



Interested in learning
more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The DevSecOps Approach to Securing Your Code and Your Cloud

DevSecOps, at heart, is about collaboration. More specifically, it is continual collaboration between information security, application development and IT operations teams. Having all three teams immersed in all development and deployment activities makes it easier for information security teams to integrate controls into the deployment pipeline without causing delays or creating issues by implementing security controls after systems are already running. Despite the potential benefits, getting started with DevSecOps wi...

Copyright SANS Institute
Author Retains Full Rights



The DevSecOps Approach to Securing Your Code *and* Your Cloud



A SANS Spotlight

Written by Dave Shackleford

February 2017

*Sponsored by
CloudPassage*

What Is DevSecOps, and How Do I Start?

DevSecOps, at heart, is about collaboration. More specifically, it is continual collaboration between information security, application development and IT operations teams.

Having all three teams immersed in all development and deployment activities makes it easier for information security teams to integrate controls into the deployment pipeline without causing delays or creating issues by implementing security controls after systems are already running.

Despite the potential benefits, getting started with DevSecOps will likely require some cultural changes and considerable planning, especially when automating the configuration and security of assets in the cloud, whether the model is software-as-a-service (SaaS), platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS). See Table 1.

Table 1.

Security Considerations	Cloud Model		
	SaaS	PaaS	IaaS
Virtual network security			X
Virtual machine instance template management			X
System build configuration		X	X
Anti-malware		X	X
Data security at rest and in transit	X	X	X
Administrative console security	X	X	X
Roles and privileges	X	X	X
Logs and monitoring for activity	X	X	X
Sensitive data and policy compliance	X	X	X

The first step is to develop a policy specifically for cloud security that defines who “owns” cloud risk. Is the CISO responsible, or are the business-unit managers responsible?

The first step is to develop a policy specifically for cloud security that defines who “owns” cloud risk. Is the CISO responsible, or are the business-unit managers responsible?

The policy should also specify how often risk reviews of cloud provider environments will be performed.

Guidelines are only a start. To help the shift toward a more collaborative culture, security teams need to integrate with the developers who are promoting code to cloud-based applications to show they can bring quality conditions to bear on any production code push without slowing the process. Security teams should also work with QA and development to define the key qualifiers and parameters that need to be met before any code can be promoted.

Within their own arena, security teams have to determine which of their existing tools can integrate into a DevSecOps environment and identify procedures or controls that have to be updated or adapted before they will work well in a continuous integration/development environment.



A threat modeling exercise can help security teams better understand the types and sensitivity levels of the assets they are protecting, how those assets will be managed and monitored in the cloud, and what the most likely vectors are for threats affecting those assets.

Such serious changes in tools, workflow and responsibility may also require the development of new standards for security prevention, detection and response capabilities. They may also create a need for more specific technical requirements in areas such as encryption, privileged user management, network security access controls and filtering, event management and logging standards.

Once initial processes, policies and standards have been defined and agreed upon, the team should focus on automation and seamless integration of controls and processes at all stages of the deployment pipeline.

Implementing DevSecOps

Implementing a shift to DevSecOps means even more planning in the form of threat models and risk assessments covering, for example, the types of deployments the security team envisions. A threat modeling exercise can help security teams better understand the types and sensitivity levels of the assets they are protecting, how those assets will be managed and monitored in the cloud, and the most likely vectors for threats affecting those assets. Some data types will dictate specific security controls before being transmitted to or processed in the cloud. Many will also have special requirements for provisioning in compliant cloud provider environments.

Risk assessment and analysis practices should be updated to continually review the following:

- Cloud provider security controls, capabilities and compliance status
- Internal development and orchestration tools and platforms
- Operations management and monitoring tools
- Security tools and controls, both in-house and in the cloud

During review, it's important to keep the "shared responsibility" model in mind, meaning cloud providers and consumers share responsibility for security at the various layers of the stack. After such risk reviews, security teams should have a better understanding of what controls they currently have, what controls they need to modify to successfully operate in the cloud, and what the most pressing concerns are (as they change). It is almost a guarantee that some security controls won't operate the way they did in-house or won't be available in a cloud service provider's environment.



DevSecOps and Cloud Configuration

Automating cloud security and management is a key DevSecOps characteristic (see Figure 1).

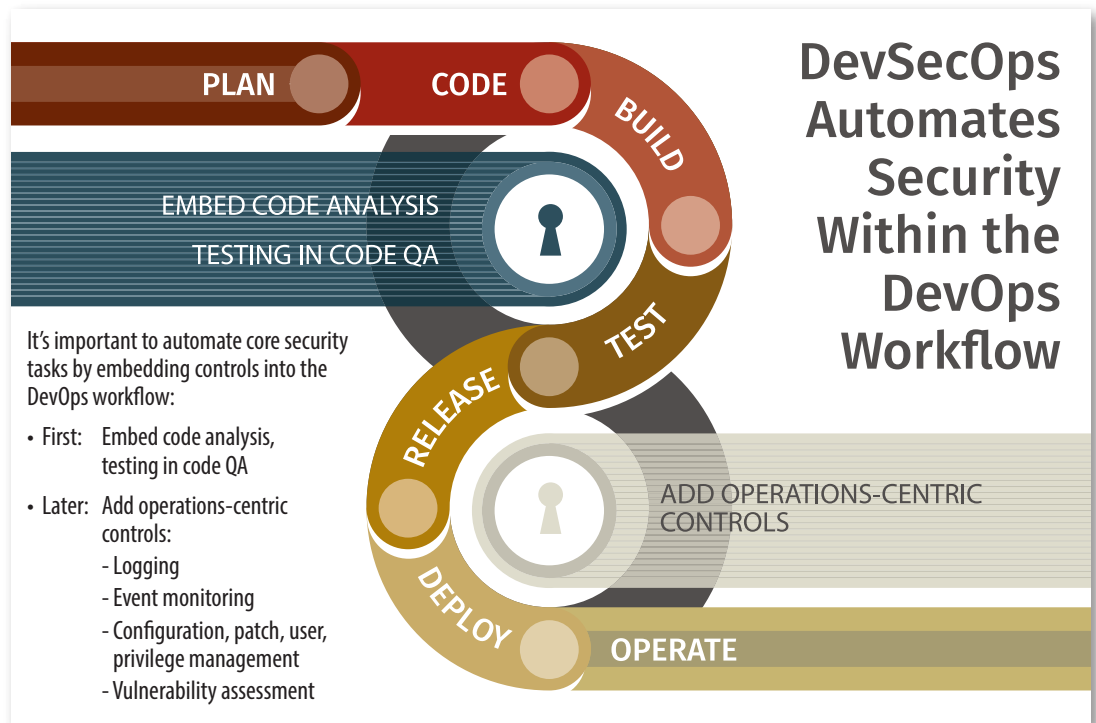


Figure 1. DevSecOps Workflow

Regular risk assessments should be conducted to determine the cloud provider's security posture.

To make it work, DevSecOps teams need visibility into what is running in the environment, as well as the state of the assets. Inventory management starts with a discovery process that leverages network scanners, system-level scanners and specialized scanning tools that can peruse files and storage infrastructure to assemble all active cloud assets into a dynamic, continually updated inventory. Once this inventory has been created and validated, a process needs to discover new assets (or changes in assets) as soon as they are online or shortly thereafter. Regular risk assessments should be conducted to determine the cloud provider's security posture.

With a sound inventory in place, organizations must determine a set of configuration items that they need to develop and maintain. Most organizations are free to develop their own internal standards that meet policies and compliance guidelines. Some others (such as federal agencies) may be required to adhere to standards such as the Defense Information Systems Agency's Security Technical Implementation Guides or the guidelines from the Center for Internet Security. Using an agent-based and/or agentless technology, organizations will need to apply the configuration standard to systems and then begin assessing the new configuration for changes or deviations from policy. Provisioning and configuration automation tools such as Salt, Puppet and Chef can help organize and coordinate configuration builds and deployment.



A critical aspect of managing security in a cloud environment is to carefully limit and control the accounts and privileges assigned to resources.

Defining configuration baselines and solidifying them into a policy that can be applied to all systems is key to properly implementing and monitoring for a secure configuration. One challenge many large organizations have had with this is the sheer diversity of system types, as well as the disparity in tools that won't work on all platforms. As organizations move to the cloud, finding some homogeneity across tools and consolidating systems will prove invaluable in maintaining system security and patch levels over time, especially in a dynamic DevOps-driven architecture. Security and operations teams have considered both "push" and "pull" methods to automate system configurations in the cloud. There are benefits and drawbacks to each, but a "pull" method that fetches updates and configurations from an embedded system agent is far simpler from a security standpoint.

A critical aspect of managing security in a cloud environment is to carefully limit and control the accounts and privileges assigned to resources. All users, groups, roles and privileges should be carefully discussed and designated to resources on a need-to-know basis. The best practice of assigning the least-privilege model of access should also be applied whenever possible. Any privileged accounts (such as root and the local administrator accounts) should be monitored very closely (or ideally disabled completely).

All systems and application stack components in the cloud should monitor configuration continuously, and ideally the DevSecOps team will embrace the idea of "immutable" systems that can be replaced quickly if integrity or other validation checks fail. This is sometimes referred to as the "cattle versus pets" concept in DevSecOps, where systems are no longer treated like unique or special entities that are maintained for long periods of time.

DevSecOps Protecting the Cloud

Once the threat assessment and inventory have listed assets in the cloud and potential vectors for attack, security and compliance teams should perform a vulnerability assessment to clarify the real risk in existing cloud deployments—including vulnerabilities that should be considered priorities based on the likelihood of an effective attack and potential impact if it were successful. One important precaution is the need to audit open-source software modules for flaws. Store those that are certified or remediated in secure code repositories, and discuss with the rest of the DevSecOps team how to protect those repositories automatically.



Some traditional vulnerability scanning vendors have adapted their products to work within cloud provider environments, often relying on APIs to avoid manual requests to perform more intrusive scans on a scheduled or ad hoc basis.

The defined processes created by the DevSecOps team should include a regular schedule for threat and vulnerability updates that involve both the development and operations teams. Vulnerability scanning of existing systems is routine in most situations, but it can be complicated when cloud providers don't provide the tools or access customers need to monitor their own assets. Some traditional vulnerability scanning vendors have adapted their products to work within cloud provider environments, often relying on APIs to avoid manual requests to perform more intrusive scans on a scheduled or ad hoc basis. Another option is to rely on host-based agents that can scan their respective virtual machines continuously or as needed. Ideally, systems will be scanned continuously and will report any vulnerabilities noted in real or near real time.

In addition to privilege management in configuration definitions, DevSecOps teams need to ensure no sensitive material such as encryption keys or credentials are stored in definition files, on systems that are exposed or in code that could be exposed. As encryption and data protection strategies are increasingly automated along with other DevSecOps activities, it's critical to make sure the proverbial keys to the kingdom are protected at all times.

All controls defined and implemented need to have continuous monitoring and feedback loops in mind. To this end, logs and events generated by services, applications and operating systems within cloud instances should be automatically collected and sent to a central collection platform. Automated and remote logging is something many security teams already feel comfortable with, so organizations implementing DevSecOps just need to ensure they collect the appropriate logs, send them to secure central logging services or cloud-based event management platforms, and monitor them closely using security information and event management (SIEM) and/or analytics tools. The entire DevSecOps group should commit to a culture of continuous monitoring, both in development within the organization as well as in assets promoted to the cloud. Once continuous monitoring of events is truly in place, events can initiate "triggered" responses that can automatically roll controls back to a known good state.

Finally, many organizations may want to investigate security-as-a-service (SecaaS) options to help augment or implement controls they need in the cloud. Many SecaaS providers offer lightweight embedded agents and service options tightly integrated with leading cloud provider APIs that can lower cost and complexity for several control areas. SecaaS options are also ideally suited for automation and continuous development and deployment strategies, making them attractive to DevSecOps teams.



About the Author

Dave Shackelford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

CloudPassage





Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Paris 2017	OnlineFR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced