WHITEPAPER

SOTER TECH SOLUTIONS

# THE CIS CONTROLS

## A Standardized Framework Alongside a Trusted Partner

BY: BRIAN VILLAMAR, CYBERSECURITY & COMPLIANCE PROFESSIONAL

*The CIS controls are an actionable security framework that allows SMBs to protect their most valuable assets. Soter Tech Solutions is a trusted and verified partner that can ensure proper implementation and maintenance of the controls through our various managed services.*

# TABLE OF CONTENTS

# CYBER ATTACKS – AN EXISTENTIAL THREAT TO SMBS

Everyday modern enterprises are faced with advanced cyber threats that, if handled incorrectly, will impact the future of the business dramatically. Failing to secure operational assets may lead to extensive financial repercussions, reputational damage, or in some cases, legal action. These consequences aren't limited only to the victim organization exclusively.

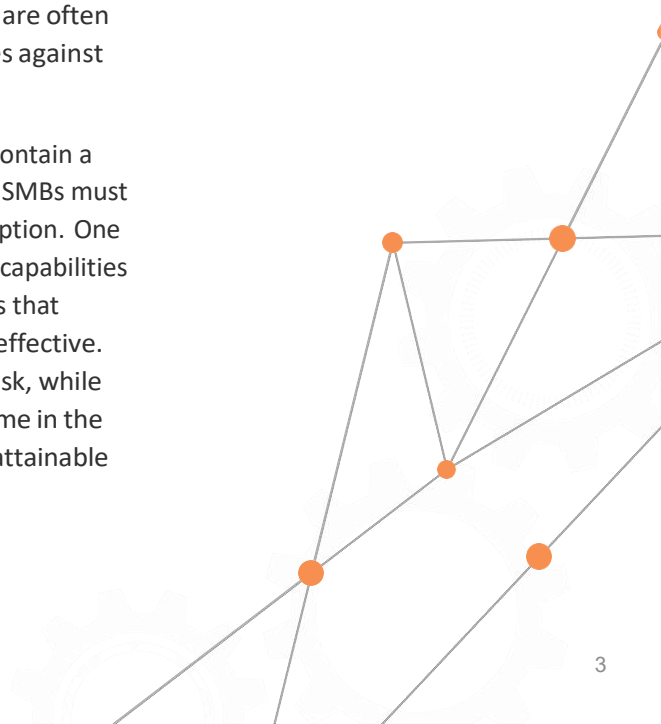
Many businesses find themselves in the headlines as the result of a third-party contractor or service provider within their trusted ecosystem falling victim to a cyberattack. These businesses are often entrusted with a litany of sensitive data that must be protected. Personal identifiable information (PII) often includes names, addresses, contact information, medical records and history, or financial information. The type of information created, stored, and transmitted varies across industries, but the responsibility to protect that data is universal and almost exclusively rests with the organization in possession of this data.

Additionally, many individuals find themselves directly impacted when critical infrastructure is targeted, and its services brought to a halt. In recent years some of these attacks have shutdown gas pipelines, electric grids are made to fail, and connectivity to critical Internet-delivered services is severed. The effects of a successful cyberattack is felt by every member of a business ecosystem, and the consequences are often dire.

**Approximately 43% of cyber-attacks are aimed at SMBs with only 18% of small-businesses having the infrastructure to defend themselves.**

This is especially true in small-to-medium sized businesses (SMBs). These organizations are faced with the same cyber threats as large enterprises but with fewer resources. In an ever-evolving landscape like cybersecurity, finding common classification is key. When determining what constitutes a small-medium sized business, The U.S. Office of Management and Budget defines a small business as any organization employing less than 499 individuals. These businesses are often too understaffed and under resourced to accurately defend themselves against advanced threat actors. Bad actors know this fact too.

Cyber criminals view SMBs as easy and lucrative targets, that may even contain a foothold into other, often larger businesses in the national **supply chain.** SMBs must take cybersecurity seriously and view it as a necessity rather than an option. One of the most effective methods for SMBs to bolster their cybersecurity capabilities is through the implementation of standardized cybersecurity frameworks that allow them to focus their resources on processes that are proven to be effective. Ideally, these frameworks should address industry specific needs and risk, while also aligning with regulatory requirements. These frameworks often come in the form of cybersecurity playbooks that outline specific practices that are attainable



and provide tangible results. SMBs can't afford to get this wrong - neither in terms of the expenditure of resources nor mitigating the often extinctual risk to the organization. It is because of these needs that finding and engaging a partner to help get it right the first time is so important.

Soter Tech Solutions, utilizing the CIS Critical Security Controls, helps SMBs implement a comprehensive security plan that addresses industry needs and secures business assets.

## WHO IS SOTER TECH SOLUTIONS?

**Soter Tech Solutions** is a managed service and security provider that provides IT and security services to small-medium sized businesses. We equip SMBs with a disproportionate advantage over their competitors, empowering the strategic use of technology while mitigating cybersecurity risks using the CIS Controls. Soter Tech Solutions offers various services including firewall management, vulnerability management, comprehensive security assessments, and compliance aid. Every security path starts with a security assessment. Soter Tech Solutions will assess your business for any vulnerabilities or gaps that may be exploited by internal and external threats. From here, Soter Tech Solutions provides a comprehensive plan for SMBs to remediate and patch any gaps in their security. Lastly, cybersecurity isn't a one-time process. Our managed services help ensure that your business is always at the forefront of security.

Soter Tech Solutions has adopted and actively implemented the CIS controls since their inception. We believe that the controls provide the resources to serve as a North star for businesses seeking to bolster their security posture. In November of 2023, **Soter Tech Solutions was officially named the first organization to become an accredited CIS controls assessor.** This speaks to our expertise in implementing the controls for not only ourselves, but our clients as well. Phyllis Lee, CIS Vice President of Security Best Practices Content Development stated:

> ***"CIS has had a longstanding relationship with Soter Tech Solutions, so it's quite fitting that they are our first CIS Controls accredited member."***
>
> PHYLLIS LEE, CIS VICE PRESIDENT OF SECURITY BEST PRACTICES CONTENT DEVELOPMENT

Our security assessments are comprehensive and use the controls as the foundation for everything we do. Soter Tech Solutions is the premier partner for comprehensive and effective IT security services.

# INTRODUCING **THE CIS CRITICAL SECURITY CONTROLS**

**The Center for Internet Security (CIS)** is a global group of security experts, and leaders within the community that work toward the common goal of securing the solutions, businesses, governments, and people that are connected across the globe. This community-driven nonprofit is responsible for the CIS Controls and CIS Benchmarks, a globally recognized set of best practices for securing IT infrastructure and data. The CIS Controls are a dynamic and evolving set of practices that have undergone several changes over the years.

Originally stemming from a project of Carnegie Mellon University's Software Engineering Institute and later SANS institute, the "Cyber Top 10" became the "20 Critical Security Controls". Once CIS took over development of the project in 2008, the CIS controls were born. Since then, the original 20 controls have been condensed to 18 and the framework is now in its 8th version. This paper will focus on the most recent version of the CIS Controls (version 8). Readers will come away with a foundational understanding of the CIS controls and how Soter Tech Solutions implements them into their security process. This paper does not describe every control in detail, but for readers who would like to dive deeper into the controls, the CIS Critical Security Controls v8 is linked below.

### THE CIS CRITICAL SECURITY CONTROLS VERSION 8

# WHAT ARE THE **CIS CONTROLS?**

The CIS Controls are a set of 18 security practices that address the most common and dangerous threats to organizations today. They are described by the CIS as "a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements".

The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. The Controls focus on a smaller number of actions with high pay-off results, which makes them especially beneficial to SMBs.

A major component of the controls is the community behind it. Groups of experts within the cybersecurity field have come together to discuss and create a prioritized list of what most impacts organizations and governments today and designs the controls with those threats in mind.

## There are several design principles that best describe how the CIS Controls are created:

### OFFENSE INFORMS DEFENSE

The CIS Controls are selected based off quantifiable data and proven; effective tactics based off knowledge of attacker's behavior.

### FOCUS

Not all assets are created equal. The CIS Controls help users identify what is most important and prioritize critical assets and operations.

### FEASIBLE

Every safeguard and best practice outlined in the controls are actionable and practical.

### MEASURABLE

The CIS Controls are measurable. Organizations can measure their effectiveness and avoid subjective language with implementation.

### ALIGNMENT

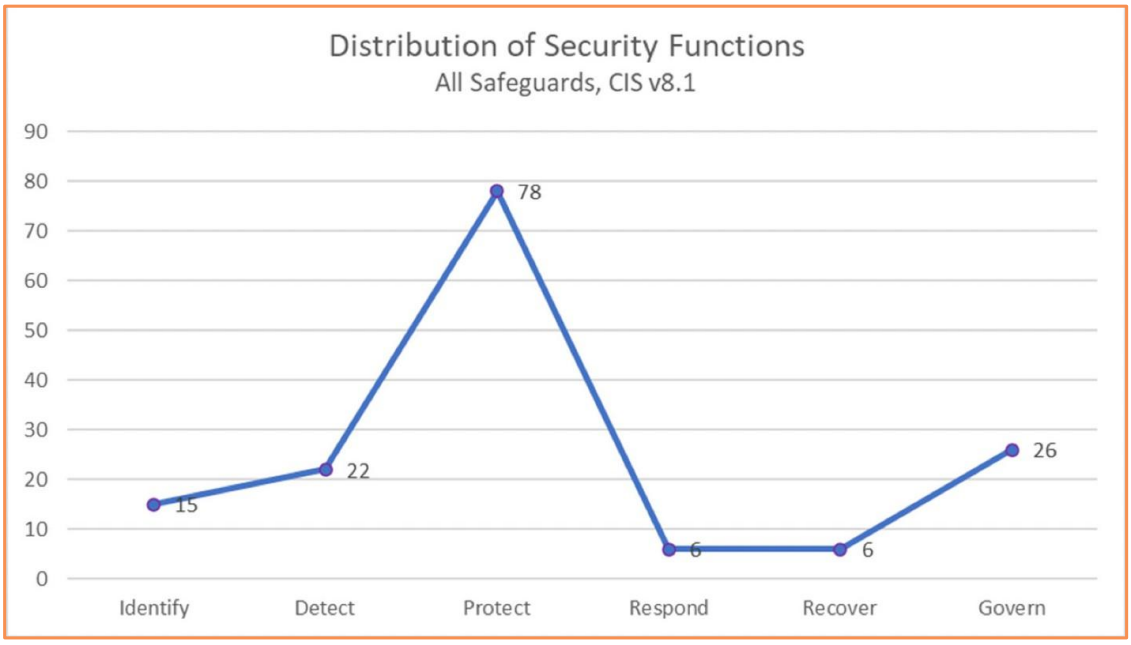
The CIS Controls align with various government regulations and compliances frameworks, schemes, and structures. The Controls map to most major compliance frameworks such as the NIST Cybersecurity Framework, NIST 800-53, ISO 27000 series, and regulations including PCI DSS, HIPAA, NERC CIP, and FISMA. While the controls are not a replacement for an existing regulatory, compliance, or authorization scheme, they provide organizations with a starting point for action. Soter Tech Solutions utilizes the CIS Controls when helping organizations achieve and maintain compliance with external regulatory bodies or standards.

As mentioned, the CIS Controls are a set of dynamic safeguards that address the most common cyber risks organizations will face. To ensure that the Controls stay relevant and are tackling risks that businesses face every day, updates to the framework are necessary. On June 25th, 2024, the Center for Internet Security released their much-anticipated v8.1 update of the CIS Controls. This update includes several changes to existing safeguards, closer alignment to the NIST CSF, along with the inclusion of the Govern security function.

There are a total of 32 changes to the security functions in v8.1 of the CIS Controls. These include new controls for mobile devices to address the security risks associated with their use in organizations as well as additional controls for supply chain security to help organizations manage the risks that come with third-party vendors. However, the largest change is the reorganization of the controls to better align with the NIST Cybersecurity Framework (CSF) with the inclusion of the Govern function.

What is the Govern Function? In the context of cybersecurity, governance refers to an organization's cybersecurity strategy and how they go about preventing cyber attacks and achieving compliance. The Govern Function provides guidance on how to effectively manage an organization's cybersecurity program to ensure their efforts are aligned with business objectives and regulatory requirements. The function includes policies, procedures, and processes to help ensure cybersecurity efforts are organized and align with the organization's cybersecurity program.

**Of the 153 total safeguards, 78 are related to protection of assets with 26 dedicated to the governance and oversight of the security program.**



# STRUCTURING THE CONTROLS

The CIS Controls are made up of 18 primary controls, each a unique cybersecurity domain. Within each primary control are multiple safeguards, or sub-controls. The safeguards contained within each of the 18 controls are then categorized into “Implementation groups”. Implementation Groups allow the controls to be made into “Risk Sized” groups rather than applying all controls to all organizations. The result is a subset of the CIS Controls that the cybersecurity community has broadly assessed to be applicable for an organization with a similar risk profile and resources to strive to implement.

## IMPLEMENTATION GROUP 1

The first implementation group or “IG1” consists of 56 safeguards that fall under “essential cyber hygiene”. These practices are the most basic and foundational steps every organization should take in securing their organization. The CIS defines an IG1 enterprise as a “small-medium sized business with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel”. The safeguard outlines contained in IG1 are effective against general, non-targeted attacks.


## IMPLEMENTATION GROUP 2

IG2 contains 74 security safeguards including those outlined in IG1. The purpose of Implementation Group 2 is to aid organizations that are tasked with balancing security across diverse departments. For many organizations, risk or even compliance may differ across various departments. For instance, an accounting department will have a unique risk profile as compared to an HR department. These organizations may be entrusted with large amounts of customer or internal data that need to be secured. IG2 helps businesses manage their diverse risk portfolio across the organization.

## IMPLEMENTATION GROUP 3

IG3 contains 23 safeguards and includes all the previous safeguards outlined in IG1 and IG2. IG3 applies to organizations that face more sophisticated cybersecurity threats or possess more valuable (or sensitive) information. G3 seeks to protect highly sensitive business assets or data whose safe handling or protection is regulatory defined. Often, these organizations possess systems or data that if compromised or lost, could result in severe consequences, dire financial consequences, and in some cases, pose a threat to public safety and security.

# THE 18 CIS CONTROLS - A BRIEF SUMMARY

## CONTROL 1: INVENTORY AND CONTROL OF ENTERPRISE

Every organization should invest time and resources into compiling a complete inventory of enterprise and software assets that are in use across the organization. This is beneficial for the purposes of organization, but also is a key component of cybersecurity. Businesses can't begin to secure their data, applications, or hardware until they have a robust understanding of what business assets are in use.

The first of the CIS Controls, Control 1 is "Inventory and Control of Enterprise Assets", which asks organizations to inventory all enterprise assets including end user devices (portable and mobile), network devices (on premises and cloud based), internet of things (IoT) devices, and servers that are connected to the network physically, virtually, remotely, or via the cloud. Control one also calls for organizations to inventory any adjacent assets that connect to the network including guest networks, test networks, or demonstration systems. This allows for businesses to have visibility over every corner of their network.

## CONTROL 2: INVENTORY AND CONTROL OF SOFTWARE ASSESTS

Control 2 asks that organizations "inventory, track, and correct" all software, including operating systems and applications, to ensure that only authorized pieces of software are allowed within the organization. This complete inventory of all software assets enables businesses to effectively limit access to corporate information assets, mitigate vulnerabilities (or "correct" software in CIS parlance) using patch management systems to remediate vulnerable applications and prevent zero-day attacks. Soter Tech Solutions offers patch management solutions to SMBs to ensure their applications are running on the most secure and stable version available.

Due to the large and changing number of assets, inventory must be consistent and comprehensive while also ingesting data from multiple sources to achieve an accurate account of business assets.

## CONTROL 3: DATA PROTECTION

When threat actors target organizations, their end goal is often to exfiltrate or deny users access via encryption to sensitive data that businesses rely on every day. For many organizations, data is everything. Into today's technological landscape, data exists everywhere. Workers are creating, transmitting, and storing data locally, in the cloud, and on unmanaged personal devices. This data may include financial information, intellectual property, customer data, personal identifiable information (PII), and more. This data is what hackers want and protecting it must become a priority for every organization. Additionally, organizations found to have mishandled sensitive information may face substantial legal repercussions. For many, data protection moves beyond a business obligation and into a regulatory requirement.

Soter Tech Solutions helps small-medium sized businesses protect their critical business data, both at rest and in motion. With services ranging from continuous data protection / backups, selective encryption, and data loss prevention (DLP) / data watermarking technologies. Our data protection services ensure compliance with regulatory frameworks while also providing peace of mind. Our services help to allow our clients to be viewed as a trustworthy guardian of their customers' data.

## CONTROL 4: SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

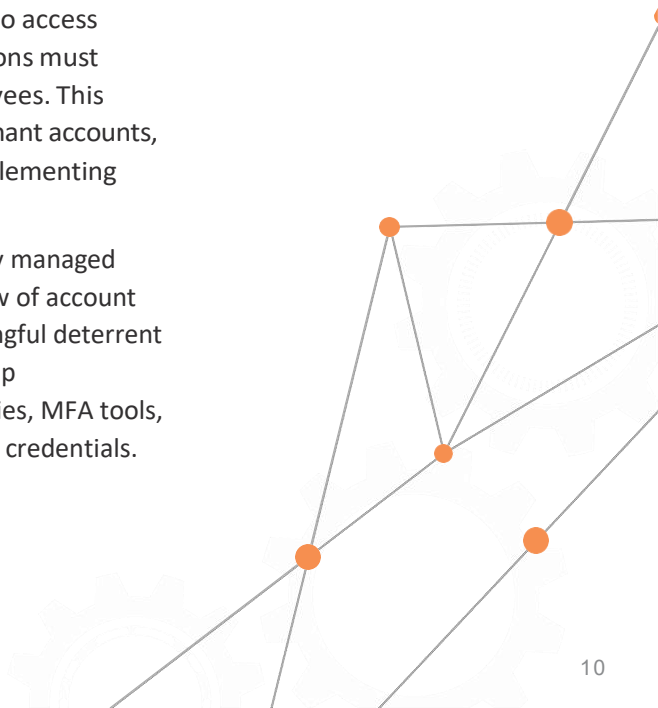
Once organizations have accounted for and made an inventory of their enterprise and software assets, they must do the work of securely configuring them. Many resellers and manufacturers deliver their hardware, software, and products in either an insecure or default configuration. This practice typically stems from the perspective of ease-of-deployment and out of the box functionality. When sent to an organization, devices may be configured with default passwords, unnecessary open ports, or unwanted software ("bloatware" or "adware") that must be secured or removed entirely. Software is commonly installed in an unpatched state that can contain vulnerabilities that expose an organization to threats. Before deploying or implementing software assets into a business's workflow, these assets must be securely configured.

Control 4 requires regular and ongoing configuration analysis of an organization's hardware and software assets to identify and correct any security concerns. Soter Tech Solutions continually manages customers assets to ensure every piece of hardware or software is configured in a way that ensures operability without sacrificing security. Soter Tech Solutions offers software vulnerability scanning to address common gaps and vulnerabilities as they appear in the wild. Our security assessments can reveal misconfigurations or vulnerabilities found in the businesses assets your organization utilizes every day.

## CONTROL 5: ACCOUNT MANAGEMENT

One of the primary ways threat actors gain access to a network is through compromised or inactive user accounts. These accounts are used to access network resources, exfiltrate data, or elevate privileges. Organizations must implement processes that secure the accounts provided to employees. This includes regularly examining all software and cloud services for dormant accounts, evaluating the password strength of the active credentials, and implementing mechanisms to secure accounts beyond a password.

One of the most effective strategies for securing accounts is centrally managed multi-factor authentication (MFA). This combined with regular review of account authorization to the corporate information assets, provides a meaningful deterrent against common account-based attacks. Soter Tech Solutions can help organizations secure their accounts by implementing password policies, MFA tools, and advanced user-behavior based controls that better secure login credentials. Through zero trust practices,



Soter Tech Solutions limits the impact of a potential breach and protects an organization's most secure, administrative accounts. Rather than implementing traditional, perimeter-based security, zero trust solutions secure individual business assets.

This includes protecting individual accounts through the practices outlined above, but also following the principle of least privilege. User accounts should only have access to the resources required to do their job. These practices are the foundation of secure account management.

## CONTROL 6: ACCESS CONTROL MANAGEMENT

Once authenticated to the network, an organization's user, administrator, and service accounts must be managed to ensure that they are only given access to what is required to perform necessary tasks. Following the "principle of least privilege", businesses must use tools to create, assign, and revoke necessary credentials to narrow their attack surface. This control moves past securing the account and focuses on what resources the account is authorized to receive once it has been authenticated. Soter Tech Solutions can help organizations to implement secure network architecture principles to effectively limit access and enforce least privilege across information assets.

## CONTROL 7: CONTINUOUS VULNERABILITY MANAGEMENT

A concrete vulnerability management plan is crucial for every organization in today's threat landscape. This plan should continuously assess and track vulnerabilities across an organization's assets while implementing controls to remediate and minimize the consequences of an attack. Through vulnerability management, organizations can monitor and track the gaps in their security to ensure threat actors aren't able to exploit them.

A business should be able to identify where their vulnerabilities lie, and what must be done to remediate them. It is also important that this process is continuous to address the ever changing and broadening attack surface. Continuous vulnerability management should include analysis of software "defects" (patches), vulnerable configurations, and deprecated/legacy software. Through V360, Soter Tech Solutions offers a comprehensive vulnerability management solution that addresses unique industry needs and prioritizes at-risk and business critical assets.

## CONTROL 8: AUDIT LOG MANAGEMENT

Audit and system logs are essential for businesses to collect information about network events to recover or protect from certain attacks. Logs are how organizations know when an event is in progress, what happened, and what the scope of the incident entails. These logs also ensure the tools a business is using are effective and working properly. Logs may also provide crucial evidence of an attack and are often required in compliance settings. Proper log management should be a part of every organization's security plan. Through our managed services, Soter Tech Solutions logs and tracks security events that may impact the security of our customers.

## CONTROL 9: EMAIL AND WEB BROWSER PROTECTION

In an organization, communication is key. Email allows employees to communicate, collaborate on projects, and share documents and files in an instant. Email and web browser applications also allow users to interact with external parties and environments. While convenient, threat actors find these attack vectors to be some of the most effective when gaining a foothold in an organization. Using social engineering, phishing, and a myriad of web-based methods, attackers can manipulate users into willingly providing access to the network.

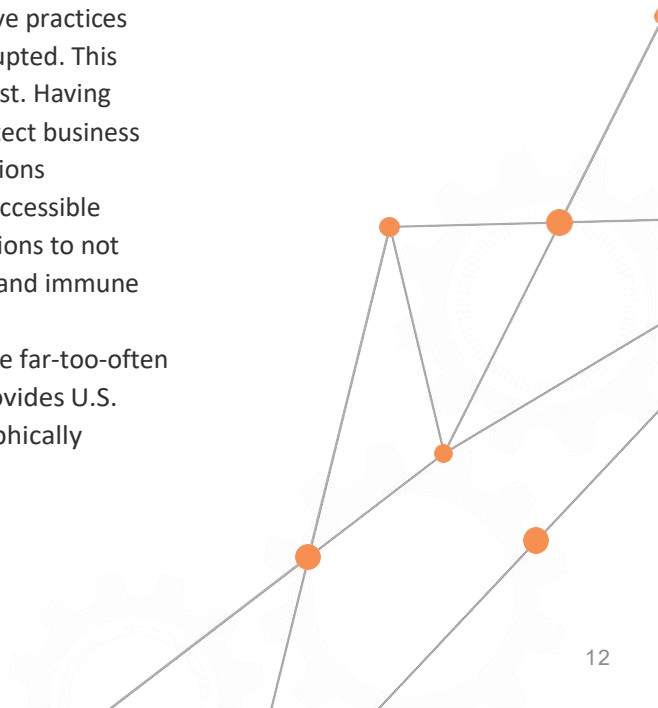
Soter Tech Solutions provides services to enforce and validate the authenticity of an organization's electronic communications, standards-based Anti-repudiation controls, and security against both individual and organization-wide impersonation attacks. We support these services with protections from social engineering, email and cloud-based malware defenses, and digital identity certificates to deliver robust protections against these common attack vectors.

## CONTROL 10: MALWARE DEFENSES

Malicious software (malware) represents one of the biggest threats to organizations today. Control 10 requires businesses to establish defenses against malware to prevent its spread and impact of critical information and assets. Threat actors (cybercriminals) utilize malware to accomplish various goals including credential harvesting, data exfiltration, and malicious file encryption (aka ransomware).
A crucial aspect of malware defense is the ability to identify and respond to incoming and present software-based threats. Soter Tech Solutions provides proven defenses against these threats. Combining Endpoint Detection Response (EDR) and Extended Detection Response (XDR) with secure Operating System and application configuration, our controls are proven effective. When combined with v360 continuous vulnerability management, the resulting software environment is one that effectively defends SMBs against both malicious software and the malicious use of legitimate software through "Living off the Land" attacks.

## CONTROL 11: DATA RECOVERY

What happens when data is lost or stolen? Every business should have practices in place to protect and restore any data that has been stolen or corrupted. This includes having recent backups to fall back on int the event data is lost. Having data recovery processes in place can help reduce downtime and protect business and client data. For small-medium sized businesses, Soter Tech Solutions provides data recovery and backup solutions to ensure your data is accessible and secure. Data recovery only goes so far, Control 11 asks organizations to not just back up their data but also keep some generations of it isolated and immune to change. Often
called immutable backups, these isolated instances of information are far-too-often the sole survivors of ransomware attacks. Soter Tech Solutions provides U.S. Based, PCI and HIPAA compliant off-site immutable and cryptographically protected data backup services to organizations of all sizes.



## CONTROLS 12 AND 13: NETWORK INFRASTRUCTURE MANAGEMENT AND NETWORK MONITORING AND DEFENSE

When configuring and managing a network it must be developed with security in mind. Control 12 focuses on secure network engineering practices that manage network devices, in order to prevent attackers from exploiting vulnerable access points. This includes ensuring firmware is up to date, implementing network segmentation with internal segmenting firewall (ISFW) capabilities and the ability to monitor and backup network infrastructure. Control 12 also calls for centralized AAA (Authentication, Authorization, Auditing) for all networking gear. Additionally, infrastructure administration should be conducted over secure protocols and with strong authentication methods. This control is important as it addresses shifting network security practices as new devices are added, architecture changes, and vulnerabilities arise.

In addition to network infrastructure management, monitoring and defense is equally important. Control 13 seeks to implement network monitoring and defense to protect organizations from advanced security threats. This control requires centralized event logging and auditing, performance of Host-Based IDS, implementation of network-based IDS, and conditional access restrictions for remote devices. These safeguards allow organizations to respond quickly to cyber threats before they impact the business. This ensures organizations are taking a proactive approach to security.

Soter Tech Solution's managed services addresses each of these integral controls with secure network infrastructure management and defense. We help organizations establish a secure network architecture that implements least privilege while using secure networking protocols and segmentation. Our services also secure remote access and administration and include robust threat intelligence that can be used to alert organizations of potential threats and attacks.

## CONTROL 14: SECURITY AWARENESS AND SKILL TRAINING

Technical controls can only do so much to protect a business from cyber criminals. An organization could have the strictest firewalls, the best email filtering services but still fall victim to social engineering or a phishing scheme. This is why it is important for businesses to educate their employees on how to address cyber threats in the workplace. An effective security awareness training program is consistent, with practical advice that is applicable to the threats employees will face every day. A user may unwittingly become an organization's greatest threat if they aren't prepared to exercise caution when working online.

Soter Tech Solutions provides a managed security awareness training platform to help train and educate end-users to be more aware of cyber risks while also increasing their overall knowledge of the very real cyber threats they will face. We've taken the complexity and tedium out of Security Awareness Training. Our content is delivered using a "meet users where they are" approach, devoid of confusing

acronyms and industry jargon. Further, to satisfy the increasing requirements of regulators and cyber-insurance companies alike, all our training can be delivered with a required skills validation exercise.

## CONTROL 15: SERVICE PROVIDER MANAGEMENT

Modern business is increasingly reliant on third-party vendors to increase efficiency, streamline operations, and outsource various tasks. Partnering with external organizations certainly has its benefits, however it also comes with substantial cyber risk that must be addressed. These third-party vendors often receive access to sensitive data and critical systems, which makes them attractive targets for cyber criminals. A breach in one organization has the potential for cascading effects that compromise both vendor and client data.

Control 15 provides safeguards for how organizations should manage vendor security. Organizations should restrict the amount of data third-party vendors have access to by only sharing what is required to provide their service. In the event of a successful data breach, this limits the potential impact across the supply chain. Every organization should do their third-party due diligence in examining whether a vendor can secure private data and if their practices align with regulatory requirements. Organizations must maintain and inventory their service providers, establish a comprehensive service provider management policy, and routinely monitor the security practices of any third-party vendors. It is also important to develop clear contractual agreements that outline security expectations and define specific security requirements.

Internally, Soter Tech Solutions works with several third-party vendors that have been assessed against our stringent security requirements. We can help organizations build a list of requirements and needs that must be addressed with their partners to ensure their data is in good hands.

## CONTROL 16: APPLICATION SOFTWARE SECURITY

An organization's application, whether developed in-house or hosted on the cloud, must be managed and secured at every stage of the production life cycle. These applications are responsible for creating, storing, and altering data and represent a momentous vulnerability if not accurately secured. A failure to secure a single application or piece of software can have cascading effects for the rest of the organization. Soter Tech Solutions ensures that an organization's applications are patched and updated regularly to avoid zero-day attacks and lateral movement across the network.

## CONTROL 17: INCIDENT RESPONSE MANAGEMENT

An incident response plan includes plans, policies, and procedures for how an organization is to respond in the case of a cyber incident. This includes an active data breach, corruption of data, or physical disaster. It's important to take a risk-based approach to Incident Response planning and management, understanding that no plan will ever be able to cover all possibilities or eventualities. and residual

risk will always exist. The most effective solution to Incident Response planning is to take a proactive position with respect to potential cybersecurity incidents and implement risk-based (risk informed) solutions that account for the most probable, most costly, or most disruptive potential incidents – whether arising from a physical disaster or cyber-attack.

A comprehensive incident response plan should include practices that detect, contain, and remove malicious entities on the network, but must also include mechanisms to inform and alert stakeholders of the potential repercussions of an attack. Soter Tech Solutions helps SMBs plan for and respond to cyber-attacks so that when the unexpected occurs, they're prepared.

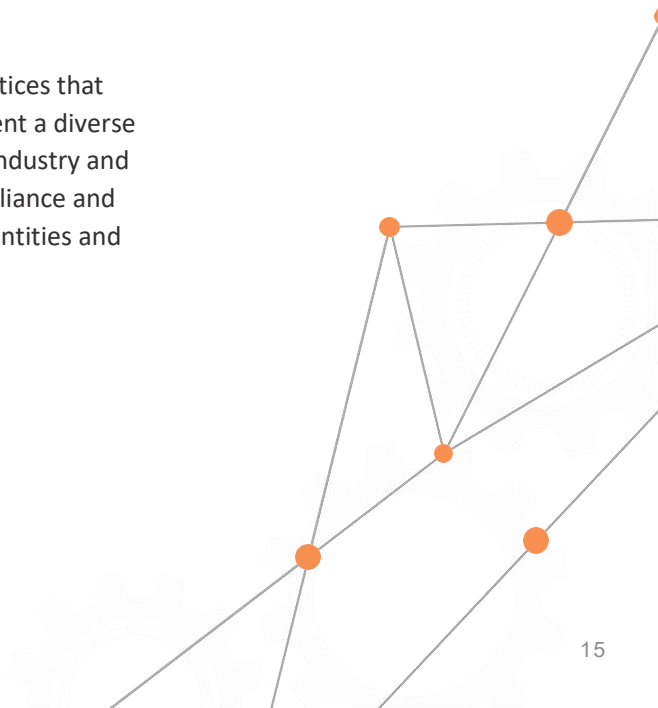
### CONTROL 18: PENETRATION TESTING

Any given IT environment contains a number of diverse technologies that work in tandem to empower business. As technology is replaced, updated, or discarded, an organization's security posture must be readdressed. Businesses must also ensure that the controls they've put in place are still effective and resilient. To accomplish this, regular penetration testing and security assessments are required. These assessments can reveal weaknesses, misconfigurations, or other vulnerabilities that may be exploitable by bad actors.

It's important to note that penetration tests and security assessments are not the same. Security assessments look for vulnerabilities present within an organization's security posture. Penetration tests assess the effectiveness of controls that have already been implemented. Soter Tech Solutions utilizes both to establish where an organization's security posture is at, and what must be fixed. These assessments are continuous and address the evolving ecosystem.

## CONCLUSION

Every organization must address cyber-risk and incorporate security practices that protect their business assets. The 18 CIS Critical Security Controls represent a diverse set of processes and safeguards that are practical and applicable to any industry and businesses of every size. The controls also align neatly with various compliance and regulatory frameworks making them a crucial tool for heavily regulated entities and organizations.



SOTER TECH
SOLUTIONS

# GET IN TOUCH

(305) 786-7490
sales@sotertechsolutions.us

Remote
Miami, FL 33176

www.sotertechsolutions.us