WhiteHat SECURITY

Application Security Testing as a Foundation for Secure DevOps

White Paper - April 2016

Introduction

Organizations realize that addressing the risk of attacks on their Website applications is critical. Given the growing number of Website applications that businesses now must manage in a highly competitive environment, organizations are quickly trying to evaluate how to deploy software faster to meet or exceed company goals. It is imperative for Information Security teams to realize that aligning to a rapidly changing business is now part of their requirement to be competitive and successful in today's digital world.

Because web application security programs are rapidly transitioning from focusing on a few key critical applications to identifying all applications across an enterprise, both the number of applications and the number of discovered vulnerabilities have grown exponentially. But the number of security professionals to manage this growth and the number of development resources required to fix vulnerabilities have largely remained the same. This discrepancy leads to longer time-to-resolution of open vulnerabilities, and increased risk for the business.

Additional complexities with application security arise when organizations move towards Agile environments automating as much functionality as possible. Because automation and/or Agile efforts are 'top of mind' for most engineers and information security practitioners, organizations are attempting to identify ways to integrate application security within their DevOps model. To improve the protection of applications from vulnerabilities and potential attacks, the DevOps efforts must be extended to include information security to become DevSecOps.

Despite making major investments to address application security vulnerabilities, many organizations find themselves still unable to defend their Web application infrastructure. Instead of focusing on just a few applications, attacks now target all Internet facing applications. Information security teams find themselves facing more vulnerabilities than they can feasibly manage and fix.

Sadly, while businesses move to support Agile functionality and the more rapid release of projects, traditional security processes may not be incorporated or simply overlooked altogether.

WhiteHat Security™ has developed the WhiteHat Sentinel™ platform to assist CISOs and engineering teams in automating their application security efforts while embedding application security into the DevSecOps model. The WhiteHat Sentinel platform allows organizations to incorporate application security throughout the software development lifecycle (SDLC) with complete transparency to engineering, information security, and operations teams.

The Application Security Challenge

The graphic below provides a summary of the application security challenge all organizations face.

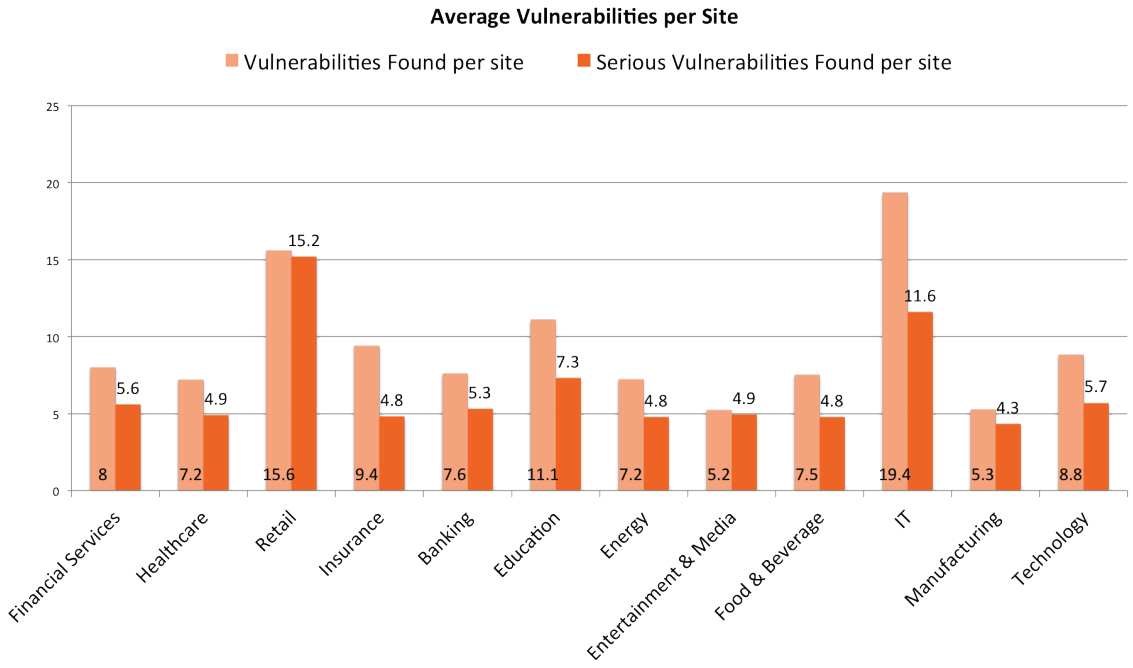

Figure 1.
Source: WhiteHat Security Statistics Report 2016 (preliminary)

DevSecOps Overview

DevSecOps origins are embedded as part of the core foundation of an Agile environment, which includes the following phases.

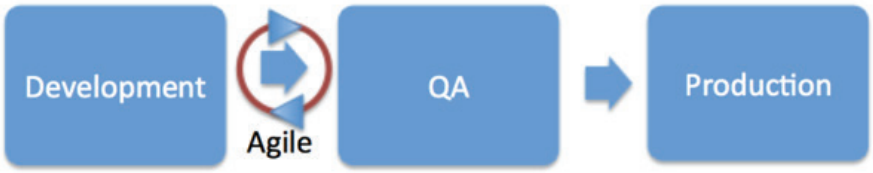

Figure 2.

Application security must be incorporated into all supporting business processes and a dedicated security team must establish alignment with the business, automating the discovery of vulnerabilities, and providing 24x7x365 automatic application security testing. Application security components emerge in a number of areas to support automation through the process of DevSecOps. This approach is best visualized in the following diagram.

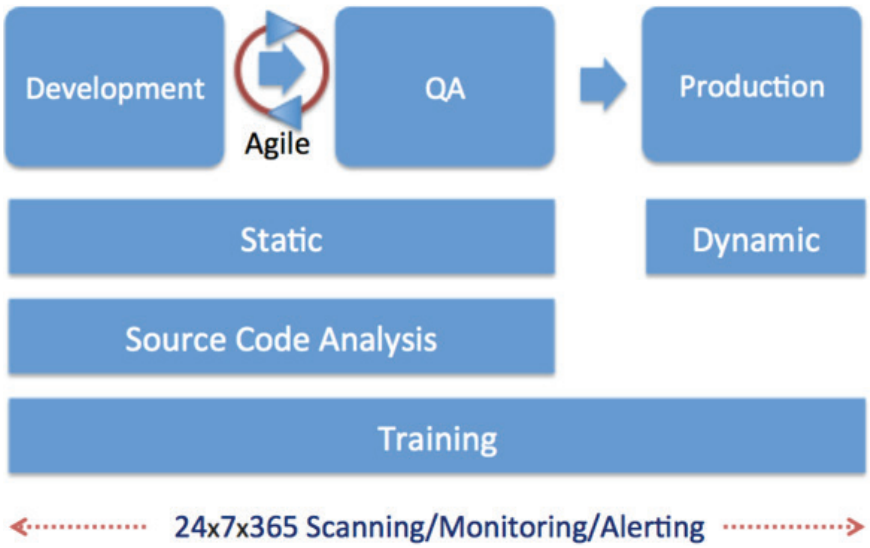

Figure 3.

Static Application Security Testing (SAST) and Source Code Analysis (SCA) functions are embedded as part of the Development and QA environments, while Dynamic Application Security Testing (DAST) functions are enabled to monitor production environments. Application Security Training is a core component to a successful foundation for DevSecOps.

By adopting DevSecOps as an organizational goal, application security engineers are able to align with the DevSecOps vision, which increases the value of the application security engineer who realizes his/her efforts are embedded as part of the entire organization's platform and infrastructure. The additional value of adopting DevSecOps is that these functions are able to monitor, attack, simulate, and identify application security vulnerabilities throughout the continuous integration and continuous deployment environments. Another benefit of taking this approach is that your organization will be able to identify application security vulnerabilities before cyber criminals or cyber gangs discover issues with Internet-facing applications and supporting systems.

Agile Operational Efficiencies

Automation of the DevSecOps solution has demonstrated that there are operational efficiencies that can be immediately recognized in engineering and application security environments.

Organizations and teams that embrace DevSecOps are set up for recognizing business goals faster than traditional alternatives.

Consider the following scenario for a Fortune 500 organization that evaluated these two options.

The Risks of Not Moving to DevSecOps

As more organizations embrace an Agile framework to realize faster deployments, the ability to incorporate DevSecOps will yield faster time-to-market while identifying risks within applications at a faster pace.

The business impact of not integrating DevSecOps is best demonstrated in the following scenario.

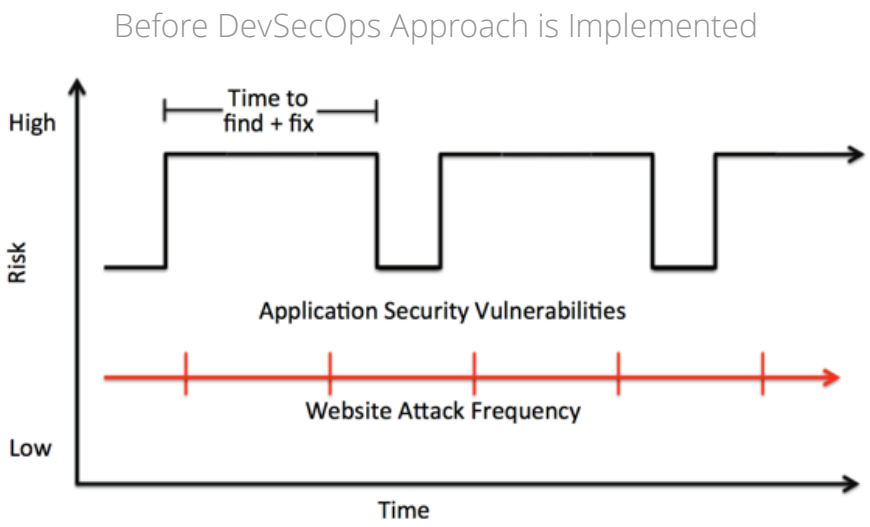

Figure 4.

In organizations that have not embraced DevSecOps, software is released and scanned for vulnerabilities through a longer release cycle. Time to discover and resolve application security vulnerabilities may take longer than in an environment where there is constant iteration with smaller code releases. The risk with this approach is that cyber criminals and/or criminal gangs will leverage the potential vulnerabilities more frequently.

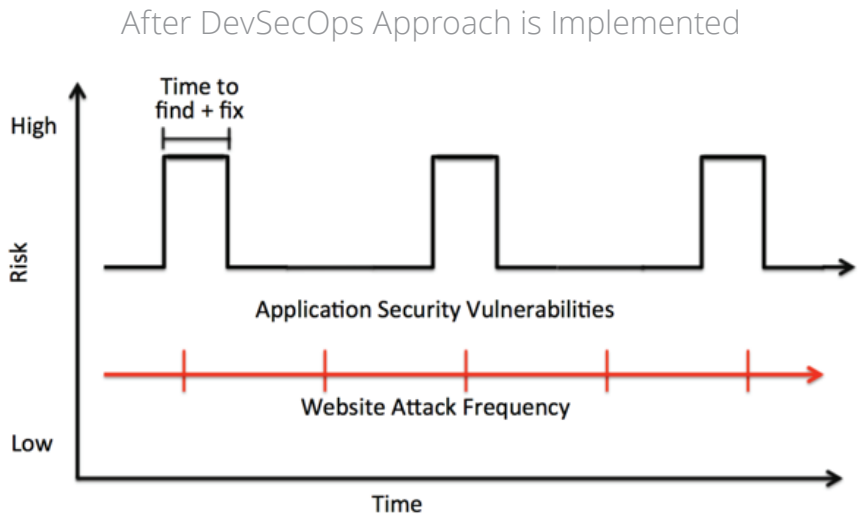

Figure 5.

For organizations that have embraced DevSecOps, software is released and scanned for vulnerabilities through a much shorter release cycle. Time to discover and resolve Application security vulnerabilities will be reduced because of the shorter 'sprints' in the development process, coupled with the 24x7x365 application scanning and monitoring functions. This approach is critical in identifying and remediating application security vulnerabilities earlier in the process, which reduces the window of exposure if code is released to production.

Recommendations

- DevSecOps is a cultural shift within the organization. Executive management should be involved in driving this change, and be provided the key metrics of how the business is operating with this new framework.
- DevSecOps is about collaboration. An effective enterprise information security program will require close cooperation among all business units, which will enable a successful DevSecOps program.
- Adopt an application security solution that can be leveraged as the foundational platform for a successful DevSecOps program. This means finding a platform that will integrate with existing development and QA tools and solutions through an open API. By embedding application security into the devops framework – DevSecOps – organizations will be able to deploy secure solutions much faster.
- Quantifying risks can help align security, operational and funding decisions across multiple teams and stakeholders by providing a common language for determining and discussing risk. Those discussions lead to alignment and mutually agreed-upon decisions, which serve as the foundation for a security program that successfully meets the needs of the business.

About WhiteHat Security

WhiteHat Security has been in the business of securing web applications for 15 years. Combining advanced technology with the expertise of its global Threat Research Center (TRC) team, WhiteHat delivers application security solutions that reduce risk, reduce cost and accelerate the deployment of secure applications and web sites. The company's flagship product, WhiteHat Sentinel, is a software-as-a-service platform providing dynamic application security testing (DAST), static application security testing (SAST), and mobile application security assessments. The company is headquartered in Santa Clara, Calif., with regional offices across the U.S. and Europe.

For more information on WhiteHat Security, please visit www.whitehatsec.com.

WHITEHAT SECURITY, INC. 3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com
© 2016 WhiteHat Security, Inc. All rights reserved. WhiteHat Security and the WhiteHat Security logo are registered trademarks of WhiteHat Security, Inc. All other trademarks are the property of their respective owners.