ecfirst | Perfecting the Art of *Active* Cyber Defense

Technical Vulnerability Assessment

A key requirement of compliance mandates and security standards such as ISO 27000, HIPAA, PCI DSS and others is that organizations *must conduct a comprehensive and thorough assessment of the potentials risks and vulnerabilities to the confidentiality, integrity, and availability (CIA) of all sensitive, confidential information*. These mandates require that organizations must complete a comprehensive and thorough vulnerability assessment on a regular schedule.

*biz*SHIELD^{tm} – An ecfirst Technical Vulnerability Assessment Service

ecfirst developed the *biz*SHIELD^{tm} program to assist organizations in addressing the requirements of compliance mandates and all subsequent guidance documentation and settlement agreements.

As a part of the *biz*SHIELD^{tm} program, ecfirst identifies vulnerabilities from the outside (external) and inside (internal) the organization. Next, ecfirst develops recommended remediation activity, and associated risk priority. All remediation activities will be listed according to recommended implementation time bands in the *biz*SHIELD^{tm} Corrective Action Plan (CAP) table. The *biz*SHIELD^{tm} report is an actionable, documented risk analysis that provides both in depth and executive summary level findings appropriate to all audiences from administrators to the Board of Directors.

Technical Vulnerability Assessment Service

The ecfirst *biz*SHIELD^{tm} risk analysis program includes a technical vulnerability assessment to address compliance mandates with the objective of establishing and prioritizing compliance and security gaps. The ecfirst *biz*SHIELD^{tm} Technical Vulnerability Assessment Service supports several distinct components, including:

- External Assessment
- Internal Assessment
- Firewall Assessment
- Wireless Assessment
- Social Engineering Assessment
- Penetration Testing (Express)

When was the last time your organization conducted a risk analysis activity that included a technical vulnerability assessment?

© Confidential I All Rights Reserved I ecfirst I 1999-2019

External Vulnerability Assessment

ecfirst will identify vulnerabilities within client's Internet-facing infrastructure, and attached network systems. The ecfirst testing will analyze client externally accessible servers. Additional IP addresses can be assessed as required. Additional costs apply. Please discuss with ecfirst.

It is recommended that the testing include the following types of systems:

- E-commerce servers
- Internet or DMZ located Database servers
- Internet screening routers
- Internet-facing firewalls
- E-mail server
- DNS servers
- Servers storing or processing EPHI
- Web Applications
- Other sensitive systems

Internal Vulnerability Assessment

ecfirst will perform an internal network vulnerability assessment on client internal network infrastructure. This testing will verify that the security controls implemented on a sample set of five (5) selected hosts, including servers located in the IT Data Center or desktop PC images provide an adequate level of protection against network attacks.

Specific IPs must be provided by ecfirst's Point of Contact at client.

The ecfirst testing will analyze client internally accessible servers. Additional IP addresses can be assessed as required. Additional costs apply. Please discuss with ecfirst.

The Internal Network Assessment addresses the following areas:

- **Active Directory**
  - Review Identity and Access Management
  - Review passwords in use for complexity

- **Endpoint data loss**
  - Review the number of removable mass storage and communication devices connected to company systems

- **SNMP settings**
  - Identify systems that respond to default or easy to guess SNMP Community strings

© Confidential I All Rights Reserved I ecfirst I 1999-2019

- **SQL servers**
  - Identify servers with SQL services listening that allow connections from any host
  - Identify SQL services utilizing default or easy to guess credentials

- **Networked systems**
  - Identify vulnerabilities and configuration issues

Firewall Assessment

ecfirst will review the organization's Internet-facing firewall to identify the current security posture in three critical areas:

- Rulebase configuration
- Current IOS (or other operating system) and patch revision release level
- Vulnerability assessment of configuration file

Rulebase configuration is critical to the integrity and operating security of a firewall. The rulebase should be tied to business requirements. Every rule that is configured on a firewall is essentially a permissible security hole into the company's network infrastructure. Each of these rules should have a well defined business need for existing. However, many corporations open rules for testing and never close them when the test has completed. Additionally, many rules are opened up because of then-current business needs, but never closed or repaired once that need, or the corresponding business contract, has ended. This results in legacy access and a vulnerability providing a pathway into the internal network.

Wireless Assessment

Wireless networks are particularly vulnerable to attacks because it is extremely difficult to prevent physical access to them. The only advantage they have in this respect is that an attacker must be in relative physical proximity to the network, which can limit the pool of potential attackers. However, with the price of high gain antennas being extremely small, attackers can strike from much further distances with affordable ease. To secure a wireless network, an administrator should know what types of vulnerabilities exist and what types of attacks can exploit them.

The ecfirst testing will analyze client wireless accessible servers. Additional IP addresses can be assessed as required. Additional costs apply. Please discuss with ecfirst.

The WiFi Vulnerability Assessment will be done as part of the internal security assessment. War Walking is the approach/methodology used for the assessment and the scope is defined as:

- ecfirst will perform a wireless assessment at one location
- Discovering the Wireless Access Points visible within the location
- Identify potentially rogue devices - Rogue access points installed by employees without IT departmental consent.

© Confidential I All Rights Reserved I ecfirst I 1999-2019

- Determine the existing WiFi Security Infrastructure such as SSID protection; MAC filtering, VPN and encryption mechanism used (if any), and possibly supplicant certificates.
- Attempt to compromise wireless security after sniffing sufficient packets or performing man-in-the-middle attacks.

Social Engineering Assessment

Organizations with excellent security programs often spend large amounts of money on capital purchases to implement technical security controls. However, employees or contractors of the entity often prove to be the weak link in the security chain. Employee and contractor education is a key component to any information security program. Authorized members of the workforce have both authenticated access to information systems as well as physical access to facilities and secured areas.

During the social engineering assessment, ecfirst will attempt to gain unauthorized or inappropriate access to facilities, secured areas, documents, credentials, or confidential data. ecfirst security personnel will attempt to bypass security controls that are in-place in order to gain access to various assets. ecfirst will attempt to bypass electronic, personnel, and procedural controls during this assessment. ecfirst will document and present a very detailed record of successes, failures, controls bypassed, access achieved and information obtained during the assessment.

Penetration Testing (Express)

The ecfirst Express Penetration Test is less comprehensive than the full Penetration Test in scope as it only addresses external and internal technical vulnerabilities & threats; physical and personnel vulnerabilities and threats are not evaluated. A detailed technical Corrective Action Plan (CAP) is included in the *biz*SHIELD™ report to provide actionable directives for addressing the identified deficiencies.

The ecfirst Express Penetration Test for additional IP addresses can be assessed as required. Additional costs apply. Please discuss with ecfirst.

The ecfirst Express Penetration Test for will be broken up into distinct phases of analysis:

- External Penetration
  - Reconnaissance phase (including the Google Hacking Database), Web Applications and Networked Systems phases are all performed in 1 day
- The Internal Penetration (including the Wireless Penetration) is generally performed in 1 day during the onsite visit.

© Confidential I All Rights Reserved I ecfirst I 1999-2019

Client Testimonial

"ecfirst provides excellent value across a comprehensive portfolio of first rate solutions for regulations such as HIPAA | HITECH compliance, risk analysis, social engineering, vulnerability assessment, disaster recovery and business continuity. They are not just experts in these respective fields but are able to communicate and motivate corporate audiences to effect change."

"ecfirst is an excellent business partner that focuses on long term, successful relationships through consistently successful project delivery."

Joe Granneman, CTO & CSO, Rockford Health System

ecfirst delivers complete end-to-end solutions for compliance information security. With over 2,100 clients across all States in the USA, ecfirst tailors its work to closely align with your requirements and culture. Whether your requirements include a resource to implement security controls and technologies, or develop policies and procedures, or comply with HIPAA, HITECH, PCI DSS, ISO 27000. ecfirst is flexible to address your workforce needs. Why ecfirst? Unconditional guarantee. Flat rate. Flexible services. And most important, we deliver and implement information security solutions world-wide. You will have one point-of-contact. The ecfirst process is based on one phone # for you to call, and one email address to work with. We want to simplify your experience. **Let's get started!**

Contact Us

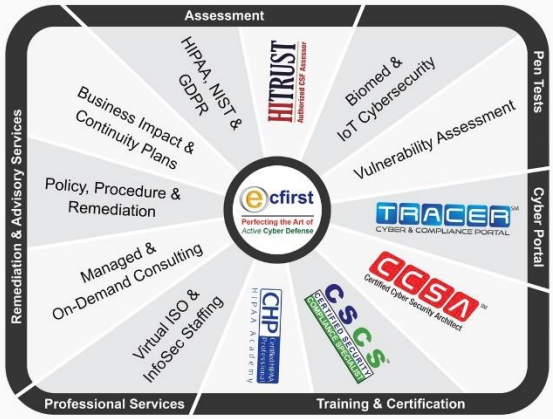
ecfirst is best positioned to be your turn-key compliance and security solutions partner. Our seasoned Practice Team and guaranteed prices will serve you best in meeting compliance and security requirements. I look forward to hearing from you and discussing how ecfirst can assist with jumpstarting your Information Security and Compliance initiatives. Thanks!

John Schelewitz
Director of Sales
Cell: +1.480.663.3225
Email: John.Schelewitz@ecfirst.com

© Confidential I All Rights Reserved I ecfirst I 1999-2019

Technical Vulnerability Assessment

ecfirst — Perfecting the Art of *Active* Cyber Defense



VISION (Mantra)

Enabling establishment of an active cyber defense program and capability.

MISSION (Karma)

Implement an evidence-based compliance program integrated within an enterprise-wide active cyber defense system.

OUR PROMISE

- Unconditional Guarantee. No Questions!
- ecfirst will not consider an engagement complete unless client is 100% satisfied.

Client Reference

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I continue to recommend ecfirst highly and often!"

BRG Berkeley Research Group — Chip Goodman | Vice President of Information Technology

"The ecfirst team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome COLLABORATIVE SYMPTOM MANAGEMENT — DerShung Yang | Founder & President

"Provant Health partnered with ecfirst to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were ***flexible, collaborative*** and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I'd recommend ecfirst to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification."

provant health life. changing. — Tom Basiliere | Chief Information Officer

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor

© Confidential I All Rights Reserved I ecfirst I 1999-2019

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

John T. Schelewitz

Director of Sales

ecfirst/HIPAA Academy

Phone: +1.480.663.3225

Email: John.Schelewitz@ecfirst.com

www.ecfirst.com

© 2019 All Rights Reserved | ecfirst