Consulting from the Mind of a Hacker

- Charles Tendell,

Charles is a Certified Ethical Hacker, Certified Hacking Forensic Investigator, and Certified Information Systems Security Professional. He is a decorated Iraq War veteran with U.S. Army including Letters of Commendation from Commanding Generals and the Army Commendation Medal for his role in developing, implementing, and securing communication infrastructures while deployed during Operation Iraqi Freedom. With over 15 years in the cyber security space, Charles has designed implemented and tested thousands of systems. With experience working with organizations from small mom and pop organizations to Fortune 50 corporations, to implement secure systems, websites and training personnel. Working with compliance standards like ISO 27001, PCI-DSS, SSAE16, HIPAA/Hitch and more, Charles' out of the box design brings cutting edge security to every client and offers a fresh look on active security measures.

Certified Ethical Hackers

The Certified Ethical Hacker is a professional certification, provided by the International Council of E-Commerce Consultants (EC-Council.) An ethical hacker is usually employed by an organization who trusts him or her to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities

Computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information Systems Security Certification Consortium, also known as (ISC) ^{2}. As of May 2014, (ISC) ^{2} reports 93391 members hold the CISSP certification worldwide, in 149 countries. In 2004 the CISSP obtained accreditation by ANSI ISO/IEC Standard 17024:2003 accreditation. It is also formally approved by the U.S. Department of Defense (DoD) in both their Information Assurance Technical (IAT) and Managerial (IAM) categories for their DoDD 8570 certification requirement. The CISSP has been adopted as a baseline for the U.S. National Security Agency's ISSEP program. [5]

Department Of Homeland Security: Information Security Certified

Network Security Assessments

- Security Testing

Find the holes in your infrastructure before a malicious hacker.

- Compliance Evaluations

HIPAA/HITECH, PCI DSS, ISO 27000 is among the list of compliance tests that require a technical review of controls.

- eDiscovery & Digital Investigation

Computer, Network and Cyber investigation services to help companies get a solid grip on evidence and data after a security breach or incident.

- Ongoing Support

Ongoing monitoring, intelligence, Micro penetration testing and training augment a well-rounded security program

At Cyber Security Integration we feel that cost shouldn’t be the barrier to knowing if you’re systems are secure. This service provides our clients, the opportunity to get a high level review of the vulnerabilities and potential threats to business owners without having to worry about sticker shock. Our FREE basic assessment will show you if you have anything to worry about before you commit to a full scope assessment. Our Free Assessment includes not only a look about your current vulnerabilities but goes over your risk from a process, procedural and legal standpoint. All before us even have a discussion about price. In doing this we accomplish setting the bar for our competitors and helping business better understand their risk. Sign up for a free assessment today and get a better understanding of your security posture. And you'll be a step ahead.

Offensive security is a proactive and adversarial approach to protecting computer systems, networks and individuals from attacks. Conventional security — sometimes referred to as “defensive security” — focuses on reactive measures, such as patching software and finding and fixing system vulnerabilities. What is offensive security? – Definition from WhatIs.com

An external assessment designed to identify application vulnerabilities in outward facing systems to determine how an attacker may gain unauthorized access to sensitive information. Validation is conducted on several layers including web, applications and databases in order to identify possible threats.