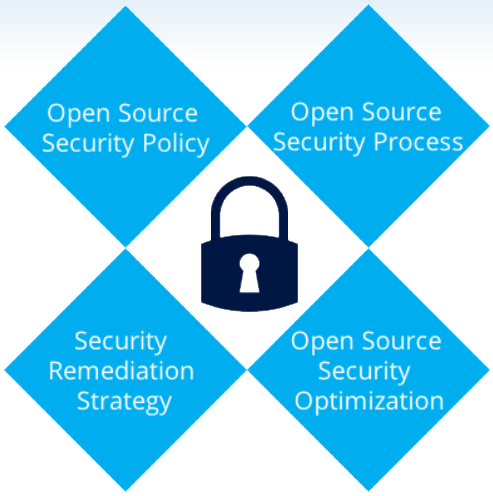
Open Source Sense
OSS Security Management

The Open Source Sense team brings decades of industry experience to help organizations understand and realize the benefits of using, developing, contributing, and commercializing open source software, while minimizing risk. Open Source Sense helps delivers those benefits with four practices focused on security:

- Security Policy Development
- Security Process Development
- Open Source Security Optimization
- Open Source Portfolio Remediation

Open Source Security Policy and Process Development

Create a reliable foundation for managing open source software security



Consistently addressing the security of open source software, like any complex organizational endeavor, depends on a clearly documented set of rules and procedures. A well-elaborated security policy forms the basis for designing and implementing the processes your organization needs to manage its open source software portfolio to minimize risk and maximize ROI.

Our Open Source Sense Security Policy and Process practice provides training and guidance for key stakeholders – IT managers, developers and devops, SQA team members and full-time security practitioners. We collaborate with your team to develop and deliver a comprehensive and comprehensible OSS security policy tailored to fit your organization's unique needs and harmonized with broader IT security. With a policy in place, Open Source Sense then works with your stakeholders to create a set pf efficient processes with minimal disruption to existing workflows or developer productivity.

Our consultants help you accomplish your OSS security goals through a combination of stakeholder interviews and workshops, documentation reviews and independent development to deliver customized policies and processes based on industry best practices and your organization's existing security framework.

OSS Security Policy Development

- Educate stakeholders on best practices in OSS management for security
- Establish consensus on mandate and specific rules for managing OSS
- Align company security policy and OSS policy
- Provide the basis for developing effective OSS management processes

OSS Security Process Development

- Train stakeholders on efficient OSS security process techniques
- Establish consensus on process workflows
- Design and document process workflows
- Provide a strategy for integrating company security processes, OSS processes and SCA tools

Contact Us Today -- info@opensourcesense.com

Open Source Security Optimization

Improve the efficiency and effectiveness of your open source security program

Many companies have open source security management programs in place, but are not realizing the expected benefit from investments in policies, process and tools. Often, organizations face unexpected challenges and unforeseen bottlenecks arising from

- Overly optimistic policies that do not reflect real-world circumstances and behaviors
- Lack of integration with other company security policies and processes
- Cumbersome processes that slow development and maintenance activities
- Limitations in existing SCA tool sets and relegation of tools to “shelfware”
- New classes of security risks from the rapidly-evolving black hat community

The Open Source Security Optimization practice addresses these and other shortcomings within your existing security policies, processes and implementations. To help your IT and development teams optimize their approach to security, we assess current practices and provide actionable recommendations to save time and reduce overhead, to address emerging security risks, and to derive maximum advantage from your OSS management programs.

This practice includes

- Assessing current OSS policy and practices
- Educating stakeholders on best practices in OSS management
- Delivering actionable recommendations to reduce risk, save time and overhead
- Providing the basis for optimum tools implementation

Open Source Security Remediation Strategy

Helping you respond to discovered vulnerabilities in your OSS portfolio

Modern Software Component Analysis (SCA) tools do a terrific job of scanning software portfolios and highlighting known vulnerabilities (CVEs, etc.). However, those tools do little to help make sense of their output. When faced with audit reports chock-a-block with discovered vulnerable components, development organizations often find themselves staring in bewilderment:

- Which vulnerabilities actually expose our code and customer data?
- How can our team prioritize addressing hundreds or thousands of warnings?
- Our IT budget and dev team has limited resources – where do we begin?

The Open Source Sense Security Remediation Strategy practice helps your team understand and digest the rich reporting in SCA output. We help you respond by building a remediation strategy and plan that includes

- SCA report analysis
- Software architecture and context analysis
- Vulnerability triage criteria creation
- Per component remediation guidance
- Integration of remediation strategy and tactics into your security policy and processes