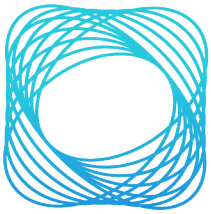
WHITEPAPER



SOTER TECH
SOLUTIONS

CIS CONTROLS

FOUNDATIONAL CYBERSECURITY RISK ASSESSMENT

Focus resources and efforts toward controls that mitigate actualized risk

BY: CHRISTIAN MEDEROS, SECURITY SOLUTIONS ARCHITECT

Information Security is a broad subject that is an imperative element of modern businesses. Many organizations implement expensive information security controls intended to mitigate risk that create no demonstrable mitigation of actual risk. This assessment intends to bridge this divide and provide objective benchmarking against a recognized cybersecurity framework and prioritized remediation guidance informed by actualized threat actor behavioral patterns and techniques.

TABLE OF CONTENTS

ABOUT US

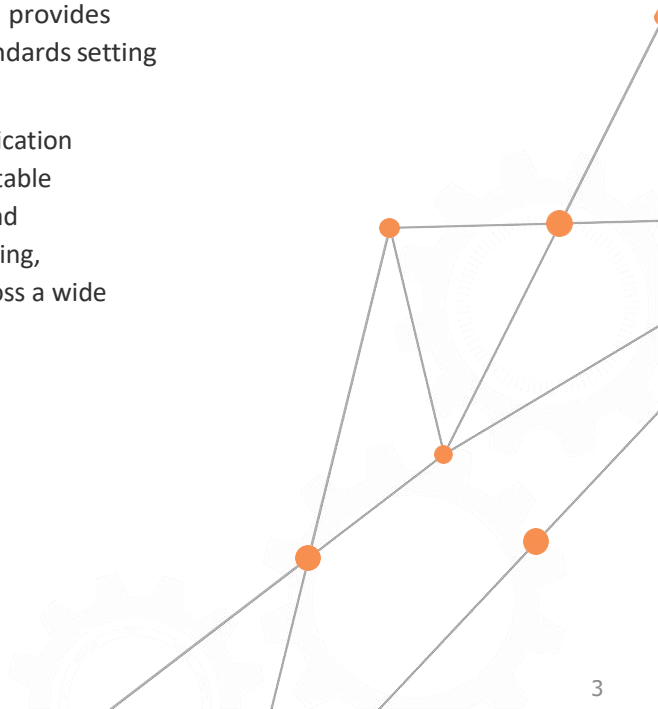
Soter Tech Solutions is a full-service technology management and cybersecurity risk advisory firm headquartered in Miami, FL.

Our 100% U.S. Based Information Security team consists of professional penetration testers, technologists, certified assessors, and risk managers that use a team-based approach to deliver a comprehensive suite of services to address the multi-disciplinary requirements of modern business cybersecurity. Our team-based approach is unique, addressing the practical, technical, regulatory, and operational elements collectively through a unified framework approach that leverages the existing internal capabilities and expertise within our clients' organizations.

Soter Tech Solutions has extensive experience in defense, energy, critical manufacturing, fintech, banking, and sensitive logistics industries. Certified and accredited by leading industry organizations including the Cybersecurity Assessor and Instructor Certification Organization **(CAICO), Cyber-AB**, The Center for Internet Security **(CIS)**, and **CREST,** Soter Tech Solutions's cybersecurity team brings both assessment experience and deep operational experience. This combination provides both robust assessment capabilities and deep experience operationalizing cybersecurity programs.

We actively contribute to the cybersecurity community as a whole and have helped develop and promote influential frameworks and security initiatives. These include Center for Internet Security Controls **(CIS Controls)**, **MITRE D3FEND** and **ENGAGE** (adversarial engagement and deception frameworks), and the Cybersecurity Maturity Model Certification **(CMMC)** through a cooperative engagement between MITRE and the U.S. Department of Defense. Our security staff maintain active and relevant information technology and information security certifications that include specialties in ethical hacking, IT governance, network security, cloud security, and Linux & Windows systems administration. Soter Tech Solutions is a member of both the Cybersecurity and Infrastructure Security Agency Joint Cyber Defense Collaborative **(CISA JCDC)** and CISA Advanced Information Sharing Consortium **(CISA AIS)**, which provides access to up-to-the-second threat intelligence and influence on the standards setting process for the cybersecurity industry.

Soter Tech Solutions was the first organization, globally, to achieve certification and accreditation by CREST as a **CIS Accredited assessment firm**. This notable achievement was the culmination of our rigorous internal process, a broad referenceable body of work, and over a decade of experience implementing, operationalizing, and evaluating organizations using the CIS Controls across a wide spectrum of industries.

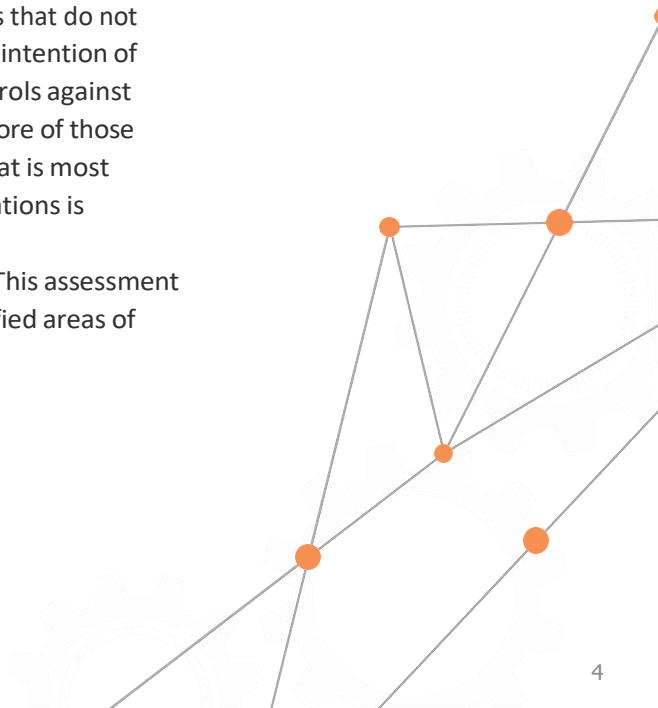


ASSESSMENT METHODOLOGY

Most often organizations focus their time, resources, and efforts in assessing cybersecurity controls solely against a static checklist. Commonly this approach does not yield substantial gains in their Information Security posture. The intention of this assessment is to ascertain the degree of effective implementation of framework-derived security controls against several of the most exploited attack vectors and provide an objective maturity score of the organization using those controls. Our approach to performing security assessments within commercial organizations is based centrally upon the use open standardized assessment methodologies that are recognized by third party certifying agencies while simultaneously ensuring objective repeatability of the assessment scope. This methodology incorporates the best practices and prescribed methodologies of the United States Cyber Emergency Response Taskforce (US-CERT) and National Institute of Standards and Technology (NIST), combined with the quantifiable security controls of the CIS Critical Security Controls.

Soter Tech Solutions will perform this assessment under the guidelines of the Center for Internet Security (CIS) Risk Assessment Model (RAM) and Penetration Testers Execution Standard (PTES) to maximize the value and repeatability of the assessment and its findings. This assessment will use the CIS Controls Framework as its reference standard with references to the MITRE ATT&CK Framework and related publications where applicable. SOTER TECH SOLUTIONS will utilize current adversarial behavioral data
to inform the selection of modeled attack vectors. This data is derived from MITRE's ATT&CK adversarial profile information. Based on the scope of the assessment, SOTER TECH SOLUTIONS will evaluate high-probability attack vectors which are representative of those most commonly exploited by malicious attackers operating in similar business areas as that of the Client. The overall security posture of in-scope systems will be characterized in relation to the CIS Controls using a commercially and risk-appropriate alignment to an appropriate Implementation Group (IG).

Most often, organizations focus their time, resources, and efforts in areas that do not yield substantial gains in their overall Information Security posture. The intention of this assessment is to ascertain if Client has implemented effective controls against commonly exploited attack vectors and provide an objective Maturity score of those controls. SOTER TECH SOLUTIONS will report its findings in a format that is most actionable for commercial clients. Risk prioritization of all recommendations is performed in
accordance with the Common Vulnerability Scoring System (CVSS) 3.0. This assessment will include a risk-prioritized set of recommendations to mitigate identified areas of exposure.



CRITICAL SECURITY CONTROLS

To better align business, technology, security, and risk stakeholders, Soter Tech Solutions has adopted the Center for Internet Security's (CIS) Critical Security Controls ("CSC") Framework as a universal reference standard within its assessment and information security consulting practices. This framework, derived from National Institute of Standards and Technology (NIST) controls, aligns well with many common security standards including

formally regulated industries that are required to comply with external regulatory oversight. This included those standards enforced by FINRA, SEC, and FFIEC Information Security guidelines within the financial services industry, HIPAA within the healthcare industry, and PCI-DSS requirements within the payments and retail industries. Using the CIS Security Controls Framework permits audit-friendly cross-reference and compliance with multiple dimensions of compliance within a single organization across many stakeholders.

The CIS Controls reflect the combined knowledge of experts from every part of the information security ecosystem; representing every role, from incident responders to policy-makers; and across many business and government sectors who have banded together to create, adopt, and support the CIS Controls. The Controls are foremost an offense-informs-defense cyber-risk mitigation framework. Individual Controls are selected, dropped, and prioritized based on data, and on specific knowledge of attacker behavior and how to stop it.

The Controls are organized using Implementation Groups (IGs) to enable a wide variety of organizations to maximize the benefit gained through their use. IGs are self-assessed categories for enterprises. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be applicable for an enterprise with a similar risk profile and resources to strive to implement. These IGs represent a horizontal look across the CIS Controls tailored to diverse types of enterprises. Within each Control are numerous individual specific actions to take, organized by IG. These actions represent the Safeguards enterprises should take to implement the respective Control.

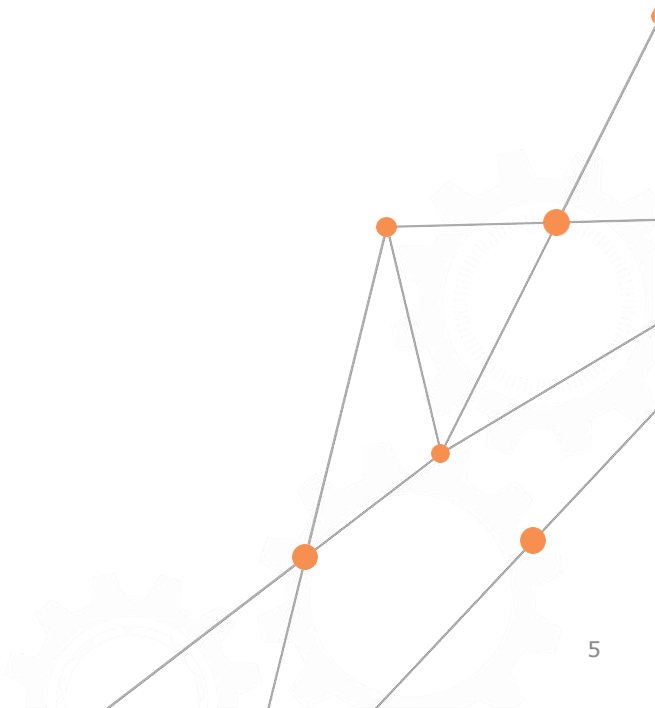
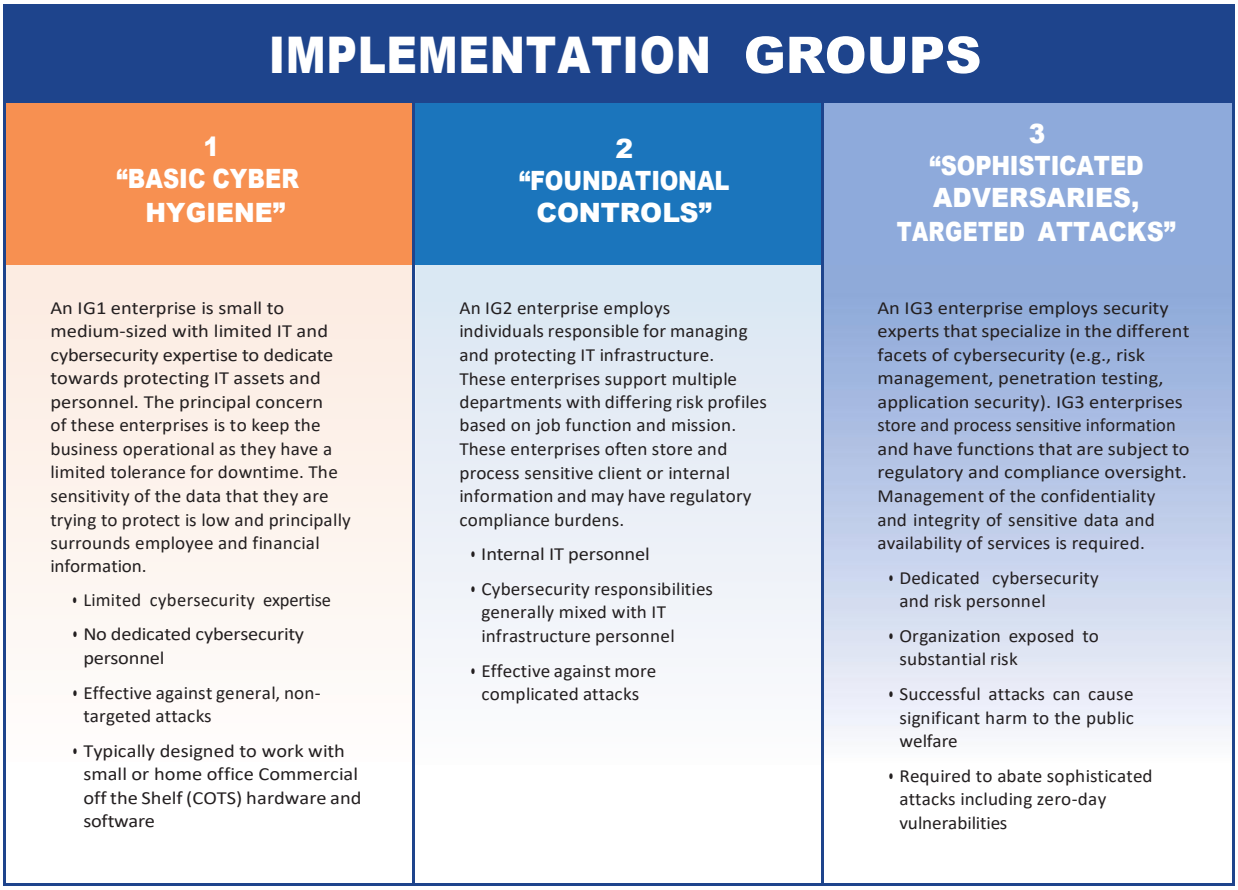


FIGURE 1: CIS CRITICAL SECURITY CONTROLS ("CSC"), V8

FIGURE 2: CIS CRITICAL SECURITY CONTROLS ("CSC"), VERSION 8 IMPLEMENTATION GROUPS



SOTER TECH SOLUTIONS leverages standardized and repeatable assessment methodologies which allow Client to evaluate its security posture to that of its peers; similar organizations that are of a comparable size and operating in similar industries. SOTER TECH SOLUTIONS will perform this analysis and provide both an overall and focused (per-control area) report to Client; Figures 3 and 4 below, respectively.

FIGURE 3: COMPARATIVE PEER ANALYSIS

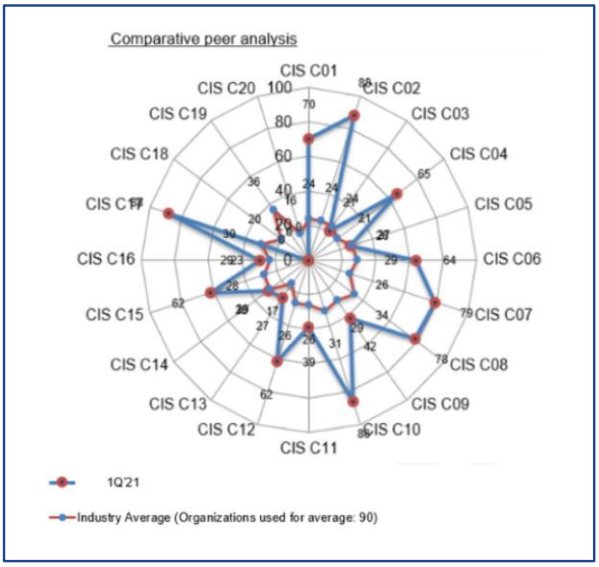
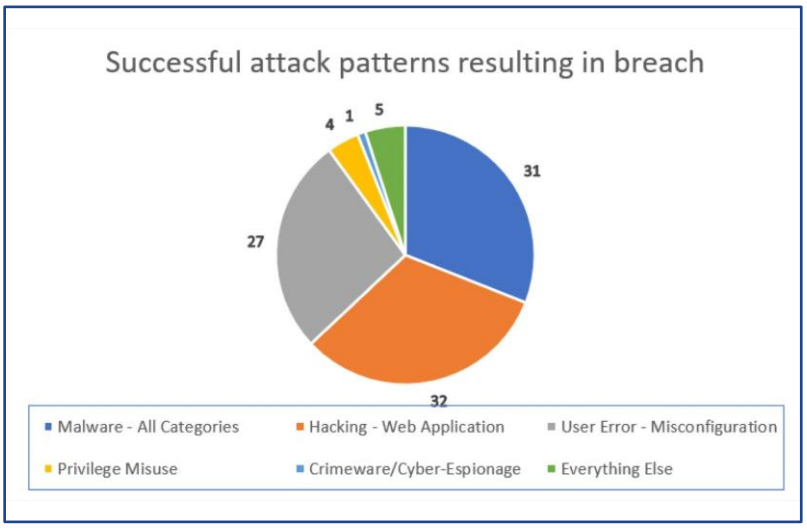
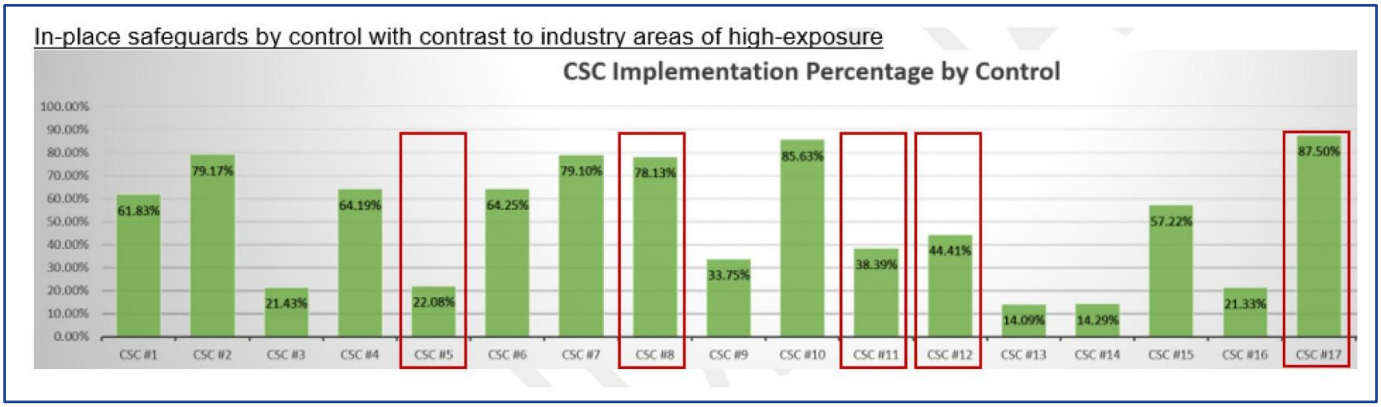


FIGURE 4: INDUSTRY ATTACK PATTERN ANALYSIS



Additionally, using this same data, SOTER TECH SOLUTIONS will evaluate the broader areas of attacks against Client's industry segment and provide recent attack patterns that have resulted in successful compromise. Pulling from the largest published database of this type of information, Client will be provided analysis which contrasts their current security controls to those which were successfully attacked in similar organizations, Figure 5, below.

FIGURE 5: EXPOSURE ANALYSIS WITH CONTRAST TO INDUSTRY ATTACK PATTERNS



The overall assessment provides Client a comprehensive assessment of its overall organizational security posture for the in-scope systems that incorporates exposure analysis of Client's industry and similar peer organizations. Remediation of identified areas of shortcomings are prioritized based upon the severity and exposure each shortcoming poses to the organization.

SOTER TECH
SOLUTIONS

GET IN TOUCH

(305) 786-7490
sales@sotertechsolutions.us

Remote
Miami, FL 33176

www.sotertechsolutions.us