ServiceNow Software Bill of Materials (SBOM)

Why it's needed

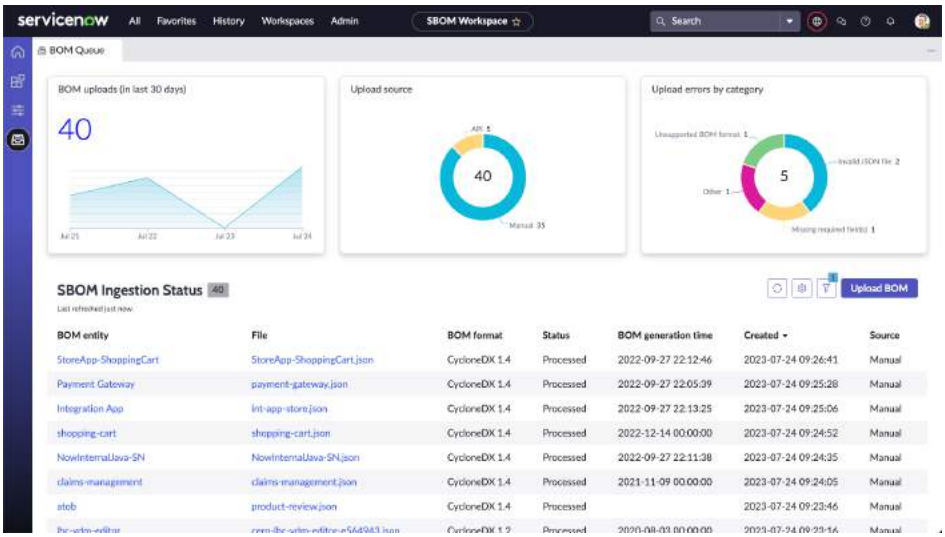
The majority of software builds today have open-source components; according to a 2020 Open Source Security Foundation (OSSRA) report, 99% of codebases analyzed contained at least one open-source component, with open source comprising 70% of the code overall.

There are several reasons for this trend, including:

- Open source software is often free to use
- Open source software can be quickly and easily integrated into existing software
- Open source software is often well-tested and maintained
- The innovation of open source software

As software becomes more complex, businesses increasingly rely on open-source components to provide the necessary functionality and features. This presents its own unique set of challenges, including:

- Open source components can introduce security vulnerabilities into software.
- Open source components can have different licensing terms, which can be challenging to manage.
- The quality of open-source components can vary, so it is essential to choose components carefully.
- Open-source components can depend on other open-source components, making tracking and managing the software supply chain difficult.



How can ServiceNow's SBOM solution help?

Know what open-source software is used in your environment

Ingest SBOMs for all home-grown applications, COTS (commercial-off-the-shelf), software, container, firmware, framework, library, etc., into the ServiceNow SBOM solution and get instant visibility into what third-party components your applications are made up of. Also, gain understanding of your exposure to all the components used across all the software in your organization. So when the next log4j hits, you have a query-able database to know your complete exposure.

Key features

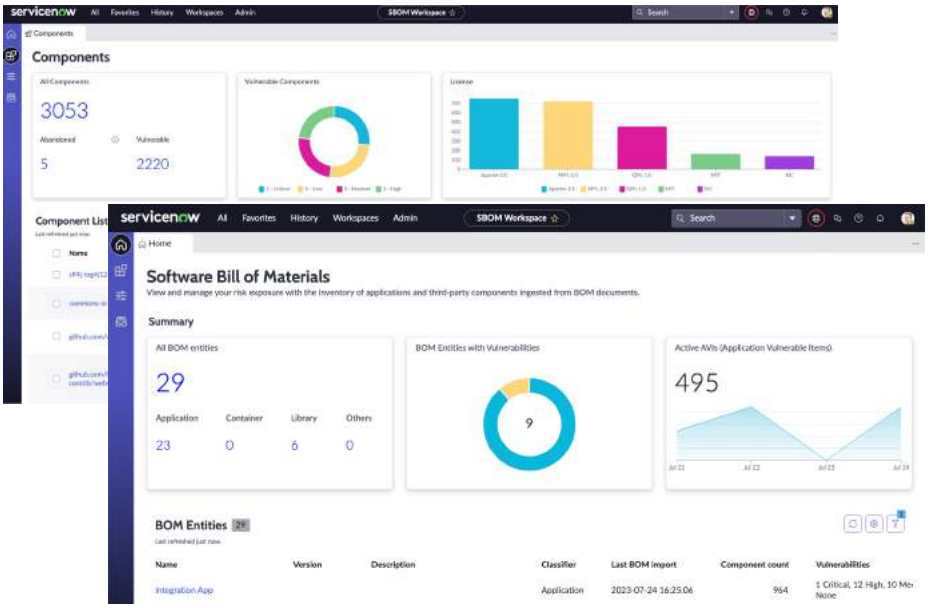
Ingest SBOMs for home-grown applications, COTS software, OT devices, IoT devices, etc., to get complete visibility into all the open-source components used in your environment.

Prioritize findings based on risks for a specific component having exploitable vulnerabilities or all components with critical vulnerabilities. Moving forward, you will be able to scope even further by limiting the findings to only external facing/ crown jewel applications

Get visibility into the security and compliance risks of using open-source components in your organization.

Understand your risks

Organizations can continuously identify vulnerabilities and understand the risks posed by the open-source software being used in their environment. Furthermore, the vulnerabilities (critical, high, medium, low) can be enriched with CISA Known Exploited Vulnerabilities (KEV) data on the third-party components, allowing vulnerability managers and application security managers to gain a better understanding of the organization's security posture. Stale (more than X releases behind current) and abandoned (no longer updated) components used in the environment can also be surfaced and addressed.



Proactively manage your risk

Automate the vulnerability management process by continuously prioritizing the vulnerabilities that pose the highest risk based on what is most important to the organization. Rules can be configured using single parameters or a combination of parameters, such as critical vulnerability with known exploit, for a specific component, or only scope the findings on the crown jewel applications or external facing applications.

As SBOMs are uploaded, risks are assessed and findings are automatically created and routed to the application owners for triaging and to provide the vulnerability disposition.

Key Stakeholders

Vulnerability Event Manager

Assess the risk of the zero-day vulnerabilities on open-source components.

AppSec Manager

Assess the risk of open-source components used across the organization and drive the risk-reduction.

Application Owner/ Remediation Owner

Remediate high-risk findings and provide the disposition.