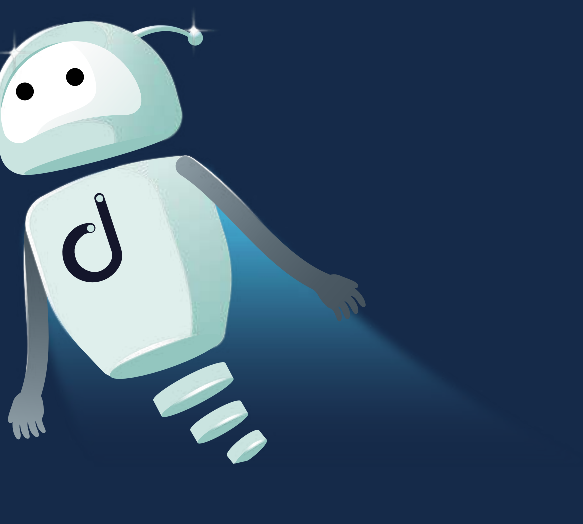
domotz

Why **Domotz** is Critical to your **Security:**

A Primer on how Domotz helps with CIS Critical Security Controls



Introduction

This paper is intended to give an overview of how Domotz helps you follow and improve upon the Center for Internet Security Controls, which are essentially a cornerstone to all security frameworks.

This paper will summarize the importance of the CIS Controls and then focus on how Domotz enables efficiency in your organization in meeting the safeguards associated with each control.

In the end, you'll have a worksheet and guide to implementing Domotz to start improving your security processes.

What's covered in this **guide**:

An **overview** of Center for Internet Security **(CIS) Controls**

As stated on the cissecurity.org website, the CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks.

The important thing to recognized about the CIS Controls is that they are mapped to and referenced by multiple legal, regulatory, and policy frameworks. The Center for Internet Security is a community-driven nonprofit that helps businesses implement best practices when it comes to information technology (IT) safety and security.

The CIS Controls are continuously evolving and improving to keep up with modern systems and software, so that users can better handle the threats toward their IT environments.

As users migrate their IT Systems from local to cloud, or some form of hybrid model, the CIS Controls provide methods and processes by which users can continuously improve their security footprint.

Why **CIS Controls** matter to you

Most security frameworks are built around the premise of the CIS Controls. Whichever security framework your company chooses to implement, you will find the basic controls put in place by CIS.

For this reason, it is good for you to understand what these controls are and why your business should implement the processes associated with the CIS Controls.

It is very important to understand that the CIS Controls are not a recipe for perfect security. They are meant to be a process for improving your security footprint. You could make an analogy about your health and exercise, where we exercise to improve our health, live longer and happy lives.

Implementing good security hygiene through best practices like the CIS Controls, help your company to decrease the threats associated to cyber-attacks. In this same vein, no amount of exercise can eliminate sickness or injuries from your body completely.

You should recognize that your company will constantly be under attack from cyber threats and hackers, doing your best to minimize it and being ready to take care of an issue when it occurs is how to keep your business running most efficiently.

The CIS Controls and their **Implementation Groups**

At the time of this writing, CIS Controls version 8 (v8) was published with 18 specific controls to consider in your business. Each individual control provides a perspective on how you can improve your cyber-hygiene within your company. Each control has specific safeguards associated to them that makes up the control.

To increase adoption of these controls and simplify the understanding of how users should get started with these controls, CIS created the idea of Implementation Groups (IGs) that are tiered toward continuous improvements. There are three IGs that build upon each other, meaning that IG2 includes IG1, while IG3 includes IG2 and IG1.

The CIS website (https://www.cisecurity.org/controls/v8/) has all the CIS Controls written in an understandable and comprehensive manner, therefore we will not repeat all the details associated with each control.

In fact, each control highlights its specific safeguards and how those safeguards apply to your asset types and security functions.

That said, it is important to recognized why the implementation groups are structured as they are with respect to safeguards in each control.

Implementation **Group 1**

IG1 caters to any business that has limited IT and cybersecurity expertise.

Most small and medium businesses fall into category. Any Managed Service Provider or IT Professional should focus their efforts IG1 to help keep their own business, plus their client's business, operational and minimize downtime.

There are some assumptions with IG1 that the data associated to the business does not need significant protections, as would be the case for financial, health or private data in general.

The safeguards within each control that are associated to IG1 can be implemented even with limited cybersecurity expertise.

Implementation **Group 2**

As previously mentioned, IG2 incorporates all the safeguards assumed in IG1, but adds extra safeguards that a typical IT department employee would typically manage. IG2 assumes that employees and job functions within an organization may have different risk or threat profiles associated with their role in the company.

Furthermore, IG2 assumes that there may be regulatory compliance burdens, such as privacy laws where sensitive data about clients, or the enterprise, must be maintained.

CIS points out that IG2 assumes that a short interruption of the enterprise's services may be acceptable. It's important to note that a good way to assess if you should be considering IG2 is if the company would lose public trust should a cybersecurity breach occur.

Implementation **Group 3**

IG3 assumes all the safeguards of each control. The assumption that an IT team, and in particular a Chief Information Security Officer (CISO), is in place within the organization holds crucial with IG3. Company assets and data are considered as sensitive. Downtime of enterprise services must be minimized and there is an assumption of high availability on IT services and infrastructure. Similar to IG2, but with more definite consequences, public trust would be significantly eroded should a breach occur.

The safeguards associated with IG3 focus on detection, response and recovery to help improve management of targeted cyber-attacks and vulnerabilities associated with zero-day attacks.

Which **Implementation Group** are you?

The IGs are outlined in a way that allows you to self-assess where you are today and where you want to go with respect to cyber-hygiene. There is no right or wrong answer to which group you are in, but you need to start with a self-assessment.

As you walk through each section of the controls, place a check mark by the ones you're implementing. Be honest with yourself on this process, again, there is no right or wrong answers here. Consider controls and sections that you have partial implementations and mark these appropriately. For some controls, you may cover all implementation groups, but for other controls, you may have nothing. This is OK.

Recall that CIS Controls are more about the process. Knowing where you are is the first step to moving in the right direction. While the CIS Controls look daunting, the segmentation of each control into IGs helps you prioritize which sections you should consider a priority. Also note, that the priority depends on your business needs and goals.

Not knowing where you are is simply not acceptable. Your first step is to do a self-assessment. Your second step is to continuously improve, no matter how small the steps.

Domotz and **CIS Control Safeguards**

Domotz helps it users with respect to key CIS Security Controls.

As with any tool, how you use Domotz will speak to the efficacy of your operations and cyber security hygiene.

There are several safeguards within the eighteen controls established within CIS Security Controls v8 that Domotz is critical to helping your business be more efficient when it comes to maintaining proper cyber hygiene.

Read on to find out which **CIS controls Domotz** can help with.

01.

Inventory and **Control** of Enterprise Assets

04.

Secure Configuration of Enterprise Assets and Software

07.

Continuous Vulnerability Management

12.

Network Infrastructure Management

13.

Network Monitoring and **Defense**

15.

Service Provider Management

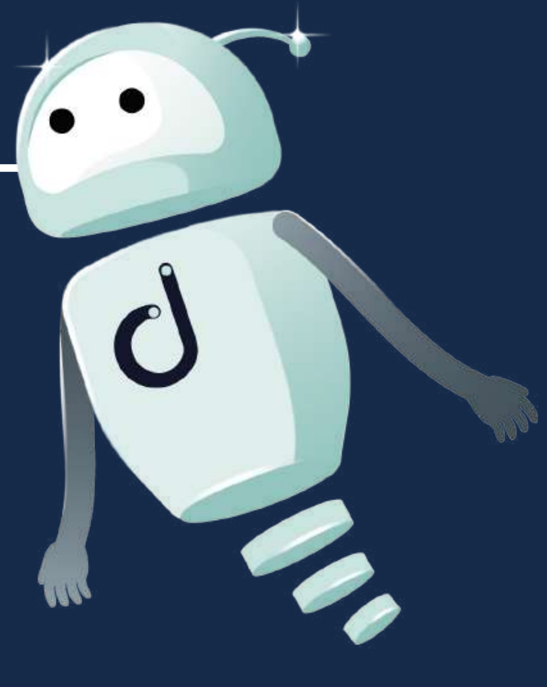
Inventory and **Control** of Enterprise Assets

01.

Many service providers stop at the endpoints (PCs, Laptops, Servers) and possibly the network infrastructure, but every device that is on the network should be managed.

Domotz can help you satisfy the safeguards in this control through discovering every MAC address on a network, discovering multiple MAC Addresses associated with a device and by classifying devices by manufacturer, model, and type of device.

Domotz also discovers when un-authorized devices connect to a network, logs historical information and performs ongoing passive asset discovery.



As stated within the CIS Security Control v8 document, this control is about actively managing all enterprise assets. Many service providers stop at the end-points (PCs, Laptops, Servers) and possibly the network infrastructure, but every device that is on the network should be managed. The primary reason for this is to understand vulnerabilities that could be exposed to the enterprise.

There are five safeguards to help ensure proper management of enterprise assets. The first one deals with establishing and maintaining a detailed enterprise asset inventory. These assets include fixed and portable devices, network infrastructure devices, as well as embedded/IoT systems and devices.

Essentially, anything touching the network needs to be documented and understood. Domotz, using its advanced scanning techniques, will discover every MAC address associated to the networks you are monitoring and will even discover when a single, physical device has more than one MAC Address associated with it, as is often the case with servers and virtual machines.

Domotz further helps by classifying each device by its manufacturer, model and type of device.

The second safeguard within Control 01 has to do with managing unauthorized devices on your networks. The first step to managing an unauthorized device is knowing that it is there. Domotz utilizes continuous discovery method on the network to bring rapid awareness to devices on the network and, as stated previously, helps you classify these devices so you can better assess the risk associated the unauthorized device.

With Domotz being used for Control 01, you immediately cover Implementation Group 1, but since you are using an active scanning tool which logs and recognizes when devices change IP addresses, you also cover the third and fourth safeguards, satisfying Implementation Group 2.

The last safeguard in Control 01 has to do with passive asset discovery. Domotz is constantly scanning and can alert you to immediately to new devices or changes on the network.

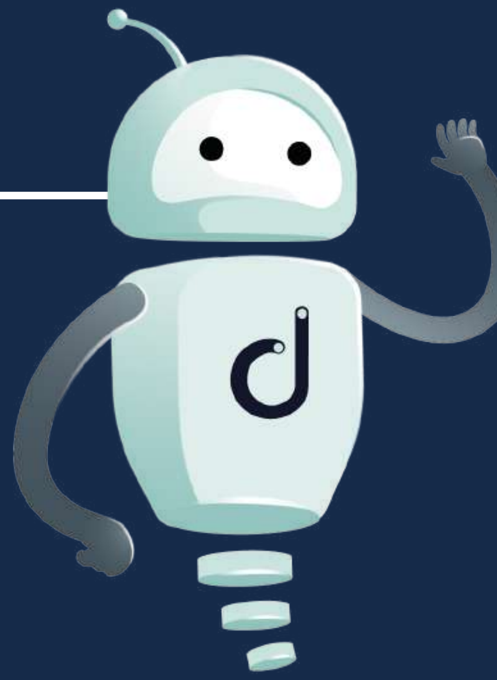
To establish yourself into Implementation Group 3 for this Control, you must review the asset list and the history of the devices getting connected to the network. This is more about process than anything but utilizing a tool like Domotz helps you and your team to be more efficient when it comes to this continuous review.

Secure Configuration of Enterprise Assets and Software

04.

To protect your environment, you must establish a process of securely configuring and maintaining your systems.

Utilizing Domotz, you can easily maintain a secure configuration process for your network infrastructure.Furthermore, your managed switch and firewall configurations are backed up in the Domotz cloud, making it easy to save and restore systems as needed. Additionally, Domotz scans each device on the network for common TCP ports.



Control 04 is a critical step in ensuring your business stays protected.

Manufacturers and resellers will enable products with default configurations so that you can easily deploy their systems into your environment.

While this is helpful during deployment, left that way, your network becomes a playground for hackers. To protect your environment, you must establish a process of securely configuring and maintaining your systems.

Utilizing Domotz, you can easily maintain a secure configuration process for your network infrastructure, which is the second safeguard in this control.

It is up to you and your implementation to ensure the integrity of that infrastructure, but with Domotz, you can easily see and be alerted to changes to the network.

Furthermore, your managed switch and firewall configurations are backed up in the Domotz cloud, making it easy to save and restore systems as needed.

Safeguard 6 of control 04 requires you to securely manage enterprise assets and software.

It is important to recognize that enterprise assets go beyond end-points (PCs, laptops and servers).

Knowing which Transmission Control Protocol (TCP) ports are available on all your network-based assets is an important part of effectively protecting your network.

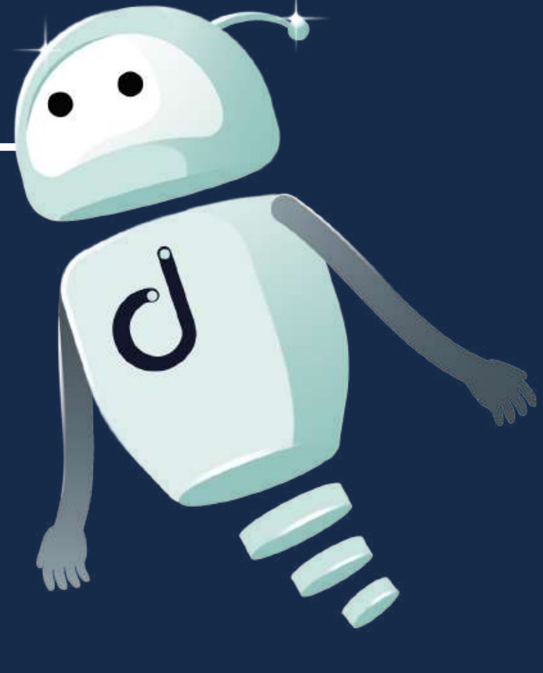
Domotz scans each device on the network for common TCP ports.

Continuous Vulnerability Management

07.

It's important to continuously check for vulnerabilities on your networks and all the enterprise assets associated with them.

Domotz will immediately recognize assets on your network and then scan for TCP ports, which can be associated with potential vulnerabilities.



It’s important to continuously check for vulnerabilities on your networks and all the enterprise assets associated with those networks.

While control 07 calls out the user of Security Content Automation Protocol (SCAP) Tools, there are some basic points that Domotz helps with to ensure you know more information about your network.

Safeguards 6 and 7 of Control 07 ask you to run vulnerability scans on a quarterly, or more frequent basis.

To minimize risks, you should know all the assets associated to your network and when new devices show up on the network

Domotz will immediately recognize assets on your network and then scan for TCP ports, which can be associated to potential vulnerabilities.

While your SCAP tool will do a thorough job of highlighting potential Common Vulnerabilities and Exposures (CVEs), you should know immediately when a device with open ports is on the network.

Remember that CIS Controls and their safeguards and put together with implementation groups.

Cybersecurity hygiene is a continuous improvement process and using a tool like Domotz to improve your cyber-hygiene process is an easy step in the healthier direction.

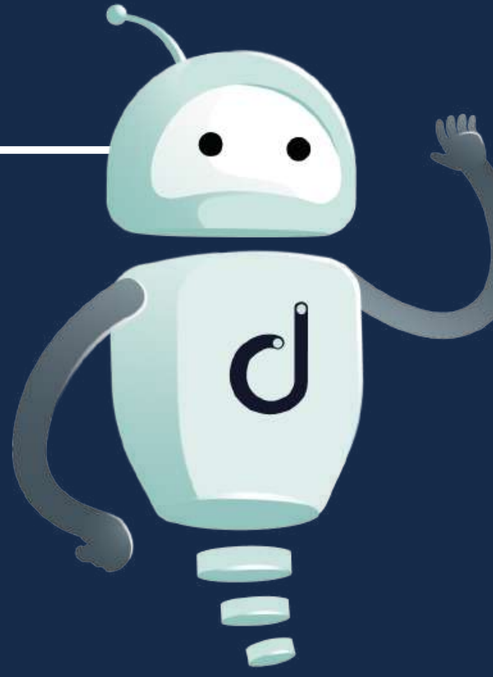
Network Infrastructure Management

12.

It's important for you to actively manage your network infrastructure to satisfy certain CIS controls.

Having a tool like Domotz to manage and maintain the network infrastructure of all your clients is extremely important and valuable.

Domotz will help you manage network infrastructure through providing you information on the equipment being used, how it connects to each other and ensuring all firmware is updated to the latest production versions released by the manufacturer.



To satisfy Control 12, you need to actively manage your network infrastructure. This means knowing what equipment you are using, how they are connected to each other and ensuring their firmware is updated to the latest production versions released by the manufacturer.

Domotz is a Network Monitoring and Management tool that enables you to satisfy in an efficient and effective way all the safeguards associated with this control. While several of these safeguards are about your process, using a tool like Domotz helps you be much more efficient when it comes to ensuring proper network infrastructure management.

As long as you have a process for ensuring your network equipment is up to date, you can easily satisfy IG1 of Control 12.

As previously mentioned, any security framework is based on continuous improvement and using Domotz to help establish Network Diagrams, as required by safeguard 4, is just another way to improve your cyber-hygiene process. Moreover, using Domotz to provide immediate and up-to-date network diagrams improves your cyber posture even more.

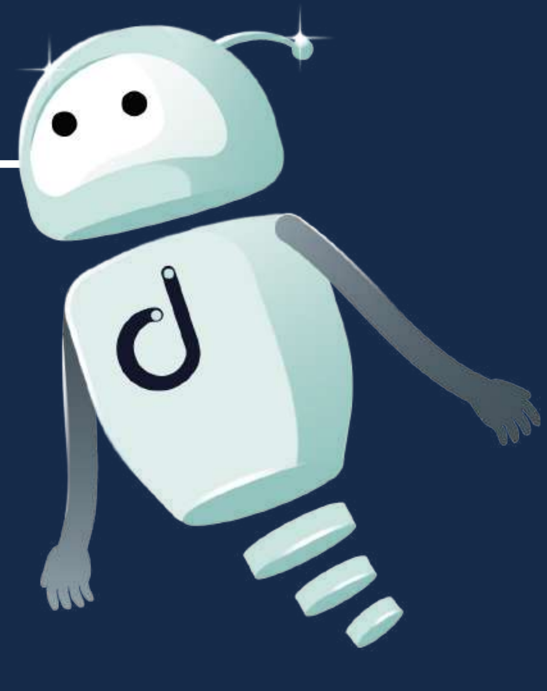
As a network monitoring tool, Domotz is agnostic to the hardware you use for your network infrastructure. This is important for your business, but as a service provider, you may be relying on multiple vendors and their equipment to build out systems that meet your clients needs. Having a tool like Domotz to manage and maintain the network infrastructure of all your clients is extremely important and valuable. Domotz helps keep all your clients’ systems managed and as clean as your process will allow for cyber-hygiene purposes.

Network Monitoring and **Defense**

13.

You can leverage Domotz to understand when new devices show up on the network.

Immediate awareness of new devices is a critical first step in network security that is often overlooked.



Control 13 is a more advanced control and the safeguards associated with this control put your company into IG2 and IG3.

This control is about comprehensive network monitoring and looking at threats coming into your network infrastructure.

While this control focuses on Security Information and Event Management (SIEM) and Network Intrusion Detection Systems (NISDs), which are more formally used by Security Operation Centers and Managed Security Service Providers, you can leverage Domotz to understand when new devices show up on the network.

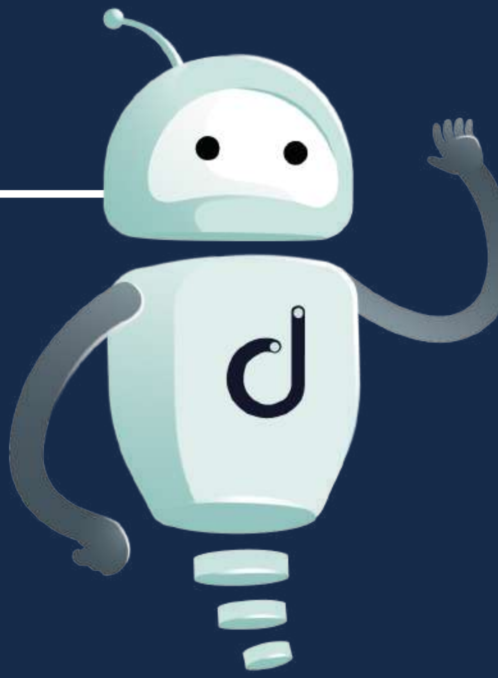
Immediate awareness to new devices is a critical first step that is often overlooked. In fact, recall that Control 01 already assumes that you are gaining awareness of unauthorized devices on the network, but this very well applies to Control 13 and safeguard 3.

Service Provider Management

15.

Domotz automatically checks your internet service provider on a regular basis, by doing speed checks across the internet and reporting on outages.

Furthermore, you can set up Domotz to perform latency testing between external hosts/services that you may be relying on.



Control 15 is primarily related to the vendors that you rely on to hold data or that provide services to your critical IT platforms, such as internet services.

In today's world, your internet service provider is just as important as water, sewer and electricity running to your business.

Control 15 is primarily built around this notion of documenting and understand how the service providers that you rely on are performing.

Domotz automatically checks your internet service provider on a regular basis, by doing speed checks across the internet and reporting on outages.

Furthermore, you can set-up Domotz to Latency testing between external hosts/services that you may be relying on.

Domotz can easily help you with safeguard 6 within Control 15 and improves up this safeguard by continuously monitoring these service providers.

Next steps for **CIS Control implementation**

As stated in the beginning, the **CIS Controls are a basis for many of the security frameworks you will encounter**. Your first step is to establish an understanding of where you are today.

In appendix A of this document, **we have provided you with a check sheet** of all the controls and safeguards associated with version 8. **Use this document to do a self-assessment on your business and your clients'**.

Remember that while this looks daunting, you must start somewhere. This is a process. Consider it a journey and every journey will begin with a single step. No matter where you are starting, being able to show where you have come from is extremely important in your defensibility of your security process.

There are many reasons that you may be considering the implementation of security framework. Your customers may be demanding it, you may have been hacked already, or you may just want to start taking a proactive approach to cyber-hygiene.

Regardless of your reasons, you should consider that cyber health and cyber awareness is becoming more and more important, and it is a metric that customers, vendors, insurance companies, regulatory bodies and governmental agencies are all starting to look at.

You can get ahead of this by understanding where you are today.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
1	**Domotz can help you with Inventory and Control of Enterprise Assets:** actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.				
□	1.1	Devices	**Identify**	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
□	1.2	Devices	**Respond**	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
□	1.3	Devices	**Detect**	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.
□	1.4	Devices	**Identify**	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.
□	1.5	Devices	**Detect**	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
2	**Inventory and Control of Software Assets:** actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.				
□	2.1	Applications	**Identify**	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.
□	2.2	Applications	**Identify**	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.
□	2.3	Applications	**Respond**	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
□	2.4	Applications	**Detect**	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.
□	2.5	Applications	**Protect**	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
□	2.6	Applications	**Protect**	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
□	2.7	Applications	**Protect**	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
3		**Data Protection:** develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.			
□	3.1	Data	**Identify**	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	3.2	Data	**Identify**	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.
□	3.3	Data	**Protect**	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
□	3.4	Data	**Protect**	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.
□	3.5	Data	**Protect**	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
□	3.6	Devices	**Protect**	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.
□	3.7	Data	**Identify**	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	3.8	Data	**Identify**	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise’s data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	3.9	Data	**Protect**	Encrypt Data on Removable Media	Encrypt data on removable media.
□	3.10	Data	**Protect**	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
□	3.11	Data	**Protect**	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.
□	3.12	Network	**Protect**	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.
□	3.13	Data	**Protect**	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.
□	3.14	Data	**Detect**	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
4	**Domotz can help you with Secure Configuration of Enterprise Assets and Software:** establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).				
□	4.1	Applications	**Protect**	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	4.2	Network	**Protect**	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	4.3	Users	**Protect**	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.
□	4.4	Devices	**Protect**	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.
□	4.5	Devices	**Protect**	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
□	4.6	Network	**Protect**	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	4.7	Users	**Protect**	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
□	4.8	Devices	**Protect**	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
□	4.9	Devices	**Protect**	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.
□	4.10	Devices	**Respond**	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.
□	4.11	Devices	**Protect**	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.
□	4.12	Devices	**Protect**	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
5	**Account Management:** use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.				
□	5.1	Users	**Identify**	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
□	5.2	Users	**Protect**	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
□	5.3	Users	**Respond**	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
□	5.4	Users	**Protect**	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.
□	5.5	Users	**Identify**	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
□	5.6	Users	**Protect**	Centralize Account Management	Centralize account management through a directory or identity service.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
6	**Access Control Management:** use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.				
□	6.1	Users	**Protect**	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
□	6.2	Users	**Protect**	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
□	6.3	Users	**Protect**	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.
□	6.4	Users	**Protect**	Require MFA for Remote Network Access	Require MFA for remote network access.
□	6.5	Users	**Protect**	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.
□	6.6	Users	**Identify**	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.
□	6.7	Users	**Protect**	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.
□	6.8	Data	**Protect**	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
7	**Domotz can help you with continuous Vulnerability Management:** develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.				
□	7.1	Applications	**Protect**	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	7.2	Applications	**Respond**	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
□	7.3	Applications	**Protect**	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
□	7.4	Applications	**Protect**	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
□	7.5	Applications	**Identify**	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
□	7.6	Applications	**Identify**	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
□	7.7	Applications	**Respond**	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
8	**Audit Log Management:** collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.				
□	8.1	Network	**Protect**	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	8.2	Network	**Detect**	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
□	8.3	Network	**Protect**	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.
□	8.4	Network	**Protect**	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.
□	8.5	Network	**Detect**	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
□	8.6	Network	**Detect**	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.
□	8.7	Network	**Detect**	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.
□	8.8	Devices	**Detect**	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	
□	8.9	Network	**Detect**	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.
□	8.10	Network	**Protect**	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.
□	8.11	Network	**Detect**	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.
□	8.12	Data	**Detect**	Collect Service Provider Logs	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
9	**Email and Web Browser Protections:** improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.				
□	9.1	Applications	**Protect**	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
□	9.2	Network	**Protect**	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.
□	9.3	Network	**Protect**	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
□	9.4	Applications	**Protect**	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.
□	9.5	Network	**Protect**	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.
□	9.6	Network	**Protect**	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.
□	9.7	Network	**Protect**	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
10	**Malware Defenses:** prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.				
□	10.1	Devices	**Protect**	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.
□	10.2	Devices	**Protect**	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.
□	10.3	Devices	**Protect**	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.
□	10.4	Devices	**Detect**	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.
□	10.5	Devices	**Protect**	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
□	10.6	Devices	**Protect**	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.
□	10.7	Devices	**Detect**	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
11	**Data Recovery:** establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.				
□	11.1	Data	**Recover**	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	11.2	Data	**Recover**	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.
□	11.3	Data	**Protect**	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.
□	11.4	Data	**Recover**	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.
□	11.5	Data	**Recover**	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
12	**Domotz can help you with Network Infrastructure Management:** establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.				
□	12.1	Network	**Protect**	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
□	12.2	Network	**Protect**	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
□	12.3	Network	**Protect**	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.
□	12.4	Network	**Identify**	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	12.5	Network	**Protect**	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.
□	12.6	Network	**Protect**	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).
□	12.7	Devices	**Protect**	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise’s AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.
□	12.8	Devices	**Protect**	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
13	**Domotz can help you with Network Monitoring and Defense:** operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.				
☐	13.1	Network	**Detect**	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.
☐	13.2	Devices	**Detect**	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
☐	13.3	Network	**Detect**	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.
☐	13.4	Network	**Protect**	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.
☐	13.5	Devices	**Protect**	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.
☐	13.6	Network	**Detect**	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	13.7	Devices	**Protect**	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.
□	13.8	Network	**Protect**	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.
□	13.9	Devices	**Protect**	Deploy Port-Level Access Control	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.
□	13.10	Network	**Protect**	Perform Application Layer Filtering	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.
□	13.11	Network	**Detect**	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
14	**Security Awareness and Skills Training:** establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.				
□	14.1	N/A	**Protect**	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
□	14.2	N/A	**Protect**	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
□	14.3	N/A	**Protect**	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.
□	14.4	N/A	**Protect**	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.
□	14.5	N/A	**Protect**	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.
□	14.6	N/A	**Protect**	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	14.7	N/A	**Protect**	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.
□	14.8	N/A	**Protect**	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.
□	14.9	N/A	**Protect**	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
15	**Domotz can help you with Service Provider Management:** develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.				
□	15.1	N/A	**Identify**	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.
□	15.2	N/A	**Identify**	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.
□	15.3	N/A	**Identify**	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.
□	15.4	N/A	**Protect**	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	15.5	N/A	**Identify**	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.
□	15.6	Data	**Detect**	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.
□	15.7	Data	**Protect**	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
16	**Application Software Security:** manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.				
□	16.1	Applications	**Protect**	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
□	16.2	Applications	**Protect**	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.
□	16.3	Applications	**Protect**	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.
□	16.4	Applications	**Protect**	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a “bill of materials,” as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	16.5	Applications	**Protect**	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.
□	16.6	Applications	**Protect**	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.
□	16.7	Applications	**Protect**	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.
□	16.8	Applications	**Protect**	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.
□	16.9	Applications	**Protect**	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.
□	16.10	Applications	**Protect**	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	
□	16.11	Applications	**Protect**	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.
□	16.12	Applications	**Protect**	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.
□	16.13	Applications	**Protect**	Conduct Application Penetration Testing	Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
□	16.14	Applications	**Protect**	Conduct Threat Modeling	Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
17	**Incident Response Management:** establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.				
□	17.1	N/A	**Respond**	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
□	17.2	N/A	**Respond**	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.
□	17.3	N/A	**Respond**	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
□	17.4	N/A	**Respond**	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
□	17.5	N/A	**Respond**	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
□	17.6	N/A	**Respond**	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
□	17.7	N/A	**Recover**	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.
□	17.8	N/A	**Recover**	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.
□	17.9	N/A	**Recover**	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS CONTROL	CIS SAFEGUARD	ASSET TYPE	SECURITY FUNCTION	TITLE	DESCRIPTION
18	**Penetration Testing:** test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.				
□	18.1	N/A	**Identify**	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
□	18.2	Network	**Identify**	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
□	18.3	Network	**Protect**	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
□	18.4	Network	**Protect**	Validate Security Measures	Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.
□	18.5	N/A	**Identify**	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

www.domotz.com