Kiteworks

COMPLIANCE BRIEF

EU Cyber Resilience Act Compliance Enablement

Kiteworks Provides Comprehensive Security Management for Products With Digital Elements

The Cyber Resilience Act introduces cybersecurity requirements for products with digital elements placed on the EU market. It aims to improve the security of hardware and software products throughout their life cycle and enable users to consider cybersecurity when selecting and using digital products. Key provisions include essential cybersecurity requirements for manufacturers regarding product design, development, and vulnerability management; conformity assessment procedures, including third-party assessment for critical products; transparency obligations on security properties and updates; and market surveillance and enforcement mechanisms. The Act applies to all connectable hardware and software products, with some exceptions. Noncompliance with the EU Cyber Resilience Act can result in severe financial penalties, with fines of up to €15 million or 2.5% of global annual turnover, whichever is higher. Beyond monetary consequences, noncompliant organizations may face market access restrictions, reputational damage, and increased regulatory scrutiny, potentially leading to significant business disruptions and loss of competitive advantage in the EU market. The Act aims to create a coherent EU framework and prevent fragmented national rules, while enhancing security and user trust in digital products.

Cybersecurity Risk Assessment and Management With a Secure-by-Design Platform

The CRA mandates comprehensive cybersecurity risk assessments for products with digital elements throughout their life cycle. This involves identifying vulnerabilities, implementing security measures, continuous updating, and adhering to "secure-by-design" principles. Kiteworks supports compliance through its secure software development life cycle, which includes internal and external testing, code reviews, penetration testing, and bug bounty programs. The company vets third-party dependencies, maintains an updated software bill of materials, and regularly checks for vulnerabilities. Kiteworks implements best practices like OWASP standards, least-privilege access, and defense-in-depth strategies. A dedicated security team manages ongoing vulnerability assessment and mitigation, ensuring proactive cybersecurity risk management throughout the product life cycle. This approach allows Kiteworks to stay ahead of potential threats, continuously improve product security, and provide customers with robust, compliant solutions that meet the stringent requirements of the CRA and other cybersecurity regulations.

Solution Highlights

- Secure development life cycle
- Continuous testing
- Least-privilege defaults
- Real-time logging
- One-click updates
- CISO Dashboard

Incident Reporting and Vulnerability Management Via Real-time Logging and Efficient Updates

Vulnerability Management and Incident Reporting form another critical set of controls. The CRA directs strict reporting requirements, including notifying ENISA of security incidents or actively exploited vulnerabilities within 24 hours of discovery. With comprehensive, real-time logging and SIEM integration, enabling rapid detection and response, Kiteworks supports compliance. The platform maintains a continuous vulnerability testing cycle, including automated and manual penetration testing, bug bounty programs, and third-party audits. Kiteworks' one-click update system ensures swift deployment of security patches across clustered environments. These features, combined with clear vulnerability disclosure processes and management mechanisms, enable organizations to efficiently address and mitigate cybersecurity threats, aligning with CRA requirements for timely response and vulnerability remediation. The platform's consolidated audit logs capture all security-related activities without throttling, providing a robust foundation for incident analysis and reporting. Additionally, Kiteworks' software bill of materials, visible to administrators with appropriate privileges, enhances transparency and facilitates thorough vulnerability management across the product's components and dependencies.

Immutable Audit Logs Provide Comprehensive Documentation and Transparency

Documentation and Transparency controls require manufacturers to provide comprehensive technical documentation, clear user instructions, and ensure products bear the CE marking indicating CRA compliance. They must maintain records of compliance and any issues that arise, and cooperate with market surveillance authorities by providing necessary information upon request. These measures promote accountability and enable effective oversight of cybersecurity practices. The platform provides a visible software bill of materials in the admin console for authorized administrators. Adhering to industry standards like NIST CSF, Kiteworks implements robust asset management, access controls, and logging capabilities. The system offers detailed audit logs, SIEM integration, and a CISO Dashboard for effective oversight. Kiteworks maintains thorough documentation of its secure software development life cycle, ensuring the availability of necessary technical documentation and user instructions. This approach facilitates the provision of comprehensive compliance records, promoting accountability and enabling cooperation with market surveillance authorities. By offering clear, accessible information and maintaining detailed records, Kiteworks helps organizations meet CRA transparency requirements and demonstrate ongoing compliance.

Kiteworks provides a robust platform that aligns with the EU Cyber Resilience Act's requirements, offering comprehensive security management for products with digital elements. Through its secure software development life cycle, continuous testing, and proactive security measures, Kiteworks ensures ongoing risk assessment and management. The platform's real-time logging, SIEM integration, and efficient update system support rapid incident reporting and vulnerability management. Kiteworks' visible software bill of materials, adherence to industry standards like NIST CSF, and detailed audit logs facilitate comprehensive documentation and transparency. These features collectively enable organizations to meet CRA compliance requirements, from secure design principles to incident reporting and thorough documentation. By implementing Kiteworks, businesses can confidently navigate the complex landscape of cybersecurity regulations, mitigate risks, and maintain a competitive edge in the EU market while avoiding potential penalties and reputational damage associated with noncompliance.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.