Securing Enterprise Software Where Development Starts: Unissant's integrated Vulnerability Assessment (iVA)

A Unissant Accelerator

Unissant White Paper Series

Securing Enterprise Software Where Development Starts: Unissant's integrated Vulnerability Assessment (iVA)

A Unissant Accelerator

Table of Contents

Copyright © 2024 Unissant, Inc. All Rights Reserved.

Today's federal software supply chain incorporates third-party solutions, open-source libraries, cloud-based components, and new technologies to enable emerging priority areas such as AI: a complex ecosystem, indeed. It's not enough to simply write secure code. Building software on secure foundations requires a structured approach to pinpointing and mitigating risks within the software supply chain.

Federal applications empower the business of government. These applications, whether developed in-house or procured from commercial vendors to be configured or customized, incorporate code from diverse sources. Code often includes third-party open-source libraries which, while valuable, can introduce vulnerabilities.

Over the past two decades, the introduction of agile practices has emphasized the need to "shift left" to reduce risk. Development teams widely embrace secure coding practices. IT shops are maturing their DevSecOps approaches, enabling faster development cycles with fewer security vulnerabilities. Applying automation in the deployment pipeline, more organizations are scanning infrastructure and software configurations for vulnerabilities sooner, preventing insecure configurations from being deployed to production.

Despite the shift left, though, these approaches don't move left enough. The 2020 SolarWinds hack and the 2021 exploit of log4j vulnerabilities highlighted weaknesses within the federal IT supply chain. In response, the 2021 Executive Order titled 'Improving the Nation's Cybersecurity' (President's EO 14028) mandated U.S. government agencies use only software vendors that provide Software Bill of Materials (SBOM) for their products and solutions.

In 2022, CISA emphasized the importance of securing the federal software supply chain, delivering specific guidance for software developers, vendors, and **customers**. Guidance covered both the procurement/acquisition phase and deployment phase (full lifecycle) of a given piece of software.

How do agencies better assess software components throughout the lifecycle of the software's use within their systems and environments?

Copyright © 2024 Unissant, Inc. All Rights Reserved.

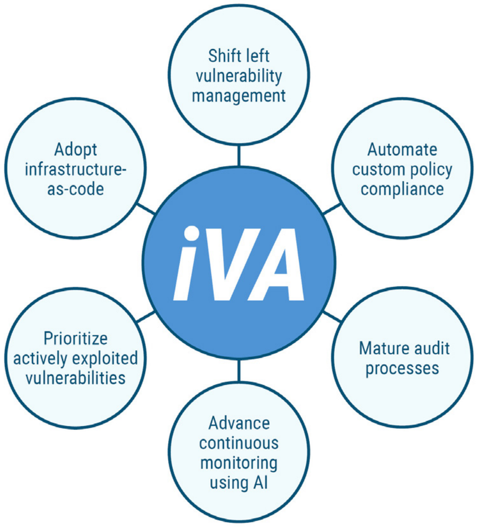
iVA
Shift left vulnerability management
Automate custom policy compliance
Mature audit processes
Advance continuous monitoring using AI
Prioritize actively exploited vulnerabilities
Adopt infrastructure-as-code

Figure 1: iVA framework best practices

Shifting "left enough"

Recognizing the imperative to reduce risk associated with the federal software supply chain, we developed Unissant's integrated Vulnerability Assessment (iVA) accelerator and associated iVA framework. Together, our accelerator and framework support a security as code (SaC) approach. They empower federal organizations to pinpoint and mitigate risks within their software supply chain prior to deployment, improving the agency's security posture.

iVA harnesses the power of SBOMs for vulnerability analysis, taking a proactive approach to monitor the utilization of software components across all versions of each application within the organization's portfolio. Notifications and alerts allow teams to understand vulnerabilities identified anywhere in the enterprise, enabling broader awareness of risks—and the ability to prioritize remediation. Artificial Intelligence (AI), integrated into existing CI/CD pipelines via APIs, enables automation of remediation activities. Role-based dashboards provide transparency at the appropriate levels to support project, program, division, and enterprise visibility into the vulnerability landscape.

Unissant's iVA accelerator is part of our iVA framework—a set of core best practices that offer a more integrated and mature approach to vulnerability management.

Copyright © 2024 Unissant, Inc. All Rights Reserved.

Unissant's iVA framework best practices

Best practice: shift left vulnerability management

Mature DevSecOps processes move vulnerability management earlier in the lifecycle. For example, when a developer introduces a new component or package into the application, the component or package is scanned for known vulnerabilities along with active exploits. The package can be verified against previous usage attempts along with any policy violations.

Unissant's approach: automate the creation and ingestion of SBOMs

Our iVA accelerator automates the creation and consumption of SBOMs, providing real-time vulnerability management analysis. iVA can instantly notify developers and security personnel of potential violations. Alerts enable teams to address issues as early as possible, reducing the risk and impact of potential threats. Programs with advanced CI/CD capabilities, producing hundreds of releases weekly or month, can catch vulnerabilities earlier in the lifecycle, avoiding costly mistakes in production.

Best practice: automate custom policy compliance

Open-source software can be a powerful tool for developers, offering flexibility, cost-efficiency, and access to innovative features. However, increased use of open-source has introduced new challenges: agencies must have clear licensing policies, maintain an up-to-date inventory of open-source components used, understand the specific terms of each license, and ensure that use complies with policies. Most agencies lack an automated means to check software for license and vulnerability policy compliance prior to deployment.

Unissant's approach: customize policy management

iVA manages policy rules, enabling the enterprise to define custom compliance standards and continuously monitor them. Leveraging our expertise in open-source licensing intricacies, we set up pre-defined license policy tracking metrics. Once defined, the system can automatically track any deviations from pre-defined policies, providing real-time notifications. This proactive approach allows organizations to promptly address issues, ensuring that teams eliminate policy non-compliance before software is released in production. A proactive approach significantly reduces security risk as well as legal and financial repercussions.

Copyright © 2024 Unissant, Inc. All Rights Reserved.

Best practice: mature audit processes

Modern software development practices that emphasize a distributed approach allow developers to reuse software components and packages across a multitude of applications. While reuse increases efficiency and reduces time-to-market, it also introduces risk. Widespread use of components that harbor vulnerabilities increases scale and impact exponentially. Every application relying on that component becomes potentially vulnerable. The log4j vulnerability serves as a perfect example. Java programming modules impacted a vast number of production applications worldwide, incurring substantial costs for organizations.

Traditionally, the tracking of vulnerabilities and associations with application components (dependency tracking) has been manual and time-consuming. Organizations need automated auditing, dynamic monitoring, and a centralized view into the extent of impact across enterprise applications.

Unissant's approach: automated, dynamic auditing

Auditing features within Unissant's iVA accelerator enable organizations to ensure their software packages are secure and compliant with industry standards and regulations. Automated processes continuously monitor all components across an organization's applications, identify any known vulnerabilities, and alert the relevant teams for further action. Alerts speed awareness of potential vulnerabilities, freeing up security teams from notification tasks. Instead, security personnel can focus on analyzing insights from iVA and identifying intricacies and nuances that might impact the organization's response.

iVA supports greater transparency with role-based dashboards. Executives can readily obtain a high-level view of vulnerabilities across the organization and delve into specific components or vulnerabilities with a simple click. As organizations mature their processes, we empower security professionals to make data-driven decisions quicker and evaluate the best options to address threats.

Copyright © 2024 Unissant, Inc. All Rights Reserved.

Best practice: advance continuous monitoring using AI

The rapid evolution of technology introduces new attack vectors, potentially compromising sensitive data and disrupting mission operations. Continuous vulnerability assessment is paramount for managing these risks. Agencies must regularly scan and test systems for potential weaknesses, identifying and prioritizing vulnerabilities based on their potential impact. Expedient action in applying patches or other remedies reduces risk. Automating tracking, notification, and remediation and leveraging AI that learns from past vulnerability data and threat intelligence enables faster detection, prioritization, and patching.

Unissant's approach: scheduled updates and targeted notifications

iVA streamlines vulnerability management with configurable templates that leverage public and private threat intelligence feeds. This approach allows organizations to automatically update vulnerability repositories at regular intervals for a head start in tracking threats. Our accelerator integrates with existing mitigation strategies, notifying affected teams and suggesting remediation steps. This minimizes the dwell time between vulnerability identification and patching. Furthermore, iVA leverages AI to learn from past incidents, improving its ability to detect and respond to emerging threats. Automated remediation workflows, either within the platform or through APIs to other security tools, further accelerate patching and reduce the risk of a full-blown breach.

Best practice: prioritize actively exploited vulnerabilities

The volume of reported vulnerabilities can put immense pressure on security teams, often causing them to operate in a reactive rather than proactive mode. The Exploit Prediction Scoring System (EPSS) aims to address this issue, providing a data-driven estimate of the likelihood that a particular software vulnerability will be exploited. Using the EPSS, organizations can prioritize their remediation efforts, focusing their resources on vulnerabilities that are actively being exploited or have a high probability of being exploited soon. While EPSS helps organizations prioritize remediation efforts, the process of accessing EPSS data is typically manual, leading to slow and inconsistent application of insights.

Unissant's approach: integrate with the Exploit Prediction Scoring System (EPSS)

iVA provides automated integration with EPSS as part of the organization's CI/CD pipeline. As new exploits are found, real-world data helps direct security teams to the most actively exploited critical vulnerabilities. This reduces a security team's manual workload and helps standardize the organization's approach to leveraging EPSS. Unissant's experts can extend the value of EPSS, using AI models built on agency data to improve prediction accuracy.

Copyright © 2024 Unissant, Inc. All Rights Reserved.

Best practice: adopt infrastructure as code

As agencies mature their DevSecOps practices, more IT organizations are emphasizing the importance of infrastructure as code. IaC automates provisioning and management processes, reducing manual effort and improving consistency while enabling agility and responsiveness to changing mission priorities. Advancing SaC by using IaC improves the agency's security posture, eliminating manual configurations that can lead to inconsistency and introduce security vulnerabilities.

Unissant's approach: scheduled updates and targeted notifications

Unissant designed iVA to be consistent with a shift left mindset, such as embedding security best practices through code. Many popular IaC tools are open source, introducing potential vulnerabilities with far-reaching impacts if code is exploited. Integrating iVA within the CI/CD pipeline enables teams to scan IaC configurations for vulnerabilities before deployment, helping identify and remediate security issues early on. Using a version control system for IaC also helps agencies respond rapidly if vulnerabilities are identified.

Empowering the evolution of DevSecOps to SecDevOps through intelligent automation

DevSecOps teams are constantly seeking ways to integrate security earlier in the development process (shifting left) and improve their agency's overall security posture. To achieve this, they need intelligent and automated tools to continuously identify and remediate potential vulnerabilities. Shifting "further left" supports maturity of processes that emphasize security first—moving to a SecDevOps model.

Unissant's iVA solution empowers organizations to take a proactive approach to software supply chain security. It combines expertise in AI, cybersecurity, operations, development, and automation, providing a comprehensive solution to navigate the ever-evolving threat landscape with confidence.

About Unissant

Mission-focused, data-driven—Unissant Inc. (Unissant) delivers for the agencies that keep our nation healthy and safe. Keeping people and mission at the forefront, we apply our domain expertise, data acumen, and technology know-how to achieve breakthrough results. Agencies turn to Unissant for our expertise in AI, advanced analytics, digital excellence, and cybersecurity solutions. Our proven frameworks drive successful execution of complex projects at enterprise scale. With an unwavering commitment to advancing mission outcomes, our teams engineer human-centered, innovative solutions that accelerate time to value. We bring honesty, integrity, and dependability to every interaction with our employees, clients, and partners.

For more information, visit us at **www.unissant.com**.

Copyright © 2024 Unissant, Inc. All Rights Reserved.