

8.1. Regulatory Frameworks Supported

The Spectra360 Security Operations Center (SOC) platform is designed to align with a variety of prominent cybersecurity regulatory frameworks, ensuring comprehensive compliance and robust security posture for organizations across different industries. Key frameworks supported by Spectra360 include:

1. NIST Cybersecurity Framework (NIST CSF):

- Developed by the National Institute of Standards and Technology, the NIST CSF provides a structured approach to managing and mitigating cybersecurity risks. It is widely adopted across various sectors for its comprehensive guidelines on identifying, protecting, detecting, responding to, and recovering from cyber threats.

2. ISO/IEC 27001 and ISO/IEC 27002:

- These international standards offer best practice recommendations for information security management systems (ISMS). ISO/IEC 27001 focuses on establishing, implementing, maintaining, and continually improving an ISMS, while ISO/IEC 27002 provides guidelines for organizational information security standards and information security management practices.

3. General Data Protection Regulation (GDPR):

- Enforced by the European Union, GDPR sets stringent requirements for the protection of personal data. Organizations handling data of EU citizens must comply with its regulations, which include ensuring data security and reporting breaches promptly.

4. Health Insurance Portability and Accountability Act (HIPAA):

- In the United States, HIPAA establishes national standards for the protection of sensitive patient health information. Organizations in the healthcare sector must implement measures to safeguard electronic health records and ensure patient confidentiality.

5. Payment Card Industry Data Security Standard (PCI DSS):

- This standard applies to entities that handle credit card information. It mandates specific security measures to protect cardholder data, including maintaining secure networks, implementing strong access control measures, and regularly monitoring and testing networks.

6. Federal Information Security Management Act (FISMA):

- Applicable to federal agencies and contractors in the United States, FISMA requires the implementation of comprehensive information security programs to protect government information and assets against natural or man-made threats.

7. Sarbanes-Oxley Act (SOX):

- Primarily focused on financial reporting, SOX also encompasses aspects of information security, requiring organizations to establish controls and procedures to ensure the integrity and confidentiality of financial data.

Revision #2

Created 9 February 2025 21:05:14 by Admin

Updated 10 February 2025 10:51:21 by Admin