exein

Exein Analyzer
Product Overview

Our products

Exein provides a **complete, end-to-end platform** for security and compliance for Linux, Docker and IDF devices.

Platform support (growing):

Linux 🐧
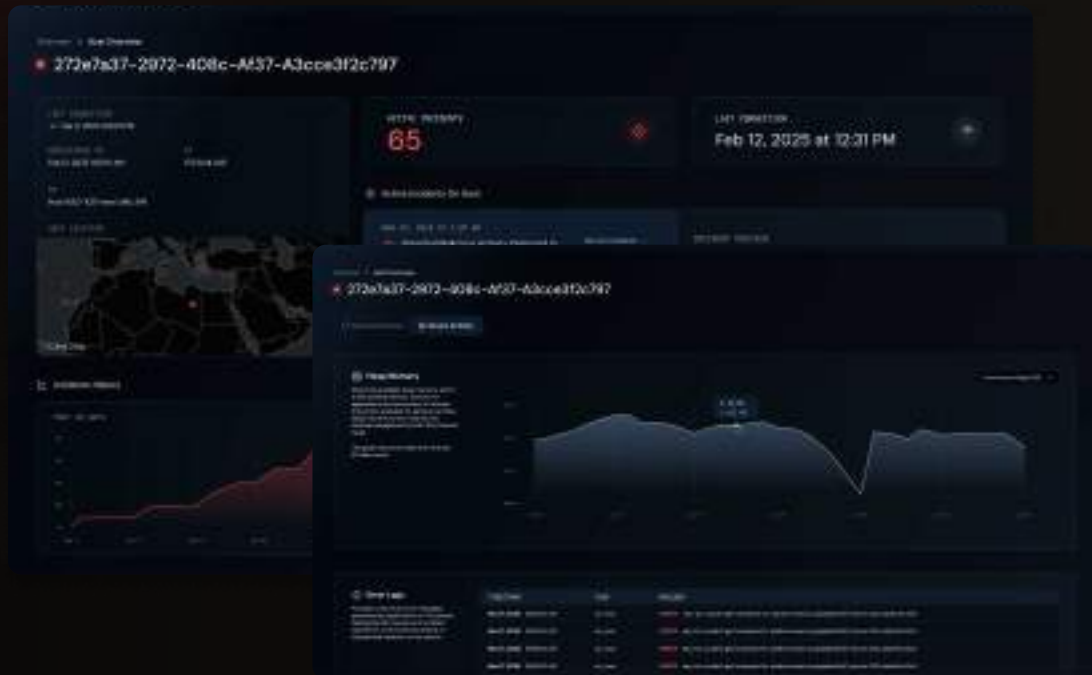
⟫ ESPRESSIF IDF

🐳 docker®

Exein **Analyzer**

Advanced firmware security and compliance analysis for Linux, Docker or ESP IDF devices: identifying vulnerabilities, ensuring compliance readiness, and automating regulatory documentation.

Exein **Runtime**

Real-time threat protection for Linux and ESP32 devices—proactively detecting, blocking, and responding to attacks across your entire fleet using AI-powered behavioral analysis.
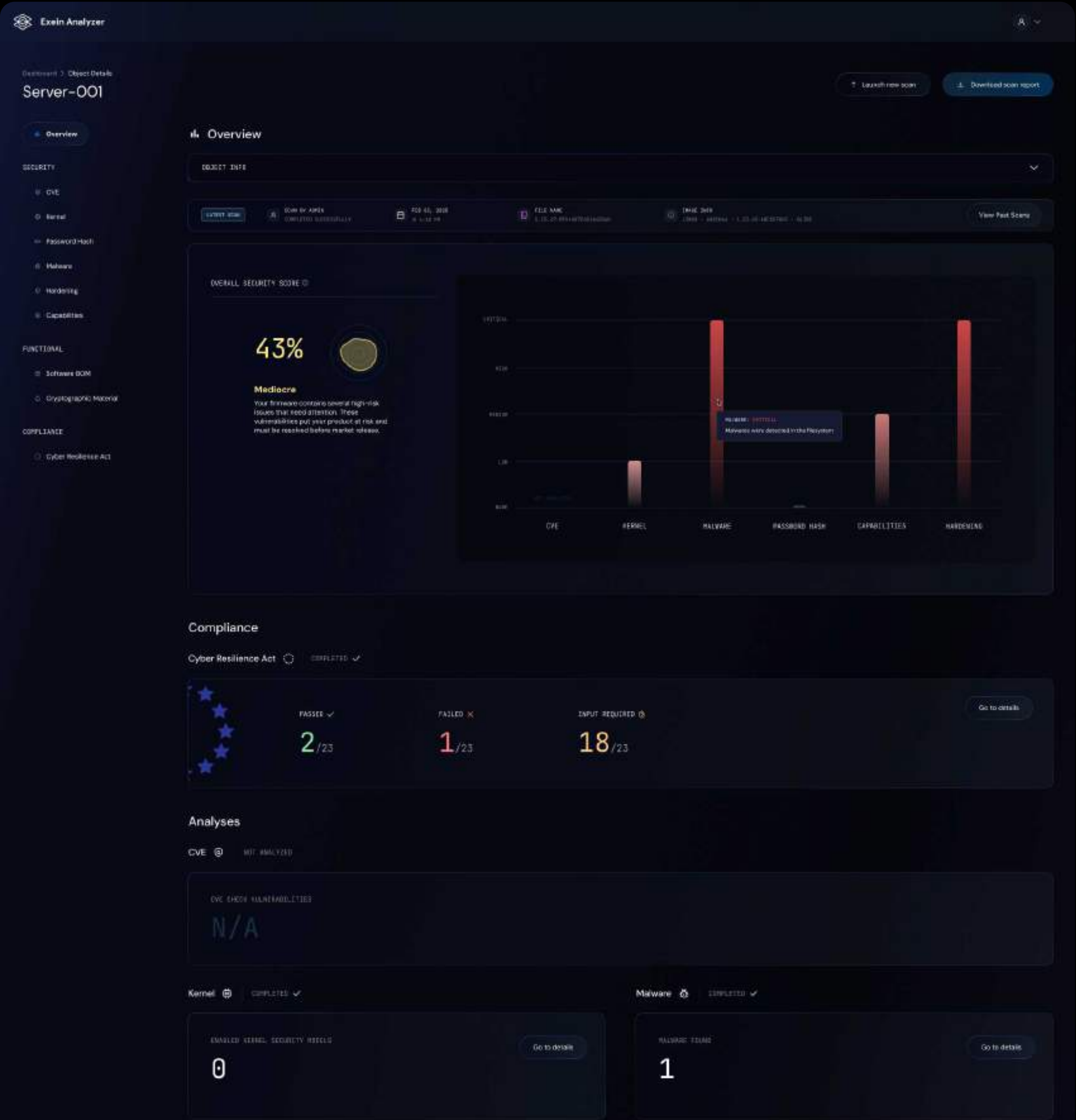
Exein Analyzer

Pre-market validation and security analysis

Detects known CVEs, misconfigurations, and supply chain risks
without source code access

- Comprehensive SBOM generation covering all
  dependencies

- Cryptographic weakness identification (weak
  passwords, insecure certificates)

- Kernel hardening and binary security assessment

- Ensures no product ships with known exploitable
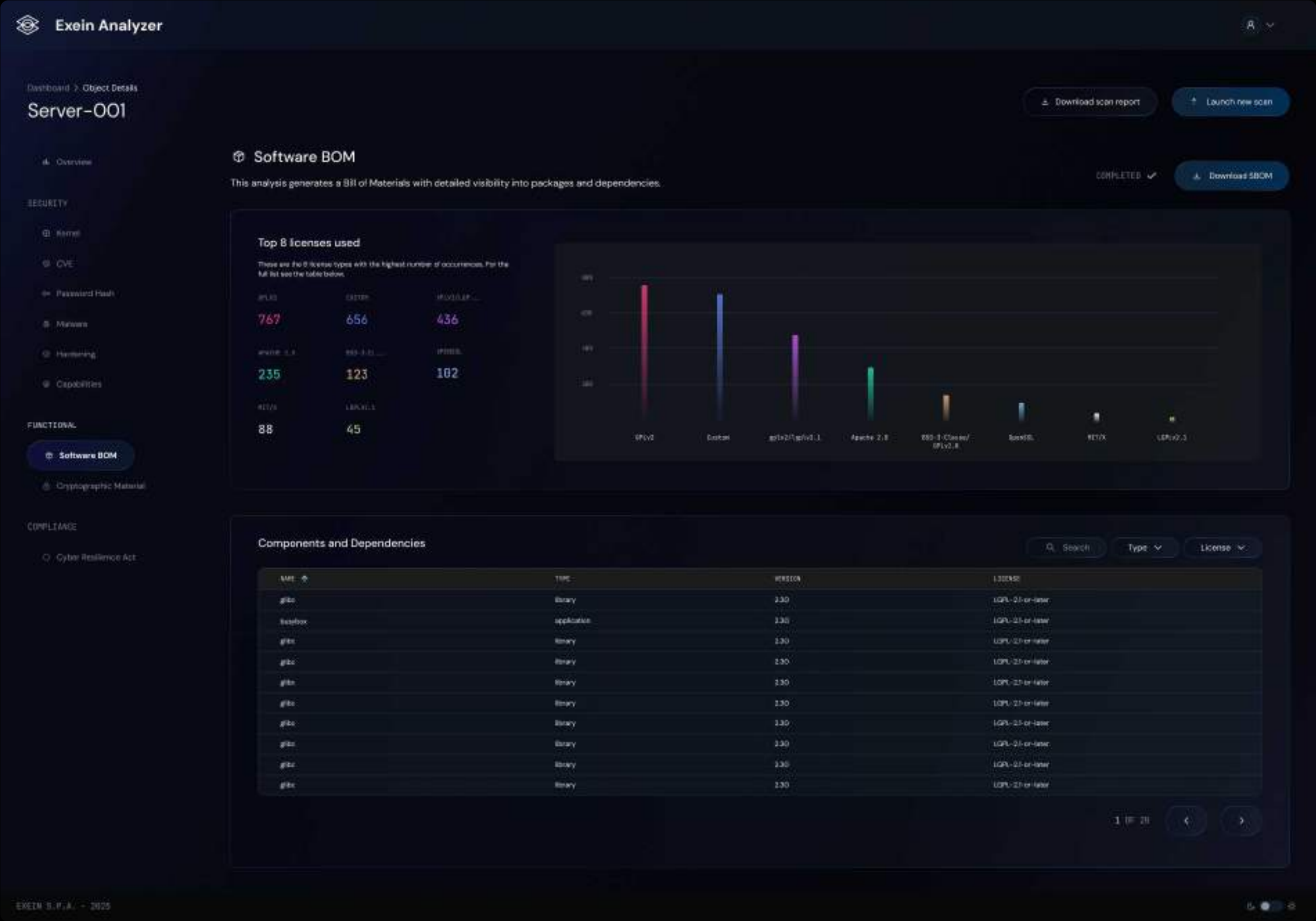 vulnerabilities

Exein Analyzer

Automated SBOM generation

Creates software bill of materials covering all dependencies in machine-readable formats required by regulators

- Exports in CycloneDX formats

- Complete dependency mapping

- Automated vulnerability checks against several databases

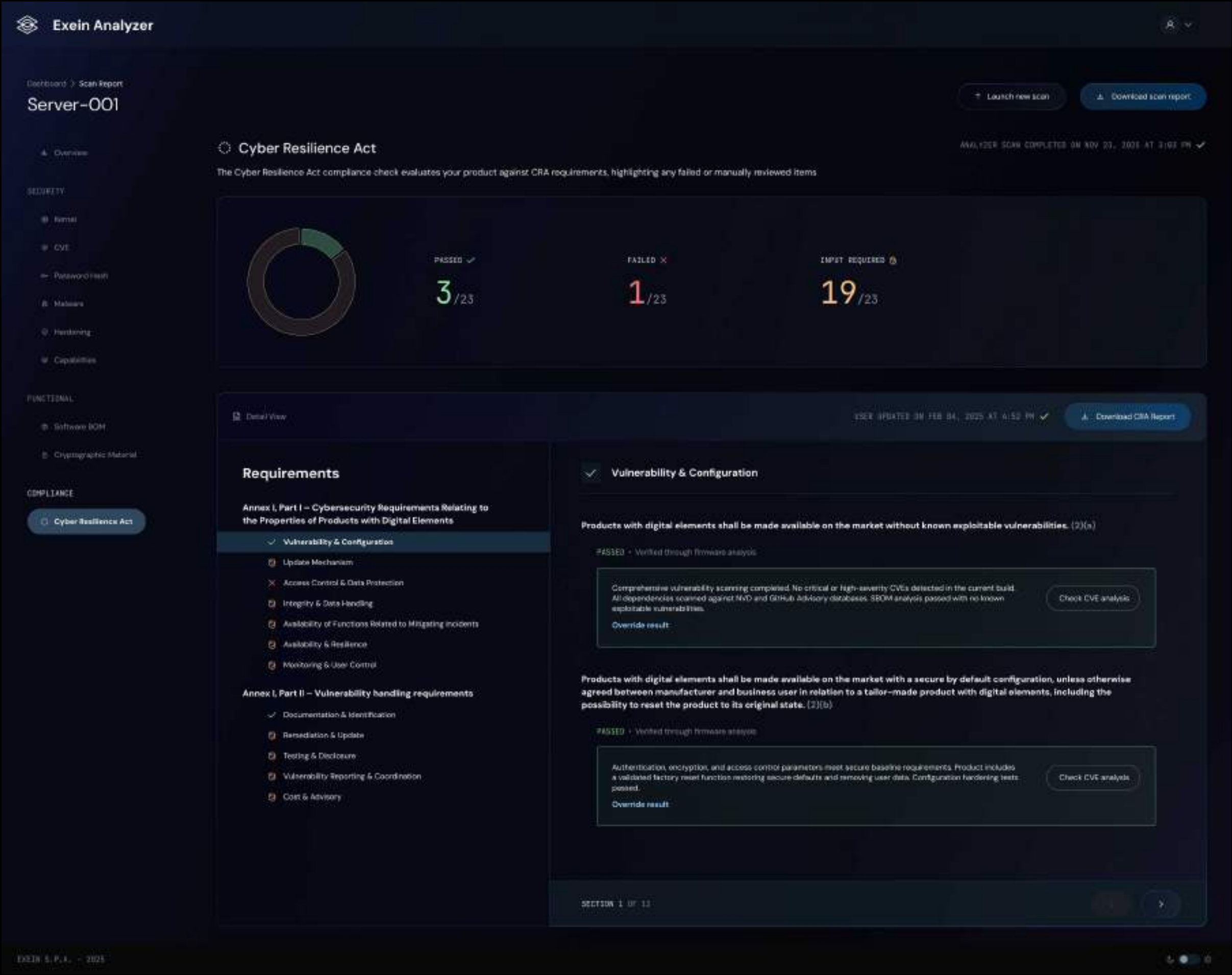- Helps satisfy CRA Part II (1) documentation requirements

Exein Analyzer

Compliance readiness check

Automatically validates firmware against CRA requirements and identifies where manual input is needed

- Maps technical evidence to CRA Part I and Part II requirements

- Highlights compliance gaps with actionable remediation guidance

- Exportable reports in audit-ready formats

- In the future, will support other compliance frameworks and additionally product documentation analysis

VISIT US AT EXEIN.IO