How to develop and maintain an ironclad security framework

Maximizing the Pax8 CIS Controls

Contents

Pax8 and CIS Controls

Introduction

The threat of a cyberattack should not be taken lightly. Every year, the number of businesses that experience cyberattacks is rising, with Cybersecurity Ventures estimating that cybercrime will cost the world $10.5 trillion in damages by 2025.

As regulation and compliance becomes a major focus of the IT world, businesses are feeling an increased pressure to implement an effective security framework.

To support these efforts, Pax8 offers security software tools in the Pax8 Marketplace so you can safeguard your clients and the future of your business. With over 25,000 managed service providers (MSPs) operating in more than 25 countries, Pax8 is one of the fastest-growing IT marketplaces worldwide, and we're here to help you mitigate risks, mature your business, and bring more value to your clients.

What are the CIS Controls and why are they important?

The Center for Internet Security (CIS) Critical Security Controls (referred to as CIS Controls) are a recommended set of actions for cyber defense, providing specific and actionable ways to thwart cyberattacks. There are 18 high-priority actions – and 153 specific safeguards – that present a strong starting point for any organization looking to enhance their security framework.

18
High-priority actions

153
Specific safeguards

A security framework is a combination of tools, policies, people, and documentation that defines policies and procedures for establishing and maintaining a set of security controls. Implementing CIS Controls endorsed by PCI, HIPAA, NIST, and cyber insurance agencies can keep your organization compliant and insulated from cyberthreats. This framework will also set you up for future success as compliance measures continue to expand. Between supply chain attacks, compliance and regulatory concerns, and subrogation from insurers, it is vital that you create a defensibility posture for your business.

The CIS Controls framework is built to protect **all** businesses, and is one of the most popular frameworks, having been implemented by 27% of MSPs worldwide.

This document presents a high-level overview of all 18 controls, tips on how to implement them within your business, and which Pax8 software solutions can help you with implementation. It's a useful reference guide in your journey toward a strong security framework. And as always, you can reach out to your channel account manager for more details.

CIS Control 1

Inventory and control of enterprise assets

Control overview

Control 1 keeps track of your assets so you can manage them properly. Inventory should be reviewed and updated on a regular basis, with counts compared against one another to establish a "true" count.

It's important to identify all organizational assets connected to your infrastructure physically, virtually, and remotely. That way, you'll understand the scope of what needs to be monitored and protected. Without keeping a proper record, you're vulnerable to insider threats, loss risk, and external attackers scanning for unprotected assets.

How to implement this control

Implementing this CIS Control requires both technical and procedural actions to create a process that accounts for and manages the inventory of all company assets and critical data. Maintaining an accurate view of organizational assets can be a challenging process because seldom is there a single definable answer. To guarantee a high-confidence asset count, assets should be scanned and assessed using a variety of safeguards. Then you must establish your "true" asset count by comparing the counts to each other.

To effectively implement this control, use both active and passive asset discovery tools to search for and address unauthorized assets. Unauthorized assets should be removed from the network, denied from connecting remotely, or quarantined. Execute the active tool daily (or more frequently) and use the passive tool to update the asset inventory at least weekly. You can also use Dynamic Host Configuration Protocol (DHCP) logging or IP address management tools as additional resources to update the asset inventory.

How Pax8 can help

The Pax8 Marketplace offers solutions to help you manage your critical assets, including Microsoft Azure, Addigy, and IBM MaaS360.

Microsoft Azure

Addigy

IBM MaaS360 | With Watson

CIS Control 2

Inventory and control of enterprise assets

Control overview

Control 2 involves the active management (inventory, tracking, and correction) of all software assets on the network, so only authorized software can be executed. It's critical to understand what's running on your systems, so that unauthorized and unmanaged software can be identified and stopped from being installed on the network.

As attackers continually scan organizations for software vulnerabilities, one of the key defenses is ensuring that all software assets are up to date and patched. By establishing an inventory of software assets, you can determine if vulnerable or outdated software is connected to your network.

How to implement this control

Start implementing this CIS Control by establishing and maintaining a detailed inventory of all licensed software installed on your systems. The inventory should document the title, publisher, initial install/use date, and the business purpose of that software, logging additional categories such as URL and version as needed.

Ensure that only currently supported and authorized software is installed on organizational assets. Implement a process for documenting software exceptions if the software is unsupported yet necessary for the fulfillment of the organization's mission. This exception process should include detailing mitigating controls and residual risk acceptance. If unauthorized software is identified and does not have a documented exception, that software should be removed from organizational assets.

Automate the discovery and documentation of installed software with technical controls such as application allowlisting. Technical controls can also be used to ensure that only authorized software libraries are allowed to load into a system process and to ensure that only authorized scripts are allowed to execute.

How Pax8 can help

The Pax8 Marketplace offers solutions to help you monitor and manage your software assets, including Microsoft Azure, SkyKick, Addigy, IBM MaaS360, Bitdefender, and SentinelOne.

Microsoft Azure · skykick · Addigy · IBM MaaS360 | With Watson · Bitdefender · SentinelOne

CIS Control 3

Data protection

Control overview

Control 3 will help you develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data. When an attacker infiltrates an organization's infrastructure, one of their primary objectives is to locate and download company data. If the company does not monitor data outflows, they are at risk of losing and exposing their sensitive data.

How to implement this control

Establish a process that includes a data management framework, data classification guidelines, and requirements for handling, retention, and disposal of data. There should also be an incident response plan developed in the event of a data breach, including a compliance and communication plan.

Data should be organized according to sensitivity level – key types of data need to be cataloged according to the overall criticality to the organization using labels such as "Sensitive," "Confidential," and "Public" to classify the data.

Once the sensitivity of company data has been outlined, a data inventory (or mapping) should be implemented that identifies the software accessing sensitive data along with the hardware being used.

Encryption is a vital component of data protection. Data should be encrypted on end-user devices, removeable media, services, applications, and databases containing sensitive data.

Data retention should be enforced accordingly and must include minimum and maximum retention timelines, and when those timelines expire data must be securely disposed. Additionally, a data loss prevention tool can be implemented to identify all sensitive data stored, processed, or transmitted through company assets.

The Pax8 Security Solution Consultant team can also evaluate your existing tech stack to make recommendations on what you can implement to better protect company data, as well as best practices to enhance your data protection process.

How Pax8 can help

The Pax8 Marketplace offers solutions to help you implement data protection, encryption, and management for your organization, including Microsoft Azure, Proofpoint, DefensX, and Avanan.

Microsoft Azure proofpoint. DefensX AVANAN A Check Point Company

CIS Control 4

Secure configuration of enterprise assets and software

Control overview

Control 4 establishes and maintains a secure configuration of assets and software to prevent exploitation from attackers. New computers acquired by a company are particularly vulnerable due to the absence of security configurations on the devices. The preset configuration can be exploitable in its default state as it uses basic controls, default accounts/passwords, and comes installed with unwanted software.

How to implement this control

You can utilize many different existing security baseline resources that are publicly developed and vetted, such as the CIS Benchmarks Program and the NIST National Checklist Program Repository.

These baselines should be reviewed and adjusted as needed to satisfy internal security policies and industry/government regulatory requirements. Any changes made to the baselines should be documented to facilitate future reviews. A good security process includes implementing and managing a firewall for services and end-user devices, uninstalling unnecessary software on all assets, configuring trusted DNS services, managing default accounts, and configuring devices to automatically lock after a defined period of inactivity or after several failed authentication requests.

Once a security configuration is established, it is important that the configuration is managed and maintained. The process should be reviewed and updated as needed annually. Additionally, implementing capabilities such as the ability to enforce remote wipes on portable end-user devices is important for maintenance in the event of lost or stolen devices.

How Pax8 can help

The Pax8 Marketplace offers solutions to ensure all hardware and software is configured and maintained properly and securely, including Microsoft Azure, Addigy, and IBM MaaS360.

Microsoft Azure Addigy IBM MaaS360 | With Watson

CIS Control 5

Account management

Control overview

Control 5 establishes a process to assign and manage authorization to credentials for user accounts. This is critical to preventing unwanted attackers from accessing your system. Controlling administrative access and enforcing strong passwords can mitigate potential phishing attacks and prevent unauthorized access to your network.

Administrative accounts are a primary target, allowing attackers to add other accounts to the network, or alter the organization's security framework to make it more vulnerable. Controlling and monitoring administrative accounts, ensuring that they have strong credentials, is important in preventing unwanted attackers from accessing and modifying your systems.

How to implement this control

First, establish and maintain an inventory of all accounts managed by the organization, including user and administrator accounts. Enforce unique passwords on all assets and encourage users to use a longer "passphrase" for added security, as well as enabling multi-factor authentication (MFA). Disable dormant accounts after a defined period of inactivity. Restrict administrator privileges to dedicated administrator accounts and centralize account management through a directory or identify service.

While this control is straightforward to implement from a software perspective, there may be some pushback from employees/end users as they believe they will need administrative access to install software or perform other parts of their job. Work with admin user staff to determine what tasks truly require administrative access and establish a process or redelegate tasks to minimize the number of active administrator accounts in the system.

How Pax8 can help

The Pax8 Marketplace offers solutions to ensure your accounts and credentials are secure, including Microsoft Azure, LastPass, and N-Able Passportal.

Microsoft Azure

LastPass ••• by LogMeIn

N-ABLE Passportal

CIS Control 6

Access control management

Control overview

Control 6 focuses on managing the access privileges of each specific account depending on the user's role within the organization.

Accounts should only have the minimal authorization needed for the role. Determining what roles need what access and developing a process to enforce and monitor these accesses is a good step to take to make your system more secure.

How to implement this control

As a baseline, a process should be established to be able to grant and revoke user privileges as needed. Role-based access is used to manage access requirements for each account based on need to know, least privilege, privacy requirements, and separation of duties.

Next, require all third-party applications to enforce multi-factor authentication (MFA) through a directory service or SSO provider. MFA should be enabled for all users accessing the system from any organization asset. This approach is more secure than a one-time code via SMS. However, administrator users should utilize privileged access management (PAM) tools for enhanced security.

High-privileged accounts should not be used for day-to-day use such as web surfing. Administrators should have separate accounts for daily office users, only logging into administrator accounts when performing tasks that require that level of authorization.

A system should also be put into place to monitor what administrator users are doing, making sure that they are logging into an administrator account only to complete required tasks.

How Pax8 can help

The Pax8 Marketplace has solutions to help you monitor accounts and grant or revoke access, including Microsoft Azure and LastPass.

Microsoft Azure

LastPass ••• | by LogMeIn

CIS Control 7

Continuous vulnerability management

Control overview

Control 7 helps you continuously assess and track vulnerabilities so you can minimize opportunities for attackers. Scanning should occur frequently and increase as the number of software assets increase to account for the different patch cycles of each new asset.

How to implement this control

There are many vulnerability scanning tools at your disposal to evaluate your security framework and monitor for new vulnerabilities. Scanning should occur frequently and increase as the number of software assets increase to account for the different patch cycles of each new asset.

Advanced vulnerability scanning tools can be implemented for administrator users to scan organization assets more comprehensively, known as "authenticated scans." Many businesses will link their vulnerability scanning tools with ticketing systems that can track the status of any issues, helping to ensure that critical vulnerabilities are tracked and resolved, not overlooked.

In addition to identifying, tracking, and resolving vulnerabilities, organizations should use NIST's Common Vulnerability Scoring System to determine the potential impact of an exploit and prioritize their response accordingly. The release of a new exploit, or new information related to a known vulnerability, should alter the priority in which the exploits are considered for patching.

How Pax8 can help

The Pax8 Marketplace offers solutions to scan for vulnerabilities within your systems, including Pillr, Bitdefender, Malwarebytes and ConnectSecure.

Pillr Bitdefender Malwarebytes for Business CONNECTSECURE

CIS Control 8

Audit log management

Control overview

Control 8 helps you keep track of anything happening within your systems so you can better understand an attack and recover from it. System logs record system-level events such as process start/end times and crashes, while audit logs record user-level events such as when a user logs in and accesses a file.

How to implement this control

If an organization has a poor log analysis process, it is possible for an attacker to infiltrate the system and control assets for months or years without anyone noticing.

An audit log would show that an unknown user is utilizing assets and accessing software/data that should not be accessed. That log could then be used to further analyze the attack, showing when the attack occurred and what information was accessed, which is helpful to identify the weaknesses in your security framework and conduct follow-up investigations into the attack.

Audit logging should be configured for any assets containing sensitive data. Most assets and software have native logging capabilities, making implementation of this control much easier. All logging features should be activated, and the logs should be sent to centralized logging servers.

To ensure that all assets are logging data as desired, compare the log records to the asset inventory established in Control 1. Firewalls, proxies, and remote access systems should all be configured for detailed logging.

To best use logs as a defense strategy, your team should define what constitutes a critical alert, and regularly review logs to watch for these alerts (ideally on a weekly basis.) Audit logs should be retained for a minimum of 90 days, but critical logs should be retained indefinitely to aid in future investigations.

How Pax8 can help

The Pax8 Marketplace offers solutions to capture, centralize, and retain audit logs, including Microsoft Azure, Pillr, and Todyl.

Microsoft Azure Pillr todyl

CIS Control 9

Email and web browser protections

Control overview

Control 9 helps you implement tools for a secure web browser and email. It is very easy for an attacker to craft an innocent looking email or web page that is designed to entice users into disclosing credentials, providing sensitive information, or exposing a vulnerability that allows hackers to gain access to the system.

How to implement this control

To prevent web browser attacks, browsers should be configured to disallow plugins from untrusted sources, and a firewall should be enabled to block untrusted or fraudulent sites asking for sensitive data. Most browsers today automatically utilize a database of phishing and malware sites and filter them out – these filters should be enabled, as well as pop-up blockers.

For email attacks, there are some basic safeguards that can be utilized to reduce the risk of attack, like using spam-filtering and malware screening tools to stop malicious emails and attachments from reaching their targets. Installing an encryption tool to secure email and communications adds another layer of security. It can also be beneficial to only give users access to certain file types they need for their role to minimize the risk of a malicious attachment.

Along with the implementation of software tools, it's also important to train employees to spot suspicious red flags in an email or web browser. A process should also be implemented for employees to report suspicious emails to IT security.

How Pax8 can help

The Pax8 Marketplace offers solutions to install web-browser and email-based security tools, including Microsoft Azure, DefensX, Proofpoint, IRONSCALES, Bitdefender, Webroot, Todyl, Avanan, DNS Filter,and TitanHQ.

CIS Control 10

Maleware defenses

Control overview

Control 10 helps you address attacks by malicious software (one of the most common threats to an organization's systems). With modern malware being developed with the assistance of machine learning and artificial intelligence, it is more critical than ever to implement a secure process of detecting and eliminating malware before it poses a risk.

Malware can be introduced in many ways – with new and creative methods being invented regularly. Which is why IT security and all company employees should never click on anything suspicious or use any untrusted hardware/software assets on company devices.

How to implement this control

Malware protection includes the typical endpoint malware prevention tools, and these should be managed centrally to provide consistency across the system. These tools function by scanning for, identifying, and blocking malware before it has the chance to damage the system. Automatic updates should be enabled to ensure that the software is always up-to-date and providing the best protection.

You should also collect logs to ensure all threat records are recorded and retained for audit purposes and future investigations.

In the last decade there has been an increase in "living-off-the-land" attacks where malicious code is embedded within trusted software to minimize the risk of being detected by anti-malware tools. Keeping careful logs will make it easier to track where the malware came from, why it happened, and what was compromised.

How Pax8 can help

The Pax8 Marketplace offers solutions to implement anti-malware software, including Microsoft Azure, Webroot, Bitdefender, Todyl, Acronis, Malwarebytes, and SentinelOne.

Microsoft Azure · WEBROOT · Bitdefender · todyl · Acronis · Malwarebytes for Business · SentinelOne

CIS Control 11

Data recovery

Control overview

Control 11 ensures that a system is in place to secure and recover data. It is important to have recent backups or mirrors of data to restore assets back to a trusted state in the event of an attack.

Attackers can take advantage of an organization's neglect to backup data by infiltrating the systems and making changes to key configurations, adding accounts, or adding software or scripts. Ransomware attackers will even try to encrypt an organization's data and demand money for its restoration.

How to implement this control

Expand data security safeguards, including backup procedures based on data value and sensitivity. Full backups should be conducted once a week, and incremental backups with highly valuable/sensitive data should be conducted more frequently.

Once per quarter, or whenever a new backup process or technology is introduced, a testing team should evaluate a random sampling of backup data and attempt to restore them in a testing environment. The backups should be evaluated to ensure that all data from the backup is intact and functional. Backups should be properly protected via security or encryption, ensuring key systems have at least one backup that is not continuously addressable through operating system calls.

How Pax8 can help

The Pax8 Marketplace offers solutions to implement data backup and recovery tools, including Microsoft Azure, Acronis, Datto, Infrascale, Axcient, Dropsuite, Otava, SkyKick, Arcserve, and Veeam.

CIS Control 12

Network infrastructure management

Control overview

Control 12 helps you create a secure network infrastructure by managing devices such as physical and virtual gateways, firewalls, wireless access points, routers, and switches. Default configurations for network devices are often geared for ease-of-use, not security. Attackers search for vulnerable default settings or gaps in a firewall ruleset to infiltrate the system.

How to implement this control

Network security is an ever-evolving issue that requires regular re-evaluation of configurations and access controls. Potential default vulnerabilities include open services and ports, default accounts and passwords, out-of-date versions, and pre-installation of unnecessary software. Establish a process to ensure that all assets have been securely configured before deploying.

Network configurations tend to become less secure over time when firewall exceptions are granted to fulfill a business need but then are never removed from the exception list. When enhancing network infrastructure management, a process for evaluating firewall exception risk should be defined. The exception list should also be regularly evaluated to determine if the exception is still necessary (with as few exceptions granted as possible).

Organizations should ensure that network infrastructure is fully documented, and architecture diagrams are established, maintained, and reviewed regularly. Remote devices should be monitored and fitted with an organization-managed VPN and authentication service, which must be utilized before accessing company resources. All assets should always be kept up-to-date with the latest secure and stable version.

How Pax8 can help

The Pax8 Marketplace offers solutions to help with network infrastructure management, including Azure Firewall, WatchGuard, Todyl, and NordLayer.

Microsoft Azure Firewall · todyl · WatchGuard · NordLayer

CIS Control 13

Network monitoring and defense

Control overview

Control 13 emphasizes continuous network monitoring for threats so your security team can be alerted and respond in a timely manner. Every moment counts when malware is discovered, credentials are stolen, or sensitive data is compromised, so having a plan in place is critical. Organizations should use software tools in conjunction with establishing security team process used to prevent, detect, and quickly respond to cyberthreats.

How to implement this control

Start by developing a process to understand critical business functions, network and server architectures, data and data flows, vendor service and business partner connections, and end-user devices and accounts. At the core of this process should be a trained and organized team that can use this understanding to develop processes for incident detection, analysis, and mitigation.

Next, the team should utilize technology to collect and analyze logs on network and data access, as well as generally monitor networks and assets for unrecognized activity. Tech solutions to analyze logs, such as security information and event management software, should be complemented by weekly log reviews by your security team. As this process develops, the organization should create and maintain a knowledge base to better document and understand the business risks.

As the security team becomes more comfortable with the organization's threat intelligence capabilities, they will be able to understand which alerts are false positives and which are relevant threats. And they can use this knowledge to become proactive instead of reactive, stopping attackers before they have a chance to infiltrate.

How Pax8 can help

The Pax8 Marketplace offers solutions to implement network monitoring tools, including Pillr, Todyl, Bitdefender, and SentinelOne.

Pillr todyl Bitdefender SentinelOne

CIS Control 14

Security awareness and skills training

Control overview

Control 14 ensures every employee has the training to identify and report suspicious behavior. No security solution alone can effectively address cyber risk. Human vulnerability is one of the biggest risks for any security framework.

How to implement this control

A security training program should be implemented to help employees understand the risks, how to avoid them, and how to report potential and actualized threats to the security team. This training should be updated regularly to comply with the latest security standards.

There should also be more frequent, topical messages about security. When an incident does occur internally, or there is a media story about a severe security incident at another company, timely messages should be sent out to remind staff about best practices like strong passwords and tips to avoid phishing.

Additionally, your security team can implement social engineering training, such as phishing tests, as a more frequent reminder of the security threat any organization faces. These are used so that the employee can become familiar with what suspicious emails may look like and how to report them. It should also identify which users passed or failed the test so that training can be assigned as needed to those who pose more of a security risk.

A combination of an annual training program, social engineering training, and timely newsletters/reminders of security best practices should be implemented to create a strong framework for security awareness and skills training.

How Pax8 can help

The Pax8 Marketplace has solutions available to help you implement security training, including Breach Secure Now, IRONSCALES, Proofpoint, and Webroot.

CIS Control 15

Service Provider Management

Control overview

Control 15 ensures vendors, partners, and third parties are properly vetted so they are equipped to handle your sensitive information properly.

There are many cases where third-party providers were breached, sensitive data was exposed, resulting in significant impact to all companies relying on that servicer. A ransomware attack is a good example of this, where many companies' sensitive data is threatened unless a hefty payment is made. The most difficult part is there's nothing your team can do in this situation, except wait and see what happens. That's why it's important to only work with trusted vendors who care just as much about security as you do.

How to implement this control

Establish and define a policy for reviewing third-party service providers and taking inventory of vendors under review, while associating a risk rating to vendors based on potential impact to the business if there were an incident. Make sure that contracts with a vendor include language holding them accountable if an incident occurs.

There are many online platforms that can be utilized to determine which third-party vendors are trustworthy and right for your business. These platforms have an inventory of thousands of businesses, providing a lot of information to make an informed risk decision. Look to see if the company has a managed security service contract and holds cybersecurity insurance.

Even if a vendor is deemed trustworthy, review them every quarter to ensure that their risk level has not increased. When contracts are completed or terminated, ensure the account is properly deactivated (with data flow terminated, and any data held by the third party disposed securely).

How Pax8 can help

Pax8 is proud to work with reputable companies who are serious about data security and tick all the boxes in our Maximizing Vendor Defensibility Checklist. You can find them in the Pax8 Marketplace.

CIS Control 16

Application software security

Control overview

Control 16 helps you monitor software to prevent, detect, and remediate security weaknesses before they can make an impact. This includes in-house developed or third-party software deployed in any type of organization.

Many applications are developed with short development cycles, and assembled using a complex mix of development frameworks, existing code, and new code. This makes security control a lot more challenging as it's difficult to test every aspect of the application for vulnerabilities before releasing it.

Software-as-a-Service (SaaS) platforms are no different. Application vulnerabilities can be present for many reasons, such as insecure design and/or infrastructure, coding mistakes, weak authentication, and a failure to test for unexpected conditions. These are the types of vulnerabilities that attackers exploit.

How to implement this control

Application security is an important topic, and there are different ways to implement it depending on the scale of your organization.

- Smaller organizations that do not require custom-built applications rely heavily on off-the-shelf software packages. This helps the organization apply basic operational and procedural best practices to manage their vendor-supplied software.
- Medium-sized businesses may rely on some in-house code applications in conjunction with third-party components, applying software development best practices to their original code and basic operational best practices to vendor-supplied software.
- Large organizations make a major investment in custom software to run the business, hosting software on their own infrastructure. This work should be completed by expert software developers, applying security and software best practices to the code, while incorporating trusted third-party open-source software components as needed.

How Pax8 can help

The Pax8 Marketplace has solutions for application software security, including ConnectSecure, Pillr, and Bitdefender.

CIS Control 17

Incident response management

Control overview

Control 17 helps you put a documented plan in place before an incident occurs. Knowing the right investigative procedures, legal protocols, and communications strategy will help you manage the incident and recover.

Without established response and recovery plans, and without fully understanding what happened and what can be done to prevent it from happening again, the system is placed at severe risk, now and in the future.

How to implement this control

All organizations should implement a plan that includes the sources for protection and detection, whom to call when an incident arises, and communication plans for conveying information to leadership, employees, regulators, and customers.

It's ideal to establish an incident response team and assign key roles and responsibilities to each member so they're prepared to act when an incident arises. Action plans should be put into effect for each team member, including staff from legal, IT, public relations, human resources, and incident responders.

The incident response team should practice their procedures with scenario-based training, working through different types of attack scenarios. Technical team members need to be prepared to handle high-stress incidents, and practicing will make the team better prepared to respond quickly and effectively.

How Pax8 can help

The Pax8 Marketplace has solutions to help implement an incident response plan, including SentinelOne, Pillr, Todyl, and RocketCyber.

SentinelOne Pillr todyl RocketCyber

CIS Control 18

Penetration testing

Control overview

Control 18 focuses on the periodic execution of penetration tests to identify and address security vulnerabilities. Penetration testing simulates cyberattacks by exploiting known weaknesses to evaluate the extent to which an attacker could infiltrate the system, and the potential severity of the ensuing consequences.

The test may be from an external or internal network, originating from an application or a specific device, and may include social engineering of users to test human vulnerabilities.

Penetration tests are expensive and complex. But they can provide valuable insights into vulnerabilities and the efficacy of defenses.

How to implement this control

Any tests which expose known vulnerabilities are a potential risk factor for the organization. Despite these concerns, it's nothing compared to the impact an actual breach may have. First, utilize scanning tools to identify vulnerabilities within the system. Once identified, create exploits to demonstrate specifically how an attacker would use it to compromise the organization's security systems.

It is crucial to engage experienced and reputable vendors to conduct penetration tests. The organization should define a clear scope and rules of engagement before beginning. This scope should include organization assets with the highest valued information and lower-value systems that could be leveraged to compromise high-value systems. The rules of engagement should describe the times for testing, duration of test(s), and the overall test approach.

After testing is complete, analyze the results of the test both from a personal and defensive standpoint. Identify any human weaknesses in the process and work on a plan to resolve them. Review the impact of any vulnerabilities in order to understand what could happen in the event of a real attack.

How Pax8 can help

The Pax8 Marketplace offers a solution from Pillr Penetration, a reputable vendor specializing in the service.

Pillr

Conclusion

While many partners already have a good number of controls implemented, CIS can help you mature your business by adding valuable documentation and reporting to the mix. And if anything has been overlooked, CIS will help identify and secure any vulnerabilities in your security framework. Implementing these controls will help show clients your unique value as a trusted MSP.

To learn more about CIS Controls,
reach out to your channel account manager or sales rep.

You can also enroll in the CIS Preparation Session, take the CIS Readiness Assessment, and have your tech stack evaluated by the SSC team.

CIS Controls, powered by Pax8, can help ensure your organization is ready to defend against and respond to any cyberthreat effectively.