Secure Digital Transformation

Cybersecurity Skills for a Safe Journey to DevOps and Cloud

CyCon 3.0 | February 15, 2020

Troy Marshall | @RTroyMarshall | /in/TroyMarshall

Digital Transformation

70%

% of companies either have a digital transformation strategy in place or are working on one according to a 2018 survey by Tech Pro Research.

“Digital transformation is a fundamental reality for businesses today. Organizations of all sizes realize that to delay digital transformation further is to risk obsolescence.”

-Warren Buffet

Cloud

94%

% of of enterprises are already using a cloud service according to a survey by Flexera.

“If someone asks me what cloud computing is, I try not to get bogged down with definitions. I tell them that, simply put, cloud computing is a better way to run your business.”

-Marc Benioff

NIST- Essential Characteristics of Cloud Computing

On-demand self-service	A consumer can unilaterally provision computing capabilities, as needed automatically
Broad network access	Capabilities are available over the network and accessed through standard mechanisms
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model
Rapid elasticity	Capabilities can be elastically provisioned and released to scale rapidly with demand.
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability

Source- NIST Special Publication 800-145

NIST- Cloud Computing Service Models

Software as a Service (SaaS)	Delivers software and applications through the internet.
Platform as a service (PaaS)	Access to a cloud-based environment in which users can build and deliver applications.
Infrastructure as a service (IaaS)	A vendor provides clients pay-as-you-go access to computing resources in the cloud.

Source- NIST Special Publication 800-145

DevOps

2,604

Times faster time to recover from incidents in elite performing DevOps organizations according to the 2019 Google State of DevOps report.

“It’s difficult to overstate the enormity of this problem—it affects every organization, independent of the industry we operate in, the size of our organization, whether we are profit or non-profit. Now more than ever, how technology work is managed and performed predicts whether our organizations will win in the marketplace, or even survive.”

-Gene Kim, The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations

What is DevOps?

DevOps is the cultural shift that combines people, practices, and tools to increases an organization's ability to deliver applications at high velocity.

Common DevOps Practices

CI/CD

Continuous integration (CI) and continuous delivery (CD) enable application development teams to deliver code changes more frequently and reliably through automation.

Infrastructure as Code

Management and provisioning of infrastructure using software development techniques like version control and CICD.

Microservices

Service scoped to a single purpose combined with other services communicating via APIs to form a single application.

Information Security Challenges

7%

% of companies that believe they have good visibility of all critical data according to a survey by ForcePoint.

“The purpose and intent of DevSecOps, is to build on the mindset that ‘everyone is responsible for security’ with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required.”

-Shannon Lietz

Common Cloud Security Issues

Misconfiguration of cloud resources

Misconfiguration of cloud resources is a leading cause of data breaches. The most commonly reported effect is the exposure of data stored in cloud repositories.

Poor secrets management

Poor identity, credential, or key management can lead to unauthorized access to data, denial of service, and elevation of privilege. Common examples include leaked API keys or lack of MFA.

Common Cloud Security Issues

Lack of secure architecture

Security in the cloud requires different mindset than traditional data center security. There is often a lack of understanding of the shared security responsibility model in the cloud leading to incorrect security assumptions.

Shadow IT

Studies from Gartner and Everest Group have estimated that 50% or more of IT spending in large enterprises is occurring outside the control of the Information Technology and Information Security organizations.

Common DevOps Security Issues

Lack of security skills and ownership

Developers tend to prioritize the functionality of the applications they build over watertight code security. They often lack the necessary security skills and knowledge.

Accelerated development leaves little time for security checks

Traditional heavy security processes cannot keep up with the pace of software development and deployment in CI/CD environment.

Common DevOps Security Issues

Infrastructure as Code

Simple configuration mistakes in software defined infrastructure can leave systems and data publicly exposed.

Microservices and serverless computing

Microservice and serverless architectures present a different set of security challenges and require different solutions than traditional monolithic applications

Skills for Secure Digital Transformation

62%

% that the U.S. cybersecurity workforce needs to grow to meet today's demands according to the 2019 (ISC)² Cybersecurity Workforce Study.

“What on earth would make someone a nonlearner? Everyone is born with an intense drive to learn. Infants stretch their skills daily. Not just ordinary skills, but the most difficult tasks of a lifetime, like learning to walk and talk. They never decide it’s too hard or not worth the effort.”

-Carol S. Dweck, Mindset: The New Psychology Of Success

Full Stack Security

Security professionals need to understand the full stack of information security in order to be successful.

Security as Code

Security can’t be bolted on, it must be directly integrated into CICD. To integrate security into the way DevOps teams work in the cloud, it must be automated.

Security is a business enabler

To help organizations succeed in digital transformation initiatives, security professionals need to understand business needs and develop security solutions to meet them.

Continuous Learning

Information security skills and talents need to evolve and grow at the same pace as technology.

Thank you!

Troy Marshall
@RTroyMarshall | /in/TroyMarshall