Risk Assessment

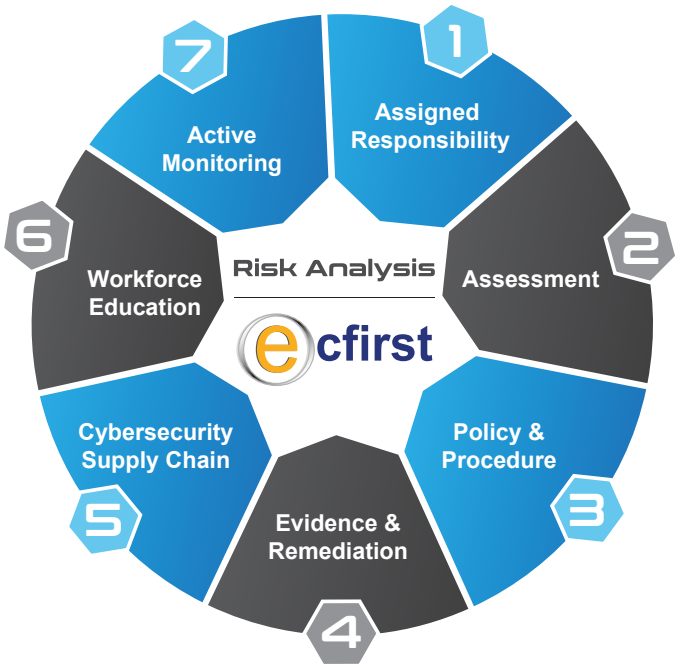
CMMC ◎ HIPAA ◎ NIST ◎ Cyber ◎ CloudFirst ◎ Pen Test ◎ Online Tracking

ecfirst

Signature Methodology

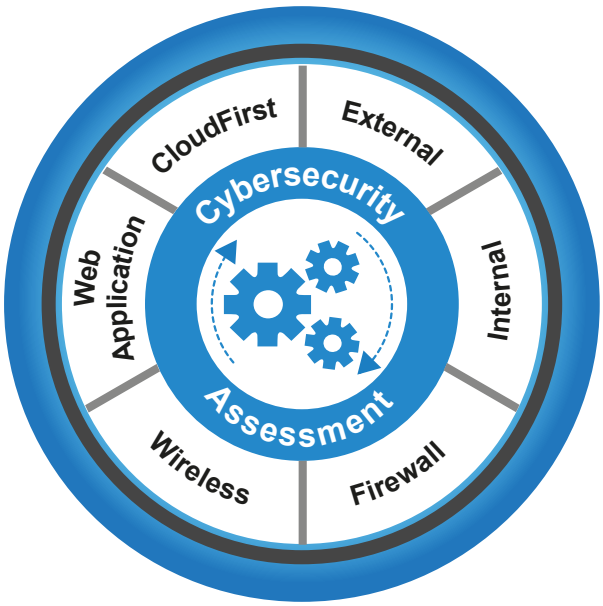
Page 3

HIPAA ◎ NIST



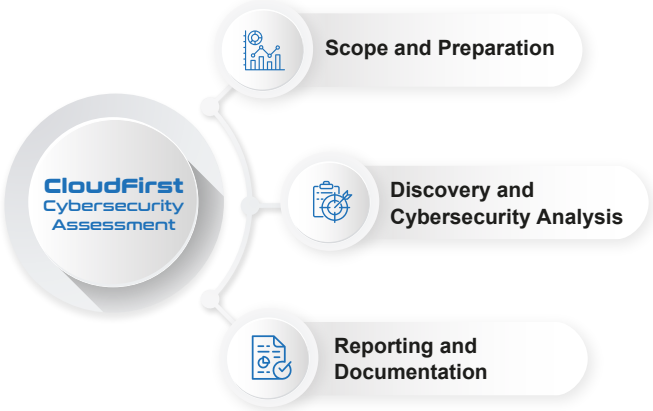
Cybersecurity Assessment

Page 4



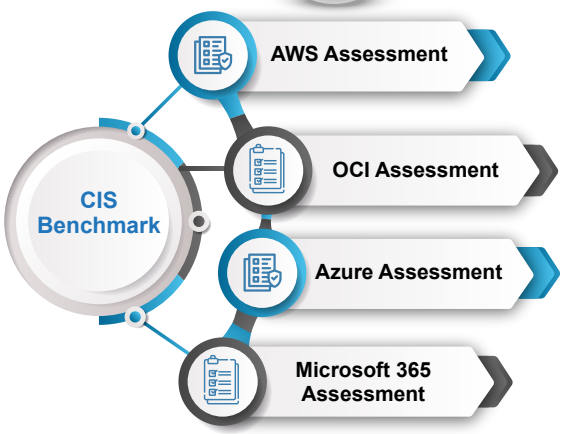
CloudFirst

Page 11



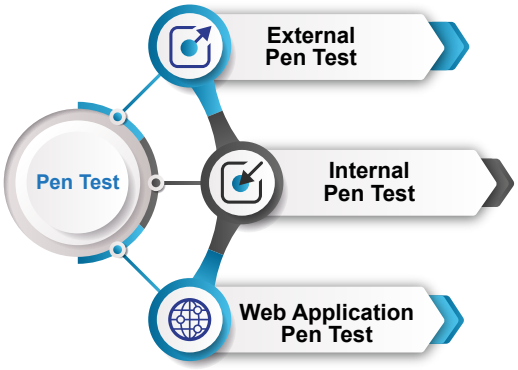
CIS Benchmark

Page 13



Pen Test

Page 16

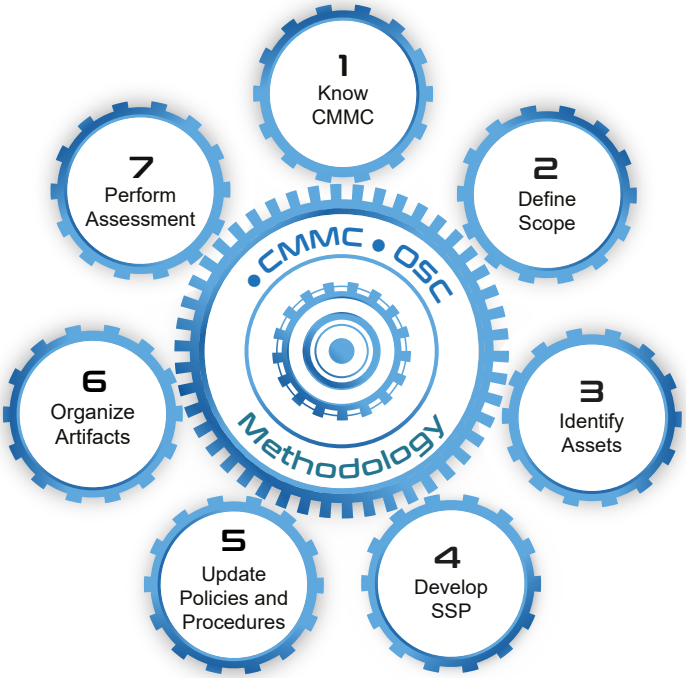


Risk Assessment

CMMC ○ HIPAA ○ NIST ○ Cyber ○ CloudFirst ○ Pen Test ○ Online Tracking

ecfirst

CMMC Readiness



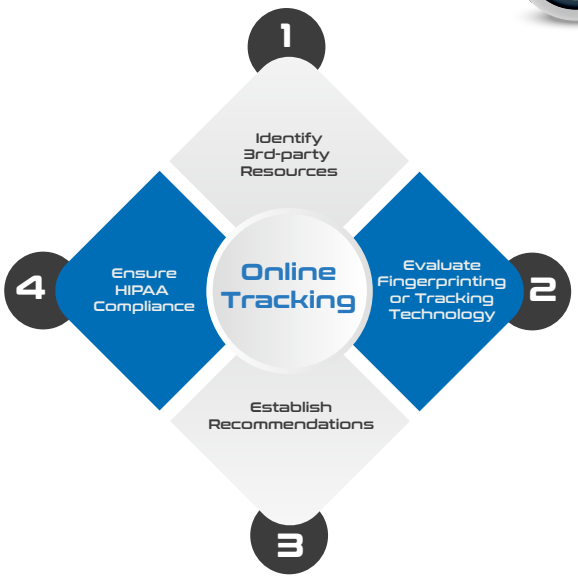
Asset Risk Management

Social Engineering

Page 18

Online Tracking Assessment

Page 20



Risk Analysis

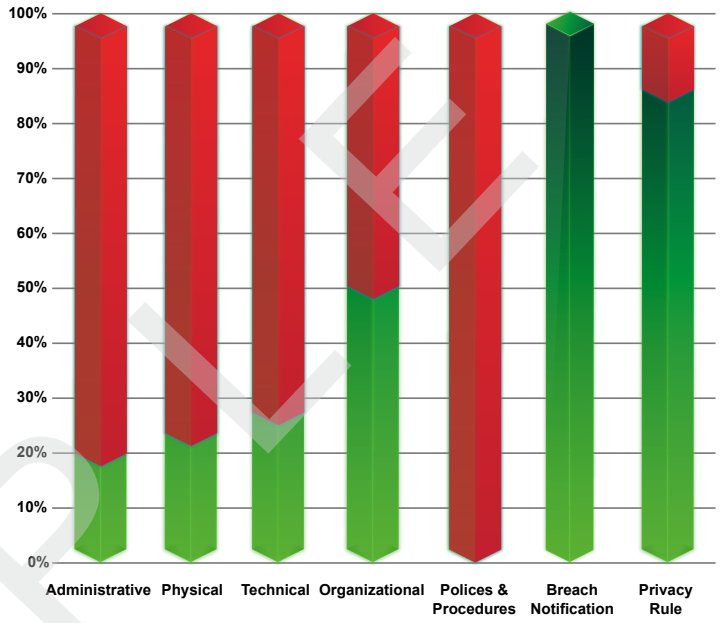
Every organization must conduct a thorough and comprehensive assessment of the potential risk and vulnerability to the confidentiality, integrity and availability of all PII.

Executive Dashboard

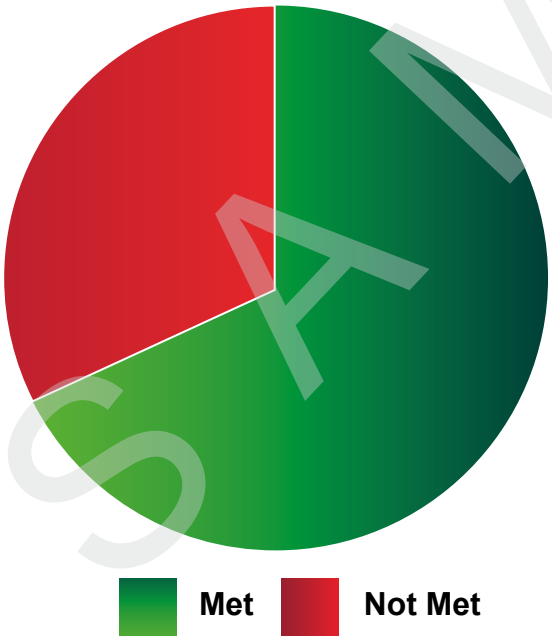
HIPAA Mandates

Grade	Security Rule
D	Administrative Safeguards
F	Physical Safeguards
A	Technical Safeguards
B	Organizational Requirements
F	Policies, Procedures, and Documentation
Privacy Rule	
B	Administrative Requirements
A-	Uses and Disclosures
Breach Notification	
C	Reporting

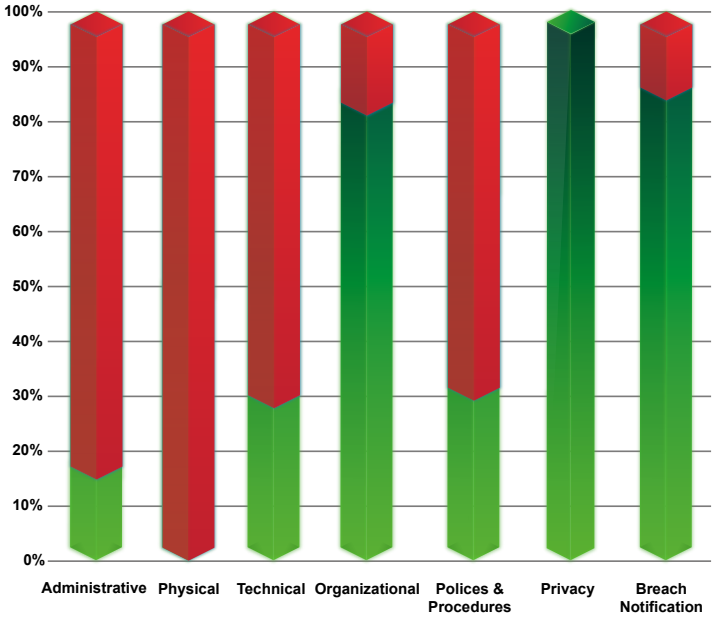
Standards



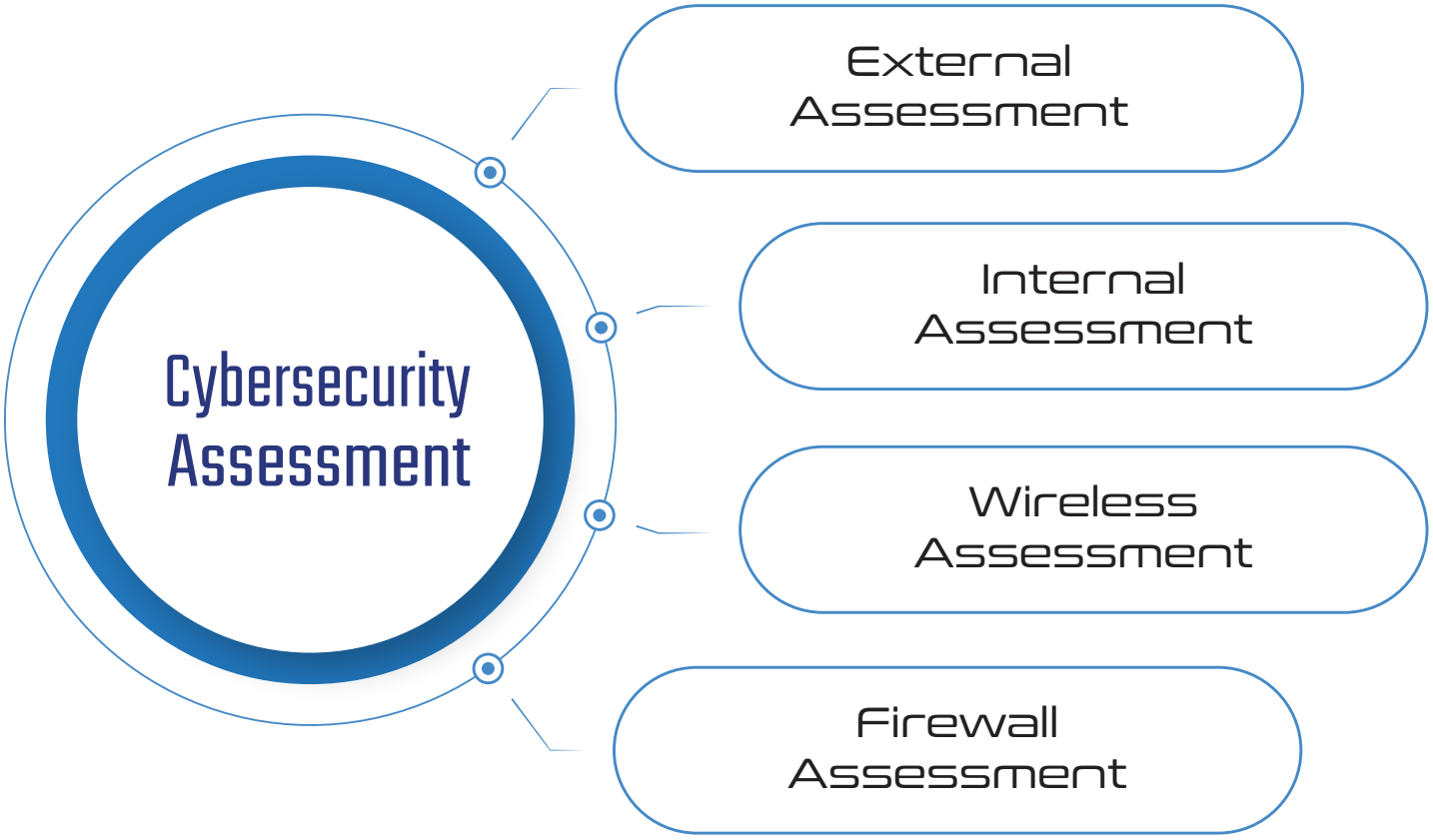
Compliance Status



Implementation Specifications



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)

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

Wireless Assessment

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

Firewall Assessment

- OS vulnerability analysis
- Security configuration & rule review

Cybersecurity Assessment

Every organization must conduct a thorough and comprehensive assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability (CIA) of all sensitive, confidential information.

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	✓	✓	✗	✗	✗

Executive Dashboard

Significant Findings

Risk Summary

- Security Grade: B
- Security Risk: Medium

Cyber Risk Status

External System Vulnerability Totals

High Risk	Medium Risk	Low Risk	Medium Risk of Successful Attack
1	27	8	

Web App Vulnerability Totals

High Risk	Medium Risk	Low Risk	Low Risk of Successful Attack
0	1	5	

Internal Vulnerability Totals

High Risk	Medium Risk	Low Risk	Medium Risk of Successful Attack
5	105	11	

Firewall Configuration Vulnerability Totals

High Risk	Medium Risk	Low Risk	Low Risk of Successful Attack
0	0	0	

Cybersecurity Assessment

Titanium

External Assessment

- Externally accessible IP addresses (up to 256) scanned for vulnerabilities; all identified vulnerabilities validated to the extent possible
- Up to four (4) external domains tested for:
  - Google Hacking Database entries
  - Domain Name Server misconfigurations
  - Metadata in publicly accessible documents
- Up to two (2) websites/applications crawled/scanned for vulnerabilities under one (1) user role
- Scope does not include Biomedical Device Cybersecurity Assessment or other specialized devices and equipment

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

Wireless Assessment

- Assessment of one (1) physical building to identify:
  - Potentially rogue Access Points/SSIDs
  - Open wireless access segmentation review, including testing of segmentation
  - Insecure authentication/encryption configurations including testing of Pre-Shared Key strength

Firewall Assessment

- Review of up to four (4) supported firewall configurations to identify Operating System-related vulnerabilities and best practice adherence
  - Includes review of firewall rules on a single (1) firewall to assist with business justification documentation and configuration according to the principle of least privilege

Internal Assessment

- Internal IP addresses (up to 4096) scanned for vulnerabilities; all identified vulnerabilities validated to the extent possible
- Up to 16 Class C network ranges scanned for:
  - Devices responding to “default” SNMP Community Strings
  - Systems running up to three (3) database server types (i.e. MSSQL, MySQL, Oracle, etc.) that allow open access
  - Identified systems also tested for “default” credentials
- Up to three (3) Active Directory domains tested for:
  - Identity and Access Management best practice adherence
  - Password Policy best practice adherence
  - User account password strength
  - USB device enumeration of systems registered in Active Directory
  - Identification of currently connected devices

Cybersecurity Assessment

Platinum

External Assessment

- Up to sixteen (16) externally accessible IP addresses scanned for vulnerabilities; all identified vulnerabilities validated to the extent possible
- Up to three (3) external domains tested for:
  - Google Hacking Database entries
  - Domain Name Server misconfigurations
  - Metadata in publicly accessible documents
- Up to two (2) websites/applications crawled/scanned for vulnerabilities under one (1) user role

Wireless Assessment

- *We will send you a handheld device (along with instructions) that someone in your organization will utilize to assist us in this portion of the assessment*
- Assessment of one (1) physical building to identify:
  - Potentially rogue Access Points/SSIDs
  - Open wireless access segmentation review, including testing of segmentation
  - Insecure authentication/encryption configurations including determination of Pre-Shared Key strength

Firewall Assessment

- Review of up to two (2) supported firewall configurations to identify Operating System-related vulnerabilities and best practice adherence

CYBERSECURITY ASSESSMENT SCOPE	PLATINUM
External Assessment	✓
Internal Assessment	✓
Firewall Assessment	✓
Wireless Assessment	✓
Detailed Analysis	✓
Corrective Action Plan (CAP)	✓
Detailed Remediation Steps	✓
Executive Brief	✓

Internal Assessment

- Up to sixteen (16) internal IP addresses scanned for vulnerabilities
  - All identified vulnerabilities validated to the extent possible
- Up to three (3) class C network ranges scanned for:
  - Devices responding to “default” SNMP Community Strings
  - Systems running up to three (3) database server types (i.e. MSSQL, MySQL, Oracle, etc.) that allow open access
  - Identified systems are also tested for “default” credentials
- Up to two (2) Active Directory domains tested for:
  - Identity and Access Management (IAM) best practice adherence
  - Password Policy best practice adherence
  - User account password strength
  - USB device enumeration of systems registered in Active Directory (AD)
  - Identification of currently connected devices

Cybersecurity Assessment

Gold

External Assessment

- Up to eight (8) externally accessible IP addresses scanned for vulnerabilities
- One (1) external domains tested for:
  - Google Hacking Database entries
  - Domain Name Server misconfigurations
  - Metadata in publicly accessible documents
- One (1) websites/applications anonymously crawled/scanned for vulnerabilities

Internal Assessment

- Up to eight (8) internal IP addresses scanned for vulnerabilities
- One (1) class C network ranges scanned for:
  - Devices responding to “default” SNMP Community Strings
  - Systems running one (1) database server type (i.e. MSSQL, MySQL, etc.) that allows open access
  - Systems also tested for “default” credentials
- One (1) Active Directory domains tested for:
  - Identity and Access Management best practice adherence
  - Password Policy best practice adherence
    User account password strength
  - USB device enumeration of systems registered in Active Directory

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

Firewall Assessment

Review of one (1) supported firewall configuration to identify Operating System-related vulnerabilities and best practice adherence

Cybersecurity Assessment

Silver

External Assessment

- Up to eight (8) externally accessible IP addresses scanned for vulnerabilities
- One (1) external domains tested for:
  - Google Hacking Database entries
  - Domain Name Server misconfigurations
  - Metadata in publicly accessible documents
- One (1) websites/applications anonymously crawled/scanned for vulnerabilities

Firewall Assessment

Review of one (1) supported firewall configuration to identify Operating System-related vulnerabilities

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

Cybersecurity Scanning

- External cybersecurity scans
  - Up to thirty-two (32) externally accessible IP addresses scanned quarterly for vulnerabilities

  Report contains:
  - Detailed cybersecurity findings
  - Corrective Action Plan
  - Detailed remediation information
- Internal cybersecurity scans
  - Up to thirty-two (32) internal IP addresses scanned quarterly for vulnerabilities

  Report contains:
  - Detailed cybersecurity findings
  - Corrective Action Plan
  - Detailed remediation information

Cybersecurity Assessment

Web Application Cybersecurity Assessment

- The scope of a Web Application Cybersecurity Assessment includes the following specific items:
  - One (1) Web Application
  - One (1) user role type to be utilized for testing
    - "Client" user account type
    - Anonymous access will also be tested

General Goal(s)

- Identify vulnerabilities related to the OWASP Top 10
- Identify deviations from best practice

Web Application Cybersecurity Assessment Methodology

Mapping

- Analyzing HTTPS support
- Analyze software configuration
- Crawl the site/application
- Application flow charting
- Relationship analysis
- Session analysis

Discovery

- Automated Vulnerability Scanning
- Information Leakage & Directory Browsing Discovery
- Username Harvesting & Password Guessing
- Command Injection Discovery
- Directory Traversal & File Inclusion Discovery
- SQL Injection Discovery
- Cross-site Scripting (XSS) Discovery
- Cross-site Request Forgery (CSRF) Discovery
- Session Flaw Discovery
- Insecure Redirects & Forwards Discovery

CloudFirst Cybersecurity Assessment

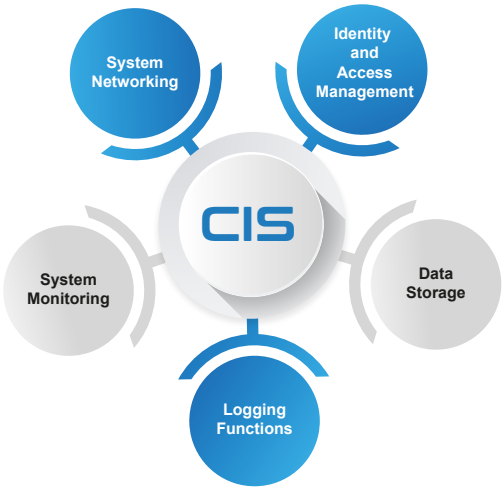
CloudFirst Cybersecurity Assessment

ecfirst CloudFirst Cybersecurity Assessment Phases

Data gathered is analyzed against policies, standard best practices, and vendor security bulletins to determine potential risks and exposures to the computing environment. The results of these cybersecurity scans/tests are to be used as the basis for determining the security posture and risk to organizational systems.

CIS Microsoft Azure Foundations Security Benchmark Assessment

With a CIS Microsoft Azure Foundations Security Benchmark Assessment, ecfirst provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. The scope is to establish the foundation level of security for anyone adopting Microsoft Azure Cloud. This benchmark is not a complete list of all possible security configurations and architecture.



CIS Cloud Management Foundations Benchmark Testing

- CIS is an internationally respected community of cybersecurity experts who provide best practice analysis and guidance for each security setting available for configuration in operational and application software across over 25 vendor product families.
- Thousands of layered, defined, and inherited security configurations are set across an organization's applications, operating systems, networks, and management systems. Where is over-protection breaking required functionality and where is under-protection exposing the organization to untenable risk? Worse, what combination of settings is doing both?
- ecfirst has created benchmark testing tools and scans based on a best practice balance between low risk and high functionality.
- All ecfirst Foundations tests ensure evaluation against Level 1 CIS recommendations. The configuration review determines the overall threat of potential compromise so that the business can make adjustments based on its organizational needs and risk tolerance.
- ecfirst maintains all the tools and knowledge needed to perform testing and reporting against the latest best practice recommendations defined in the benchmark. ecfirst benchmark testing reports provide all the information required to enable risk-informed and efficient business decision-making and strengthen the organization's resistance to cyber attacks.

CIS System Configuration Benchmark Assessment

CIS Benchmarks are best practices for the secure configuration of a target system. CIS Benchmarks are consensus-based, best practice security configuration guides developed and accepted by the government, business, industry, and academia. The ecfirst CIS System Configuration Benchmark Assessment scans the system to identify if the configuration is aligned with defined requirements.

CloudFirst Cybersecurity Assessment

CloudFirst Scope

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

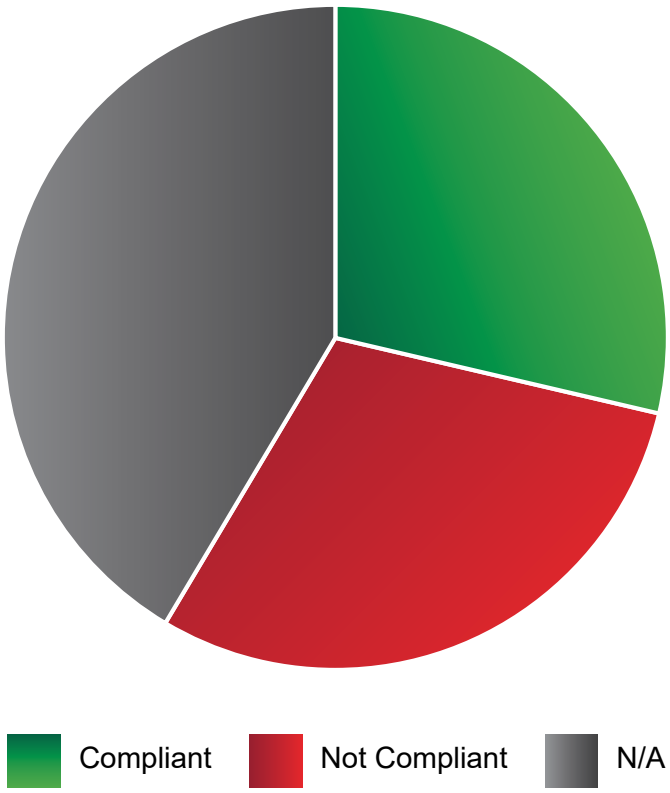
External Assessment
- Up to 32 IP addresses

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

CloudFirst Risk Status

Significant Findings

Compliance Status Example



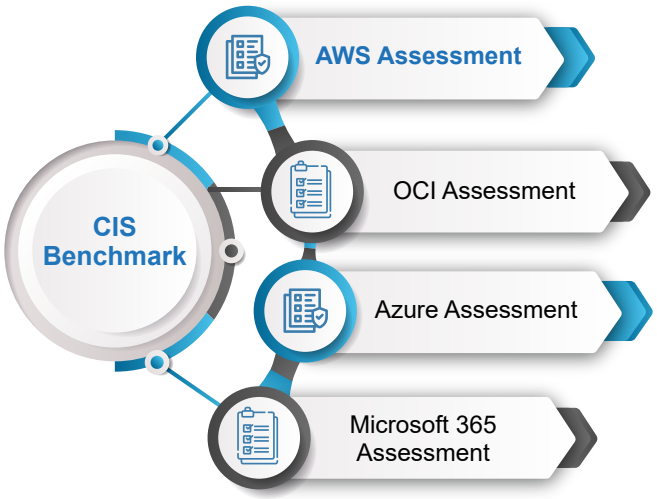
Compliant | Not Compliant | N/A

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

CIS Benchmark Assessment

AWS Assessment

Advancing Cloud Security with CIS on AWS



The AWS Shared Responsibility Model makes it easy to understand the role cloud consumers play in protecting their unique AWS environments. CIS security best practices can help organizations achieve cloud security from the customer's side of the responsibility model.

Best practice configuration guides include the CIS AWS Foundations Benchmark, CIS Amazon Linux 2 Benchmark, and service-based guidance like the CIS Amazon Elastic Kubernetes Service (EKS) Benchmark. Guides contain prescriptive guidance to secure configurations for a subset of AWS services and account-level settings.

The ecfirst AWS Report includes,

- Alignment with CIS Benchmark for AWS Foundations, Level 1 settings
- Correctly configured settings where further action is required to achieve full security benefits
- Review of available versus used licenses and their impact
- Analysis of findings, including strengths and prioritized areas for improvement

Configuration benchmark alignment areas include,

- Identity and access management
- Storage
- Logging
- Monitoring
- Networking

Readiness Assessment

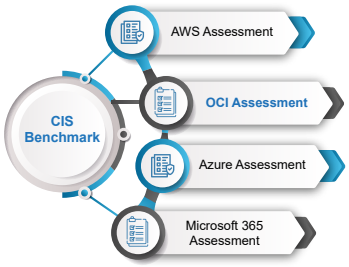
The AWS Cloud Readiness Assessment is **your first step in organizational readiness for leveraging the cloud effectively.** The assessment provides analysis and planning to identify, measure, and create business value using technology services and document current business objectives for cloud enablement.
The Phases for this assessment are:

- **Initiation:** Capture the business context, including the general and specific drivers for the assessment.
- **Preliminary Analysis:** Establishes the architecture frameworks to be used and data-points to be collected. In this phase, we also identify sources of information, and named points-of-contact.
- **Discovery:** Construction of a catalogue of applications, data, technologies, processes and organization structure, which is populated with multiple data points against each element.
- **Analysis:** Interpretation and presentation of the assessment findings, typically expressed in terms of the fitness of each component and its sustainability and contribution to the overall risk profile.

CIS Benchmark Assessment

OCI Assessment

CIS Foundations Benchmark for Oracle Cloud



The recommendations in the CIS Foundations Benchmark for Oracle Cloud include:

- Encouraging the use of multi-factor authentication (MFA) for all console users
- Restricting remote administration ports outside of the enterprise network
- Configuring logging and notifications to aid in identifying anomalous behavior and investigate potential compromise

The CIS Oracle Cloud Infrastructure Foundations Benchmark provides prescriptive guidance to securely configure an Oracle Cloud account. The step-by-step checklist includes detailed recommendations for Identity and Access Management, Networking, and Logging and Monitoring. It's available as a free download to public and private organizations worldwide.

The CIS Oracle Cloud Infrastructure (OCI) Foundations Benchmark provides prescriptive guidance for establishing a secure baseline configuration for the OCI environment. The scope of this benchmark is to establish a base level of security for anyone utilizing the included OCI services.

While all organizations require a prudent level of cybersecurity these days, it is recommended for organizations who use OCI meet the CIS Benchmark for OCI Foundations at Level 1.

- Review of compliance with each "Level 1" item contained in the Benchmark
- Report detailing each item contained in the assessment along with your Compliant/Non-Compliant status

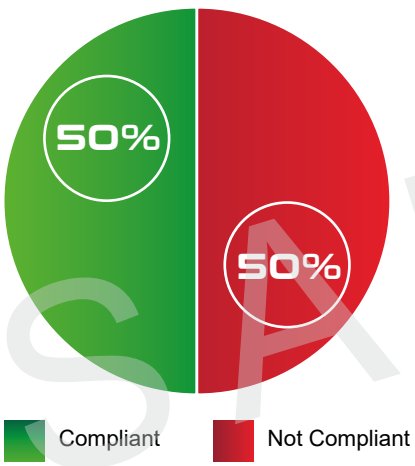
The ecfirst OCI Report includes,

- Alignment with CIS Benchmark for OCI Foundations, Level 1 settings
- Correctly configured settings where further action is required to achieve full security benefits
- Review of available versus used licenses and their impact
- Analysis of findings, including strengths and prioritized areas for improvement

Configuration benchmark alignment areas include,

- Identity and access management
- Network configurations
- Log management
- Object storage
- Asset management

Executive Dashboard

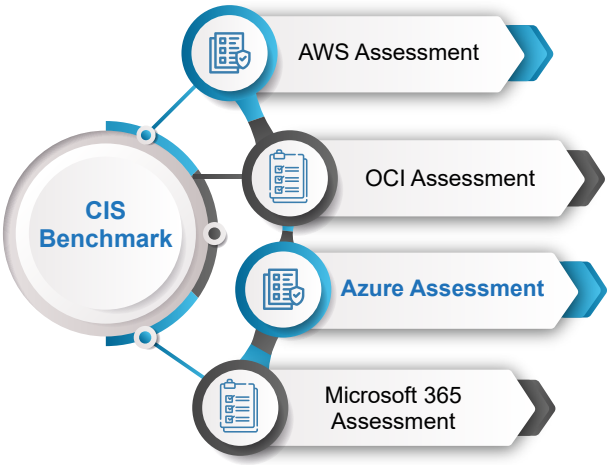


Area	Total # of CAP Items	Not-Compliant CAP Items	Compliant
IAM	12	3	9
Networking	5	2	3
LogMon	17	12	5
Object Storage	2	1	1
Asset Management	2	1	1
Total	**38**	**19**	**19**

CIS Benchmark Assessment

Azure Assessment

CIS Microsoft Azure Foundations Benchmark



The CIS Foundations Benchmark provides prescriptive guidance for various areas including: Identity and Access Management (IAM), database services, logging and monitoring, networking, virtual machines, and Azure's Security Center and Storage Accounts. Key changes to this new release include:

- Reference links in multiple recommendations to the CIS Azure Security Benchmark v2
- Multiple recommendations for the change of Advanced Data Security to Azure Defender New recommendations for additional Azure Defender bundles
- Multiple activity log alert console remediation steps
- Removal of multiple recommendations for features that have been deprecated

Azure Virtual VM Assessment

The ecfirst Azure VM Assessment describes:

- **Azure Readiness:** Whether servers are suitable for migration to Azure
- **Monthly Cost Estimation:** The estimated monthly compute and storage costs for running the VMs in Azure
- **Monthly Storage Cost Estimation:** Estimated costs for disk storage after migration

The ecfirst Azure Report includes,

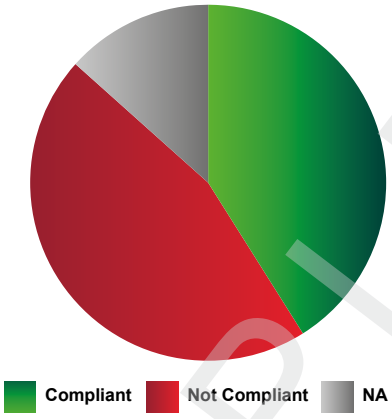
- Alignment with CIS Benchmark for Azure Foundations, Level 1 settings
- Correctly configured settings where further action is required to achieve full security benefits
- Review of available versus used licenses and their impact
- Analysis of findings, including strengths and prioritized areas for improvement

Configuration benchmark alignment areas include,

- Identity and access management
- Data storage
- Logging functions
- System monitoring
- System networking

Executive Dashboard

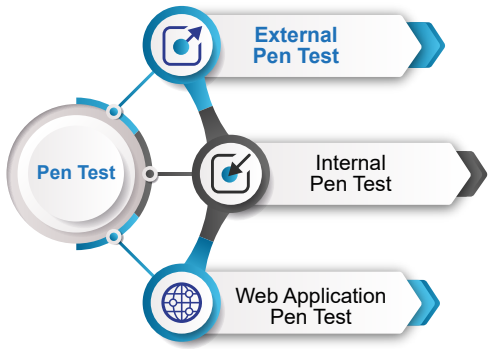
Compliance Progress



Area	Compliant	Non-Compliant	N/A
IAM	1	1	0
SecCenter	11	8	0
StorageAccounts	2	1	0
Database	2	9	8
Log Monitor	9	7	0
Networking	3	2	0
VM	1	2	0
Other	1	2	1
AppService	2	3	0

Pen Test

External Penetration Test



- The External Penetration Test is “pre-scoped” to the following general criteria:
  - A “grey box” test provides the following:
    - IP address ranges owned/operated
    - All domains owned/associated with up to sixteen (16) external systems
  - Testing takes place across 5 business days, primarily during business hours

Primary Goal

- Primary goal is to gain unauthorized elevated access to an externally accessible system
  - A secondary goal is to gain unauthorized access to other systems utilizing the primary goal system

- The External Penetration Test methodology is organized into three (3) distinct phases:

Reconnaissance

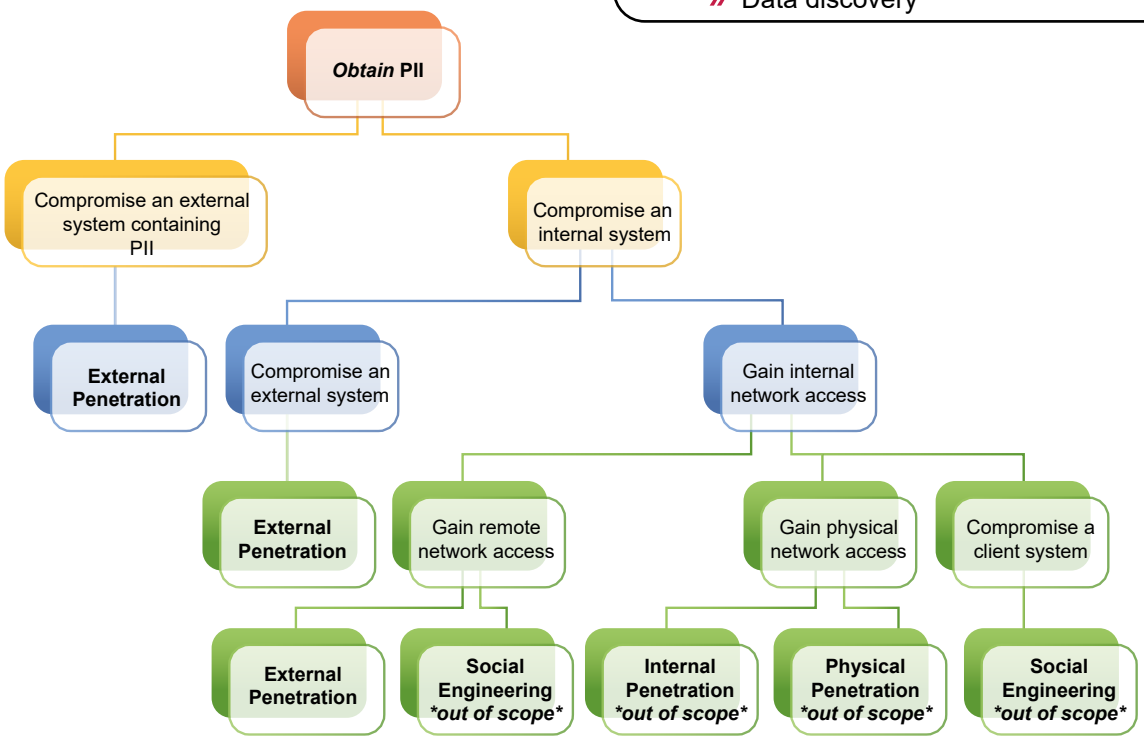
- Client personnel and cultural information
- Client business terminology
- Technical infrastructure information

Scanning

- Network discovery
- Network port and service identification
- Cybersecurity identification
- Enumeration

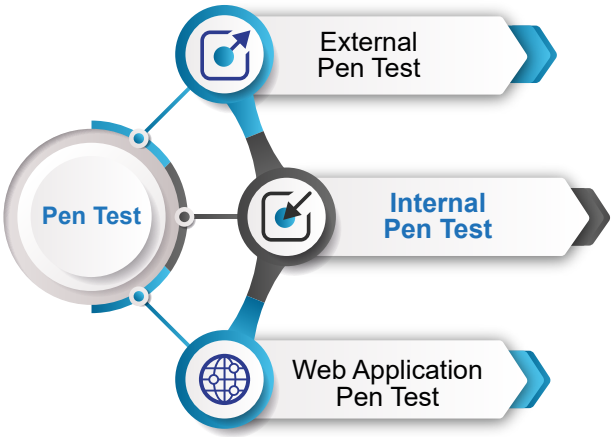
Exploitation

- Password cracking
- Discovered credential usage
- Manual and automated cybersecurity validation
- Phishing attempts
  - For credential gathering
  - For exploitation delivery
- Privilege escalation
- Additional tool installation
- Data discovery



Pen Test

Internal Penetration Test



- The Internal Penetration Test is “pre-scoped” to the following general criteria:
  - A “grey box” test provides the following:
    - Domain User account configured as a “regular” employee
    - Remote access to the internal network via a virtual machine or physical device provided by ecfirst
  - Not all vulnerabilities identified will be validated and/or exploited
    - Only those deemed most likely to assist in reaching the defined Goal will be further validated and exploited

Primary Goal

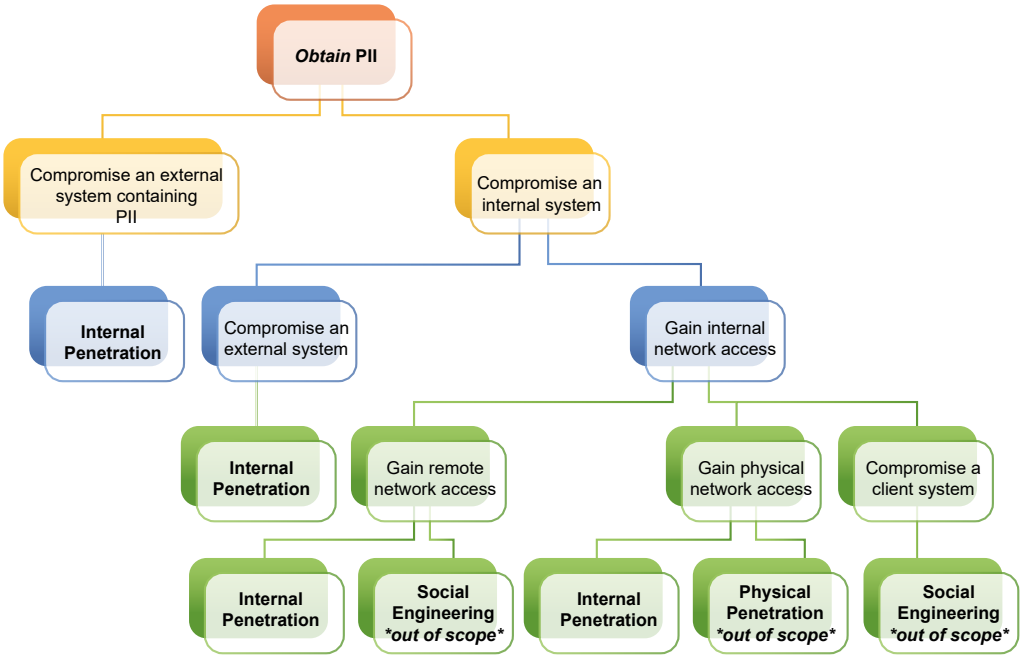
- Primary goal is to gain Domain Administrator level access on the internal network.
  - Secondary goal is to gain unauthorized access to sensitive data

Scanning

- Network discovery
- Network port and service identification
- Cybersecurity identification
- Enumeration

Exploitation

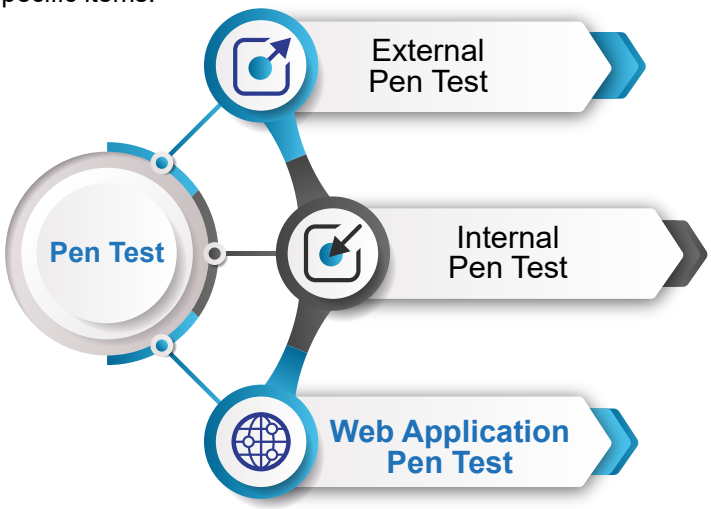
- Password cracking
- Discovered credential usage
- Manual and automated cybersecurity validation
- Privilege escalation
- Additional tool installation
- Data discovery



Pen Test

Web Application Penetration Test

- A Web Application Penetration Test includes the following specific items:
  - One (1) Web Application
  - One (1) user role type to be utilized for testing:
    - "Client" user account type
    - Anonymous access will also be tested



General Goal(s)

- Gain anonymous access to authenticated sections of the application
- Gain access to other client data within the application

The Web Application Penetration Test methodology is organized into four (4) distinct phases,

Reconnaissance

- Technical infrastructure information

Discovery

- Automated cybersecurity scanning
- Information leakage and directory browsing discovery
- Username harvesting and password guessing
- Command injection discovery
- Directory traversal and file inclusion discovery
- SQL injection discovery
- Cross-site scripting discovery
- Cross-site Request Forgery discovery
- Session flaw discovery
- Insecure redirects and forwards discovery

Mapping

- Network discovery
- Network port and service identification
- Analyzing HTTPS support
- Identify virtual hosting and load balancers
- Analyze software configuration
- Spider the site/application
- Application flow charting
- Relationship analysis
- Session analysis

Exploitation

- Exploit identified enumeration flaws
- Exploit identified bypass flaws
- Exploit identified injection flaws
- Exploit identified session flaws
- Chain exploits together, pivot to other systems, data exfiltration, raid, etc.

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

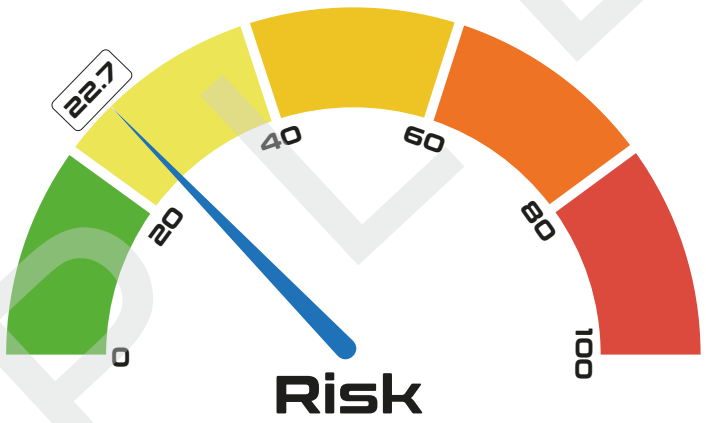
Phish-prone % **23.9%**

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

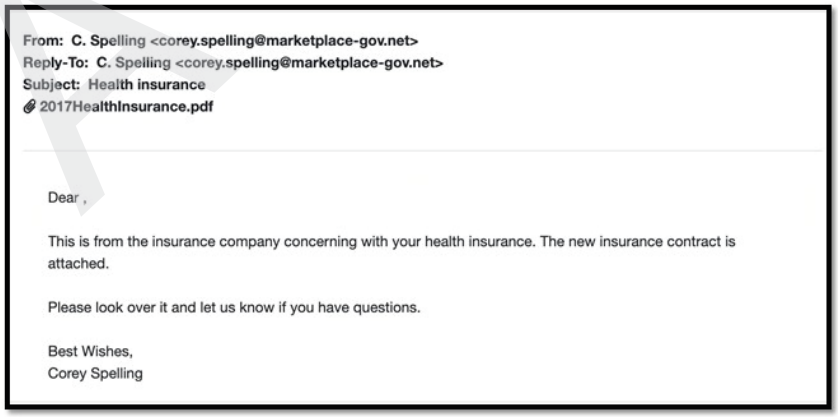
Based on the number of users that fell victim to the phishing performed, ecfirst estimates the risk of a successful Social Engineering attack against to be a Medium risk.



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

Performed an Online Tracking Assessment?

OCR Mandate for HIPAA Compliance

Objectives

- Identify 3rd-party resources across websites.
- Evaluate 3rd-party resources using fingerprinting or tracking technology.
- Establish actionable recommendations.
- Ensure HIPAA compliance with OCR guidance for online tracking.

Online Tracking HIPAA Compliance

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.

OCR Guidance

Project Scope

Crawl the in-scope websites to identify calls to 3rd-party resources.

Review 3rd-party resources to identify those implementing tracking or fingerprinting technologies.

Provide report on websites employing tracking or fingerprinting technologies, including identifying the specific 3rd-party resources on each crawled page potentially providing those features.

Certification Training

CHP Certified HIPAA Professional HIPAA Academy | CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST | HIPAA Academy | CCSA Certified Cyber Security Architect | aiCRP AI Cyber Risk Professional

Peter Harvey Peter.Harvey@ecfirst.com www.ecfirst.com

AI Defense, *Beyond Cyber*