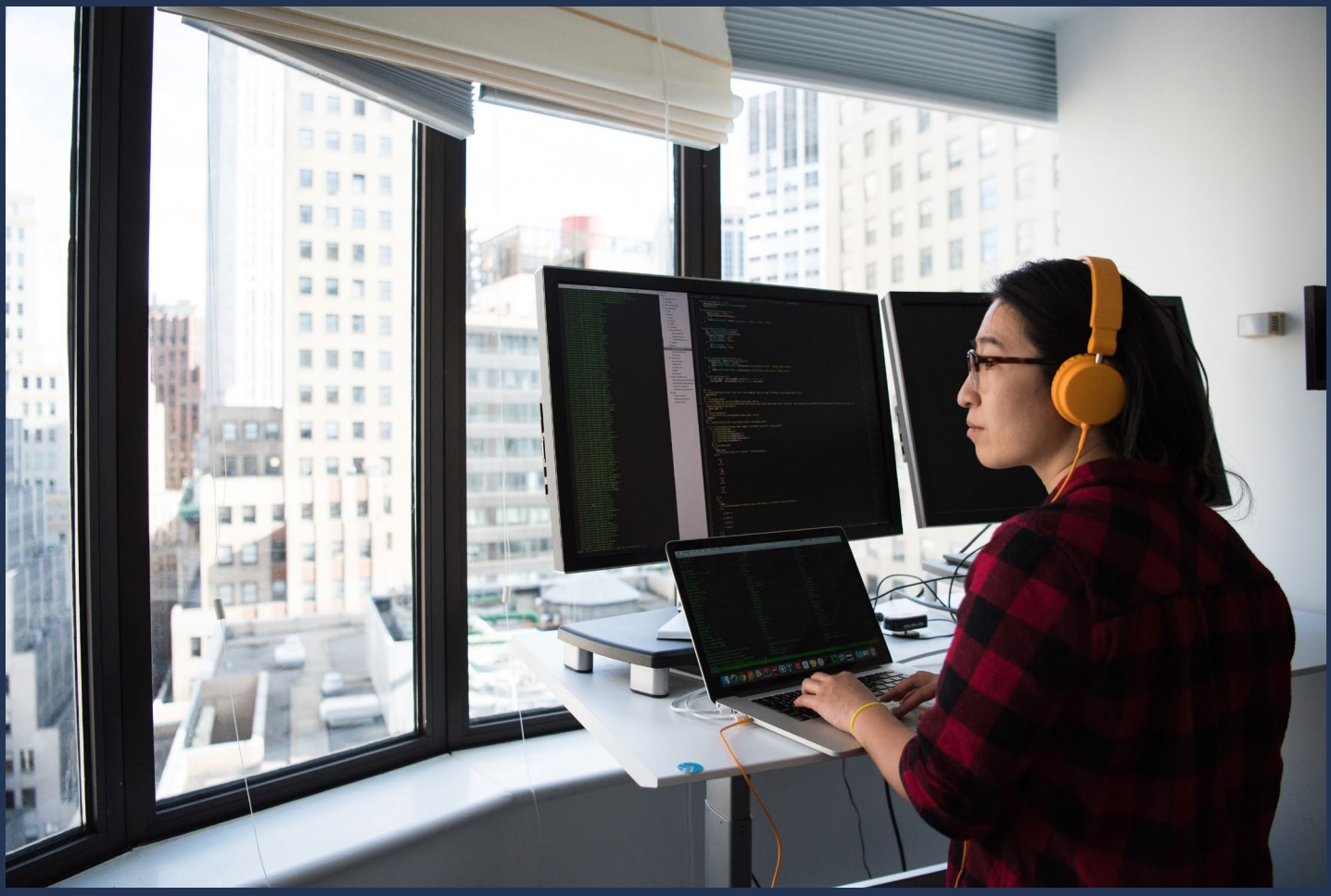
OMNI



Cybersecurity Compliance: Achieving a Single Pane of Glass

A GOAL FOR DEVSECOPS AND RMF IT SECURITY ENGINEERS

EXECUTIVE SUMMARY

From a risk-management perspective, DevSecOps engineers and Risk Management Framework (RMF) IT security engineers are, in many ways, operationally out of sync. Although the tools and methodologies they use are similar to some degree, there are areas of significant disparity that lead to the two communities speaking different operational languages.

In this paper, we discuss the reasons for this disparity and the potential benefits of bringing these two communities together. We also present what we think needs to be done so they can integrate with each other, speak a common language, and automate implementations—particularly with regard to the RMF process.

Our hope is that this paper will be used as a guideline to spur further research and development that will lead to a more forward leaning and comprehensive security posture. Such a posture will rely less on intermittent monitoring, sporadic manual intervention, and documentation. Instead, it will embrace the principles of agile methodologies, ensuring overall life-cycle security and compliance through automation using emerging tools and technologies.

THE GOAL: A SINGLE PANE OF GLASS

The goal is to establish a way to integrate tools and methodologies used by DevSecOps and IT security engineers with regard to the RMF process. From a technical implementation perspective, when integrating tools and data from disparate sources, we must establish a shared means for interfacing and normalizing data.

One of the greatest challenges in this process is the wide range of technologies and different standards for managing data that are used across the Department of Defense's (DOD's) organizations. Without a translation layer to successfully ingest and map different data sources to key controls and intent, there can be no truly shared technology or scalable end-to-end automation for RMF workflows and analyses.

That said, we can pave the path forward for the entire DOD. The key is to adopt a shared standard or point of ingestion (such as a REST API). It's also crucial to develop a solution for mapping keywords, fieldnames, and technology types as inputs to corresponding risk assessments, levels, and evaluations.

If we can succeed at this, we will come away with a single pane of glass—a singular, definitive, data-fusion view that provides a constructive and holistic understanding of the overall system security posture and risk profiles. This single pane of glass is what would allow us to understand the true end-to-end cybersecurity risk posture—from software development operations to systems in production.

Components of such a solution may include the following:

Common operational language and standards

The DevSecOps world focuses on agile tooling, but often foregoes the larger, more ancillary risks that RMF catches. On the other hand, the traditionalists often get a limited view of nuanced technical risks and automation opportunities the DevSecOps world benefits from. Instead of choosing one or the other, marry the best of both worlds.

Data normalization

What if we could take a tool, like the results aggregator OWASP Defectdojo, and map it to the RMF framework? It's a win-win scenario if we can normalize the data using all-new tooling. This will inherently improve an information systems security posture and benefit the RMF assessment and authorization (A&A) process. This is achieved by reducing the manual mapping and Level of Effort for addressing all of the Information Assurance (IA) controls and Control Correlation Identifiers (CCI) individually.

Furthermore, it would be wonderful if we had the ability to ultimately ingest that data into something like an eMASS/Xacta as well. Currently, those solutions do not correlate with any of the cybersecurity compliance expressions from industry-standard software development (DevSecOps) tools. However, seeing the different results map onto RMF compliance control requirements would be a massive win.

Shared data dictionary

Documenting shared data models and precise definitions of terms for the handling of data helps enable standardization across the board. Shared dictionaries ensure that understanding and integrity of data elements are maintained across all users. Such a resource not only serves as a common, reliable reference, but also the beginning of a shared knowledge base and culture around data and risk.

Instead of choosing between DevSecOps and the traditionalists, marry the best of both worlds.

WHY IS THIS GOAL SO IMPORTANT?

Achieving a single plane of glass will help engineers, project managers, and acquisition officers come to a better, more concise, and more accurate understanding of what cybersecurity posture and risk management actually look like through the evolution of each of their respective pipelines while developing and/or sustaining their applications and larger architectures.

Furthermore, this solution would reduce misalignment and human error and improve accuracy and reliability, leading to enhanced security posture visibility and improved outcomes.

Finally, all of these components lend themselves to increased automation and reduced manual labor requirements while enhancing the responsiveness and quality of data.

THE CHALLENGE

RMF provides a process that integrates activities concerning security, privacy, and cyber supply chain risk management into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations.

What we seek to create is a single pane of glass that both DevSecOps engineers and IT security engineers can look through.

Unfortunately, there are lots of barriers to adoption on both sides.

The technical challenge

The challenge is that the Development, Security, and IT Operations worlds don't currently have a tight correlation between how they each evaluate, monitor, report, and manage security risks. Consequently, from a workflow perspective, it's necessary to use a number of different tools and processes involving significant manual data manipulation to create the necessary alignment.

RMF traditionalists tend to focus on legacy architectures. Such architectures don't map well to the cloud-native, microservice-based, containerized architectures that characterize most modern enterprise-level development architectures.

DevSecOps professionals leverage a massive amount of new tooling, technologies, and approaches incorporated into their nearly continuously run and rapidly iterated processes. Unfortunately, few of those new tools and technologies map directly to RMF controls or their CCIs. Therefore, RMF traditionalists have not been jumping at the chance to adopt these techniques, even though such techniques may offer a more comprehensive risk profile, especially in modernized architectures.

Then, there's data analysis. Much of it has to be performed manually. Some technologies can automate pieces of it, but the field values, meanings, and measurements don't correlate very well across systems and operational standards.

Let's not forget, DevSecOps focuses on maximizing the automation of tasks while traditional IT security engineers tend to adhere to manual processes. RMF is the gatekeeper in this case, and the manual aspect creates operational roadblocks that slow down system development, monitoring, and deployment.

The cultural challenge

Unfortunately, there is a cultural challenge at play. The traditionalists focus on "checking the boxes" related to compliance and RMF instead of adopting a more comprehensive, operations-wide process that targets dynamically managing the risk associated with near-real-time (NRT) operations.

Currently, in executing RMF, organizations must stop the development of an information system despite the significance of a proposed initial implementation or modification to have an independent assessment of the security posture (compliance measurement) conducted. This process is only automated in the delivery of the paperwork and artifacts required to slowly and methodically evaluate the security posture of the information system. There is no continuous end-to-end monitoring and analysis used in NRT to provide a dynamic understanding of the compliance of an information system in accordance with its authorized operational environment.

On the other hand, the methodologies used for DevSecOps and Agile software development are the opposite of that. The objective of these methodologies is to use the latest technology and newest threat models to integrate and iterate fast. DevSecOps pushes software out of the door, sees what breaks, learns from it, and fixes it quickly. There is an emphasis on security-focused development and the automation of vulnerability detection to enable the ability to deliver digital products faster and more securely.

DevSecOps tools simply don't map to RMF compliance requirements at a defined technical level to support security implementation or known inheritance. At a high level, the two processes are related. They both incorporate items like system security and boundary protection. When you try to get the two processes to link up, they don't fit. It may seem like forcing a square peg into a round hole.

However, this is also where the opportunity lies. By laying the groundwork with proper initial tooling and collaboration, these barriers can begin to fall fast, and the two communities can begin to learn and profit from one another.

OMNI

CONCLUSION

The two different paradigms don't speak the same language, and the way the risk is measured and ranked/weighted is different. They use disparate systems, processes, and data sources. This brings us back to where we started, with a clear need and opportunity for standardization and a shared culture.

Software is growing larger and more complex, in parallel with its benefits. The historical processes are weakening, and automation is needed. For automation to take place, there must be standardization so we can automate the collection and analysis of data to produce beneficial insights for all parties.

Unfortunately, a solution does not yet exist, and more research and development are needed.

However, there is an evolution that can help facilitate a solution. First, we must work to correlate the data so both communities can view it in one instance. Then, we can start building toward more advanced capabilities and insight into comprehensive risk postures.

Clearly, more research and development are needed.

OMNI is a global solutions provider that delivers innovative, technology-driven solutions and services in the public, private, national defense and intelligence sectors so they stay ready in an ever-changing technological environment. We help our clients strategize for their most important goals and use advanced business intelligence to understand the drivers behind their performance. We innovate to help our clients deliver advanced systems, products, and services.