Cyber Defense
Program Catalog

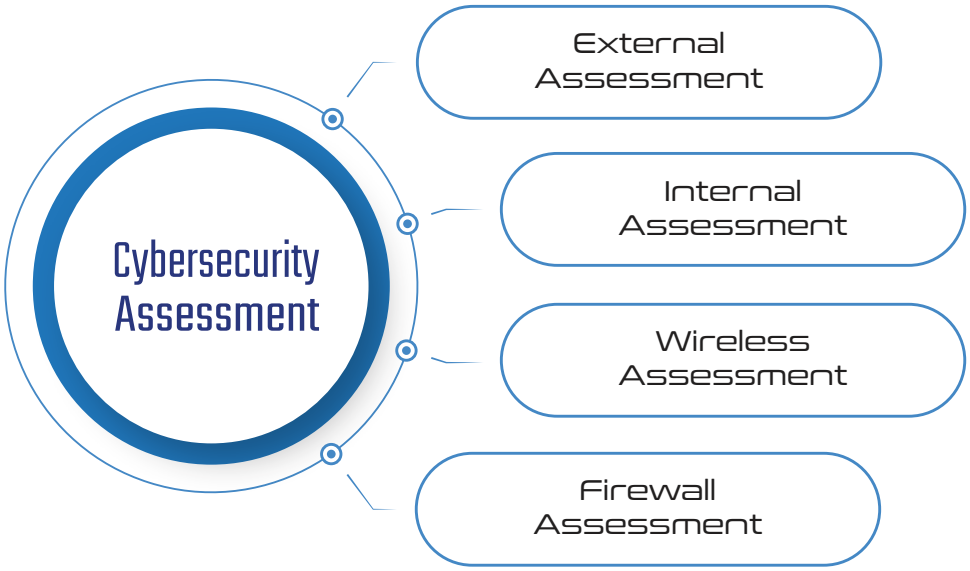
ecfirst

Table of Contents

John.Schelewitz@ecfirst.com

www.ecfirst.com

Cybersecurity Assessment



External Assessment

- AI-assisted open-source intelligence gathering
- DNS misconfiguration review
- Publicly leaked credentials search
- Anonymous external vulnerability scanning
- Website security testing (OWASP Top 10)

Wireless Assessment

- Facility walkthrough for rogue wireless networks
- Wireless security settings & Pre-Shared Key strength analysis

Internal Assessment

- Authenticated vulnerability scans of internal systems
- Identity & Access Management (Active Directory review)
- Password policy & strength analysis
- Offline password cracking attempts using a custom wordlist
- SNMP and default credential testing
- Security software enumeration

Firewall Assessment

- OS vulnerability analysis
- Security configuration & rule review

CYBERSECURITY ASSESSMENT SCOPE	TITANIUM	PLATINUM	GOLD	SILVER	BRONZE
External Assessment	✓ Customized	✓	✓	✓	✓
Internal Assessment	✓ Customized	✓	✓	✗	✗
Firewall Assessment	✓ Customized	✓	✓	✓	✗
Wireless Assessment	✓ Customized	✓	✗	✗	✗
Detailed Analysis	✓	✓	✓	✓	✗
Corrective Action Plan (CAP)	✓	✓	✓	✗	✗
Detailed Remediation Steps	✓	✓	✓	✗	✗
Executive Brief	✓	✓	✗	✗	✗

CloudFirst Assessment

CloudFirst Assessment

Compliance Status Example

Compliant | Not Compliant | N/A

Area	Compliant	Not-Compliant	N/A
IAM	1	3	1
DefenderCloud	5	0	0
StorageAccounts	1	2	0
Database	0	0	5
Log Monitor	1	3	0
Networking	2	3	0
VM	2	0	0
KeyVault	0	0	4
AppService	0	0	7

CloudFirst Risk Status

CloudFirst Scope

The ecfirst CloudFirst Cybersecurity Assessment is organized into two (2) distinct areas of analysis:

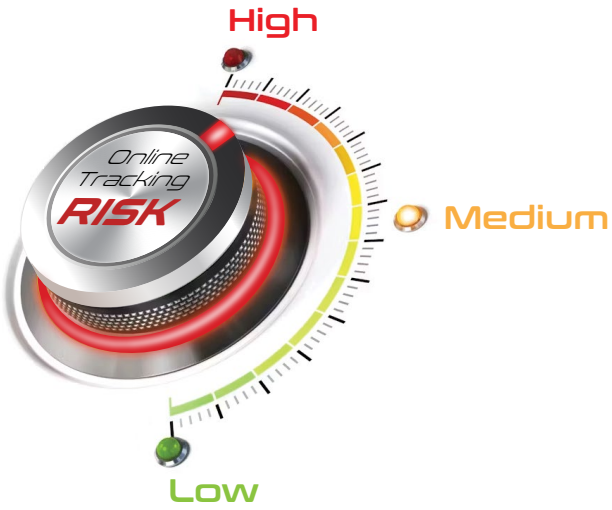
External Assessment
- Up to 32 IP addresses

Internal Assessment
- An Active Directory (AD) domain is tested

Significant Findings

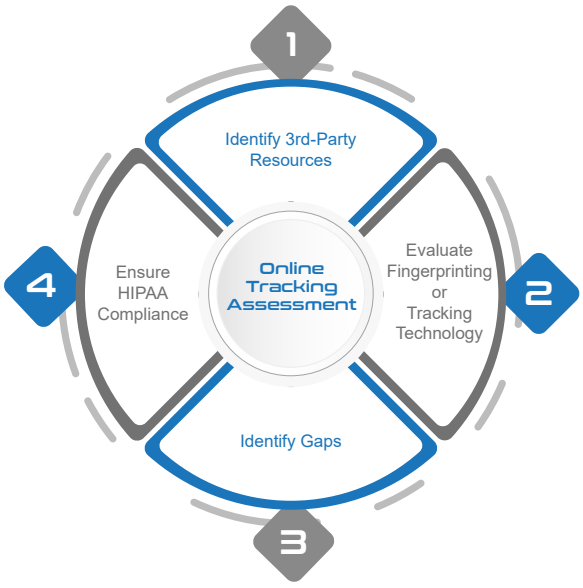
Online Tracking Assessment

ecfirst



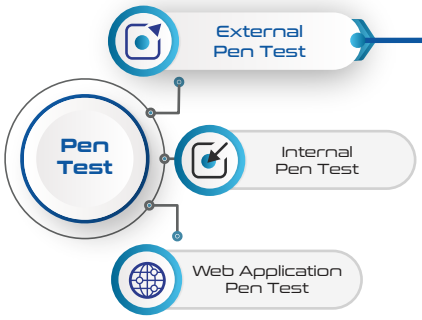
Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

> "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."



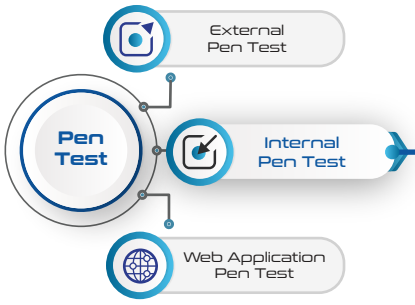
Pen Test

External Pen Test



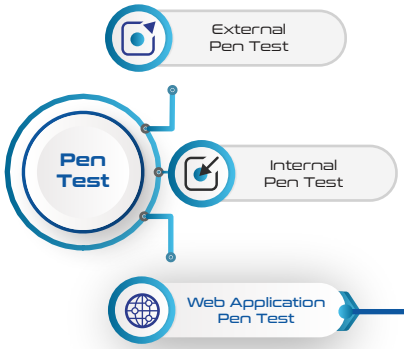
- Up to 16 externally accessible systems (IP ranges and domains)
- Grey box approach with network scanning and reconnaissance
- Password cracking, phishing, and vulnerability exploitation
- Actionable insights to strengthen external security defenses

Internal Pen Test



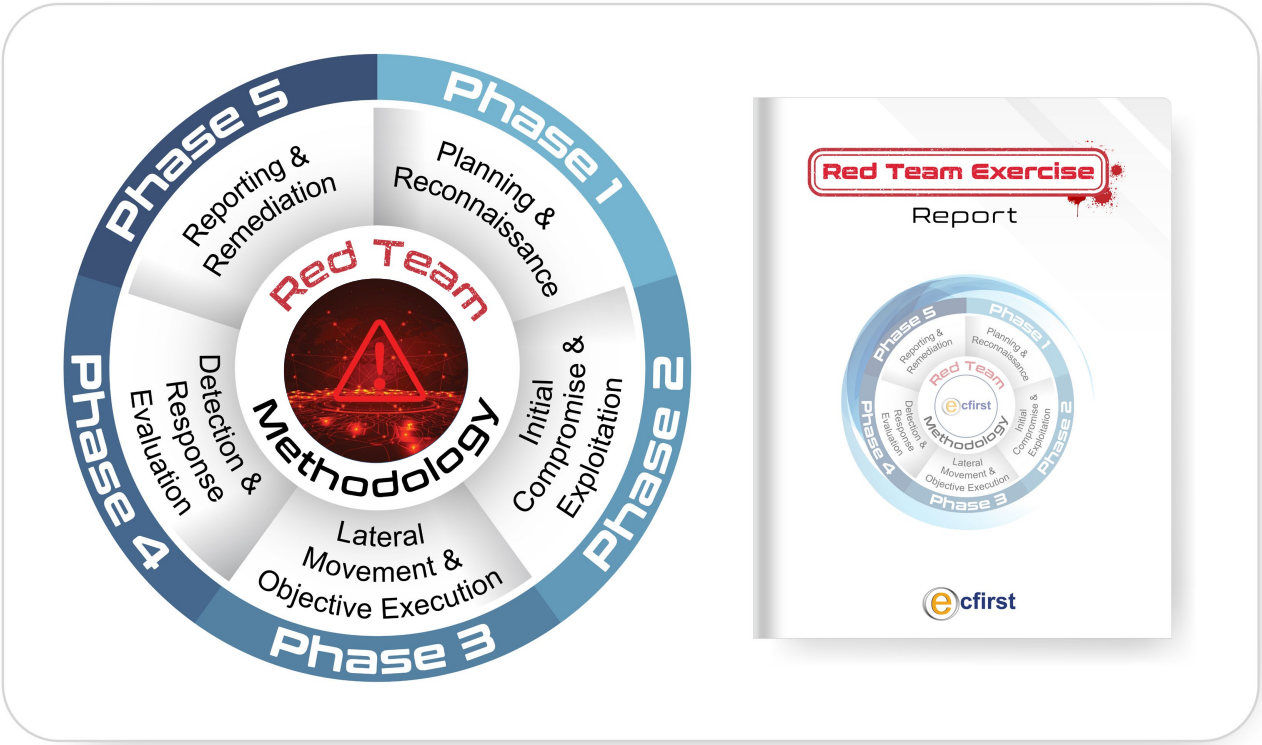
- Grey box test simulating an insider attack
- Network discovery, port scanning, and vulnerability scans
- Password cracking, credential validation, and privilege escalation
- Identifies weaknesses, evaluates password policies, and strengthens security

Web Application Pen Test



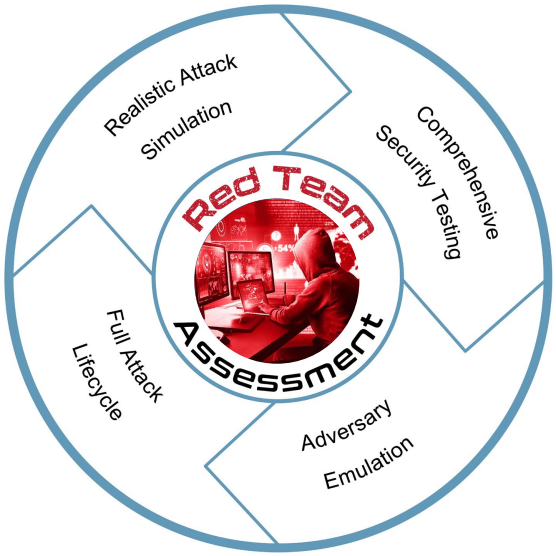
- Tests one web app with "Client" user and anonymous access
- Conducts reconnaissance, mapping, and vulnerability scans
- Identifies injection flaws, session issues, and misconfigurations
- Assesses authentication, access control, and data security
- Provides remediation strategies

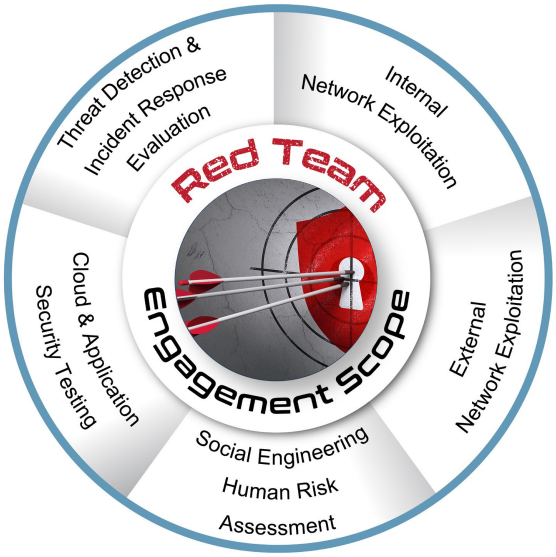
Red Team Exercise



Red Team Exercise

A simulated adversarial exercise that mimics real-world attacks to assess an organization's security capabilities and resilience of its systems and operations.





Social Engineering

- Customized phishing campaigns to identify % of phish-prone users
- Targeted end user security awareness training to reduce risk from phish-prone users
- Development of tailored phishing, vishing, pretexting, CEO Fraud cam paigns to understand business risk
- Detailed reports that describe findings from social engineering campaigns
- Access to security awareness emails for compliance with mandates such as HIPAA, CCPA, GDPR

Executive Dashboard

Significant Findings

Industry Benchmark Data

- Phish-prone % **23.9%**

Phishing emails sent to users that did not fall victim in the previous 4 weeks	
Campaign Start Date	Number of Phishing Victims
Dec 6, 2021	11

Phishing emails sent to users that fell victim in the previous 4 weeks	
Campaign Start Date	Number of Phishing Victims
Dec 3, 2021	1
Nov 19, 2021	0

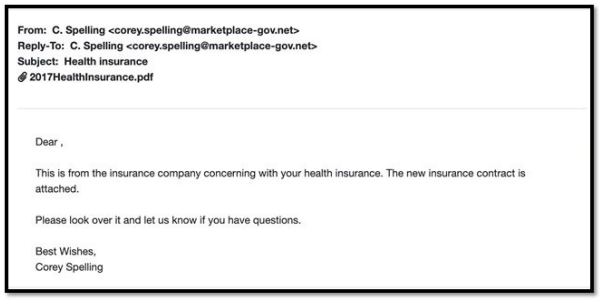
Risk Summary

- Based on the number of users that fell victim to the phishing performed, ecfirst estimates the risk of a successful Social Engineering attack against to be a Medium risk.

Findings

ecfirst was successful in the Social Engineering campaign by enticing 15 users to open and interact with phishing emails we sent. Users that interacted with the emails were then presented information informing them they had fallen victim to a phishing test and identified “red flags” in the email they received that could have indicated the email was not legitimate. Had the users interacted with real phishing emails, the attackers could potentially have performed a number of malicious actions, such as collecting sensitive data or delivering malware to the user.

Sample email sent to user:


From: C. Spelling <corey.spelling@marketplace-gov.net>
Reply-To: C. Spelling <corey.spelling@marketplace-gov.net>
Subject: Health insurance
2017HealthInsurance.pdf

Dear ,

This is from the insurance company concerning with your health insurance. The new insurance contract is attached.

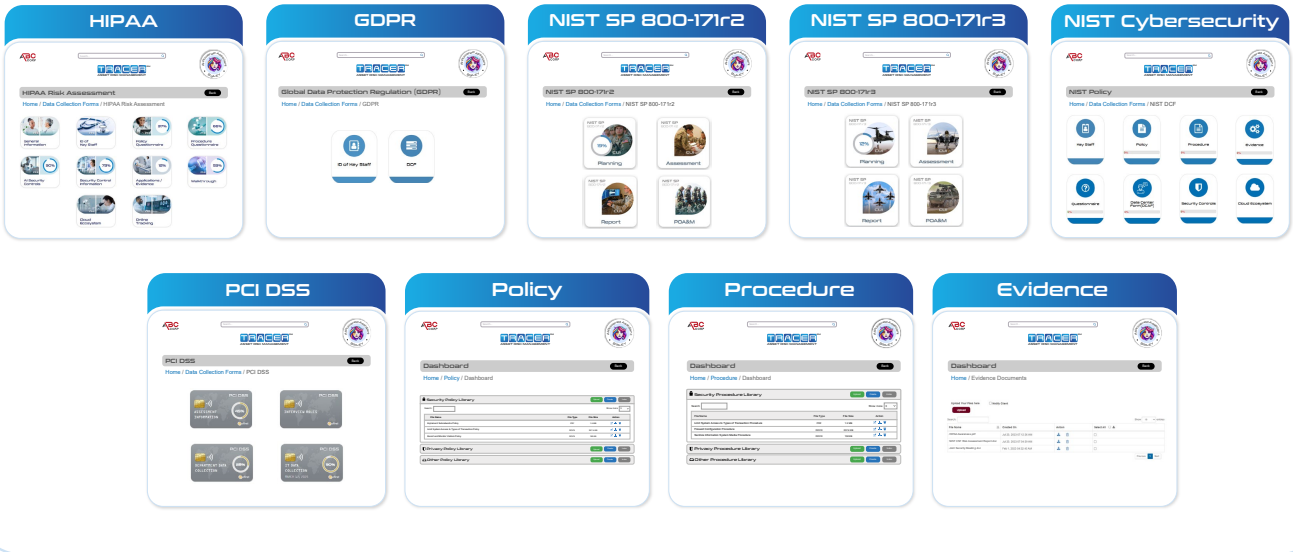
Please look over it and let us know if you have questions.

Best Wishes,
Corey Spelling

TRACER℠ ASSET RISK MANAGEMENT | Cyber Defense Platform

ecfirst

Compliance Portals

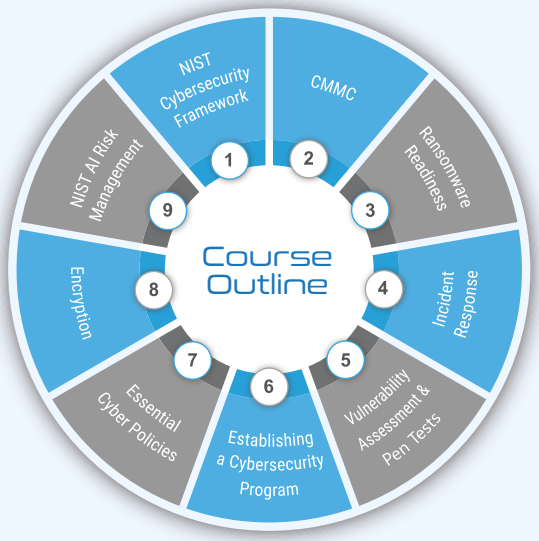


CCSA SM
Certified Cyber Security Architect
Online | Self-Paced

ecfirst

An Executive Cybersecurity Program

HIMSS APPROVED EDUCATION PARTNER | CEU 8 Hours



> **Comprehensive cybersecurity program**. Excellent coverage of the NIST Cybersecurity Framework, CMMC & more. **Relevant scenarios & policies covered**, including encryption & ransomware.

What's in it for you?

- Examine how to establish a cybersecurity program based on the NIST Cybersecurity Framework
- Learn how to establish a credible Ransomware Readiness Program based on NIST Standards
- Walk through core components, organization, and CMMC Levels
- Review encryption implementation across the enterprise to mitigate business risk
- Examine NIST guidance for AI Risk Management

Digital Badge

ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.

CCSA Certified Cyber Security Architect

Client References

ecfirst

"I appreciated the examples and scenarios that brought the material to life."

"The training provided clarity on complex cloud compliance issues."

I loved the training

Prepared me for exam

Privileged to participate

Excellent introduction to NIST

References

Clear concise and to the point

Well organized and informative

CMMC was well covered

Great course!

"Very knowledgeable instructor, provided timely and relevant examples and resources."

"Great overview of cloud security with real-world relevance."

"A crash course covering cybersecurity assessment, NIST and more."

"The training was point on for the core material."

John.Schelewitz@ecfirst.com

www.ecfirst.com