1. Cybersecurity & Risk: Overview

The **Cybersecurity & Risk** module serves as the central hub for all security operations within your environment, providing a unified platform to safeguard system integrity and protect sensitive data. By integrating multiple layers of defense and proactive monitoring tools, Security Core enables your organization to anticipate, detect, and respond to threats in real time.

Security Core includes the following sections:

1. Incident Reports
2. Violation Reports
3. Malware Reports
4. Penetration Reports

Benefits at a Glance

1. **Holistic Visibility:** Correlate data across incidents, vulnerabilities, malware events, and testing results to identify systemic weaknesses and emerging attack vectors.
2. **Faster Response:** Automated alerts, playbooks, and remediation tools reduce mean time to detect (MTTD) and mean time to respond (MTTR).
3. **Regulatory Compliance:** Maintain comprehensive logs, audit trails, and evidence of controls to satisfy GDPR, HIPAA, PCI DSS, and other industry mandates.
4. **Continuous Improvement:** Ongoing vulnerability scans and regular pen tests feed back into your security strategy, driving a cycle of assessment, remediation, and validation.

Use Cases

#1. Security Assurance
Detects and manages vulnerabilities to prevent security breaches, ensuring system integrity.

#2. Operational Continuity
Minimizes disruptions by quickly identifying and resolving issues, maintaining business operations.

#3. Improved Collaboration
Facilitates seamless tracking and assignment of tasks among teams, enhancing efficiency.

#4. Root Cause Analysis
Collects closure details for lessons learned, helping prevent similar incidents in the future.

Security Core ensures robust protection by providing structured workflows for detecting, tracking, and resolving security threats across the ecosystem.

Revision #16
Created 27 February 2025 08:42:50
Updated 27 January 2026 12:06:03