LYNX
SOFTWARE TECHNOLOGIES

LYNX MOSA.ic.SCA™
Software Composition Analysis for Supply Chain

Supply chain disruptions in industries such as aerospace can result in costs ranging from $100,000 to over $1 million per day, depending on the severity of the disruption *(Deloitte, "Annual Cyber Threat Trends report: Insights, emerging threats, and their potential impact", 2024). Gartner estimates that proper software supply chain management, including Software Bill Of Materials (SBOM) implementation, could prevent up to 70% of security incidents related to vulnerabilities.*

Get a Clear View of Your Software's Components with MOSA.ic.SCA

Identify, analyze, and manage both proprietary and open-source libraries in your code. Ensure security and compliance by enforcing policies that meet internal standards and external regulations. All are securely stored and managed on your premises, visible from your desktop, and seamlessly integrated with your DevOps infrastructure.

Governance and Policy Enforcement

Software Composition Analysis (SCA) identifies and manages open-source components and third-party libraries across your entire software project. It helps organizations understand the composition of their software, including all open-source components being used, and provides insights into potential security vulnerabilities, licensing risks, and outdated dependencies. Managing the vulnerabilities that open systems to devastating cyberattacks is a critical aspect of SCA. With 350+ new Common Vulnerabilities and Exposures (CVE) identified every week and the number increasing drastically over the past five years, companies are making headlines worldwide for the wrong reasons. Companies need a tool to manage the onslaught of new vulnerabilities, cut through the noise, and identify the most pressing threats for which to take appropriate action.

LYNX MOSA.ic.SCA Capabilities

MOSA.ic.SCA is a collection of products, services, and best practices that empower customers to confidently monitor their software vulnerability exposure for components enumerated in the Software Bill of Materials (SBOM). It ensures that threats are identified in a clear, easily manageable format and addressed quickly. With integrated and automated monitoring, companies can keep engineers focused on developing cutting-edge products. At the same time, the SCA process minimizes risk and automatically stays up to date with the latest industry and government cybersecurity processes and mandates.

12.7%

In 2022, the average cost of a data breach was $4.35 million, which is a 12.7% increase from 2020

IBM Cost of a Data Breach Report 2022

46%

A 2022 government study found that 46% of large businesses say they have had to take up new measures to save them time and protect their assets.

Cyber Security Breaches Survey 2022

10,000

In 2021 alone, nearly 10,000 known security vulnerabilities were detected in open source components.

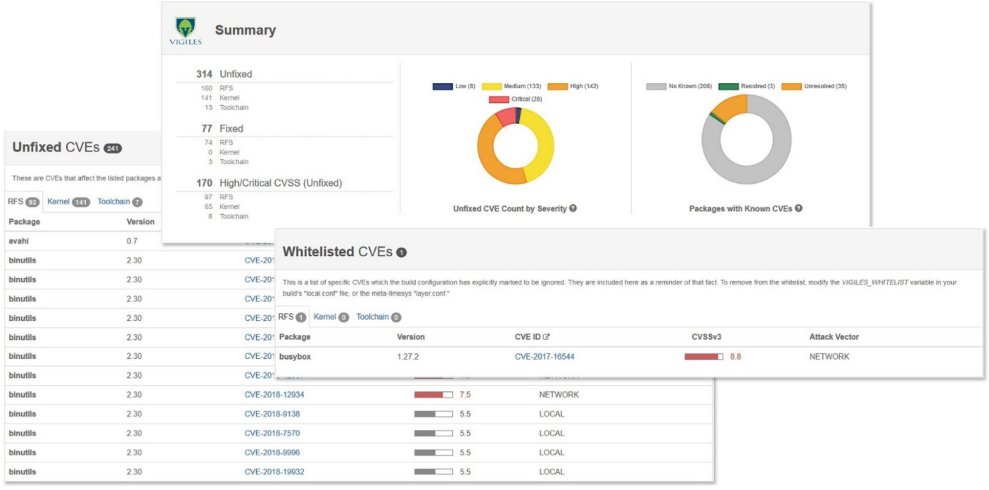
All About Mend's 2021 Open Source Security Vulnerabilities Report

www.lynx.com | 408-979-3900 | inside@lynx.com

Key Customer Benefits of LYNX MOSA.ic.SCA

Customer Benefits	Capabilities Enabled by LYNX MOSA.ic.SCA
Efficient vulnerability tracking. Reduces irrelevant CVEs, providing 85% fewer CVEs to analyze and 95% fewer false positives.	· Offers robust solutions for managing and generating SBOMs · Support multiple industry-standard SBOM formats · Enhanced team collaboration across multiple SBOMs · Automated, real-time tracking with CVE filtering · Curated CVE database
Shorter time to identify and apply remediation. The publication of a CVE may be delayed by up to four weeks depending on the source.	· Enhances the mapping of package names to CVE identifiers, package versions, and applied patches · Parse the kernel and boot configuration, list only the CVEs related to features in use in your embedded system · Detailed fix recommendations and patch links
Highly scalable to meet the needs of large projects. Scaling a "do it yourself" solution can cost an additional $100,000 - $300,000 in engineering time.	· Patch notification and management features to quickly identify how to remediate issues · Offers powerful triage and collaboration tools, allowing teams to prioritize, assess, and remediate security issues quickly
Workload reduction The labor cost of a "do it yourself" solution is in the 3 to 5 times the cost of MOSA.ic.SCA license	· User-friendly interface to process the SBOM and visualize the results · Integration with Jira for issue tracking · Seamless integration in a CI/CD pipeline for automation
Risk mitigation A "do it yourself" solution leads to 2x to 3x times the risk of missing vulnerabilities and a $1M to $4M data breach	· Automated tracking, regular updates, and professional support minimizing the risk of missing vulnerabilities · Efficient tracking of changes between builds to simplify reporting for compliance · Track changes between releases and automatically create a summary report for release notes
Lower the costs for compliance and audits The MOSA.ic.SCA license includes professional support, which translates a savings of to up to $200,000 over per year doing it yourself	· Maintain an audit trail of changes and triaging information · Meet cybersecurity documentation requirements · On-premises deployment on the customer's IT infrastructure · Single sign-on integration, project-specific access controls, and role-based access management.

MOSA.ic.SCA automates Software Bill of Materials (SBOM) management with the Vigiles™ suite, ensuring compliance with government mandates, standards, and best practices. This is particularly valuable for highly regulated industries such as aerospace and defense, where long-term security and ongoing regulatory compliance are essential.



Vigiles ensures component transparency and aligns with mandates like the White House EO 14028, FDA Cybersecurity, and the EU Cyber Resilience Act (CRA). Vigiles provides the desktop user with a powerful dashboard that acts as the aggregation console for all projects, SBOMs, and teams. A CI/CD pipeline accesses Vigiles through APIs for continuous vulnerability monitoring.

Vigiles Key Capabilities

Vigiles leverages over 20 years of industry expertise in secure embedded software design and development, addressing fundamental challenges in managing vulnerabilities and maintaining compliance. This expertise results in a product that delivers key benefits to users:

Faster Reporting: Instead of relying on a single source, Vigiles reduces reporting delays by up to four weeks by aggregating data from multiple sources, providing faster access to critical information.

Relevant CVE Filtering: Vigiles filters vulnerabilities to show only those relevant to your specific SBOM configuration, reducing unnecessary analysis:

- 85% fewer CVEs to review
- 95% fewer false positives, cutting down on irrelevant alerts

Improved Accuracy: With a curated CVE database, Vigiles improves accuracy by up to 40% over the National Vulnerability Database (NVD). Security experts continuously update and validate CVEs for correctness and relevance. Vigiles also provides references to the Common Platform Enumeration (CPE) to better identify packages. Security experts continuously update and validate CVEs for correctness and relevance, referencing the Common Platform Enumeration (CPE) to identify packages better.

Optimized for Embedded Systems: Vigiles is tailored for embedded systems, understanding your kernel and U-Boot configurations. It uses intelligent curation algorithms for daily monitoring, which is crucial for aviation and defense systems requiring stringent, ongoing surveillance.

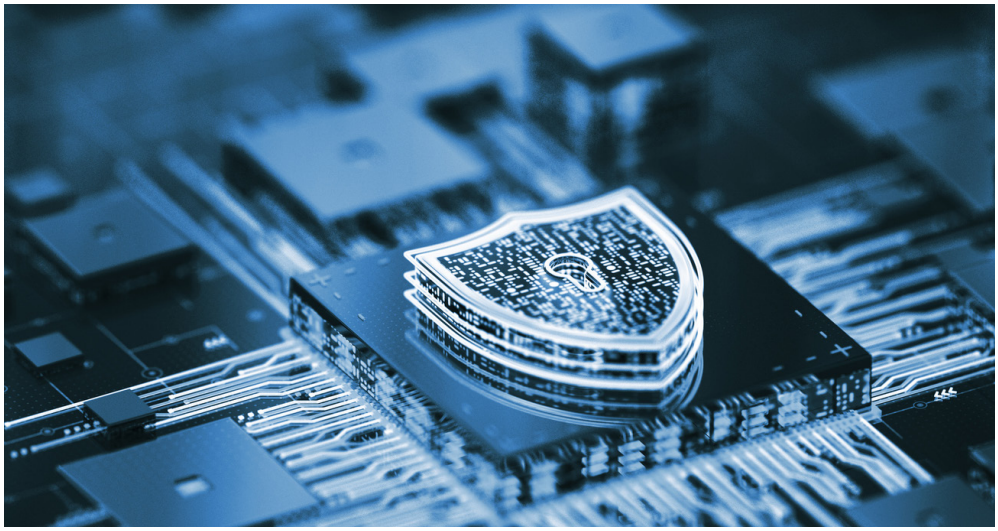
Streamlined Remediation: For each vulnerability, Vigiles provides detailed fixes, patches, and configuration recommendations for rapid resolution. It includes links to patches, workarounds, and testing resources, making the remediation process faster and more efficient.

LYNX MOSA.ic.SCA with Vigiles offers faster vulnerability reporting, more accurate and relevant CVE filtering, and targeted solutions, specifically designed for embedded systems.

Vigiles Ecosystem

Vigiles is continuously expanding support for a diverse range of systems using various languages and operating systems. The current list includes:

- Rust/crates.io
- Go
- Haskell/Hackage
- Erlang/Hex
- Kotlin/Maven
- Java/Maven
- .NET/NuGet
- Node.js/NPM
- Python/PyPI
- Ruby/RubyGems
- Debian/Debian Container
- Dart/Pub
- RunSafe
- C/C++
- LYNX MOSA.ic



Lynx MOSA.ic.SCA is compatible with all major Linux build systems, such as:

- Yocto
- Buildroot
- PetaLinux

Users can intuitively track and manage SBOMs across various products and releases. Vigiles supports industry-standard SBOM formats such as:

- CycloneDX
- SPDX
- SPDX lite

Eliminate Vulnerabilities and Future-Proof Your System with RunSafe™

RunSafe™ Security focuses on protecting embedded systems from cyber threats. RunSafe Security targets memory corruption vulnerabilities, common attack points in embedded systems. Its fine-grained Address Space Layout Randomization (ASLR) integrates seamlessly into existing development workflows, providing robust protection without impacting performance.

The RunSafe Code™ Vulnerability Mitigation Visualizer integrates with Vigiles to identify vulnerabilities that are mitigated by applying RunSafe Code, allowing your team to focus on feature development.

By combining RunSafe with Vigiles, you can significantly reduce risks from zero-day attacks and known memory-related bugs, which make up 40% of exploited vulnerabilities and over 60% of high and critical CVEs.

Education and Services

Lynx offers a range of services to accelerate the deployment of your SCA strategy, including:

- **Quick Start Training:** Quickly identify vulnerabilities in your project's Software Bill of Materials (SBOM)
- **Self-help & Education:** Access a comprehensive library of documents, videos, demos, and webinars, catering to all skill levels
- **Deployment Service:** Receive on-site or remote assistance to seamlessly integrate Lynx MOSA.ic.SCA into your on-premises infrastructure
- **Managed Services:** Let Lynx manage your vulnerability management, from detection to remediation, via our Lynx Managed Services

These services are designed to streamline and support the implementation of your SCA strategy. Our team of experienced subject matter experts hold security clearances and offer the ability to work with customers in controlled environments.