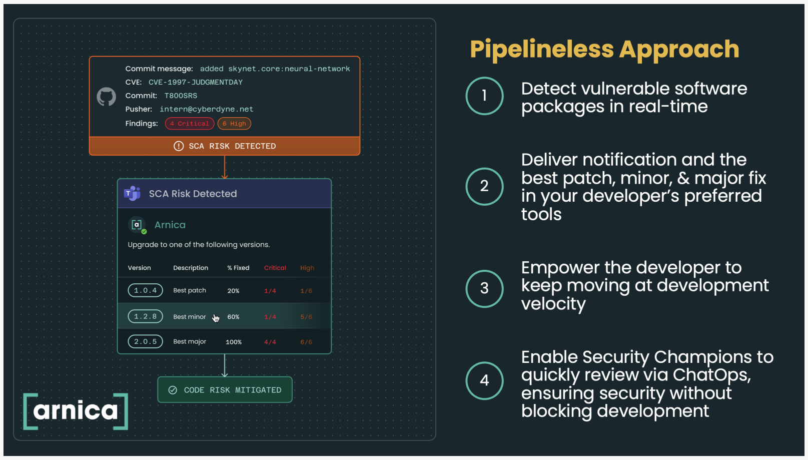
EINPRESSWIRE

Arnica Launches “Security Champions with Arnica” Feature for AppSec and Dev Teams

New feature addresses key challenges organizations face in identifying, engaging, and empowering security champions within their development teams

ATLANTA, GA, UNITED STATES, April 7, 2025 /EINPresswire.com/ -- [Arnica](), the leading pipelineless, developer-native workflows provider, today launched its newest feature, called [Security Champions]() with Arnica, for the company’s Developer-Native Security Workflows platform. The new feature is a first-of-its-kind designed to automate the identification, engagement, and empowerment of security-minded developers.



Commit message: added skynet.core:neural-network
CVE: CVE-1997-JUDGMENTDAY
Commit: T800SRS
Pusher: intern@cyberdyne.net
Findings: 4 Critical 6 High

SCA RISK DETECTED

SCA Risk Detected

Arnica

Upgrade to one of the following versions.

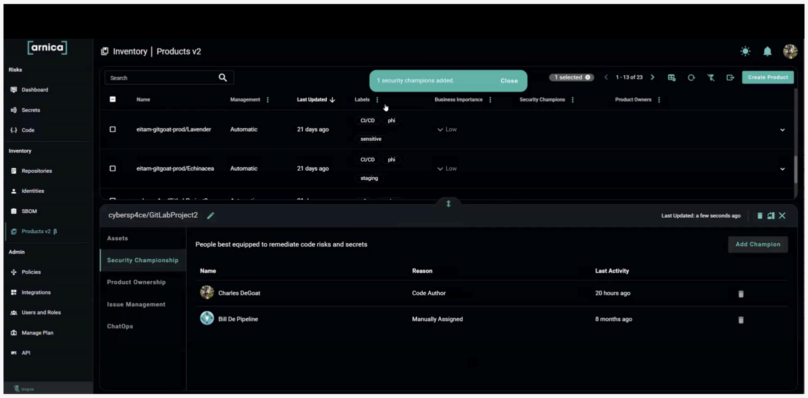
Version	Description	% Fixed	Critical	High
1.0.4	Best patch	20%	1/4	1/6
1.2.8	Best minor	60%	1/4	5/6
2.0.5	Best major	100%	4/4	6/6

CODE RISK MITIGATED

Pipelineless Approach

1. Detect vulnerable software packages in real-time
2. Deliver notification and the best patch, minor, & major fix in your developer’s preferred tools
3. Empower the developer to keep moving at development velocity
4. Enable Security Champions to quickly review via ChatOps, ensuring security without blocking development

Security Champions Workflow



1 security champions added. Close

Name	Management	Last Updated	Labels	Business Importance	Security Champions	Product Owners
eitam-gitgoat-prod/Lavender	Automatic	21 days ago	CI/CD phi sensitive	Low		
eitam-gitgoat-prod/Echinacea	Automatic	21 days ago	CI/CD phi staging	Low		

cybersp4ce/GitLabProject2

Last Updated: a few seconds ago

People best equipped to remediate code risks and secrets

Name	Reason	Last Activity
Charles DeGoat	Code Author	20 hours ago
Bill De Pipeline	Manually Assigned	8 months ago

Security Champions Dashboard View

This update, alongside powerful issue management integrations and enhanced access controls, enables organizations to more easily scale their security programs while maintaining developer productivity. A recent survey by Nominet showcased the true power of security champions -- it found that organizations with a Security Champion program were 65 percent less likely to experience a data breach than those without one.

“For years, organizations have struggled to identify, train, and retain security champions within their development teams,” said Nir Valtman, chief executive officer at Arnica. “Developers who are identified as ‘Security Champions’ are not over-burdened by the designation. Security engagement is effortless and directly benefits their existing workflow, while also making their expertise more visible across the organization. This can improve career growth opportunities and help them influence security culture.”

Security champions are essential in bridging the gap between rapid software development and robust security. However, traditional methods rely on self-nomination or manual selection, making it difficult to engage the right individuals.

Arnica’s innovative behavioral analysis and automation ensure that organizations accurately identify and seamlessly activate security champions:

* Identity Mapping & Behavioral Analysis - automatically identifies security champions based on real developer actions, coding behaviors, and risk management efforts.

* Target Risky Development - detects frequent risk creators to provide targeted security interventions.

* Real-time Insights - leverages real-time insights to enhance security culture without disrupting development.

* Developer-Native Workflows - utilizes fast, nimble security workflows to engage with security champions in the tools where they already work including Slack, Microsoft Teams, and in pull requests.

* Risk Dismissal Workflow - A developer requests to dismiss a vulnerability, which is then sent for review by security champions or the security team. They evaluate the justification and approve or reject it in real time via ChatOps, ensuring security without blocking development

NEW FEATURE UPDATES TO SUPPORT SECURITY CHAMPIONS:

The automation security champions really need - managing security risks has never been easier to ensure security issues are resolved efficiently and to empower security champions to customize granular workflows at scale.

* Automate Risk Mitigation - automate risk identification, generate context-rich tickets, automatically mitigate or track mitigations in real-time, and close tickets in Jira (or Azure DevOps Boards)
* Route Tickets By-Product - automatically assign issues where they belong
* Open & Close Multiple Tickets at Once - save time with bulk actions □
* Easily Copy/Paste Settings Across Products - effortless configuration
* Dynamic Field Mapping - seamlessly sync Jira and Arnica fields with if/then logic for smarter workflows

Role-Based, Row-Level, and Product-Level Security Access - Arnica introduces enhanced access control features that give administrators the power to define and enforce precise user permissions and so that security champions can see their own products automatically instead of requiring complex provisioning.

* Role-Based Access Control (RBAC) - enhances security, supports compliance, and reduces risks with role-based access controls. Administrators can now assign roles to users, determining their level of access to resources and functionalities. Custom roles can be created to meet unique organizational requirements, ensuring users only interact with the data and tools necessary for their role. With a centralized interface, permissions can be easily managed and updated, providing seamless security oversight.

* Row-Level Security - Arnica's row-level security feature allows administrators to control access to specific rows within a table based on a user's identity or assigned role. By implementing fine-grained filtering logic, organizations can restrict which rows users can query, update, or delete, ensuring data is accessed only by those with the proper authorization.

* Product-Level Security - the newly introduced product-level security ensures developers only see and engage with the products they are assigned to. This prevents unnecessary exposure to risk findings across the organization and enables developers to focus on addressing security issues relevant to their responsibilities.

* Ask for Your Risks - Enable seamless risk management through Microsoft Teams bot commands. Security champions can instantly access relevant vulnerabilities using the risks product command, eliminating the need for complex dashboards. This automation enhances efficiency, allowing security champions to focus on risk mitigation while maintaining developer productivity.

For more information about Arnica and the Security Champions with Arnica update, visit www.arnica.io

LINKEDIN

###

About Arnica
Arnica, headquartered in Atlanta, Georgia, powers the most effective application security programs in the world. At Arnica, we envision and build toward a future in which software development is unimpeded by risk. We build solutions that secure the software development lifecycle, align to developers rather than disrupt them, remove barriers to security by simplifying risk mitigation, and are loved by both security and developers. For more information on Arnica, visit www.arnica.io

Nicolia Wiles
PRIME|PR
+1 512-698-7373
email us here