sonatype

Improving RMF Practices Through Automation

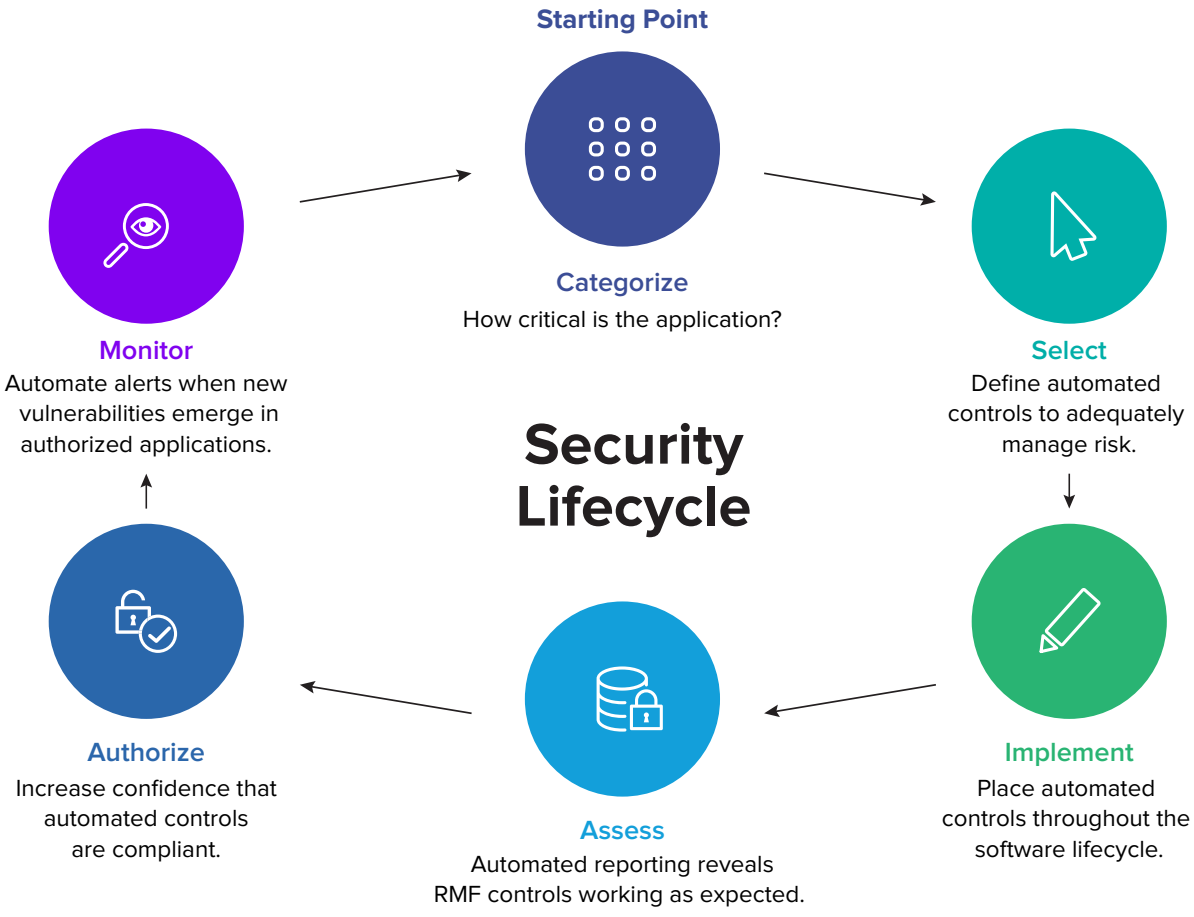
Introduction

Six Steps to Continuous Risk Management

Relentless cyber attacks from adversaries have prompted federal agencies to take a more holistic and systematic approach to integrating information security into broader organizational risk management strategies. Practices defined in the Risk Management Framework (RMF) are being employed across the federal government to improve visibility, implement better controls, and support faster responses to cyber threats across IT applications and infrastructure.

Developed by the National Institute of Standards and Technology (NIST), the RMF requires agencies to continually understand, assess, monitor and document their cyber risks over the lifecycle of their IT assets. The six-step RMF process aims to makes the IT authorization process less of a check-the-box, "accredit-and-forget-it" type of exercise and more of a continuous, risk management-focused approach.

Unfortunately, RMF practices that many federal agencies are implementing have significant blind spots when it comes to securing critical applications. Furthermore, lack of automated practices hinder their ability to scale, respond, and adjust to changes in the applications they are tasked with simultaneously building and protecting.



To minimize these blind spots, federal agencies can employ software supply chain automation solutions that closely align to each step of their RMF practice. Embedding software supply chain automation within RMF practices can dramatically improve cyber security controls, accelerate remediation efforts, and track improvements.

We Don't Build it Like We Used to

We don't build software like we used to. Today, agencies are under increasing pressure to stand up higher-velocity development practices (e.g., Agile, DevOps) such as those outlined in the U.S. Digital Services Handbook. Furthermore, expansion of organizations like U.S. Digital Services and the 18F group at the General Services Administration are driving this trend. These developments translate into less costly projects, lower risk of large-scale failure, and more iterative approaches to creating digital services supporting federal missions. These trends are also placing an increasing pressure on development teams to roll out releases faster.

To keep pace, software — once coded from scratch — is now primarily assembled from open source and third-party components. It is estimated that 85% of a typical application is now composed of these open source building blocks. In fact, research shows that a single development team within a federal agency or a large government contractor might consume 300,000 open source and third-party software components each year to accelerate application development.

of the components in most modern applications are open source.

We Can't Protect it Like We Used to

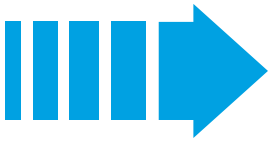
While the consumption of open source components by development organizations continues to improve delivery speed and innovation, there is a growing realization that not all parts are created equal. Sonatype's State of the Software Supply Chain Report revealed that 1 in 10 components used by development organizations to build applications contained at least one known security vulnerability. Well known vulnerabilities like Heartbleed, Struts, Poodle, Bash, Shellshock represent only a few of the thousands of defective components that have been used across applications supporting the Federal government.

As the dependence on open source components grows, it is increasingly clear that the ability to secure it has not kept pace. In some cases, we are not using the right tools. In others cases, our practices don't scale.

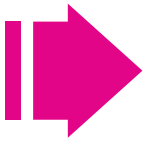
Adoption of Secure Devops Practices

SOURCE: 2019 DevSecOps Community Survey

27% have **mature** DevOps practices



48% are **improving** their maturity.



25% **immature** practices

Among the reasons components have become a favorite target for cyber adversaries is that they are a highly efficient gateway. A single open source component may be embedded in hundreds or even thousands of applications, so the force multiplication effect is stunning. Why launch a single attack on a single application, when you can target a vulnerable component and potentially compromise thousands of applications at once?

The most common application security tools employed today within RMF practices are Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). SAST and DAST approaches discover vulnerabilities in custom code while neglecting to evaluate the open source and third-party components used in the application. The result is that many RMF practices are blind with respect to vulnerabilities and security risks that lurk within open source components.

Recognizing the growing threat posed by vulnerable open source components, some federal agencies have employed open source governance practices within their RMF controls. These agencies define policies to identify which open source components are acceptable, and which one are not. These same agencies then rely on development teams or security personnel to manually assess each component before it is used. Although these manual efforts represent the best of intentions, the truth is that they are prone to error and are not scaleable. Simply stated, development and security teams don't have the time or resources to manually inspect the massive volume and variety of open source components that are feeding government software supply chains. When assessments take too long or happen too late, pressure to meet development deadlines can result in workarounds to manual RMF controls.

How to Reduce Application Cyber Risk

The Sonatype Edge for a Stronger RMF Process

The RMF requires cybersecurity risk management plans for all IT systems and prescribes a six-step process for accomplishing that objective. An effective approach to minimizing cyber risks associated with known vulnerabilities in open source components is for Federal agencies to automate many of their RMF security controls.

Sonatype's software supply chain automation solutions were purpose-built to closely align with RMF controls. These solutions can scale alongside the highest velocity development practices while simultaneously ensuring continuous controls recommended within the RMF. Sonatype's software supply chain automation solutions — **Nexus Auditor, Nexus Lifecycle,** and **Nexus Firewall** — are ideally suited to perform the security control functions recommended within the RMF.

NEXUS AUDITOR provides the ability to continually assess applications already in production. Nexus Auditor precisely identifies components and vulnerabilities within those applications. Customized or out of the box policies can be used over time to trigger alerts on components with known security vulnerabilities.

NEXUS LIFECYCLE applies user-defined policies and security controls to govern which open source and third-party components can be used for application development. Nexus Lifecycle integrates component intelligence directly into the development tools used by an agency — eliminating context switching for developers operating

under RMF security controls. When open source components are used that violate security policies, development teams are immediately alerted and guided through prescribed remediation options. Nexus Lifecycle also produces a precise software bill of materials for each application detailing compliance to RMF security controls.

NEXUS FIREWALL can automatically and continuously block substandard components from entering into government software supply chains. Nexus Firewall creates a trusted repository using automated policies that meet RMF security control requirements. Nexus Firewall serves as the first automated line of defense for RMF security controls aimed at software development.

Each Nexus product provides component intelligence to Federal agency software supply chains. Depending on the agency's requirements, this component intelligence can be delivered on-premises or as a hosted service. The intelligence provides a continuously updated set of public and proprietary data about the quality and security of open source components used to create the applications which support agency missions.

An attribute shared by each of these products is Advanced Binary Fingerprinting that is used to precisely identify components, including partial/modified matches. This technology minimizes false positives and false negatives and gives Federal agencies the ability to precisely identify the open source components underpinning their mission critical applications.

Without precise identification of components it is impossible to automate the discovery and remediation of vulnerabilities. Imprecise component identification such as File Name, File Hash, Namespace/Metadata or Source Code matching inevitably leads to significant investments in manual processes that fail to keep pace with development. The result is vulnerabilities persist.

Precision is the only way to empower teams to make better decisions, so that they can scale faster with RMF controls that are flexible enough to reflect the policies of the organization in the context of the applications that are being developed. Availability of precise data also eliminates the need to staff research teams to keep up with the volume of open source component vulnerabilities being announced.

To better understand how Nexus products support automated, continuous RMF security controls, we'll take a look at each step of the RMF security lifecycle.

RMF Step 1: Categorize Systems

Before automating RMF controls across the landscape of applications in a Federal agency, systems and applications must first be categorized.

For many Federal agencies, determining which controls to apply will be accomplished in a top-down "command and control" approach. In these instances, a select group of officials are responsible for categorizing the systems that will be managed through RMF controls. System categorization includes specifying the impact values (high, medium or low) for the confidentiality, integrity and availability security objectives. Then subordinate organizations may add specific systems or applications specific to their mission.

For some agencies or departments, the systems and applications their teams work on exhibit more logical categories, such as Internal, Classified, or citizen facing. Appropriately categorizing systems includes determining their security profiles and objectives.

Once systems are categorized, open source governance and security policies can easily be defined

in Nexus products that map to any organization, mission, or logical structure in step 2 of the RMF.

RMF Step 2: Select Security Controls

Security controls within the RMF address multiple areas such as risk assessment, supply chain protection, vulnerability scanning, flaw remediation, continuous monitoring and security alerting. Using Nexus software supply chain automation solutions, Federal agencies have the latitude to tailor 'organization defined parameter values' for each of these controls. Controls can be applied at many stages along the application development lifecycle, targeting specific types or groups of applications.

Nexus products allow flexible and granular control over open source governance policies empowering RMF participants from independent security assessment professionals, to program managers, to information security architects to meet their specific responsibilities.

For example, using Nexus Firewall, information security architects may want to define a control that restricts downloads of known vulnerable open source components with CVSS scores with severity levels ranging from 7.0 to 10.0. Architects might also want to establish policies to prevent components four years or older from being downloaded as research indicates they have 3x the security defect rates of newer versions.

In another instance, program managers or system owners may be responsible for ensuring the appropriate security controls are selected for a category of citizen self-service applications outside the firewall. In this instance, the program manager could recommend Nexus Lifecycle be used to define a control that prevents vulnerable versions of the Struts 2 web application framework from being used in the development of those applications. If a developer attempts to use a vulnerable version, controls can block the use of that component and also be used to indicate other versions that do not pose a security risk.

In Step 2, users of Nexus products can focus on defining controls that can be automated. While experts define the controls, implementation of those controls is focused on machines, not humans. Using machine-based adjudication of controls with Nexus solutions enables agencies to scale their application security practices to any level.

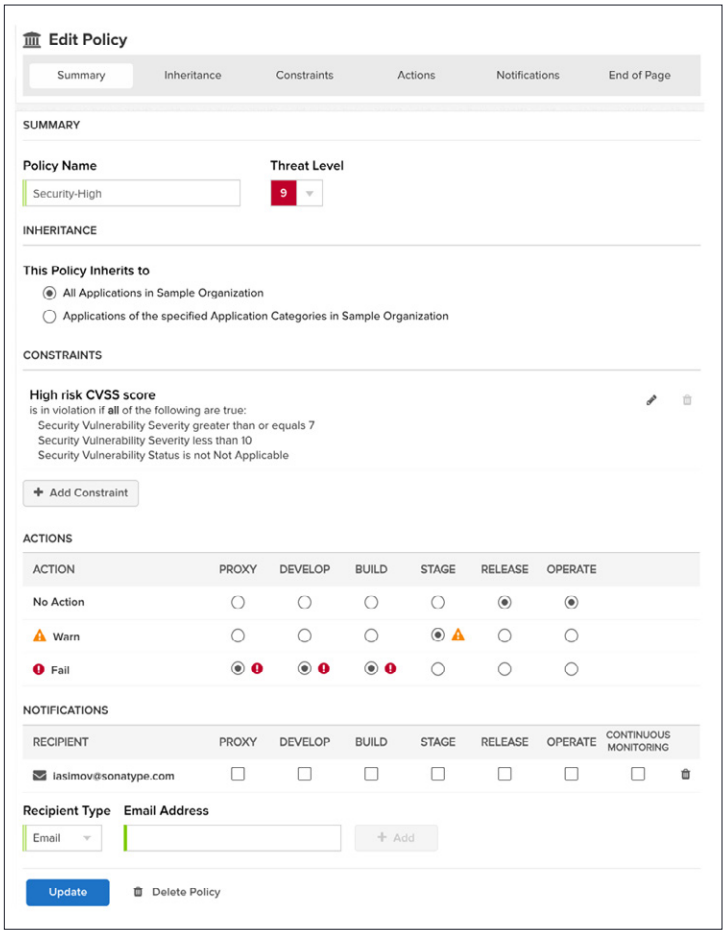
RMF Step 3: Implement Security Controls

According to NIST's RMF Guide, organizations are best served by implementing application security controls within software engineering methodologies and secure coding techniques. When controls are placed earlier within development practices, notifications of security vulnerabilities can be addressed sooner thereby reducing risk. An additional benefit is the reduction in rework by development teams and a corresponding decrease in the cost of developing and sustaining applications.

Software supply chain automation supported by Sonatype's Nexus products enable development teams to implement security controls directly into the environments where applications are being designed, built, tested, and released. For example, Nexus Lifecycle can apply automated controls directly into the tools development teams use every day, including Eclipse, IntelliJ, Jenkins, Bamboo, JIRA, Sonarqube and others.

The policy definition features provided in Nexus products detail the control name, threat level, constraints, conditions, actions and notifications that will be automated. For example, a control might

be added to prevent a developer from using any open source component with a CVSS score between 7 and 10. When this control is adding to a Jenkins continuous integration server, it can be set to break the build, and notify the appropriate personnel of the violation. Controls are also established to help developers evaluate safer, alternative component choices. All Nexus products also support automatic dissemination of security alerts or advisories across the organization based on customizable threat profiles.



▲ Documentation of each security control inside Nexus tools allows for easy auditing of controls and traceability of actions prior to and after development of the application.

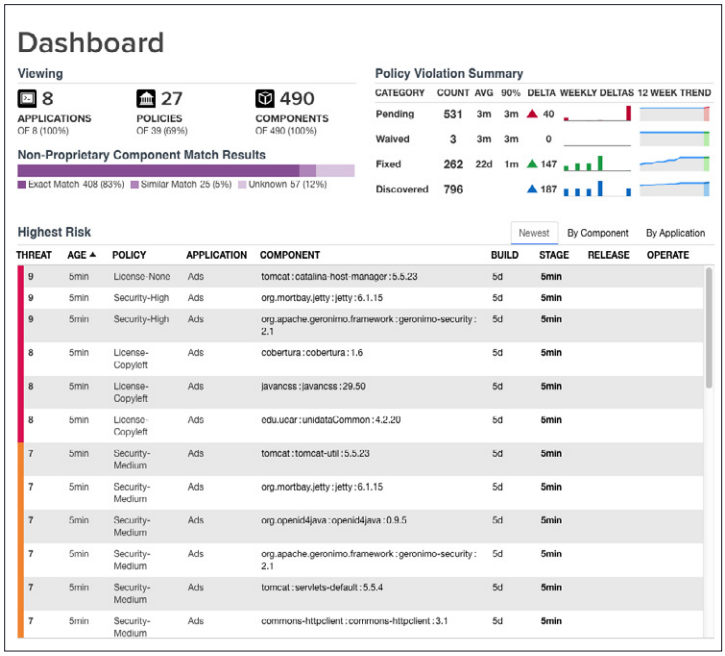
▶ Reports in Nexus Lifecycle and Nexus Auditor automate the assessment of security controls across the application portfolio. Every open source component is automatically identified across development and production.

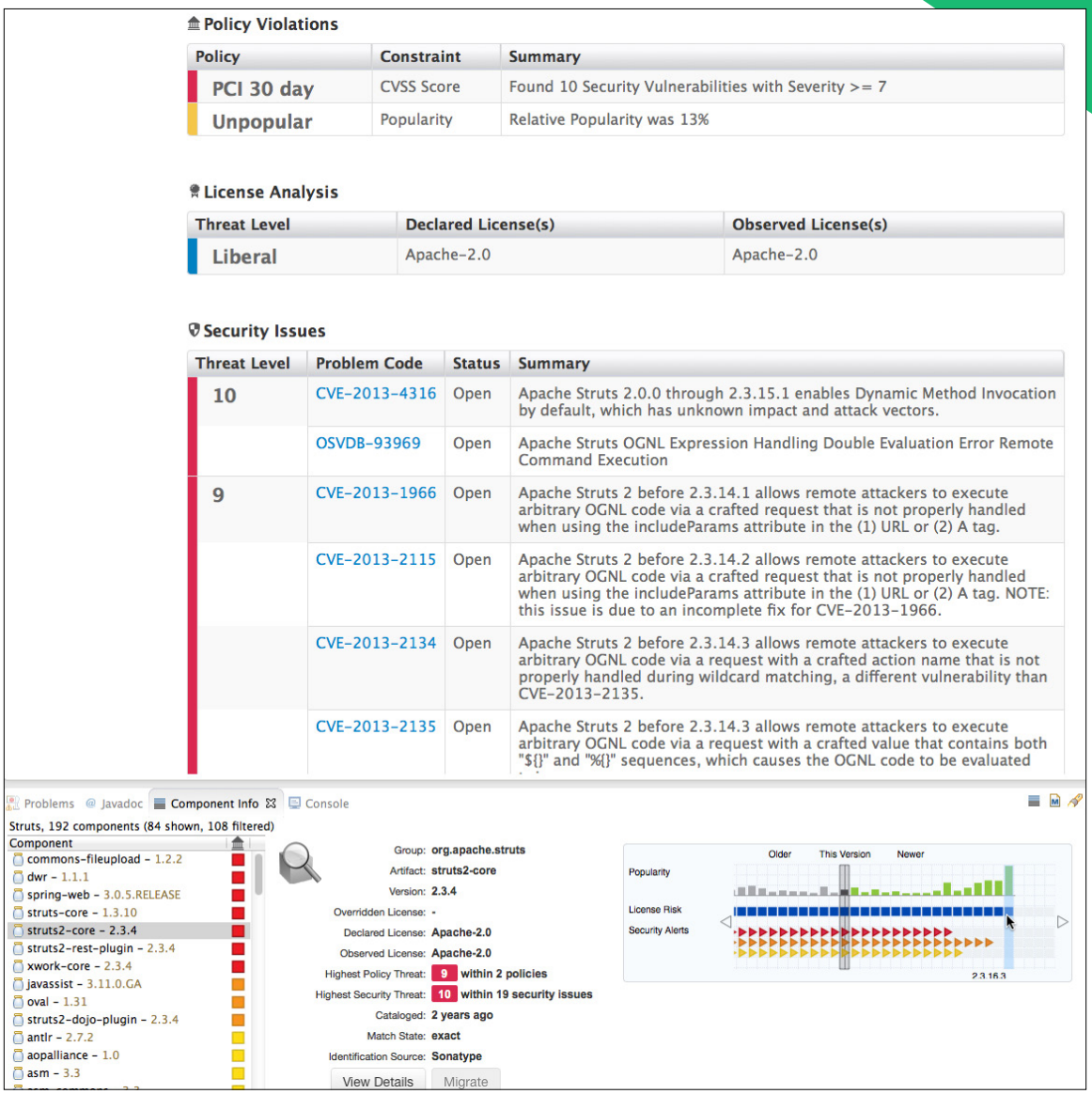
RMF Step 4: Assess Security Controls

NIST's RMF guidelines state, "Organizations are encouraged to maximize the use of automation to conduct security control assessments to help: (i) increase the speed and overall effectiveness and efficiency of the assessments; and (ii) support the concept of ongoing monitoring of the security state of organizational information systems.

Assessing security controls with Nexus products is straight-forward for program owners, development managers, and independent security teams. All teams can utilize the same reporting dashboard that offers customizable views on security controls and their effectiveness.

Security assessment reports are automatically created via the reporting dashboard in Nexus Lifecycle and Nexus Auditor. The dashboard precisely identifies all open source and third-party components used during design, build, and release phases of development. The dashboard offers an intuitive assessment of applications under control,





▲ Developers can use Nexus Lifecycle to understand which versions of a given open source component meet or violate the security control policy.

highlighting any issues and their threat level based on sensitivity to a particular type of risk.

Every open source and third-party component used across development is recorded by attribute data including version, age, popularity, potential license issues and known security vulnerabilities. Risk levels are also assessed per application, while highlighting which stage of development the application is in at the moment (e.g., build, test, production).

By enumerating the risk levels, the dashboard helps assessors, development managers, and security teams understand where and how controls are working. Teams can also use the report to prioritize remediation efforts and track their progress toward resolution.

The dashboards in Nexus Lifecycle and Nexus Auditor are especially helpful when assessing controls and the zero-day impact for new security vulnerabilities. For example, let's say a critical vulnerability was discovered in a well-known open

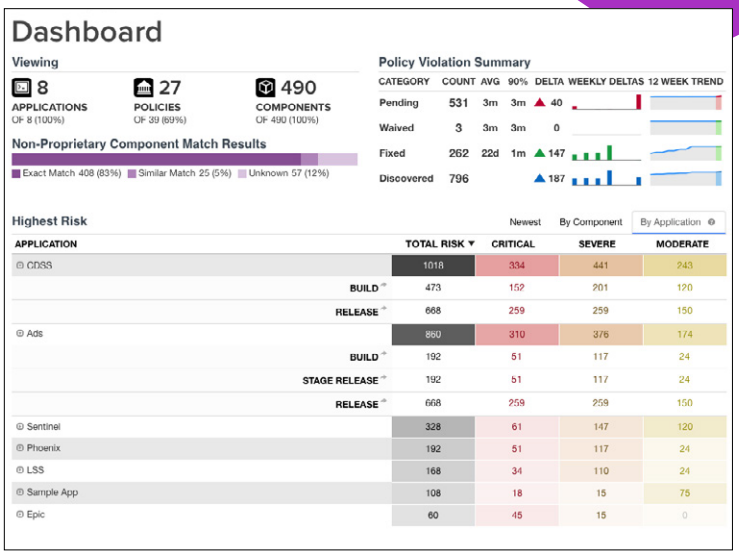
source cryptographic library. The dashboard in Nexus Lifecycle would immediately highlight if and where that component was being used in development. The same dashboard in Nexus Auditor would detail where it exists across any application in production. Development, security and assessment teams relying on the same automated policy controls and real time component intelligence could simultaneously evaluate the vulnerability and determine its risk to the agency's operation or mission.

When all parties are assessing the same automated controls through common tools and data services, the result will be a much higher rate of compliant controls for open source and third-party components during the assessment phase of the RMF. This will also lead to a reduction in re-work by development teams and a corresponding decrease in the cost of development.

RMF Step 5: Authorize Systems

All of the dashboard reports generated by Nexus products can be used as artifacts for the preparation of an IT security plan of action. The dashboard reports help identify top priorities and also track progress toward remediating known open source vulnerabilities across the applications where they exist. Because the security policies, controls, remediation priorities and reporting are all available to all parties using Nexus products, risk mitigation efforts are consistent across the organization.

The risk assessment reporting provided within Nexus Lifecycle and Nexus Auditor help inform the creation of the security authorization package in Step 5. Information in the Nexus dashboard reports are used by authorizing officials to make risk-based decisions. The reports also serve as an effective audit trail for the Authorizing Official.



▲ Reports in Nexus Lifecycle and Nexus Auditor automate the assessment of security controls and help inform the plan of action.

Nexus products minimize false positives and false negatives, providing the Authorizing official greater confidence that the controls are compliant and accomplishing the security objectives for that application.

RMF Step 6: Monitor System Controls

As open source and third-party components age, is it more likely that security vulnerabilities will be discovered in them. Research shows that open source component version between 7 and 10 years of age have 3x higher vulnerability rates than components between 1 and 3 years old. Therefore, it is critical to track components throughout the lifecycle of an application, especially after they are released into production environments where exploits occur.

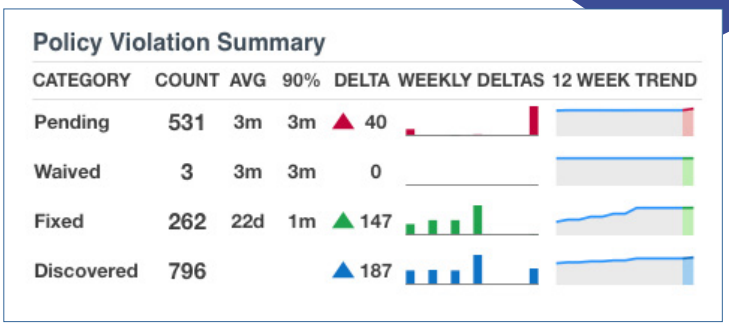
The RMF requires continuous monitoring of systems. Each Sonatype product described in this white paper provides continuous real time

component intelligence that can be delivered as an alert within a dashboard, a detailed report, or integrated within an application development tool.

For example, the dashboard available in Nexus Lifecycle and Nexus Auditor continuously tracks policy violations that have been discovered, alerts pending further investigation, and the number of risky open source components that have been fixed. Program Managers can use this view to quickly assess progress being made to manage open source component vulnerabilities across their application portfolio.

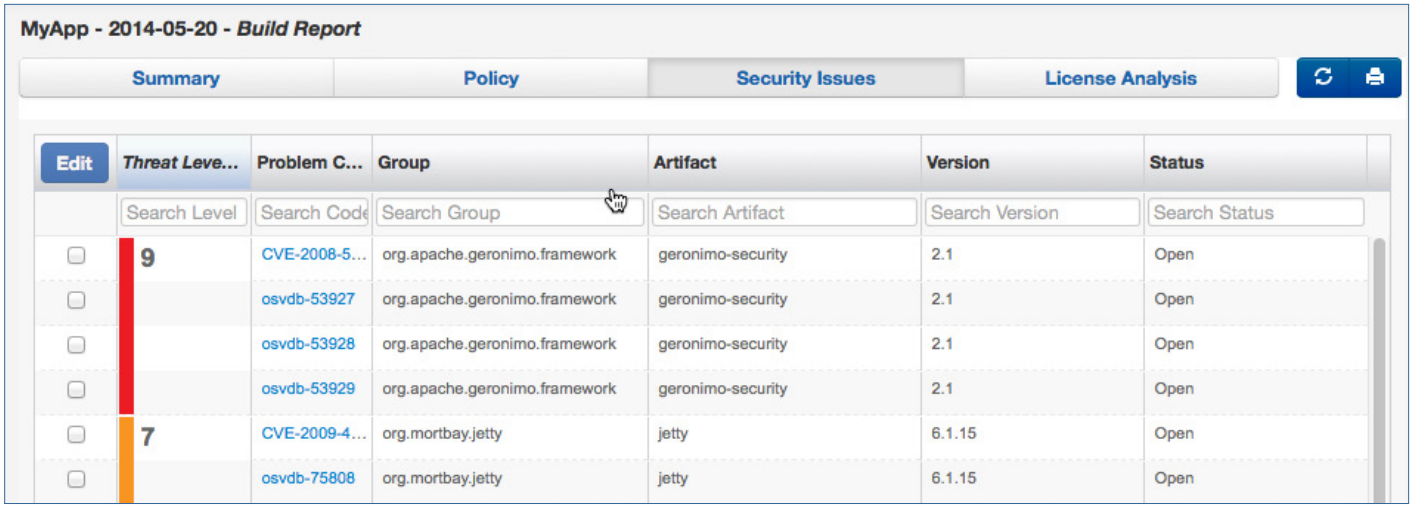
As an additional example, Nexus Firewall produces an audit report of quarantined components in a repository manager that triggered policy violations. This information can be used to help refine and strengthen security controls for open source components used in development.

Nexus Lifecycle maintains a complete inventory of components used in development to produce a software Bill of Materials for each application. It constantly monitors which components are used and analyzes them for known vulnerabilities. When vulnerabilities are discovered, Nexus Lifecycle provides automatic alerts to developers and quickly informs them of alternative, safer component choices.



▲ Nexus Lifecycle and Nexus Auditor dashboards help Program Managers quickly assess progress on open source component security controls.

Nexus Auditor can be used to continuously monitor open source components within an application after it has received Authority to Operate and it is no longer active in development. If new security vulnerabilities arise, Nexus Auditor automatically sends an alert or advisory based on customizable policy guidelines. The ability to track vulnerabilities for fielded applications will improve incident response times for remediating those security issues.



▲ A Software Bill of Materials automatically generates a report of each open source component in an application and provides details of any known security vulnerabilities.

Summary

Open source and third-party components are the foundation of mission-critical applications in the Federal government. Today, those components often contain cyber security vulnerabilities that represent a large and fast-expanding attack surface for adversaries. Consequently, agencies must take new approaches to ensure those components are of the highest quality and free from known vulnerabilities that put their missions, their information, and their IT assets at risk.

Practices detailed within the Risk Management Framework prescribe a comprehensive approach to continuous risk management. When it comes to managing risks within open source and third-party components, many of the RMF security controls can now be automated. Automation of RMF security controls enables agencies to operate at unprecedented speeds that significantly accelerate mean times to remediate risks while reducing the landscape vulnerable to exploits.

Agencies that are not evaluating, monitoring, and tracking the use open source and third-party application components within the scope of their RMF assessment and authorization programs are exposing themselves to significant and elective risks. The potent combination of RMF tactics — employing Sonatype purpose-built products — can effectively minimize this critical segment of application security for federal agencies.

sonatype

More than 10 million software developers rely on Sonatype to innovate faster while mitigating security risks inherent in open source. Sonatype's Nexus platform combines in-depth component intelligence with real-time remediation guidance to automate and scale open source governance across every stage of the modern DevOps pipeline. Sonatype is privately held with investments from TPG, Goldman Sachs, Accel Partners, and Hummer Winblad Venture Partners. Learn more at **www.sonatype.com.**

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
1 Primrose Street
London EC2A 2EX
United Kingdom

APAC Office
5 Martin Place, Level 14
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com