DerScanner

DerScanner Software Composition Analysis

In the current cybersecurity landscape, ensuring the security and transparency of software has never been more crucial. Across the globe, regulatory bodies are mandating the deeper understanding of Software Bill of Materials (SBOMs) to safeguard software from open source born risks throughout its lifecycle. These regulations mandate that manufacturers document and report on software components and vulnerabilities, enhancing accountability and transparency for consumers.

Executive Order 14028 on Improving the Nation's Cybersecurity mandates SBOMs for all software sold to federal agencies.

The EU Cyber Resilience Act (CRA) requires the use of SBOMs to boost software security.

Germany's IT Security Act 2.0 (IT-SiG 2.0) includes requirements for the use of SBOMs to ensure software security and transparency.

Japan's Cybersecurity Framework, led by the Information-technology Promotion Agency (IPA), emphasizes software component transparency.

Australia's Cyber Security Strategy 2020 stresses the importance of protecting the software supply chain.

Gain visibility into SBOM and protect your codebase against open-source risks with DerScanner Software Composition Analysis. Empowering cybersecurity professionals and developers, DerScanner allows you to proactively identify and mitigate vulnerabilities in third-party components. Going beyond basic vulnerability scanning, it assesses license compliance and provides a data-driven health score for each open-source package. This enables informed decision-making, prioritization of remediation efforts, and avoidance of potential legal pitfalls. With DerScanner SCA, you can confidently build secure, compliant software while minimizing the risk of zero-day exploits and supply chain attacks.

FORRESTER®

DerSecur Recognized among Notable Vendors in The Software Composition Analysis Landscape Q2 2024

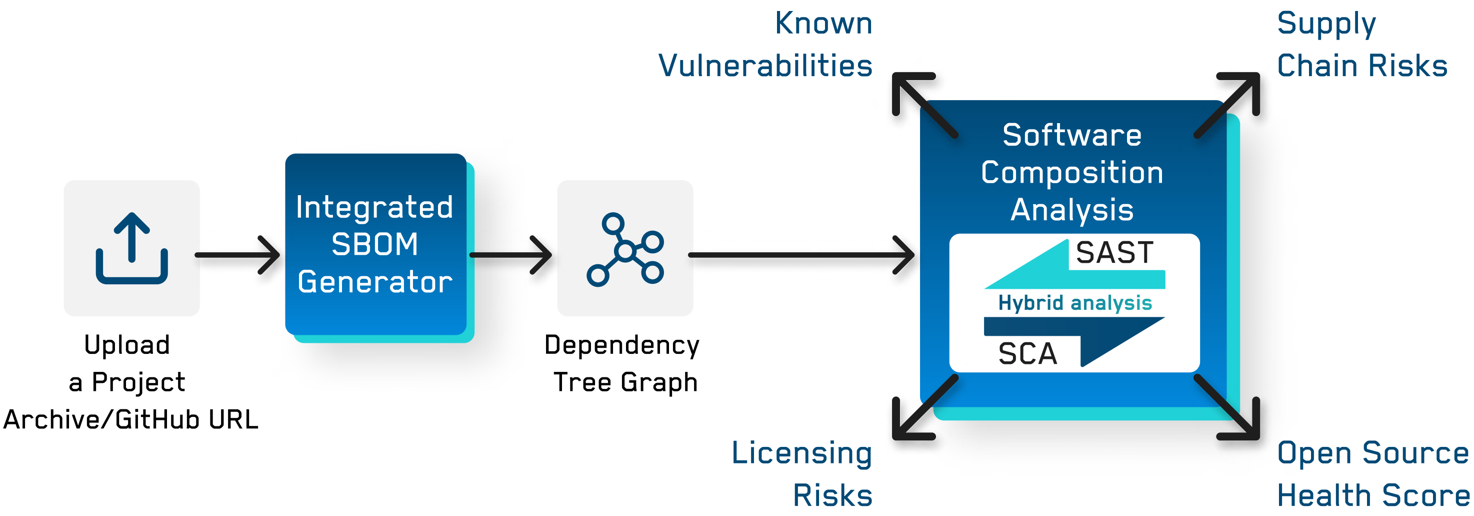
Streamline SBOM Management with DerScanner

Simplify Your SBOM Generation Process

Managing Software Bill of Materials (SBOM) can be a complex and time-consuming task. Traditional external SBOM generators often require extensive configuration and setup, leading to frustration and delays in your Open Source security projects.

Effortless SBOM Generation

With DerScanner, you no longer need to wrestle with external tools to generate your SBOM. Our integrated SBOM generator streamlines the process, allowing you to effortlessly create detailed SBOMs. Simply upload your project to DerScanner, and our tool will automatically generate an SBOM, ready for comprehensive Software Composition Analysis (SCA).



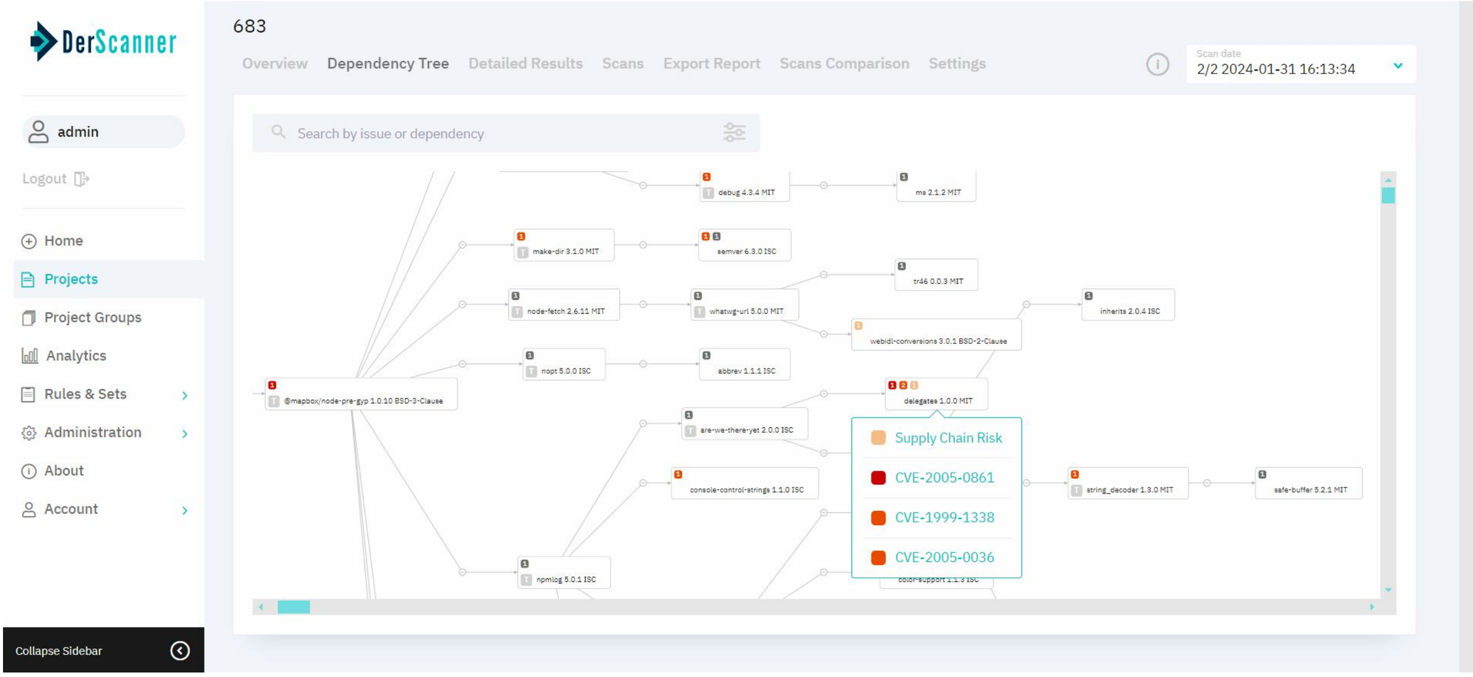
Visualize and Manage Dependencies with DerScanner's Dependency Tree Graph

Comprehensive Dependency Visualization for Enhanced Security

Managing complex project dependencies can be a daunting task. Projects often include deep structures of direct and transitive dependencies, making it challenging to understand the full scope and pinpoint where vulnerabilities are hidden.

Clarity Through Visualization

DerScanner's Dependency Tree Graph transforms how you manage your project's dependencies. It visualizes your entire project structure, allowing you to see exactly where vulnerable packages reside. With this clear, visual representation, you can quickly and efficiently identify and address security risks.



Gain Visibility into Open-Source Composition to Prevent Known Vulnerabilities

DerScanner SCA maintains vast databases of known vulnerabilities in open-source software, sourced from various security advisories and databases. By cross-referencing the SBOM with the vulnerability database, DerScanner SCA pinpoints vulnerabilities that directly affect your application. It can even identify vulnerabilities hidden deep within your dependency tree.

The Value of Open-Source Visibility

Proactive Security: By detecting vulnerabilities before they're exploited, you can patch or update vulnerable components, reducing the risk of security breaches.

Compliance: Many industries and regulations like Executive Order on Improving the Nation's Cybersecurity require you to track and manage open-source usage and vulnerabilities. SCA aids in compliance efforts.

Informed Decision-Making: Understanding your open-source usage helps you make informed decisions about which components to use and prioritize for updates.

Reduced Remediation Costs: Fixing vulnerabilities early in the development cycle is far less costly than addressing them after a breach.

Check Package Health to Avoid Supply Chain Risks

Open-source health scoring in DerScanner is a metric that assesses the overall well-being and security posture of an open-source project. It combines various factors into a single score, making it easier to evaluate the potential risks and benefits of using a specific package.

How Open-Source Health Scoring Helps Avoid Zero-Day Vulnerabilities

Early Warning: By considering a package's health score, you can avoid projects with a history of vulnerabilities or poor security practices. This reduces the risk of introducing known vulnerabilities or unknowingly using packages that might be prone to future zero-day exploits.

Reduced Attack Surface: Limiting the use of risky packages minimizes the potential attack surface for zero-day vulnerabilities.

Proactive Selection: Choosing packages with high health scores means you're more likely to select well-maintained and secure components.

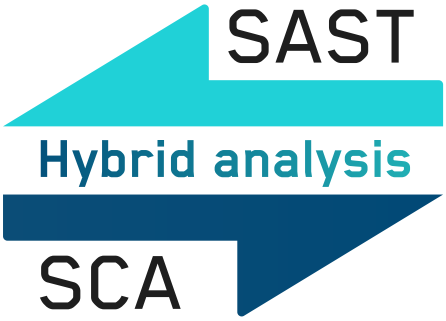
Faster Response: If a vulnerability is discovered in a well-maintained project, the community and maintainers are likely to respond quickly with patches and updates, mitigating the risk of zero-day attacks.

Hybrid SCA+SAST Analysis with DerScanner

Precision Vulnerability Assessment in Open-Source Rich Projects

Understanding the true risk of vulnerabilities in dependencies is crucial. Merely identifying a CVE in a dependency doesn't necessarily mean the entire package is at risk. It is essential to pinpoint which method calls could lead to vulnerability exploitation.

Comprehensive Hybrid Analysis



DerScanner's hybrid SCA+SAST analysis combines the strengths of Software Composition Analysis (SCA) and Static Application Security Testing (SAST) to provide a precise assessment of your application's security. This advanced hybrid approach ensures you know exactly which packages contain CVEs that are reachable and exploitable.

Don't Let Open-Source Licensing Land You in Legal Trouble

DerScanner SCA determines the licenses associated with each identified open-source component. This is crucial because open-source licenses have different terms and conditions regarding usage, modification, distribution, and attribution.

> *"Ensuring open source license compliance was a complicated task until we started using DerScanner. Their solution has streamlined the process, allowing us to focus on innovation without the constant worry of legal issues."*
>
> Aleksandr Slobodchikov, CEO, CT Mobility Solutions

DerScanner SCA assesses whether the usage of each open-source component complies with its license terms. This involves:

Checking for Copyleft Obligations
Some licenses, like the GPL, have "copyleft" provisions that require you to release your software under the same license if you distribute a modified version. DerScanner SCA flags these components and ensure compliance.

Identifying Restrictions
Certain licenses may restrict commercial use or require specific attribution.
DerScanner SCA highlights these restrictions and helps you avoid legal issues.

Monitoring Dependencies
DerScanner SCA tracks dependencies of your open-source components, as they may also have licensing obligations you need to comply with.

Reduce False Positives in Open-Source Security Projects with Confi AI

Precision and Efficiency in Managing Open-Source Dependencies

Managing open source security can be overwhelming, especially when dealing with large numbers of dependencies. False positives in SCA (Software Composition Analysis) projects not only waste valuable time but also divert attention from genuine vulnerabilities that need immediate action.

Introducing Confi AI for Accurate Vulnerability Management

With Confi AI integrated into your SCA projects, you can leverage a sophisticated AI-driven engine designed to minimize false positives. Trained using the Exploit Prediction Scoring System (EPSS), as well as SAST and SCA findings in DerScanner, Confi AI helps you focus on vulnerabilities that truly matter.

Mitigate MavenGate Threats with DerScanner's Expired Domain Detection

How DerScanner Mitigates MavenGate Attacks

By continuously monitoring and analyzing domain status, DerScanner ensures that you are alerted to any dependencies linked to expired or outdated domains that could be exploited by attackers.

Protect Your Applications from Supply Chain Attacks

Expired domains pose a significant security threat in MavenGate attacks. When a domain associated with a legitimate Maven package or developer expires, attackers can re-register it and gain control. This re-registered domain, previously listed in package metadata, developer profiles, or as a repository URL in Maven POM files, is then used to upload malicious packages. Developers and CI/CD systems, still trusting the now malicious domain, unknowingly integrate these harmful packages into their projects. Once included, the malicious code executes, leading to potential data breaches, system compromises, and other malicious activities. This threat primarily affects projects using Java, but also extends to other JVM languages such as Kotlin, Scala, Groovy, and Clojure, all of which rely on Maven for dependency management.

Why choose DerScanner SCA?

DerScanner SCA delivers unmatched accuracy and actionable insights for your open-source security. By leveraging PURL package naming instead of CPE, we minimize errors and ensure precise identification of vulnerabilities. Our unique blend of GitHub Advisory, GitLab Advisory, Google OSV Database, EPSS, and NIST NVD databases provides the most comprehensive vulnerability coverage with the fewest false positives, empowering you to make informed decisions and remediate risks efficiently.

In-house know-how +

Github Advisory

GitLab Advisory

Google OSV Database

EPSS (Exploit Prediction Scoring System

NVD

About DerSecur

DerSecur, established in 2011, is at the forefront of application security. Its team of 70 experts has developed DerScanner, a versatile application security solution that supports 43 programming languages and provides static, dynamic and software composition analysis. DerSecur is committed to furthering cybersecurity research and development, ensuring a more secure digital future.

https://derscanner.com/