Rapid Application Security

The Intersection of Risk with Compliance, Security, and DevOps

AUGUST 2021

PREPARED FOR

Security Compass

ALPINE Security Consulting

Executive Summary

Speed limits on our freeways exist for a reason. Above certain speeds, the increasing risks of how fast you move rise dramatically compared to the time you can save and safely arrive at your destination. In today's rapidly developing and changing IT landscape, speed is being demanded and the risks of that speed are rarely understood. Developers are under pressure to meet changing requirements from multiple sources, including configuration management, asset identification, automated pipelines, several different standards/regulations and more. How can developers meet these demands in a way that the corresponding business teams can leverage and meet their critical business objectives?

This paper will endeavor to answer that question with the premise that understanding the risks of rapid development are at the core of answering how to successfully integrate DevOps with a secure and compliant approach. The Payment Card Industry Data Security Standards (PCI DSS) will be used as an example of one of the common standards that developers must translate into different applications with different contextual challenges. How can a developer understand the security risks and translate that into meeting the new PCI Software Security Framework (SSF)? How can security and functionality be orchestrated from a single location in a way that hardware, software, and firmware are all properly developed and maintained?

Security Compass offers SD Elements, a tool that speaks the language of risk to both developers and business teams. The features of SD Elements will be reviewed to see how well they can meet this challenge of needing to go fast and still stay safe on the road to a successful go-to-market strategy.

DevOps and Risk

As organizations have learned to integrate critical software development with everyday IT operations, efficiencies as well as improved functionality for the applications developed have been gained. While this has certainly sped up GTM timeframes, there are additional challenges and risks with the demand to develop as fast as possible. Here are a few key challenges:

- Hardware and software convergence
- Maintaining process and pipeline through automation
- Balancing asset identification, protection and data classification with a large number of constantly changing compliance standards, security frameworks and privacy laws
- Integrating each of the above with business objectives

Every organization faces these and many other challenges in order to stay competitive. Finding a way to track and manage these challenges within development processes can maintain speed and avoid the following potential risks that are present if these challenges are not well managed:

- Releasing vulnerable applications and solutions
- Not protecting sensitive data to the various standards and requirements correctly
- Failing to know what sensitive data you have where

Many more risks exist, and each environment presents unique challenges that must identified in order to understand what is most at risk. These risks can lead to some of the following consequences:

- Brand and reputation damage
- Slower time to market
- Additional development costs
- Fines and penalties
- Remediation and breach mitigation costs

In addition to avoiding the consequences, here are some benefits to a well-managed approach that puts security and compliance at the beginning of the development process:

- More options to meet the security or compliance requirements – meaning the most functional and efficient approach can be chosen at the beginning
- Consistent and measurable development timelines and quality
- Ability to focus more on functionality and the customer experience

Once an understanding of the risks of rapid development is determined, a strategy to minimize those risks can be developed to avoid the consequences and maximize the balance between speed and security. For these specific challenges, understanding the context of the risk, automating the assessment of that risk, and identifying the top risks with a single strategy

that allows for communication and maintenance of that risk will provide tremendous value for any software development process. To better understand what this might look like, let's turn to the new PCI SSF program.

PCI SSF Challenges

OVERVIEW

The PCI Security Standards Council has replaced the Payment Application Data Security Standard (PA-DSS) with the new PCI SSF, a more flexible and software development centric approach to payment applications. For a more detailed look at navigating this new SSF framework see this paper.

The primary goal of PCI SSF is to protect cardholder data (CHD) within an application for the purposes of processing a payment transaction. This includes a secure approach to the Software Development Lifecycle (SDLC). The PA-DSS was prescriptive in most areas where the SSF program is more flexible.

PASSWORD EXAMPLE

One example that illustrates this is the approach to passwords.

PA-DSS – Passwords must contain a minimum of 7 characters and use both alphabetic and numeric characters (see requirement 3.1.6). This means that "Password" could be considered an acceptable password, not exactly an ideal baseline. SSF does not provide this detail but instead says this: "The software implements strong authentication and access control to help protect the confidentiality and integrity of critical assets." (See Control Objective 5 from the Secure Software Standard). There are of course additional details in the Control Objectives and the Test Requirements, but the details on how specific to code for password length and character requirements are left up to the software developer.

This flexibility allows for appropriate security measures to be implemented, but in order to do so, the risks of different requirements for passwords within different software application uses, environments the software runs in and the different use cases for the software must all be fully understood. This typically puts the pressure onto the development team to understand the risks, controls, and security best practices and then balance that with the functionality requirements received while developing code quickly enough to meet GTM demands. This often results in either a weak password approach, or one so strong users easily get frustrated.

This is just one example of the dozens of Control Objectives and hundreds of Test Requirements within the SSF that must be tracked and managed by developers. The PCI SSF framework in turn is just one of dozens of different compliance standards, security frameworks and privacy regulations that must be considered when developing applications in today's modern environment.

SOLUTIONS

With the flexibility added into the PCI SSF, tracking how to meet each objective and test requirement becomes a complex task. Lining these up from each required compliance standard or security framework with business objectives and application functionality can also be difficult for developers. Here are some key things to do or look for that will help organizations overcome these challenges:

- Automation – automating the development process and tracking the various compliance and security requirements
- Training – with all the changes and complexities, advanced training helps, and having real-time training available is even better
- Documentation – with automation, documenting policies and procedures can be simplified and more efficient
- Evidence – demonstrating compliance through logs, configuration settings and other testing will streamline assessment and audit activities
- Integration – any tool to automate should be able to help you integrate your DevOps processes internally as well as integrate to business objectives

SD Elements

OVERVIEW

SD Elements integrates DevOps with security and compliance across multiple standards and frameworks. Using the example of PCI SSF objectives, SD Elements can help insert security and compliance into the development of payment applications at the beginning of the software development life cycle and verify compliance throughout the development process. This reduces time to market, minimizes repetitive development cycles, improves consistency, traceability, and compliance with PCI SSF for payment applications.

SD ELEMENTS BENEFITS

SD Elements has several unique features that address the challenges organizations face with secure and compliant development:

- Simplification of the software development process and the administration of security and compliance controls. SD Elements automates what can be cumbersome or time-consuming processes such as identifying, tracking, disseminating, and managing security and compliance controls. This accelerates development timeframes.
- Software is understandable to developers and trains in real time. SD Elements maps the security or compliance requirements into instructions that developers can follow and implement. It also provides Just in Time training throughout the SLC process.

- Scale Security, Risk and Compliance controls across the software development project by converting those controls into policy and clear guidance.

- Automate the tracking of development activities. Projects are automatically classified by risk, driving consistency into the identification of the right security and compliance controls. This translates the controls that enable developers to integrate them effectively and easily into the secure development life cycle.

- Open API's and SDK's fit seamlessly into existing DevOps processes. SD Elements has programmatic access to a library of security content and services to provide flexibility while building a DevSecOps vision.

Conclusion

Speed to market will always be a critical factor for developers. Balancing that speed with a secure and compliant development process is the only way to ensure that going to market quickly doesn't backfire and become the source of a newsworthy breach or security story.

Organizations who are able to leverage the benefits of a mature DevOps program still need to support those efforts with automated and well managed secure approach to software development. This automation will overcome the challenges faced today with integrating multiple compliance standards, security regulations, privacy laws with asset identification, development pipelines and configuration management.

PCI SSF demonstrates just one of many of today's standards that has complex and changing requirements to track and manage. Developers need to have the tools to both track these concerns and be trained and supported during the development process in order to support the business needs that are the ultimate objective of the applications being produced.

SD Elements meets each of these challenges by offering the ability to reduce time to market, minimize repetitive development cycles, improve consistency, traceability, and compliance with multiple standards for any application. SD Elements stands out as a product that can uniquely support these challenges and move into the next generation of secure application development for any modern software development organization today.

About Alpine Security Consulting:

Alpine was founded to fulfill a passion for helping businesses and the people that work in them overcome today's cybersecurity challenges and succeed in new ways by leveraging the untapped value that an innovative approach to security can provide. With a background of over 20 years in technology, security, and compliance, Alpine can help virtually any business learn how to leverage innovative technologies to translate their security investments into tangible business value. www.alpineconsults.com

About Security Compass:

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, allows organizations to balance the need to accelerate software time-to-market while managing risk by automating significant portions of proactive manual processes for security and compliance. SD Elements is the world's first Balanced Development Automation platform. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defence, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and India. For more information, please visit www.securitycompass.com.

About Dan Fritsche, CISSP:

Dan Fritsche, CISSP, is the Founder of Alpine Security Consulting. Dan's specialty is in security innovation, wherein he helps companies turn security from a hurdle into a strategic investment. Dan started his career with a security-focused role at IBM, where he supported functions like penetration testing, vulnerability scanning, application security, and business intelligence across multiple units during his decade-long tenure. After IBM, he worked at Coalfire where he helped companies improve their posture in application security, encryption, tokenization, and many other security specialties. Dan went on to help Global Payments drive the value and involvement of innovative security approaches as early in the application development life cycles as possible. Dan has held several certifications such as PCI QSA, PA-QSA, P2PE QSA/PA-QSA for at least five to 10 years.