cybersecurity Technician (CCT)

CompTIA Security+ (expired)

Education

University of Miami – Cybersecurity Professional Bootcamp

Miami Dade College A.A Computer Science

[3] is a security consultant with Emagined Security, providing expertise in Ethical Hacking/Penetration Testing. [3] has a strong background in network administration as well as experience in the Security Operations Center (Blue Team). Before joining Emagined, [3] worked as a network consultant at an MSP that serviced various small to medium businesses that dealt in a variety of industries, from Healthcare Vendors to Venture Capital firms.

Penetration testing accomplishments:

- [3] has performed more than 50 network penetration tests during his four (4) years career in ethical hacking.
- [3] brings a tenacity to learn and build advanced penetration testing skills to every engagement.
- [3] s proficient in the following network and application-based tools: Dirbuster, OWASP ZAP, NMAP, Nessus, and NetCat to name a select few utilities.

Other key accomplishments:

- [3] recently obtained his Certified Cybersecurity Technician certification from EC-Council through the Emagined Security in-house training program. The CCT consisted of 40 hours of in-classroom work, over 25 hours of labs (90+ labs) and offline study. The CCT extends Mr. [3] developing cybersecurity skills.
- [3] brings an additional two years of security operations center (SOC) experience to his engagements, allowing him the unique opportunity of providing detailed remediation expertise, as well as implementation and vulnerability management practicality and empathy to Emagined Security clientele.