cyera

Deliver Cybersecurity Maturity Model Certification 2.0 Compliance

Manage security risks of Controlled Unclassified Information (CUI)

Defense Industrial Base contractors are tasked with protecting national security interests. Cyera enables you to achieve Cybersecurity Maturity Model Certification (CMMC) 2.0 compliance by securing CUI and other sensitive data across your multi and hybrid cloud domains.

Support CMMC Readiness with Cyera

Understand CUI risks and enforce appropriate controls to minimize data exposure so that you can confidently implement the CMMC model.

Maintain a comprehensive CUI data inventory

Create a dynamic inventory of CUI and other regulated data, highlighting data risks including the number of records, their sensitivity, and insight into what the data represents

Enforce appropriate access controls

Leverage Cyera to get full visibility into data exposure stemming from misconfigurations, stale users, and overly permissive access, enabling you to achieve least privileged, secure access

Ensure audit and accountability readiness

Cyera's policy framework continuously analyzes the structured, semi-structured, and unstructured data, ensuring that the appropriate logging is in place so that auditable events are available for reporting

Strengthen configuration management

Harden your security posture against data store misconfigurations and errors that could lead to public exposure, misuse, and loss of CUI

Improve incident handling capabilities

Immediately understand the potential blast radius of a threat signal to proactively address vulnerabilities and limit the impact of a breach

Harden your security posture to prevent breaches

Continuously scan for vulnerabilities in data stores that could lead to data breaches, with workflow automation to quickly resolve issues

Critical data security requirements under CMMC

Access Control

Limit access to authorized users and control information posted on publicly accessible information systems

Audit and Accountability

Ensure the use of audit logs to monitor unauthorized system activity, user actions, and data deletion

Configuration Management

Establish, maintain, and enforce security configurations for information systems

Identification and Authentication

Enforce password complexity and cryptographic protection of passwords and prohibit password reuse

Incident Response

Establish incident handling capabilities for information systems including preparation, analysis, recovery, and response activities

Media Protection

Protect, limit access to, and identify systems containing CUI and other regulated data

Risk Assessment

Assess risks, scan for vulnerabilities, and remediate issues affecting organization assets and systems

System Assessment

Periodically assess the security controls in organization systems

System and Communications Protection

Prevent unauthorized information transfer and protect the confidentiality of CUI at rest

System and Information Integrity

Scan, monitor, and identify information system risks and take action on security alerts

About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure and delivers automated remediation to reduce their attack surface. Learn more at www.cyera.io or follow Cyera on LinkedIn.

Backed by the best:

SEQUOIA Accel cyberstarts

WINNER 2022 CISO CHOICE AWARDS Data Security CYERA

AICPA SOC

ISO 27001 Certified

GDPR

CCPA

www.cyera.io • info@cyera.io