Blueprint for Ransomware Defense

Original Blueprint for Ransomware Defense CIS Safeguards Mapped to the NIST 2.0 Security Functions

Category	CIS Safeguard #	NIST Security Function	CIS Safeguard Title	Type
Govern				
Governance	3.1	Govern	Establish and Maintain a Data Management Process	Foundational
	4.1	Govern	Establish and Maintain a Secure Configuration Process	Foundational
	4.2	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Foundational
	6.1	Govern	Establish an Access Granting Process	Foundational
	6.2	Govern	Establish an Access Revoking Process	Foundational
	7.1	Govern	Establish and Maintain a Vulnerability Management Process	Foundational
	7.2	Govern	Establish and Maintain a Remediation Process	Foundational
	8.1	Govern	Establish and Maintain an Audit Log Management Process	Foundational
	11.1	Govern	Establish and Maintain a Data Recovery Process	Foundational
	14.1	Govern	Establish and Maintain a Security Awareness Program	Foundational
	17.2	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	Actionable
	17.3	Govern	Establish and Maintain an Enterprise Process for Reporting Incidents	Foundational
Identify				
Know Your Environment	1.1	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Foundational
	2.1	Identify	Establish and Maintain a Software Inventory	Foundational
	2.2	Identify	Ensure Authorized Software is Currently Supported	Actionable
	5.1	Identify	Establish and Maintain an Inventory of Accounts	Foundational
Protect				
Secure Configurations	4.4	Protect	Implement and Manage a Firewall on Servers	Actionable
	4.7	Protect	Manage Default Accounts on Enterprise Assets and Software	Actionable
Account and Access Management	5.2	Protect	Use Unique Passwords	Actionable
	5.3	Protect	Disable Dormant Accounts	Actionable
	5.4	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Actionable
	6.3	Protect	Require MFA for Externally-Exposed Applications	Actionable
	6.4	Protect	Require MFA for Remote Network Access	Actionable
	6.5	Protect	Require MFA for Administrative Access	Actionable
Vulnerability Management Planning	7.3	Protect	Perform Automated Operating System Patch Management	Actionable
	7.4	Protect	Perform Automated Application Patch Management	Actionable
	12.1	Protect	Ensure Network Infrastructure is Up-to-Date	Actionable
Malware Defense	9.1	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Actionable
	9.2	Protect	Use DNS Filtering Services	Actionable
	10.2	Protect	Configure Automatic Anti-Malware Signature Updates	Actionable
	10.3	Protect	Disable Autorun and Autoplay for Removable Media	Actionable
Security Awareness & Skills Training	14.2	Protect	Train Workforce Members to Recognize Social Engineering Attacks	Actionable
	14.6	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	Actionable
Data for Response and Recovery	8.3	Protect	Ensure Adequate Audit Log Storage	Actionable
	11.3	Protect	Protect Recovery Data	Actionable
Detect				
Detect	8.2	Detect	Collect Audit Logs	Actionable
	10.1	Detect	Deploy and Maintain Anti-Malware Software	Actionable
Respond				
Incident Response	17.1	Respond	Designate Personnel to Manage Incident Handling	Actionable
Recover				
Data Recovery	11.2	Recover	Perform Automated Backups	Actionable
	11.4	Recover	Establish and Maintain an Isolated Instance of Recovery Data	Actionable