Accenture Security

ACCENTURE CYBERSECURITY FORUM

Can we "bake in" security within a DevOps culture? Key imperatives for security, collaboration and innovation

Accenture Cybersecurity Forum
Virtual Roundtable Summary
November 14, 2018

DISCUSSION

The Accenture Cybersecurity Forum (ACF) conducted a virtual roundtable on November 14, 2018, on the subject "Can we 'bake in' security within a DevOps culture? Key imperatives for security, collaboration and innovation." CISOs from multiple industries and organizations joined the discussion with our guest subject-matter expert Steve Curtis, managing director and Communications, Media & Technology lead – Accenture Security. The host was Andy Vautier, Accenture CISO and ACF co-chair.

Prior to the roundtable, interviews were conducted with a cross-section of ACF members to explore imperatives for security, collaboration and innovation in a DevOps environment.

The roundtable was conducted under the Chatham House Rule: All ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Security in a DevOps environment

Over the last 10 years, application delivery has shifted from large-scale, project-based systems implementation to an ongoing collaboration between software development and IT teams. DevOps makes this shift possible by bringing business, development and operations teams together to streamline development and improve communication and collaboration, with a focus on applying more automated processes.

ACF Co-chair Andy Vautier noted that "building security into DevOps environments is a critical but relatively immature process. The definition of 'good' in terms of compliance and security among DevOps teams is often incomplete."

Steve Curtis added, "There is real pain at the development team level about addressing security vulnerabilities."

DISCUSSION

Vautier recommended repositioning security in a DevOps environment from something that is bolted on or inspected in at the end to a first-order concern that is embedded throughout the systems development lifecycle (SDLC). In a mature DevOps model, "it would be culturally difficult for developers to put a system into production with security vulnerabilities," he said.

Developing applications that are secure to the fullest extent possible "requires the right kind of top-down mindset from leadership to developers, and the right kinds of technology tools," Vautier stated. "The current paradigm focuses on 'inspecting in' security at various points in the development lifecycle, particularly during pre-production. But what I'd like to see is a pivot where security is fully embedded into the development community and its processes from project inception onward."

Curtis reported that security in DevOps is top of mind with senior executives. However, embedding security presents major challenges. "Our client development teams are saying they've been told by security that they have tens of thousands of vulnerabilities in their applications that they need to resolve. This is usually found in post-production and is becoming an emergency. They're asking, "How do I deal with all of these vulnerabilities and backlog?'

"The question we're asking clients is, 'Why did you build so many vulnerabilities to begin with?' This is clearly too late in the lifecycle. It's costing a lot of money and making it very difficult to successfully deploy and operate secure applications. This issue is exacerbated as more organizations move to the cloud, and the challenge gets to be not just doing security by design, or at build, or in pre-production, but really about connecting all of those things at speed and scale."

ACF members participating in the roundtable discussed how CISOs are addressing DevOps security requirements across a variety of dimensions: governance and standards; automation and technology; culture change; process change; and training.

DISCUSSION

Governance and standards

Establishing pervasive security standards is a tremendous challenge, particularly across large enterprises. Governance is a key ingredient in "baking in" security.

"Most of the executives I speak with have a pretty good idea of how to do it, but getting it done is very difficult because they may have thousands of feature teams building products and applications that vary in their risk profiles," said Curtis. "Being able to integrate security techniques across the entire lifecycle, across all feature teams, at the speed the feature teams want to move, that's really the biggest and hardest part of the whole conversation."

He continued, "The conversation becomes less about what to do from a technology perspective and more about culturally how to roll this out across thousands of developers and feature teams and get them to apply security practices on a regular basis."

The CISO of a government agency said that moving applications to the cloud adds even greater focus on security accountability. At the same time, budgetary pressures call for greater efficiency. Establishing the right governance model and focusing senior management attention on application security are key to operating successfully in this environment, he said.

Vautier declared that the cost of security should be lower when incorporated earlier in the SDLC. Setting baseline policies using public standards such as the National Institute of Standards and Technology can be an efficient way to get started.

A UK-based CISO reported success in relying on publicly available standards such as those from the National Cyber Security Centre. "That has allowed us to write up those baseline requirements and consistently deliver them to the various teams," he noted. "For DevOps in particular, they know they have to come to us and ask what's the standard you want us to hit."

Curtis said that governance must be established to avoid and address unproductive conflicts that can occur between developers and the security function. Vautier added, "When developers know they have to engage with the security team earlier in the design process, it can mean the difference between an effective roll-out or shutting the system down before exposing the enterprise to vulnerabilities."

For example, bringing threat modeling earlier into the design process and creating tiers of risk profiles can be effective ways of establishing governance across developer and security domains.

Automation and technology

Technology is but one key to baking security into DevOps, Vautier asserted. "Absent technology, I think it is hard to get to a satisfactory conclusion, but clearly technology on its own doesn't solve the problem.

"Systems architecture is one area where security can be added to the SDLC. Establishing standard APIs and isolating security functions from other system elements can help developers and the CISO team more quickly identify and remediate common mistakes that create vulnerabilities. Applying a modular architecture model can be useful in isolating functions," Vautier said.

He added that intelligent IT platforms that have security features locked in can be useful for DevOps teams that otherwise find it difficult to meet the security requirements of new apps. "Embedding security expertise into technology, platforms and tools will be an ongoing journey rather than a concrete destination," he added.

One CISO reported, "We put in some automated tools and processes to make that as seamless and easy as possible. We've had some challenges, but it's still the best way we've found to make sure that the applications that are going into production aren't filled with malicious code."

Curtis said a best practice was "having core architectural patterns, common code, and common tooling being able to directly integrate security into the continuous integration (CI) and continuous delivery (CD) pipelines that are driving many of these development techniques and the integrated development environment. Automate where possible, but since not everything can be automated, create a capability to allow the development teams to order security tasks as needed, such as threat modeling and penetration testing, for example."

Culture change

Getting DevOps teams to adopt security best practices often requires a cultural shift that starts at the top of the organization.

The CISO of a public entity explained, "If we can get senior leadership and the command team of the organization on board, we can make sure that certain governance stage gates are always heeded. For example, if someone tries to bypass an organization or policy and goes straight through to deliver something too quickly as an agile service involving DevOps, they will be called and notified that the app will be IT health checked, penetration tested, and documented. We've tried to get the DevOps team on board and really drill them on the importance of security.

"We're trying to make sure that it comes from the top down to say you're going to have to go through this process to get new apps formally launched. We're finding that message drifting down now into the culture, and it is changing the ethos of the DevOps team so that they're actively engaged with us now as security professionals," he added.

Other CISOs said that DevOps teams are required to understand security requirements and confirm compliance at every stage of the SDLC before new apps are released. The CISO of a global manufacturer added that "cultural change

can be driven by introducing developers to common security tools, and then supporting them in using those tools effectively and consistently."

A security executive of a defense company noted, "It is really about shifting culture. We needed to have a culture where our app developers really lean on the security organization. Empowering our application developers to be security champions is crucial, to feel ownership of these choices. As the security organization, we provide the capability to help developers go from 'I wrote a piece of code' to 'I'm going to push it to production with the right security features.'"

Process change

A global manufacturer CISO said, "From a process standpoint, we're trying to implement a common set of frameworks, practices and principles for both our enterprise applications and the software handed over to clients as deliverables. That's probably our biggest priority and challenge right now—trying to make sure that we're staying consistent across the enterprise." He remarked that DevOps teams are required to understand security requirements and confirm compliance at every stage of the SDLC before new apps are released.

Threat modelling was recognized as an important process. "Threat modeling can be an important design element to bring security into the design process," Curtis reported. "We're showing developers how to hack into designs before we even start building them. That can be really enlightening for developers."

Curtis and several CISOs commented on the value of data classification schemes for prioritizing security efforts. Curtis summarized, "We see success in large development shops where applications with personally identifiable information (PII) and transaction features are Tier 1. There are other applications that don't have PII and are only internal, maybe that's a Tier 3."

DISCUSSION

Training

Building strong security skills within DevOps teams may not be possible for a variety of reasons. Other solutions, such as training at the point of need, can be more efficient and effective.

"The shortage of security talent makes it impossible to incorporate it into every DevOps team," said the CISO of a global financial services firm. Another financial services CISO agreed that expecting developers to add deep security knowledge to their skill sets is impractical.

Curtis observed that even real-time feedback from the security team to developers is important and possible throughout the development process. "Sprints in an agile development environment are often two to four weeks long. Each sprint should be viewed as an opportunity for the security team to provide feedback," he said.

He compared the process to training a puppy, where immediate positive reinforcement is most effective in promoting new behaviors. "Provide developers with the opportunity to 'phone a friend' and get feedback from the security team in real time," he suggested. "Make it easy for developers to engage in getting questions answered upfront."

Conclusion

Curtis summarized the four key strategic elements of a DevSecOps program and four specific activities for developers. The program is: 1) governance and reporting; 2) assets and accelerators; 3) design, build, test and deploy activities; and 4) operational security. The four activities, highlighted in item No. 3, are: 1) threat modeling; 2) static application security testing integrated into the integrated development environment (IDE); 3) dynamic application security testing and manual penetration testing for each build; and 4) integration into security operations such as security information and event management (SIEM) and identity and access management (IAM).

DISCUSSION

In addition, Curtis recommended plugging in security across the entire DevOps CI/CD process. Tools for penetration testing, static and dynamic application security testing have value, but sometimes the work cannot be automated. In those cases, on-demand support from security experts can be invaluable.

Vautier reinforced the importance of governance, training, culture, process and technology. Embedding them as early as possible in the SDLC is critical to reducing overall implementation and security risk.

He commended the CISO community for a collective recognition that they need to support DevOps innovation. But he also cautioned that the pain CISOs have been feeling in "having to say no" to developers may increase in the short term as security regulations and threats increase.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us **@AccentureSecure** on Twitter or visit us at **www.accenture.com/security**.

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us