

# Exiger Software Supply Chain Risk Management

Illuminate risk wherever you have software, including IT, OT, and IoT devices – with or without an SBOM.

## Gain Total Visibility of Your Software Supply Chain



### Generate

SBOMs from software and firmware binaries without contractual modifications or source code.



### Validate

the completeness and accuracy of internal or third-party SBOMs.



### Analyze

SBOMs for known and unknown vulnerabilities.



### Monitor

SBOMs and their components continuously.

## Identify and Prioritize Risks Outside of Known Vulnerabilities

By the time you have identified known vulnerabilities (CVE), you're already 8-12 months behind. Ion Channel goes beyond checking for known vulnerabilities or binary analysis that limit many SCA tools and vulnerability detectors.

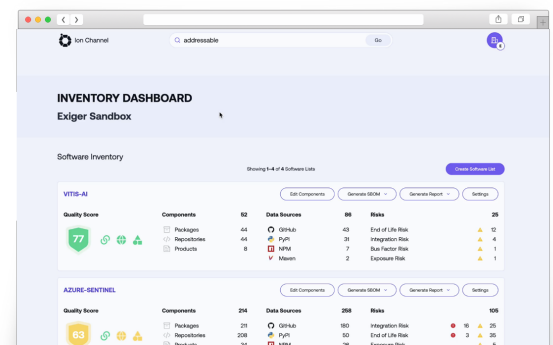
Ion Channel identifies supplier risks in software with no known or published vulnerabilities by using leading risk indicators including:

- Single committers (one person maintaining the code)
- FOIC signals, including contributions from developers from sanctioned entities
- End-of-life and project abandonment
- Supply chain fragility
- Pedigree and provenance
- Anomalies in the chain of custody (such as propensity for malware because of missing or false links to source code repositories)

## Satisfy Regulatory Requirements

Exiger's Ion Channel helps you proactively meet government expectations, including:

- EO 14028
- NTIA SBOM Minimum Requirements
- NIST SP 800-218
- All 15 Supply Chain Controls in NIST 800-53 (CM-7(8))
- M-22-18
- NERC-CIP-013-1
- DHS Supply Chain Risk Management Act
- FDA Premarket Guidance
- Cyber Resilience Act (CRA) SBOM requirements



# Understand Your Complete Software Risk

Ion Channel is unrivaled in the depth and granularity of its data on upstream risk, including 6.5 billion events, greater than 375 million repositories, more than 88 million packages, 250,000 vulnerabilities, and 1.5 million common platform enumerations in the software supply chain in open-source, IT, OT, and IoT software.

Ion Channel capabilities exceed those of many SCA tools and vulnerability detectors by including:



Comprehensive risk profiles on software components across open-source, IT, OT, and IoT environments, offering a holistic understanding of software supply chain risks.



A data backplane to map adversarial contributions to open-source components and a risk-scoring methodology.



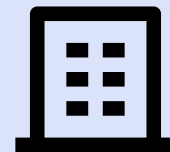
Proactive risk detection that goes beyond known vulnerabilities or binary analysis.



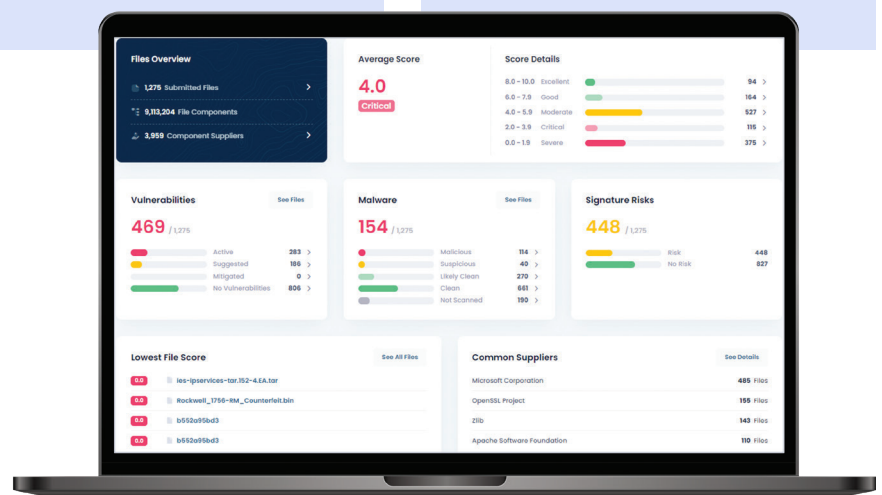
Accurate attribution of proprietary software components, even if modified by OEMs, including those from foreign corporations.



Continuous monitoring of vulnerabilities and automatic updates to trust scores, reflecting evolving risks.



A scalable solution for the whole enterprise.



## Discover More

Want to know more? Take a look at our web resources simply by navigating your way to our website using the QR code.

All information contained within this document was correct at the time of printing. ©EXIGER 2024

