KPMG CYBERARK

Boost competitiveness and reduce risk with secure DevOps

DevOps accelerates speed to market and reduces the barriers between development and operations. But even as developers and operations teams work together and share a common goal—to develop and run better products faster—the rapid pace of development cycles can leave applications unsecured, and DevOps tools and CI/CD pipelines vulnerable to increasingly sophisticated cyberattacks.

Organizations need to create a frictionless experience for developers to build code securely, eliminate hand-offs between groups, including security, and then adopt these practices across the enterprise to reduce risk.

Addressing vulnerabilities in developer tools and environments

In today's cloud, continuous integration and delivery (CI/CD), and containerized environments, DevOps has evolved from a methodology to accelerate speed to market and reduce operational barriers, to an acknowledged aspiration or even the "new normal" for some application teams.

While the powerful business benefits of DevOps have led to wide-spread awareness and increasing adoption, high profile and costly breaches have also exposed potential security vulnerabilities. Additionally, these breaches have increased recognition of the risk that inadequately secured DevOps environments and processes can introduce to the enterprise.

For example, by:

- Inadequately protecting code repositories
- Hardcoding credentials
- Using unprotected 3rd party code and libraries
- Failing to shut down test instances and build environments that are no longer needed
- Creating security gaps with poor configuration of code and infrastructure
- Sprawling secrets, vault sprawl and siloed controls

Attackers recognize the power of injecting their malicious code into development pipelines, which is why they seek to include their malicious code in the build before it even gets into production, enabling attackers to penetrate devices across the enterprise for maximum impact. At the same time, DevOps environments in the cloud are also exposed to the very threats other cloud workloads need to be protected against. Administration tools have become a popular focus for attackers who can exploit unsecured consoles to target other resources in the developer value chain. Attackers may also use bot crawlers to systematically search out the use of default configurations of CI/CD pipeline, as well as provisioning and container orchestration tools, which too often do not require passwords for privileged access.

Most developer work takes place on a Mac or Windows workstation that needs access to privileged credentials to access platforms and services such as Kubernetes and Git, or a Jenkins admin console. Some of these processes and systems require a high level of privilege, if only for specific actions and for limited time periods. Yet too often these credentials are saved locally, making developers' workstations high-value targets for attackers.

Businesses compete better when software is developed faster and more securely

The premise behind the adoption of DevOps is simple: Businesses compete better when software is developed and deployed faster. DevOps is instrumental to the development of new services by driving automation and orchestration in key security processes. Unfortunately, too often DevOps teams view security teams as too slow, inflexible or unfamiliar with DevOps processes, tools and methods to keep up. And they're right: security teams who have not invested in modern approaches can be unnecessarily burdensome on efforts to grow the business. At the same time, an escalating threat landscape and new ways of working create security concerns for SecOps teams who need to ensure that cybersecurity risks are managed when building software at DevOps speed and cloud scale.

Despite the drive to release quality products more quickly, traditional security approaches introduce too much friction and slow the software development lifecycle (SDLC). But trading off security for speed introduces risks that can have devastating business consequences.

By working together, Secure DevOps (DevSecOps) helps organizations optimize for speed and security. When security teams are part of the DevOps conversation, they can integrate capabilities, behaviors and controls throughout the SDLC to reduce risk while supporting speed. This helps:

— Reduce the security friction for software development

— Make work visible so everyone can better understand where constraints happen and work together to solve them

— Enable continuous learning so developers and operations teams can reduce security risks continuously over time

Secure DevOps enhances the integration of development, IT operations, and security throughout the SDLC. It also reduces the likelihood of vulnerabilities being introduced by enabling organizations to shife left early, to quickly address any vulnerabilities without slowing down the development process.

Prioritizing security & reducing friction

Today's developer culture emphasizes high velocity, intensive sharing of code, ad-hoc tooling, and automation. In this culture, low-security shortcuts often flourish, and traditional security processes are not always easy to integrate. For an organization to reap the rewards of short development cycles, the security team must work with their Dev and DevOps counterparts to follow cybersecurity best practices, including securing privileged access.

DevOps roles need expansive privileged access via applications, tools, consoles, and more, and attackers are exploiting these new vulnerabilities to access tools, services and platforms. It's more important than ever for security to understand risks and appropriately prioritize opportunities to secure their organization's development environments.

Privileged access management, secrets management and endpoint management play a key role in reducing risk across the application life cycle. A secrets management solution reduces the risks introduced with hardcoded credentials by centrally managing, rotating, and monitoring secrets and credentials in a centralized vault. Protecting developer workstations, where credentials are often saved locally, helps secure the supply chain. Implementing privilege functionality, adopting capabilities to ensure secure by design principles, and then embedding these capabilities in use cases enables organizations to take a holistic approach to reducing risk.

The CyberArk identity security platform and secrets manager reduce DevOps risk

CyberArk enables organizations to secure the privileged credentials and secrets used across the entire enterprise, including the development environments that are driving digital transformation.

Privileged access manager (deployed as self-hosted or SaaS) provides a thorough set of capabilities for securing the credentials used by human users, including:

— Credential protection and management,

— Session isolation and monitoring,

— Privileged analytics and threat detection, and

— Least privilege management.

CyberArk secrets manager solution, Conjur Enterprise, is designed to address the unique requirements of cloud-native and DevOps environments while simplifying how developers secure and use secrets. The solution integrates with a wide range of DevOps tools such as Ansible, Jenkins, and Azure DevOps; PaaS/Container orchestration platforms such as Kubernetes, Red Hat OpenShift and VMware Tanzu whether running on hybrid or multi-cloud platforms.

Endpoint privilege manager is designed to prevent attacks that start at the endpoint by removing local admin rights, while minimizing impact on user productivity. With Endpoint Privilege Manager's Application Control capabilities, IT operations and security teams can allow approved applications to run while restrict the unapproved ones. To be less restrictive with the DevOps teams, "greylisting" enables unknown applications to run in 'Restricted Mode' which prevents them from accessing corporate resources, sensitive data or the Internet.

Secure DevOps with KPMG

We believe organizations should take a holistic view of DevOps, prioritizing speed and agility while implementing a comprehensive governance framework characterized by a suite of business-conscious controls, security scanning, and automated testing. Through this approach organizations align development, security, and risk/operations to create a unified and optimized software delivery architecture that includes key roles, processes, and technologies and increases competitiveness while reducing risk.

Many KPMG clients' software development efforts have begun the DevOps journey for some of their application portfolio. KPMG accelerates the transition by guiding the strategy and operational aspects of secure DevOps. By automating as many aspects of the software development life cycle (SDLC) as possible, including testing and deployment, DevOps teams are able to release more secure working code on a continuous basis, rather than at the end of a two-week sprint as may be found in agile environments. We help our clients implement processes, controls, and capabilities to makes security as frictionless as possible in the application delivery pipeline so the business can deliver value rapidly.

Our services include:

Advanced Engineering and Orchestration

Design and implement AWS/Azure/GCP-based DevOps processes and tools. Engineering integrations with security platforms such as SPLUNK ES, Threat Analytics, Conjure (CyberArk), ITSM tools such as ServiceNow, and other CI/CD tools (multiple).

Software Supply Chain Security

Reduce the risk of organizations' increasing use of free and open source software (FOSS) by delivering visibility and automation across six stakeholder groups in large organizations.

Secure DevOps Managed Services

"Run the business" support to the DevOps lifecycle once transformation and/or advanced engineering services have been delivered.

Secure DevOps Transformation

Achieve enterprise agility by tailoring DevOps approach for accelerated delivery through the optimization of tools, processes, and architecture. Services focus on transforming agile/DevOps PMO, DevOps target operating model, cloud integration architecture, DevSecOps tool chain configuration and deployment, and organization change management.

KPMG and CyberArk: Securely accelerating business

KPMG and CyberArk work together to help organizations accelerate time to market with a tested approach that securely reduces DevOps risk and friction.

Established track record with CyberArk— Since 2011, KPMG has been working with CyberArk to secure identity and privilege accounts for organizations across a range of industries.

Commitment to continued education— With dozens of team members successfully completing CyberArk-led product training, KPMG has developed the skills and expertise to execute on demanding DevOps engagements.

Distinct deployment methodology and engagement accelerators— KPMG has developed a distinct deployment methodology based on a combination of multiple industry frameworks, as well as a wealth of experience deploying PAM solutions for some of the world's largest enterprises.

Contact us

Hemal Shah
Principal | Cyber Security Services
T: 214-601-8198
E: hpshah@kpmg.com

Caleb Queern
Director | Cyber Security Services
T: 571-228-8011
E: cqueern@kpmg.com

Mike Battillo
Sr Director, Solution Relations
T: 305-358-2300
E: mbattillo@kpmg.com

Debbie Patterson
Sr Director, Alliances | Alliances
T: 512-423-6150
E: deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia