CYBRIC

VISIBILITY & ASSURANCE

FOR THE **APPLICATION SECURITY LIFECYCLE**

~90%

of security breaches are due to software defects and poor secure-coding practices.

The megatrends of Digital Transformation and Cloud Migration have fueled the “Application Economy” as software is now being incorporated into all lines of business. This new economy is driving rapid innovation to stay ahead of the competition. Development teams are being pushed to release software updates at a much higher velocity, resulting in security either being a barrier to deployment, or dealt with via manual processes and controls well after the deploy.

CURRENT APPLICATION AND CODE SECURITY APPROACHES

Source code and application-level vulnerabilities continue to be the leading causes of security breaches. But next-generation industry investments are focused on controls and processes related to protecting, detecting and remediating the network. According to the Department of Homeland Security (DHS), ~90% of security breaches are due to software defects and poor secure-coding practices. Application layer attacks continue to increase, but overall approaches to application security have lagged behind the increasing speed at which businesses are delivering solutions to market.

Application development is occurring in most lines of business, accelerated by public cloud adoption and platforms and tools such as AWS and Docker. Development teams and processes vary across organizations, which require more adaptive development models and security approaches. Gone are the days of months- or years-long application delivery cycles where static security assessments were enough to deliver reliable assurance or at least pass the security check required at that time. Development methodologies are changing rapidly and security needs to shift from static, siloed verticals to a dynamic, strategic framework that addresses the evolving software development cycle. Organizations should consider a continuous process for code and application security, unifying testing across the software development lifecycle.

Current approaches such as point-in-time scans, penetration tests and code validation lack a holistic view of security posture as there is typically no systemic-level integration and strategy. Current processes are leaving CIOs blind to the real risk their applications pose to their organization. Investments have been in tools that only address a small vertical "slice" in the software development lifecycle such as code security, open source security, audit, inventory, compliance and/or post-production application vulnerability scanning. The security teams are often focused on putting mitigating controls into place to address these specific areas, instead of understanding the overall context of software development workflow and architecting a strategy to seamlessly integrate into it.

CURRENT APPROACHES LACK A HOLISTIC VIEW OF SECURITY POSTURE AS THERE IS TYPICALLY NO SYSTEMIC-LEVEL INTEGRATION AND STRATEGY.

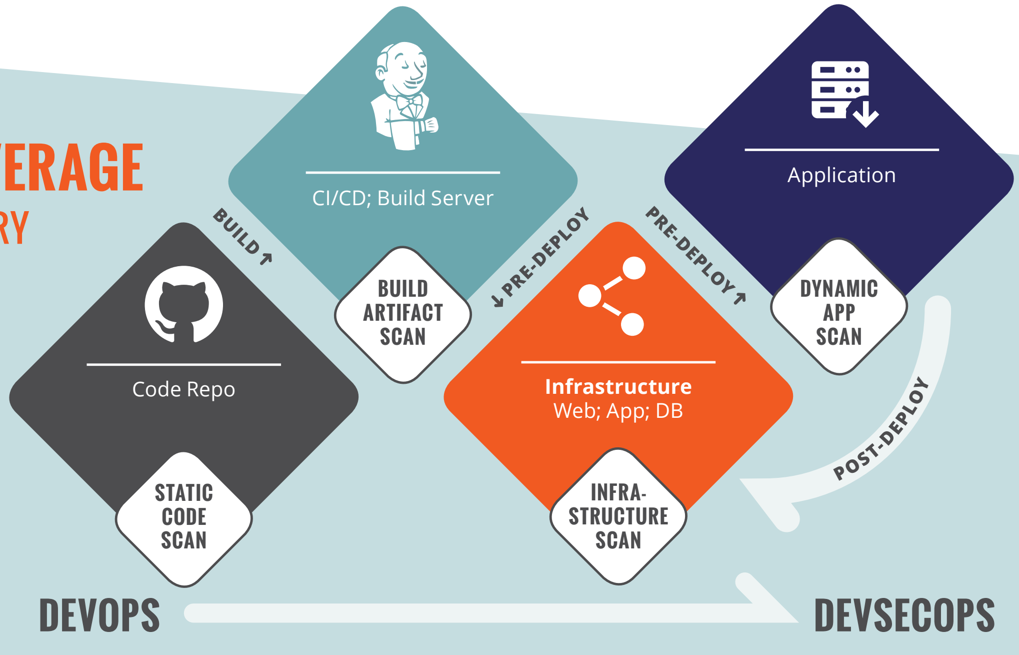
IMPACT OF CURRENT STATE OF APPSEC

The Cultural Divide: Defenders vs. Builders

There are several significant challenges with current code and application security practices, including the cultural divide between the developers ("builders") and the security team ("defenders"). Security teams are overburdened with keeping up with the increasing number of application vulnerabilities and exploits. Complicating the issues further, the velocity of development is accelerating as enterprises adopt DevOps methodologies. Security is still not integrated into the coding and deployment processes and security teams are falling further behind as their manual processes and controls can't scale at the same rate as development. Attempts to implement security are often bypassed by developers, who view it as a hindrance to productivity. This often results in a contentious relationship between the teams. The defenders can't keep pace with the builders and are perceived as a lag on velocity and innovation.

Board Directors and CEOs are now asking direct questions about the overall risk landscape and security posture of the company. Some of these questions include "When was the last time we ran a penetration test, what were the findings and how have we dealt with any issues?", "What is our overall maturity level?", "What are our most critical applications and data?" and "What is

CONTINUOUS COVERAGE
FROM COMMIT TO DELIVERY



our remediation process?" CIOs and CISOs don't have data-driven answers to these, due largely in part to the lack of overall visibility across code repositories and application deployments. It is an extremely difficult, and typically manual, to correlate and aggregate security testing results.

Shift Left

To solve for this contentious, manual, periodic and reactive approach to application security, organizations need to be able to discover and remediate critical code and application vulnerabilities before they are delivered to the production environment. Security and development teams should have the same visibility into all aspects of the security tool chain, top issues to be remediated and status. Application security should be integrated seamlessly into the software lifecycle from the ground up, without impacting development velocity—essentially operating in the background, invisible to developers. This can be accomplished with automatic code analysis and vulnerability scans being orchestrated and automated based upon simple policies and running continuously. Software assembly and delivery is now a continuous process; security testing must be too.

With this drive to "shift left," security teams are now integrated as early as possible into the development process. By employing orchestration and automation, organizations can improve efficiency and reduce DevOps and security team friction, manual errors and overall risk exposure.

Driving Business Results by Shifting Left

By shifting security left in the application development process, by seamlessly integrating it "early and often" and providing holistic visibility to key constituents, security is no longer an obstacle to velocity, innovation and competitiveness. Instead, it's an asset. With frictionless security assurance from code commit to application delivery, companies have peace of mind they are delivering high-quality software to the market.

The positive effects are significant. Releasing high-quality software faster means more satisfied customers and a more satisfied Board. Companies can compete more aggressively and are less likely to have to address brand damage in the face of a security event. By delivering more resilient software, security teams are more efficient and can utilize their resources for the more emergent threats targeting their enterprise. And with unified visibility and reporting across internal security landscapes, CIOs, CISOs or whomever is charged with the security posture can more confidently and readily answer "What is our risk exposure?" and "How secure are we?"

With a continuous, integrated approach to application security, companies can more easily move forward with their digital transformation efforts. They can take advantage of all the cloud and various cloud vendors have to offer by creating a security posture that is centralized to the organization and is platform- and provider-agnostic. Instead of pushing multiple version of the same security requirements out across individual clouds, this posture is "transferable" from one platform to another or interoperable across multiple platforms. And instead of monitoring each environment separately, monitor your posture through a single dashboard.

THE CYBRIC APPROACH

Confidence, Assurance, Resiliency and Visibility – a Single View Into the Application Security Lifecycle

Cybric's adaptive policy-driven platform orchestrates and automates security testing from code commit to application delivery. By integrating with security and DevOps tools across the development lifecycle, Cybric provides continuous visibility and assurance across all code repositories, application deployments and cloud infrastructure. Cybric detects any changes to code, applications and infrastructure configurations to automatically adapt to the elastic development environment and associated risk.

The Cybric platform integrates with best-of-breed open source and commercial tools to support an organization's code and application security ecosystem across all levels of maturity. Through these integrations,

ARE YOU **PREPARED** TO ANSWER THESE **QUESTIONS?**

Board Directors and CEOs are now asking direct questions about the overall risk landscape and security posture of the company. Some of these questions include:

- **When was the last time we ran a penetration test, what were the findings and how have we dealt with any issues?**
- **What is our overall maturity level?**
- **What are our most critical applications and data?**
- **What is our remediation process?**

CIOs and CISOs don't have data-driven answers to these, due largely in part to the lack of overall visibility across code repositories and application deployments. It is an extremely difficult, and typically manual, to correlate and aggregate security testing results.

Cybric provides a holistic view across the application testing landscape and aids in rationalizing investments and understanding the efficacy of current and future tools.

With Cybric, organizations no longer need to rely on periodic point-in-time testing or limited visibility into the true risk of an application. Cybric automates what many organizations address manually or through costly integrations and will continue to leave security out of step with development and the speed required for application delivery.

Cybric's platform also provides vulnerability assessment, notification and prioritization by polling the top threat and vulnerability feeds, correlating them with repositories and associated libraries and packages.

The platform data derived from the orchestration and automation of the security tool chain is presented via Cybric's rich analytics. The correlated data provides an accurate, continuous view of security posture with critical risks prioritized and integrated with IT solutions to track and speed remediation.

FIND OUT MORE

To learn more about how the Cybric platform can provide continuous visibility into your security posture, reach out to us at secure@cybric.io.

BY INTEGRATING WITH SECURITY AND DEVOPS TOOLS ACROSS THE DEVELOPMENT LIFECYCLE, **CYBRIC PROVIDES CONTINUOUS VISIBILITY AND ASSURANCE ACROSS ALL CODE REPOSITORIES, APPLICATION DEPLOYMENTS AND CLOUD INFRASTRUCTURE.**

CYBRIC

Cybric is the first to orchestrate and automate code and application security across the DevOps lifecycle. The company's platform leverages patent-pending technology to seamlessly integrate security into the development process, delivering frictionless security assurance from code commit to application delivery.

If you are interested in learning more or seeing a demo, please contact us at **secure@cybric.io**.

cybric.io