NETRISE

Enabling CJIS Compliance

With the NetRise Platform

The Criminal Justice Information Services (CJIS) Security Policy is a document outlining security requirements for handling protected information within criminal justice information systems. Adherence to CJIS is essential for criminal justice agencies and their vendors. One key aspect of compliance is firmware security, which necessitates comprehensive software component vulnerability identification and efficient remediation. The NetRise Platform enables criminal justice organizations to effectively demonstrate the security of their environment.

Key Benefits of the NetRise Platform

Firmware Analysis & Security

- Gain insights into shared vulnerabilities across firmware images
- Reduce the time investment and cost of firmware security programs
- Answer critical questions about device vulnerabilities, compliance, and backdoors

Risk & Vulnerability Management

- Go beyond CVEs, track key factors like known exploits by threat actors
- Prioritize risks effectively and reduce response time

Remediation Enablement

- Focus remediation efforts on the greatest exposures
- Deprioritize vulnerabilities which don't pose an immediate threat

Asset Build Assurance

- Assess the risks of asset builds before deployment, enabling safer patching and procurement
- Enhance compliance efforts by avoiding unsecure software components

Supply Chain Risk Management

Effective Supply Chain Risk Management (SCRM) relies on deep binary analysis of firmware and accurate Software Bills of Materials (SBOMs).

The NetRise Platform simplifies this process by continuously assessing risks and vulnerabilities within software and firmware, prioritizing risks based on exploitability. NetRise's risk scoring enables quicker and more impactful remediations. This assessment includes factors like the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog and other key indicators of exploitability.

netrise.io | sales@netrise.io