CIS Critical Security Controls Mapping Guide

CyFlare Solutions

OVERVIEW

The CIS Critical Security Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls[1].

The CyFlare Center for Internet Security (CIS) Critical Security Controls Mapping Guide aims to outline these prioritized set of actions released by the CIS that form a defense strategy to mitigate the most common cyber attacks and map them to a CyFlare-offered solution or service. By simplifying and boiling down each control to easily align with one of our offerings, we hope each enterprise feels ready to utilize this guide to help create an easy-to-follow, well-thought-out, full-proof security strategy.

To review the entire CIS Critical Security Controls Version 8, you can download it **here**.

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
1	1.1	Devices	Identify	XDRaaS	Establish and Maintain Detailed Asset Inventory	Asset Management Tools/AD
1	1.2	Devices	Respond	XDRaaS	Address Unauthorized Assets	Asset Discovery and Management Tools/AD
1	1.3	Devices	Detect	XDRaaS	Utilize an Active Discovery Tool	Asset Management Tools/AD
1	1.4	Devices	Identify	N/A	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Internal Policies
2	2.1	Applications	Identify	Managed Endpoint	Establish and Maintain a Software Inventory	N/A
2	2.2	Applications	Identify	N/A	Ensure Authorized Software is Currently Supported	N/A
2	2.3	Applications	Respond	Managed Endpoint	Address Unauthorized Software	N/A
2	2.4	Applications	Detect	Managed Endpoint	Utilize Automated Software Inventory Tools	N/A
2	2.5	Applications	Protect	Managed Endpoint	Allowlist Authorized Software	N/A
3	3.1	Data	Identify	Penetration Testing Services	Establish and Maintain a Data Management Process	DLP Solutions
3	3.2	Data	Identify	Penetration Testing Services	Establish and Maintain a Data Inventory	DLP Solutions
3	3.3	Data	Protect	Penetration Testing Services	Configure Data Access Control Lists	DLP Solutions
3	3.4	Data	Protect	Penetration Testing Services	Enforce Data Retention	DLP Solutions
3	3.5	Data	Protect	N/A	Securely Dispose of Data	Internal Policies
3	3.6	Data	Identify	N/A	Encrypt Data on End-User Devices	Internal Policies
3	3.7	Data	Identify	Penetration Testing Services	Establish and Maintain a Data Classification Scheme	DLP Solutions
3	3.8	Data	Protect	N/A	Document Data Flows	Internal Policies
3	3.9	Data	Protect	N/A	Encrypt Data on Removable Media	Internal Policies

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
3	3.10	Devices	Protect	N/A	Encrypt Sensitive Data in Transit	Certificate and Key Management Tools and Internal Policies
3	3.11	Data	Protect	N/A	Encrypt Sensitive Data at Rest	Internal Policies
3	3.12	Network	Protect	N/A	Segment Data Processing and Storage Based on Sensitivity	Internal Policies
4	4.1	Applications	Protect	Penetration Testing Services	Establish and Maintain a Secure Configuration Process	vCISO Activities or Internal Policy Management Methodologies
4	4.2	Network	Protect	Penetration Testing Services	Establish and Maintain a Secure Configuration Process for Network Infrastructure	
4	4.3	Users	Protect	Penetration Testing Services	Configure Automatic Session Locking on Enterprise Assets	
4	4.4	Devices	Protect	Penetration Testing Services	Implement and Manage a Firewall on Servers	
4	4.5	Devices	Protect	Managed Endpoint Penetration Testing Services	Implement and Manage a Firewall on End-User Devices	
4	4.6	Network	Protect	N/A	Securely Manage Enterprise Assets and Software	Internal Policies
4	4.7	Users	Protect	N/A	Manage Default Accounts on Enterprise Assets and Software	Internal Policies
4	4.8	Devices	Protect	N/A	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Internal Policies
4	4.9	Devices	Protect	N/A	Configure Trusted DNS Servers on Enterprise Assets	Internal Policies
4	4.10	Devices	Respond	Penetration Testing Services	Enforce Automatic Device Lockout on Portable End-User Devices	
4	4.11	Devices	Protect	N/A	Enforce Remote Wipe Capability on Portable End-User Devices	Internal Policies

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
5	5.1	Users	Identify	XDRaaS	Establish and Maintain an Inventory of Accounts	Internal Policies/AD Monitoring and Management
5	5.2	Users	Protect	N/A	Use Unique Passwords	Internal Policy Management and Configuration Management
5	5.3	Users	Respond	N/A	Disable Dormant Accounts	Internal Policy Management and Configuration Management
5	5.4	Users	Protect	N/A	Restrict Administrator Privileges to Dedicated Administrator Accounts	Policy and Configuration Management
5	5.5	Users	Identify	XDRaaS	Establish and Maintain an Inventory of Service Accounts	Internal Policies
5	5.6	Users	Protect	N/A	Centralize Account Management	Okta, Ping Other Identity Management Solutions
6	6.1	Users	Protect	N/A	Establish an Access Granting Process	
6	6.2	Users	Protect	N/A	Establish an Access Revoking Process	
6	6.3	Users	Protect	N/A	Require MFA for Externally-Exposed Applications	
6	6.4	Users	Protect	N/A	Require MFA for Remote Network Access	
6	6.5	Users	Protect	N/A	Require MFA for Administrative Access	
6	6.6	Users	Identify	N/A	Establish and Maintain an Inventory of Authentication and Authorization Systems	
6	6.7	Users	Protect	Penetration Testing Services	Centralize Access Control	Okta, Ping Other Identity Management Solutions

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
7	7.1	Applications	Protect	Vulnerability Management Services	Establish and Maintain a Vulnerability Management Process	
7	7.2	Applications	Protect	Penetration Testing Services	Establish and Maintain a Remediation Process	Internal Policies
7	7.3	Applications	Protect	Penetration Testing Services	Perform Automated Operating System Patch Management	Internal Policies
7	7.4	Applications	Identify	Penetration Testing Services	Perform Automated Application Patch Management	vCISO Activities or Internal Policy Management Methodologies
7	7.5	Applications	Identify	Vulnerability Management Services	Perform Automated Vulnerability Scans of Internal Enterprise Assets	
7	7.6	Applications	Respond	Vulnerability Management Services	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	
7	7.7	Applications	Respond	Penetration Testing Services	Remediate Detected Vulnerabilities	
8	8.1	Network	Protect	XDRaaS	Establish and Maintain an Audit Log Management Process	
8	8.2	Network	Detect	Penetration Testing Services	Collect Audit Logs	
8	8.3	Network	Protect	XDRaaS	Ensure Adequate Audit Log Storage	
8	8.4	Network	Detect	N/A	Standardize Time Synchronization	
8	8.5	Network	Detect	XDRaaS	Collect Detailed Audit Logs	
8	8.6	Network	Detect	XDRaaS	Collect DNS Query Audit Logs	
8	8.7	Devices	Detect	XDRaaS	Collect URL Request Audit Logs	
8	8.8	Network	Detect	XDRaaS	Collect Command-Line Audit Logs	
8	8.9	Network	Protect	XDRaaS	Centralize Audit Logs	
8	8.10	Network	Protect	XDRaaS	Retain Audit Logs	
8	8.11	Network	Detect	XDRaaS	Conduct Audit Log Reviews	

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
9	9.1	Applications	Protect	N/A	Ensure Use of Only Fully Supported Browsers and Email Clients	
9	9.2	Network	Protect	Penetration Testing Services	Use DNS Filtering Services	
9	9.3	Network	Protect	Penetration Testing Services	Maintain and Enforce Network-Based URL Filters	
9	9.4	Applications	Protect	N/A	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	
9	9.5	Network	Protect	Penetration Testing Services	Implement DMARC	
9	9.6	Network	Protect	N/A	Block Unnecessary File Types	
10	10.1	Devices	Protect	Managed Endpoint	Deploy and Maintain Anti-Malware Software	
10	10.2	Devices	Protect	Managed Endpoint	Configure Automatic Anti-Malware Signature Updates	
10	10.3	Devices	Protect	Managed Endpoint	Disable Autorun and Autoplay for Removable Media	
10	10.4	Devices	Detect	Managed Endpoint	Configure Automatic Anti-Malware Scanning of Removable Media	
10	10.5	Devices	Protect	Managed Endpoint	Enable Anti-Exploitation Features	
10	10.6	Devices	Protect	Managed Endpoint	Centrally Manage Anti-Malware Software	
10	10.7	Devices	Detect	Managed Endpoint	Use Behavior-Based Anti-Malware Software	
11	11.1	Data	Recover	N/A	Establish and Maintain a Data Recovery Process	
11	11.2	Data	Recover	N/A	Perform Automated Backup Penetration Testing Services	
11	11.3	Data	Protect	N/A	Protect Recovery Data	
11	11.4	Data	Recover	N/A	Establish and Maintain an Isolated Instance of Recovery Data	
11	11.5	Data	Recover	N/A	Test Data Recovery	

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
12	12.1	Network	Protect	Penetration Testing Services	Ensure Network Infrastructure is Up-to-Date	
12	12.2	Network	Protect	Penetration Testing Services	Establish and Maintain a Secure Network Architecture	
12	12.3	Network	Protect	Penetration Testing Services	Securely Manage Network Infrastructure	
12	12.4	Network	Identify	Penetration Testing Services	Establish and Maintain Architecture Diagram(s)	
12	12.5	Network	Protect	Penetration Testing Services	Centralize Network Authentication, Authorization, and Auditing (AAA)	
12	12.6	Network	Protect	Penetration Testing Services	Use of Secure Network Management and Communication Protocols	
12	12.7	Devices	Protect	Penetration Testing Services	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	
13	13.1	Network	Detect	XDRaaS	Centralize Security Event Alerting	
13	13.2	Devices	Detect	XDRaaS	Deploy a Host-Based Intrusion Detection Solution	
13	13.3	Network	Detect	XDRaaS	Deploy a Network Intrusion Detection Solution	
13	13.4	Network	Protect	Penetration Testing Services	Perform Traffic Filtering Between Network Segments	
13	13.5	Devices	Protect	Penetration Testing Services	Manage Access Control for Remote Assets	
13	13.6	Network	Detect	XDRaaS	Collect Network Traffic Flow Logs	
14	14.1	N/A	Protect	Penetration Testing Services	Establish and Maintain a Security Awareness Program	Security Awareness Training and Management
14	14.2	N/A	Protect	Penetration Testing Services	Train Workforce Members to Recognize Social Engineering Attacks	Security Awareness Training and Management
14	14.3	N/A	Protect	Penetration Testing Services	Train Workforce Members on Authentication Best Practices	Security Awareness Training and Management

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
14	14.4	N/A	Protect	Penetration Testing Services	Train Workforce on Data Handling Best Practices	Security Awareness Training and Management
14	14.5	N/A	Protect	Penetration Testing Services	Train Workforce Members on Causes of Unintentional Data Exposure	Security Awareness Training and Management
14	14.6	N/A	Protect	Penetration Testing Services	Train Workforce Members on Recognizing and Reporting Security Incidents	Security Awareness Training and Management
14	14.7	N/A	Protect	Penetration Testing Services	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Security Awareness Training and Management
14	14.8	N/A	Protect	Penetration Testing Services	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Security Awareness Training and Management
14	14.9	N/A	Protect	Penetration Testing Services	Conduct Role-Specific Security Awareness and Skills Training	Security Awareness Training and Management
15	15.1	N/A	Identify	N/A	Establish and Maintain an Inventory of Service Providers	
15	15.2	N/A	Identify	N/A	Establish and Maintain a Service Provider Management Policy	
15	15.3	N/A	Identify	N/A	Classify Service Providers	
15	15.4	N/A	Protect	N/A	Ensure Service Provider Contracts Include Security Requirements	
15	15.4	N/A	Protect	N/A	Ensure Service Provider Contracts Include Security Requirements	
16	16.1	Applications	Protect	N/A	Establish and Maintain a Secure Application Development Process	
16	16.2	Applications	Protect	Penetration Testing Services	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Policy Management and Validation

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
16	16.3	Applications	Protect	Vulnerability Management Services	Perform Root Cause Analysis on Security Vulnerabilities	
16	16.4	Applications	Protect	Vulnerability Management Services	Establish and Manage an Inventory of Third-Party Software Components	
16	16.5	Applications	Protect	N/A	Use Up-to-Date and Trusted Third-Party Software Components	
16	16.6	Applications	Protect	Vulnerability Management Services	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	
16	16.7	Applications	Protect	N/A	Use Standard Hardening Configuration Templates for Application Infrastructure	
16	16.8	Applications	Protect	N/A	Separate Production and Non-Production Systems	
16	16.9	Applications	Protect	Penetration Testing Services	Train Developers in Application Security Concepts and Secure Coding	
16	16.10	Applications	Protect	N/A	Apply Secure Design Principles in Application Architectures	
16	16.11	Applications	Protect	N/A	Leverage Vetted Modules or Services for Application Security Components	
17	17.1	N/A	Respond	Penetration Testing Services	Designate Personnel to Manage Incident Handling	
17	17.1	N/A	Respond	XDRaaS/ Penetration Testing Services	Designate Personnel to Manage Incident Handling	
17	17.2	N/A	Respond	XDRaaS	Establish and Maintain Contact Information for Reporting Security Incidents	Penetration Testing Services and Internal Security Team Involvement

CIS Control	CIS Sub-Control	Asset Type	Security Function	CyFlare Solution Mapping	Title	Other Solutions
17	17.3	N/A	Respond	XDRaaS	Establish and Maintain an Enterprise Process for Reporting Incidents	Penetration Testing Services and vCISO Involvement in Policy Level Communication, Maintenance and Management
17	17.3	N/A	Respond	Penetration Testing Services	Establish and Maintain an Enterprise Process for Reporting Incidents	Security Awareness Training and Management
17	17.4	N/A	Respond	Penetration Testing Services/XDRaaS	Establish and Maintain an Incident Response Process	
17	17.4	N/A	Respond	Penetration Testing Services	Establish and Maintain an Incident Response Process	vCISO Activities or Internal Policy Management Methodologies
17	17.5	N/A	Respond	Penetration Testing Services	Assign Key Roles and Responsibilities	vCISO Activities or Internal Policy Management Methodologies
17	17.5	N/A	Respond	Penetration Testing Services	Assign Key Roles and Responsibilities	
17	17.6	N/A	Respond	XDRaaS	Define Mechanisms for Communicating During Incident Response	Internal Policies
17	17.7	N/A	Recover	Penetration Testing Services	Conduct Routine Incident Response Exercises	Internal Policies and Procedures
17	17.8	N/A	Recover	XDRaaS	Conduct Post-Incident Reviews	Internal Policies and Procedures
18	18.1	N/A	Identify	Penetration Testing	Establish and Maintain a Penetration Testing Program	
18	18.2	Network	Identify	Penetration Testing	Perform Periodic External Penetration Tests	
18	18.3	Network	Protect	Penetration Testing Services	Penetration Test Findings	

Contact us to learn more!

600 Fishers Station Drive
Suite 125
Victor, NY 14564

1 (877) 729-3527

sales@cyflare.com
www.cyflare.com