

Aug 2024

Rapid7-Compliance Powerplay

NIS2, ISO 27001 & DORA



Requirements

Standards

Rapid7



Patch and vulnerability management, protection against unauthorized software, secure configuration of IT systems

- NIS2 9a, 9c, 9e, 9j
- ISO27002:2022 8.8
- DORA Art 9, Art 24

- Attack Surface Management (Surface Command)
- Vulnerability Management (**InsightVM**)
- Cloud Native Security Platform (**InsightCloudSec**)
- Dynamic Application Testing (**InsightAppSec**)
- [Top 25 Remediations Report](#)
- [Critical Security Controls Assessment](#)
- [Cloud Vulnerability Management](#)
- [View Risk Across Cloud and On-Prem Environments](#)
- [Web application Vulnerability Details](#)

Asset Management

- NIS2 4
- ISO27002:2022 5.9
- DORA Art 8

- Attack Surface Management (Surface Command)
- SIEM / XDR / Intrusion Detection & Response (InsightIDR)
- Vulnerability Management (**InsightVM**)
- Cloud Native Security Platform (**InsightCloudSec**)
- [Rapid7 List of Report Templates for Asset & VM Reports](#)
- [Cloud Inventory](#)
- [Assets Overview](#)

Monitoring and logging

- NIS2 11b
- ISO 27002:2022 8.15
- DORA Art 10

- SIEM / XDR / Intrusion Detection & Response (InsightIDR)

Detection of attacks

- NIS2 11d
- ISO 27002:2022 8.16
- DORA Art 10

- SIEM / XDR / Intrusion Detection & Response (InsightIDR)
- Cloud Native Security Platform (**InsightCloudSec**)
- Dynamic Application Testing (**InsightAppSec**)
- [Security Posture Assessment Report](#)
- [D&R Readiness Assessment Report](#) (page 3)
- [Cloud Threat Finding](#)
- [Web Application Attack Replay](#)

Response to attacks

- NIS2 11e
- ISO 27002:2022 5.25, 5.26
- DORA Art 11

- Security Orchestration & Response (**InsightConnect**)
- [IR Planning Workshop](#) (page 2)
- [Incident Response Report](#)

Reporting of attacks (to authorities)

- NIS2 11c
- ISO 27002:2022 5.26
- DORA Art 19

- Security Orchestration & Response (**InsightConnect**)

What's Included: Exposure Command

EXPOSURE COMMAND ADVANCED	
ATTACK SURFACE MANAGEMENT	
Asset Discovery & Unified Inventory	✓
Attack Surface Visibility including Identities, Software and Controls	✓
Asset Enrichment with Security Context	✓
Blast Radius Mapping with Asset Graph	✓
Built-In Automation and Policy Enforcement	✓
External Attack Surface Discovery	✓
Attack Surface Validation (Coming Soon)	Add-On
EXPOSURE MANAGEMENT	
↳ Cloud Security	
Multi-cloud Visibility Across AWS, Azure, GCP and K8s	✓
Cloud and Container Vulnerability Assessment	✓
Best Practices Configuration Assessment including CIS	✓
Contextual Risk Prioritization (Layered Context)	✓
Attack Path Analysis	✓
Notifications and Integrations	✓
Extended Cloud Visibility (Oracle Cloud Infrastructure, Alibaba Cloud)	✓
100s of out-of-the-box Compliance Policies and Industry Standards	✓
Infrastructure as Code (IaC) Scanning	✓
Effective and Least Privilege Access (LPA) Management	✓
Cloud Threat Detection	✓
Automated Cloud Remediation (BotFactory)	✓
↳ On-Prem Vulnerability Management	
Discovery, Vulnerability and Policy Scanning	✓
Agent-based Vulnerability and Policy Assessment	✓
Dynamic Asset Tagging with Criticality Rating	✓
Threat Aware Active Risk Score	✓
Customizable Live Dashboards and Reporting	✓
Remediation Workflows	✓
Goals & SLAs	✓
↳ Application Security	
Dynamic Application Security Testing (DAST)	✓
↳ Shared Analytics	
Executive Risk View	✓
Remediation Hub (Coming Soon)	✓
Bulk Data Export API (Coming Soon)	✓
EXTENSIBILITY AND WORKFLOW AUTOMATION	
450+ Out-of-the-Box Integrations with Security and ITOps Tools	✓
Security Orchestration, Automation and Response (SOAR)	✓
ONBOARDING EXPERIENCES	
Attack Surface Management	
Cloud Security	2 days
On-Prem Vulnerability Management	2 days