TAG CYBER

ACHIEVING FULL LIFECYCLE DEVOPS SECURITY USING SYSDIG

EDWARD AMOROSO, TAG CYBER

TAG CYBER

ACHIEVING FULL LIFECYCLE DEVOPS SECURITY USING SYSDIG

EDWARD AMOROSO

Key protections required to achieve DevOps security include pre-delivery testing during CI/CD pipeline processes as well as run-time detection and response for vulnerability management and attack mitigation. The Sysdig platform is shown to implement these full lifecycle cyber security capabilities including protection of infrastructure-as-code (IaC) for cloud-native software environments.

INTRODUCTION

For many years, applications were hosted in private data centers protected by traditional corporate firewalls. Built in a monolithic manner, these applications were often easy to manage because they had few dependencies other than front-end interfaces and back-end databases. This is not to say that they were bug free. In fact, such applications were typically riddled with exploitable flaws due to crude coding practices and insecure programming languages.

More recently, applications have come to be developed in containerized manner, orchestrated with tools such as Kubernetes.[1] The goal is to leverage automation and infrastructure-as-code (IaC)[2] to define and control the computational environment. This allows for reuse of existing modules and reproducibility of environments, which in turn reduces costs and increases flexibility. This does increase, however, the number and types of dependencies that must be identified and managed.

In this report, we outline the cybersecurity issues that emerge in modern DevOps environments with emphasis on the types of identities used by cloud-native applications. This includes threats related to permissions and entitlements, and enforcement of which identities have been granted access to which cloud resources. The commercial Sysdig[3] platform is introduced and shown to effectively implement advanced controls for DevOps-related threats. It does so through emphasis on early pre-delivery protections as well as runtime controls designed to support vulnerability management, detection, and response.

SECURITY ISSUES IN DEVOPS

One of the most challenging aspects of modern DevOps practices is the rapid rate of change for applications and associated delivery. Where previously, it might have been expected that a given application would be modified only occasionally or not at all (e.g., early mainframe applications), modern security and DevOps engineers must deal with an on-going demand for new features, upgrades, fixes, and enhancements. The rate of such change, known as release velocity, is now often measured in hours or days rather than weeks or months.

This on-going update and delivery process drives the need for security engineers to design controls that can keep up with change. Automation is the only reasonable choice, especially for non-trivial applications, and when such controls are integrated into DevOps, the enhanced DevSecOps designation is often used to describe the resulting secure software development lifecycle (SDLC). Not all engineering teams have made this transition, but many have.

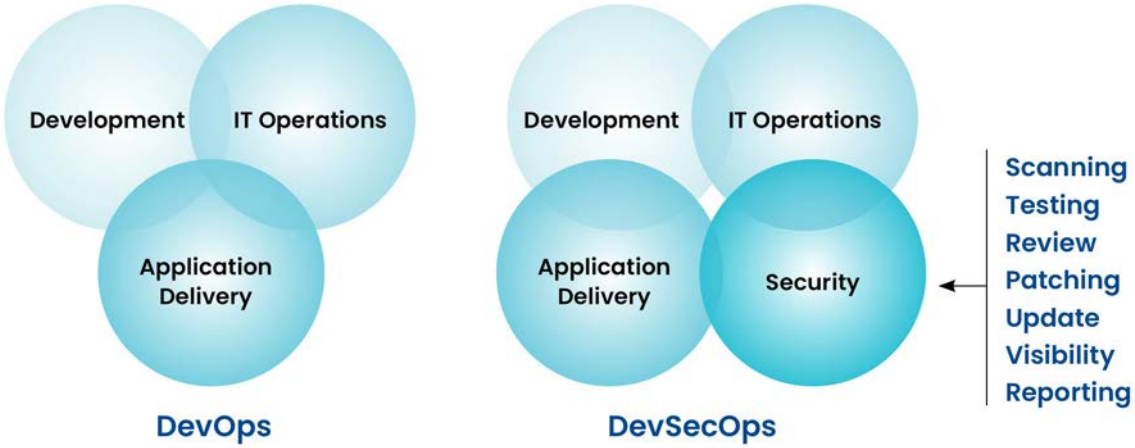

Figure 1. DevOps versus DevSecOps

The security threats that emerge in modern DevSecOps practices can be mapped to all phases of the SDLC. For example, malicious insertions into application code or IaC might be introduced during coding updates. This requires controls to deal with rogue application developers or infrastructure engineers, some of which may operate external to the organization. At the other end of the DevOps process, malicious actors might degrade production environments through exploitation of running applications and gaining access to the underlying run-time systems. This must also be mitigated.

The result is that security engineers have now realized that the best underlying framework for identifying and addressing security threats to applications is by integrating security processes and toolchains into engineering workflows and system life cycles. This is good news because it covers all phases of potential attacks, but it is also challenging news due to the breadth of DevOps coverage which demands that many different types of cybersecurity controls be deployed, automated, and administered.

VISIBILITY AND MANAGEMENT IN DEVOPS

Legacy applications and systems have been protected in traditional data centers using a range of cyber controls that can be viewed roughly as preventive, detective, or reactive. All these security controls depend on the ability to achieve visibility into both static and dynamic aspects of the applications. This includes identifying application configurations and observing behavior. Comparison to an expected profile can then drive insight into determining security posture.

Traditional cybersecurity controls also depend on the ability to manage the application and its associated run-time environment. This is done with familiar security methods such as endpoint controls, security information and event management (SIEM), next generation firewall (NGFW) and so on. Frameworks such as NIST 800-53[4] provide application and security teams with guidelines on how such controls should be arranged in the typical corporate data center.

With the shift to public, hybrid, and multi-cloud, however, these controls also shift. Thus, rather than using a scanner to probe monolithic apps in legacy data centers, modern environments typically involve containerized workloads, orchestrated with Kubernetes, and secured through modern tools such as cloud security posture management (CSPM), cloud workload protection platforms (CWPP), secure access service edge (SASE), and cloud detection and response (CDR).

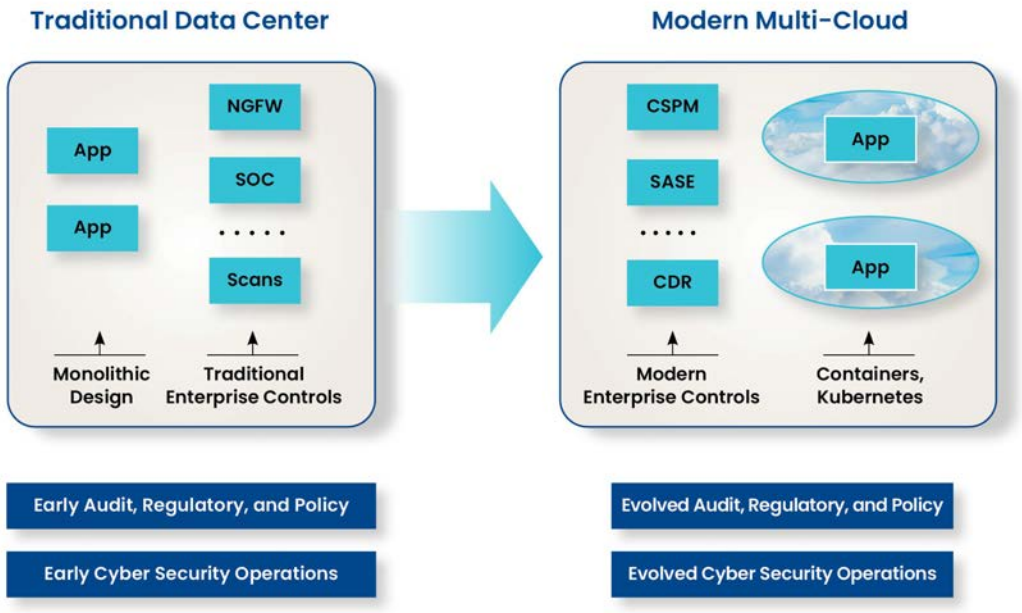

Figure 2. Shift in Controls from Legacy Data Center to Public Multi-Cloud

Security engineers have typically categorized modern cloud security controls into two main groupings: Controls that collect data for posture visibility, and controls that take mitigation action to prevent threats or corrective action (pre-delivery or at run-time) when responding to identified vulnerabilities or threats. Such combination of active and passive security results in an effective means for optimizing security posture – but deployment can be challenging. Combining the best open-source tools with commercial support also requires selecting the right mix of vendor partners.

Perhaps the greatest change that comes with the shift to hybrid or multi-cloud is that both active and passive controls for hosted apps in distributed and diverse environments have had to evolve. In the next section, we will examine a commercial platform from Sysdig that was designed with this shift in mind. The goal is to create an evolved architecture that can support both compliance and cybersecurity obligations for the modern enterprise.

OVERVIEW OF SYSDIG PLATFORM

The commercial Sysdig platform was developed for modern environments that are using containers, Kubernetes, and hybrid cloud infrastructure. The platform is built on an open-source foundations that include the following components:

- *Falco*[5] – Supports run-time detection
- *Sysdig* – Captures and analyzes Linux system calls for forensics and troubleshooting
- *Prometheus*[6] – Provides application and Kubernetes monitoring
- *OPA (Open Policy Agent)*[7] – Enforces policy and is used for IaC security

Sysdig combines these open-source tools with commercial support capability to enable a full lifecycle protection approach for DevSecOps.

Sysdig Secure Architecture
The Sysdig platform includes an agent that is integrated into the host environments in which containers and orchestration are supported. This agent feeds metadata, event, and other information to the Sysdig component which in turn provides event information to the security information and event management (SIEM) platform and notification to workflow. Sysdig APIs support integration with additional tools including open-source capabilities.

The Sysdig Secure platform includes several components which are integrated into the host environments in which containers and orchestration are performed, as well as in the cloud infrastructure. This includes the Workload Agent, which analyzes system calls, and cloud components which analyze cloud logs directly within the cloud account. This instrumentation model feeds metadata, event, and other information to the core Sysdig Engine. This in turn provides notification to workflow systems and relevant information to other integrated enterprise security controls such as the security information and event management (SIEM) system. Integration is also available to additional systems including open-source tools via APIs

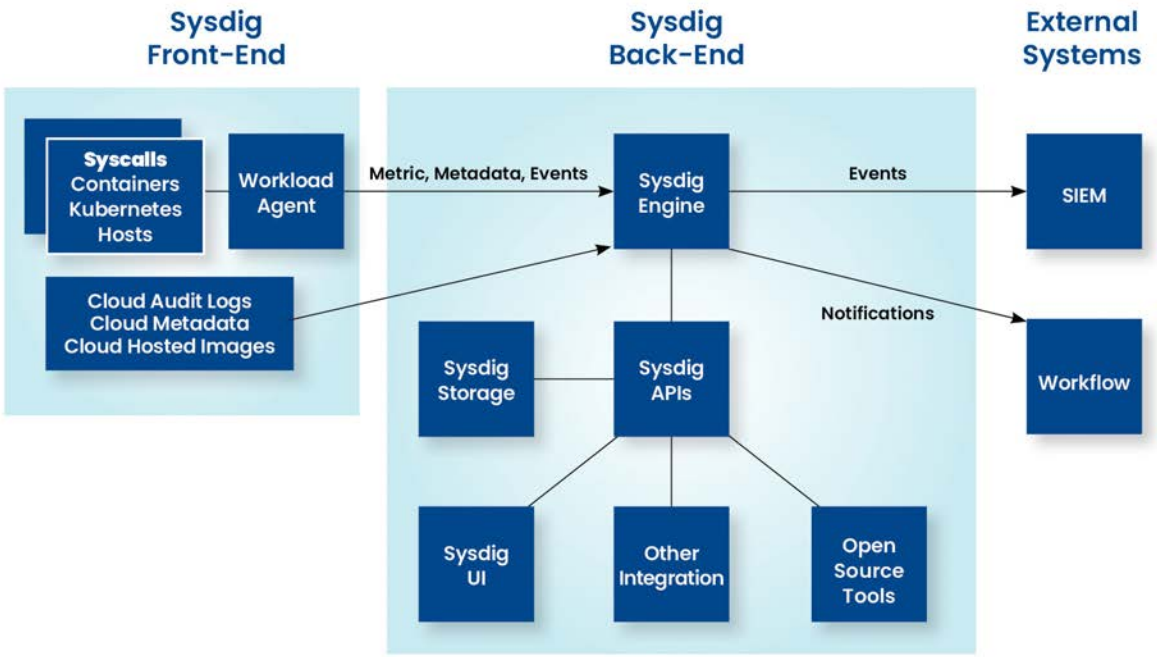

Figure 3. Sysdig Architecture

An objective is to support testing through pre-delivery in CI/CD pipelines (i.e., shifting left) while also monitoring and protecting the workload at runtime (i.e., shield right). The platform closes the loop between shifting left and shielding right using the following components, which are best described as capabilities groups:

- *ContainerVision* – Supports deep visibility into containers, networks, applications, and systems by accessing system call activity. The objective is to support incident response and troubleshooting during DevOps.
- *ImageVision* – Scans CI/CD pipelines and registries for vulnerabilities and misconfigurations. The objective is to block vulnerabilities and monitor for new CVEs in advance of production.
- *CloudVision* – Consolidates cloud activity from logs such as AWS Cloudtrail into a single view. The objective is to support alerting on configuration changes to permissions, AWS buckets, and other cloud resources. It also provides a more secure and cost-efficient approach by processing the data within the cloud account.
- *ServiceVision* – Provides context for Kubernetes and cloud service metadata to support dashboards, metrics, and security status reporting. This group also detects anomalies and supports identifying the correct team to resolve a vulnerability quickly.

In addition, the Sysdig platform integrates with open-source tools that are widely used for troubleshooting cloud applications, workloads, and low-level issues. The open-source Falco tool is used in the context of a Sysdig Secure deployment to help detect vulnerabilities and threats from users, workloads, or services in the local environment. Falco provides cloud activity logs that offer context for the overall Sysdig Secure protection.

Sysdig Capabilities

The Sysdig platform provides DevOps teams with a variety of important security capabilities for their workload applications hosted in AWS, GCP, and Azure. These capabilities, which include asset discovery, cloud security posture management, cloud workload protection, and threat detection, are not only useful for avoidance of cyber threats during the entire software process, but also for establishing compliance in hybrid and multi-cloud environments using data rich reporting.

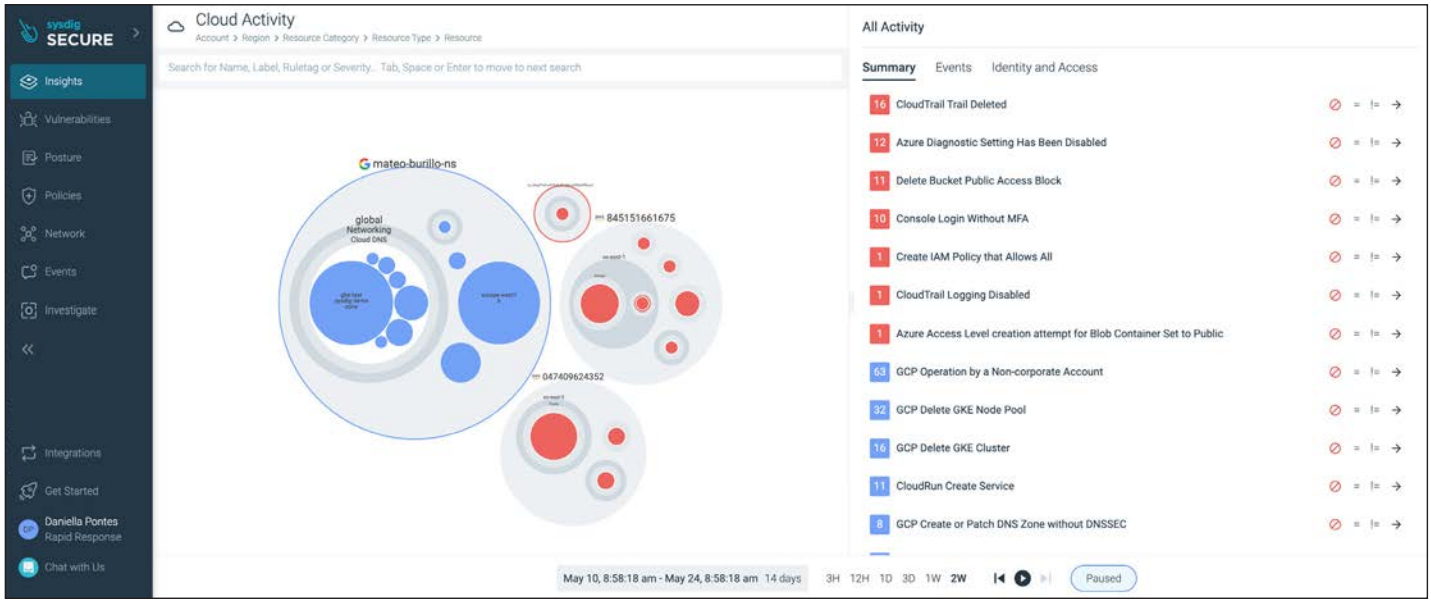

Figure 4. Sample Sysdig Reporting Screen

PROPOSED ACTION PLAN

For DevOps teams who seek to improve the cyber security of their applications, workloads, and operating environments, it is recommended by the TAG Cyber analyst team that the following management steps be initiated immediately:

Step 1: Inventory Current SDLC and Security Tooling
It is useful to begin by reviewing existing security tools being used to protect the current DevOps environment as well as for traditional and legacy environments. This should include both functional capabilities as well as any procedural controls. Particular attention should be placed on whether effective metrics can be derived from these existing security capabilities. Emphasis should include both pre-delivery (shift-left) and runtime (shield-right) functions.

Step 2: Review Security and Compliance Requirements
The next step in the action planning is to review existing and expected security and compliance requirements. This will differ by industry or vertical, economic sector, and organization size. Regulatory requirements and standards bodies also introduce particularly intense security and privacy requirements in cloud infrastructure. Expect to see increased emphasis on pre-delivery visibility into application functionality.

Step 3: Review Commercial and Open-Source Options to Address Security Gaps
The third step is to systematically review options for improving DevOps security using open-source tools as well as commercial solutions. TAG Cyber analysts are always available to assist with both open source and commercial solution review and selection.

[1] *https://kubernetes.io/*
[2] *https://en.wikipedia.org/wiki/Infrastructure_as_code*
[3] *https://sysdig.com/*
[4] *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*
[5] *https://falco.org/*
[6] *https://prometheus.io/*
[7] *https://www.openpolicyagent.org/docs/latest/*

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and nonclients alike—all from a former practitioner perspective.