Red Hat Summit

Connect

Shift left in software security
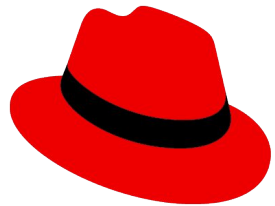
Red Hat

Increased security risks for application development

Growing concerns that open source is vulnerable to exploit and attack

742%

average annual increase in software supply chain attacks over the past 3 years[1]

84%

of open source scanned codebases contained at least one vulnerability[2]

31%

of organizations are not monitoring these open source dependencies[3]

The increase in the number of applications, systems and environments causes organizations to have larger exposure to malicious attacks and compels them to look for strategies that reduce the surface area of attack.

[1] State of the Software Supply Chain | [2] Open Source Security and Risk Analysis

Red Hat

Build security checks into the software development lifecycle

Maintaining security policies and compliance

- **Secure open source production** – identify open source code dependencies

- **Improve vulnerability detection and remediation** – find and fix vulnerabilities in source code and images

- **Continuously monitor for threats** – Monitor applications' codebase risk profile

design ← code ← build ← deploy ← monitor

Secure the software supply chain

4
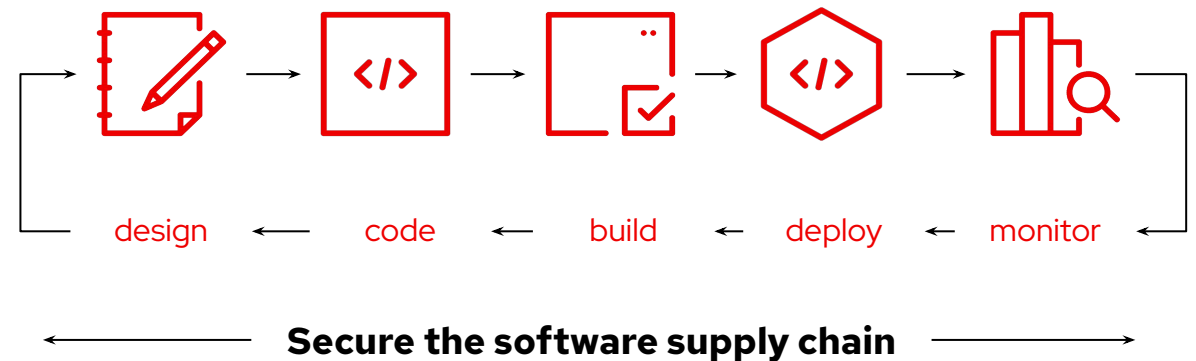
What are the minimum regulatory requirements for trusting the source code?

Access to curated and trusted open and proprietary source code libraries for developers to use on business critical applications

Software Bill of Materials (SBOMs)

Understand where your software comes from (provenance), who created it (licensing) and who certifies it (signatures/attestation)

Vulnerability management

Access to vulnerabilities databases, understand vulnerability exploitability (VEX) and access to fixes and remediations

Software composition analysis

Understand and map relationships to open source software for all business critical applications across all environments

Red Hat

Why should you care?

Procurement and Audit

Ensure compliance

Assess vendor's risk

Enforce security requirements
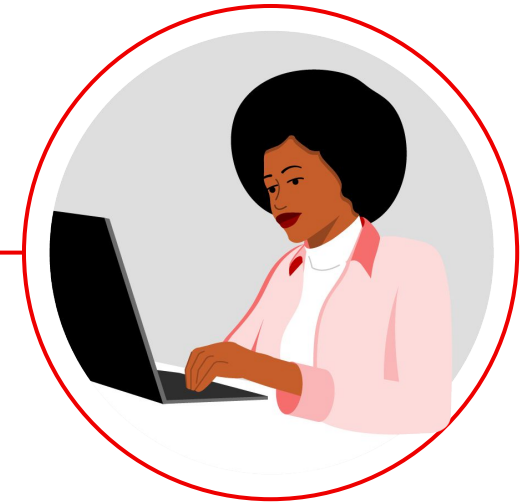
Risk Management

Identify surface area of attack

Assess threats to digital assets

Create an incident response plan

Assurance

Meet regulatory compliance

Reduce cyber threats and attacks

Comply security & privacy regulations

Red Hat

Red Hat
Trusted Profile Analyzer

Red Hat Trusted Profile Analyzer provides development and security teams **visibility and insights into the risk profile of an application's codebase** to ensure security threats and vulnerabilities are minimized and caught promptly.

Aggregate, manage and analyze software assets composition and security documentation of custom, 3rd party and open source software without slowing down development or increasing operational complexity.

Red Hat

The value of Red Hat Trusted Profile Analyzer

INCREASE DEVELOPER PRODUCTIVITY

Easy and quick access to trusted, verified content directly from your local IDE

IMPROVE OPERATIONAL EFFICIENCY

Increase team collaboration with a single source of truth for securing source code

GET ACTIONABLE INSIGHTS

Manage and reduce the potential business impact of malicious attacks

Red Hat

Red Hat Trusted Profile Analyzer

Shift security left providing:

- Simple source of truth for security documentation (SBOMs, and VEXs)
- Single view for vulnerability analysis and risk profiling during design and code
- Simple way for analyzing and measuring the blast radius of a security incident

design → code → test → deploy → monitor

TRUSTED CONTENT

DEPENDENCY ANALYTICS

SUPPLY CHAIN MANAGER
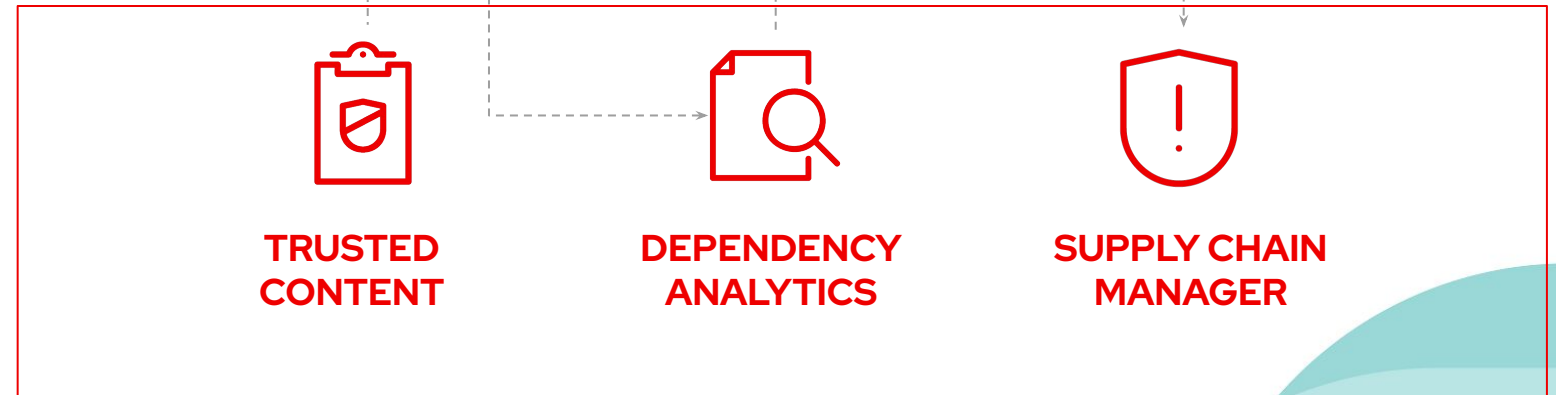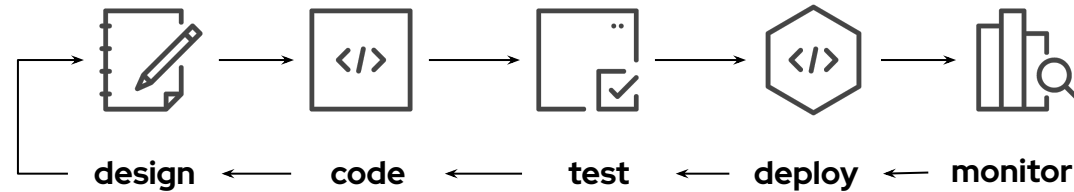
Dependency Analytics

Find and fix vulnerabilities during the development process

IDE plugins***

Software Composition Analysis*

Vulnerability information**

Red Hat dependency analytics
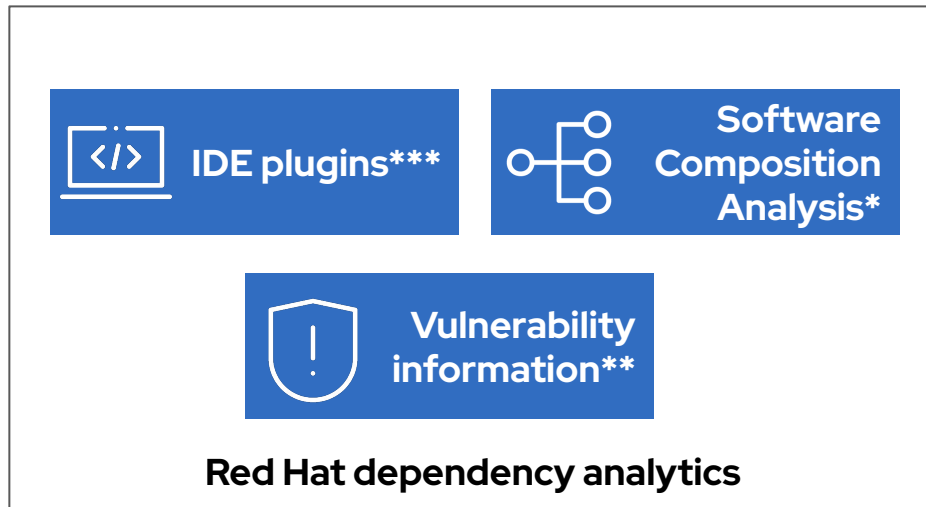
▸ **Run on-demand software composition analysis** to identify transitive dependencies and potential vulnerabilities in the code

▸ Identify the right open source component to use and **apply suggested recommendations** in your application code to minimize your risk profile

▸ **Allow developers to solve problems locally** in their preferred integrated development environment (IDE)

Red Hat

Simplify vulnerability management at code-time

Track source code provenance and attestations for actionable insights

Red Hat
Trusted Profile
Analyzer

Home
Search
Scan SBOM
Extend
Support

Search Results

Clear all filters

CVEs 377   Packages 1623   Products and containers 3   Advisories 38

State
- Any
- Published
- Rejected

CVSS
- Low
- Medium
- High
- Critical

Published
- Last 7 days
- Last 30 days
- This year
- 2022
- 2021
- Any time

1 - 10 of 377

ID	Description	CVSS	Date published
CVE-2023-40151	Red Lion Controls Sixnet RTU Exposed Dangerous Method Or Function	Critica 10.0/1 l 0	Nov 21, 2023
CVE-2023-42770	Red Lion Controls Sixnet RTU Authentication Bypass Using An Alternative Path Or Channel	Critica 10.0/1 l 0	Nov 21, 2023
CVE-2023-6248	Data leakage and arbitrary remote code execution in Syrus cloud devices	Critica 10.0/1 l 0	Nov 21, 2023
CVE-2023-49103	An issue was discovered in ownCloud owncloud/graphapi 0.2.x before 0.2.1 and 0.3.x before 0.3.1. The graphapi app relies on a third-party GetPhpInfo.php library that provides a URL. When this URL is accessed, it reveals the configuration details of the PHP environment (phpinfo). This	Critica 10.0/1 l 0	Nov 21, 2023

https://issues.redhat.com/browse/TC

Key Features:

- Identify, analyze dependencies to map, evaluate impact radius
- Generate, manage SBOM/VEX to stay regulatory compliant
- Curate content that's verified, trusted to prevent malicious code
- Act on recommendations directly from the IDE, as code is written
- System of record to store, index, query security documentation

Red Hat
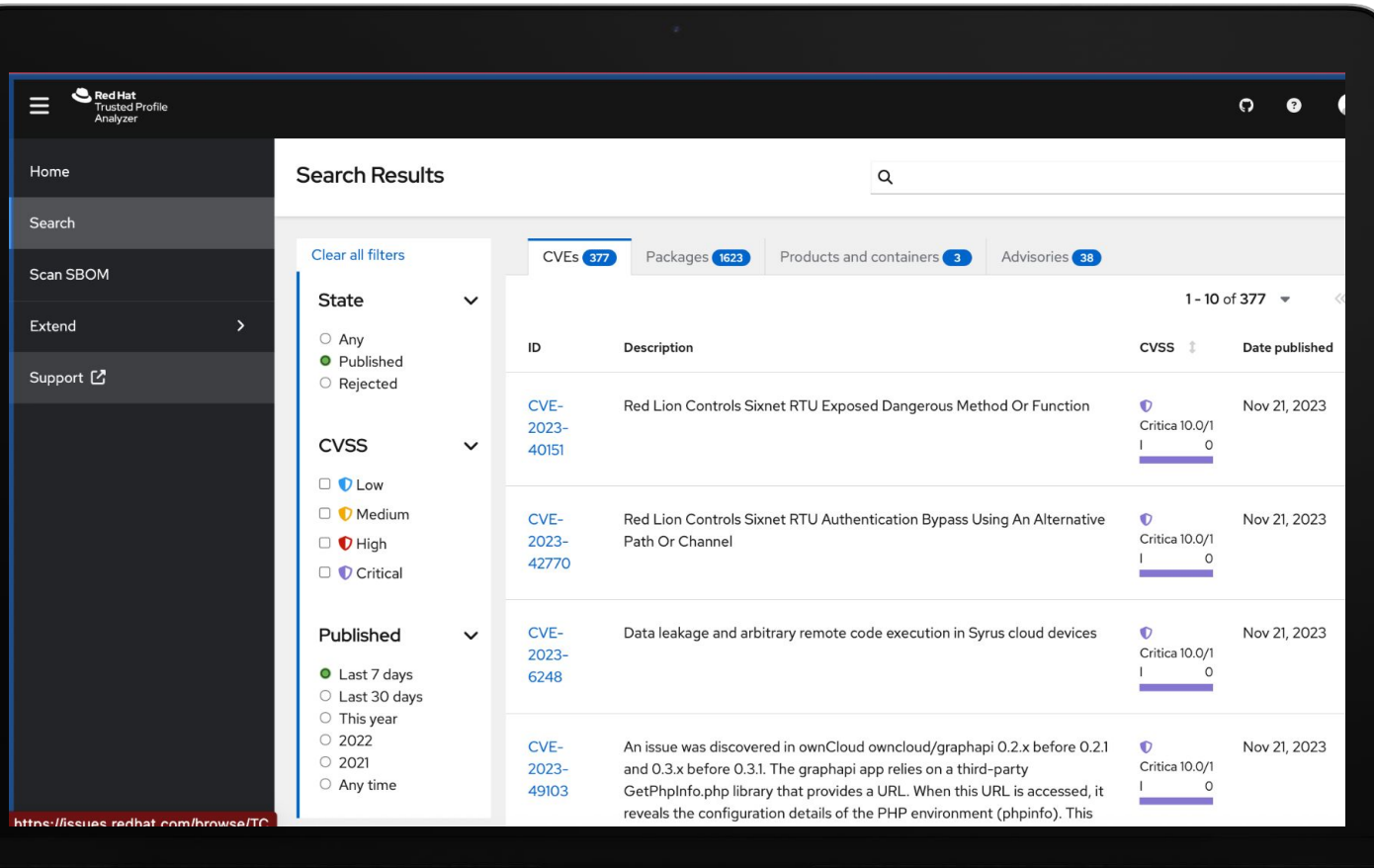
Dependency Analytics


```
my-quarkus-app  >   pom.xml
44          <dependency>
45              <groupId>io.quarkus</groupId>
46              <artifactId>quarkus-arc</artifactId>
47          </dependency>
48          <dependency>
49              <groupId>io.quarkus</groupId>
50              <artifactId>quarkus-junit5</artifactId>
51              <scope>test</scope>
52          </dependency>
53          <dependency>
54              <groupId>io.rest-assured</groupI
55              <artifactId>rest-assured</artifa
56              <scope>test</scope>
57          </dependency>
58
59          <dependency>
60      <groupId>org.apache.logging.log4j</group
61      <artifactId>log4j-api</artifactId>
62      <version>2.15.0</version>
63  </dependency>
64  <dependency>
65      <groupId>org.apache.logging.log4j</group
66      <artifactId>log4j-core</artifactId>
67      <version>2.15.0</version>
68  </dependency>
69
```

```
org.apache.logging.log4j/log4j-core@2.15.0

osv-nvd(osv-nvd) vulnerability info:
Known security vulnerabilities: 3
Highest severity: CRITICAL

snyk(snyk) vulnerability info:
Known security vulnerabilities: 3
Highest severity: CRITICAL
```

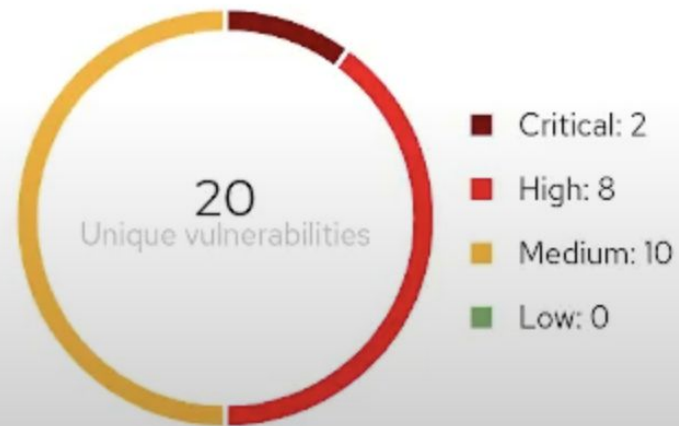Source: Red Hat Dependency Analytics

Open detailed vulnerability report

Dependency Analytics

Dependency Analytics

Dependency Name	Current Version	Direct Vulnerab...	Transitive Vuln...	Remediation a...
io.quarkus:quarkus-resteasy	2.11.3.Final	1 🛡 1	31 🛡 8 🛡 14 🛡 9	Yes
io.quarkus:quarkus-smallrye-openapi	2.11.3.Final	0	39 🛡 10 🛡 17 🛡 12	Yes
io.quarkus:quarkus-arc	2.11.3.Final	0	22 🛡 4 🛡 9 🛡 9	Yes

Shift Left Security early across the software supply chain

Trust, transparency in code management with security–focused golden paths, integrated guardrails

Red Hat
Trusted Application
Pipeline

Software Catalog	Provenance, Attestation of Trusted Curated Content	Digitally Signed & Verified	Immutable Certificate Authority	Software Composition Analysis	Generate & Manage SBOM/VEX
Software Templates	**Application Libraries**				
Red Hat Plug-ins for Backstage	**Language Runtime**	Keyless Signing	Transparent, auditable logs	Dependency Management	OSS Risk Profiles
	Universal Base Image				

Red Hat
Developer Hub

Red Hat
Trusted Content

Red Hat
Trusted
Artifact Signer

Red Hat
Trusted Profile
Analyzer

Deploy automatically as–code
to an auditable, declarative state
that's continuously monitored

Red Hat
OpenShift

Red Hat
OpenShift
Platform Plus

Security at every layer
with consistency across
all target destinations

Physical   **Virtual**   **Hybrid**

aws   Azure   IBM **Cloud**

Red Hat

Customer Benefits

- Meet compliance regulations for SBOM management and archiving

- Deploy applications with fewer vulnerabilities

- Know that trusted components are in use as early as possible

- Reduce alert fatigue with fewer false positive by getting vendor vulnerability information

  from the actual vendor (VEX)

- Analyze applications without downloading and installing

Red Hat