mimecast

How Incydr Supports Compliance and Meets Security Framework Controls

Supported frameworks:

CIS Critical Security Controls Version 8
CIS Controls

The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, working from home, and changing attacker tactics prompted the update, which supports enterprise security as companies move to fully cloud or hybrid environments.

Learn about CIS Controls v8

NIST 800

NIST 800 deals with computer security and is commonly used in the United States. Both 800-171 and 800-53 deal specifically with guidelines for securing and protecting data, often called, “Controllled Unclassified Information [CUI].” 800-53, though, is the working standard for the Federal Government. Both provide organizations with a set of security requirements intended to protect data, maintain data privacy and confidentiality, and build resilience.

Learn about NIST 800-171 r2

Learn about NIST 800-53 r5

NIST National Institute of Standards and Technology

ISO – ISO/IEC 27002:2022

The ISO and IEC work together to develop international standards, and in 27002, they focus on standards for cybersecurity, information security, and data protection. Their guidance for data risk mitigation is important for organizations that do business internationally and for organizations developing the maturity of their risk management program.

Learn about ISO/IEC 27002:2022

mimecast

Security framework control map

CONTROL FAMILY	HOW INCYDR ADDRESSES THIS CONTROL	FRAMEWORK	CONTROL ID
Data Protection	Incydr is a data protection solution that allows you to detect, investigate, and respond to data exposure and exfiltration from corporate computer, cloud, and email systems. Incydr gives you the visibility, context, and controls needed to stop valuable data from going to untrusted locations, including blocking where applicable.	CIS CSC v8	– 3.13 Deploy a Data Loss Prevention Solution*
		ISO 27002:2022	– 8.12 Data Leakage Prevention
		NIST 800-53	– AC-4 (3) Information Flow Enforcement | Dynamic – Information Flow Control* – AC-20 Use of External Systems* – AC-21 Information Sharing* – IR-9 Information Spillage Response* – SC-7 (10) Boundary Protection | Prevent Exfiltration*
		NIST 800-171	– 3.1.20 Access Control*
Insider Risk	Incydr provides detailed information to manage and support investigations for incidents involving insiders. Incydr's case management retains file activity details, allows access to file contents, provides space to summarize findings and recommended actions, and can be quickly exported to communicate with relevant stakeholders. Incydr's Expert Services offerings include support for the development of an insider threat program.	NIST 800-53	– IR-4 (6) Incident Handling | Insider Threats – IR-4 (7) Incident Handling | Insider Threats - Intraorganization Coordination – PM-12 Insider Threat Program

mimecast

CONTROL FAMILY	HOW INCYDR ADDRESSES THIS CONTROL	FRAMEWORK	CONTROL ID
Monitor & Alert	Incydr monitors data movement across users and channels, including unsanctioned cloud collaboration platforms. Technical preventative controls are available to respond to unsanctioned movement. Incydr detects anomalous user behavior by pinpointing deviations from baseline behaviors such as off-hours file activity, the first use of a destination, and rare use of a destination. The risk settings for Incydr Risk Indicators and alerts can be adjusted to changing risk tolerance.	ISO 27002:2022	– 6.7 Remote Working* – 8.16 Monitoring Activities*
		NIST 800-53	– AC-2 (11) Account Management | Usage Conditions* – AC-2 (12) Account Management | Account Monitoring for Atypical Usage* – AU-13 Monitoring for Information Disclosure* – SI-4 System Monitoring* – SI-4 (5) System Monitoring | System-generated alerts* – SI-4 (7) System Monitoring | Automated Response to Suspicious Events* – SI-4 (24) System Monitoring | Indicators of Compromise*
		NIST 800-171	– 3.13.1 System & Communications Protection* – 3.14.6 System & information Integrity* – 3.14.7 System & Information Integrity*
Watchlist	Incydr closely monitors users of similar risk levels using Watchlist groups, which can be automated with IAM, PAM, and HRIS.	NIST 800-53	– SI-4 (19) System Monitoring | Risks for Individuals* – SI-4 (20) System Monitoring | Privileged Users* – SI-4 (21) System Monitoring | Probationary Periods*
Storage Media	Incydr can detect, block, and alert on file activity to/ from storage media.	ISO 27002:2022	– 7.10 Storage Media*
		NIST 800-53	– MP-2 Media Access* – MP-7 Media Use*
		NIST 800-171	– 3.1.21 Access Control* – 3.8.1 Media Protection* – 3.8.7 Media Protection*

mimecast

CONTROL FAMILY	HOW INCYDR ADDRESSES THIS CONTROL	FRAMEWORK	CONTROL ID
Awareness & Training	Instructor includes security awareness and Insider Risk video lessons. Instructor's integration with Incydr provides training as a corrective response control through recorded micro-trainings that provide just-in-time training to correct user behavior.	CIS CSC v8	– 14.2 Train Workforce Members to Recognize Social Engineering Attacks* – 14.4 Train Workforce on Data Handling Best Practices* – 14.5 Train Workforce on Causes of Unintentional Data Exposure* – 14.6 Train Workforce Members on Recognizing and Reporting Security Incidents*
		ISO 27002:2022	– 6.3 Information security awareness, education and training*
		NIST 800-53	– AT-2 Literacy Training & Awareness* – AT-2 (2) Literacy Training and Awareness | Insider Threat* – AT-2 (3) Literacy Training and Awareness | Social Engineering and Mining* – AT-2 (4) Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior*
		NIST 800-171	– 3.2.1 Awareness & Training* – 3.2.3 Awareness & Training*
Audit	Incydr provides detailed information at a user level and file metadata level.	NIST 800-171	– 3.3.2 Audit & Accountability*

*Mimecast Incydr partially covers this requirement

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.