Collaborative DevSecOps in a Service Provider Environment

ATIS-I-0000082 | March 2021

Abstract

Telecom service providers are increasingly migrating their software development, deployment and lifecycle environments to a cloud native architecture. This migration dovetails with a second trend: the use of DevOps for continuous delivery models and automation of system management. When security expertise and responsibilities are tightly integrated within the DevOps processes, the result is DevSecOps. Together, cloud native and DevOps/DevSecOps enable the creation of loosely coupled systems that are scalable, resilient, manageable, observable and secure.

Cloud native and DevOps trends have been led by enterprise IT. However, service providers have unique requirements that may make it impractical to simply import enterprise cloud native architectures and practices. Specifically, the service provider environment often has more stringent requirements for security, resiliency, availability, scalability and performance due to a larger, more diverse customer base that may be covered by a variety of SLA requirements. In addition, service provider networks must meet these more stringent requirements given a highly diverse environment where many different vendors and integrators must closely collaborate.

This report explores the unique challenges associated with collaborative DevSecOps in a service provider cloud native environment. It also provides best practices for creating and maintaining a secure environment.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' 150 member companies are currently working to address network reliability, 5G, robocall mitigation, smart cities, artificial intelligence-enabled networks, distributed ledger/blockchain technology, cybersecurity, IoT, emergency services, quality of service, billing support, operations and much more. These priorities follow a fast-track development lifecycle from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org. Follow ATIS on Twitter and on LinkedIn.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Table of Contents

1 Executive Summary

Network service provider environments include deployment scenarios where large, complex systems are created through the integration of a variety components provided by a multitude of vendors. *Section 3 – Use Cases* discusses examples of these deployment scenarios in more detail.

Service providers are increasingly leveraging cloud native software development, deployment and lifecycle environments to implement the use cases noted above. Cloud native technologies enable service providers to build and run scalable applications in modern, dynamic environments using containers, service meshes, microservices, immutable infrastructure and declarative APIs to capture the key benefits of a cloud native architecture. Combined with DevOps, continuous delivery models and automation, this approach enables the creation of loosely coupled systems that are scalable, resilient, manageable and observable.

In a cloud native DevOps model, development and operations teams are no longer "siloed." Instead, they are merged into a collaborative team where the engineers work across the entire application lifecycle, from architecture, design, development and test to deployment and ongoing operations. DevSecOps refers to scenarios where security expertise and responsibilities are also tightly integrated within the DevOps processes. DevSecOps incorporates security culture, practices and tools to drive visibility, collaboration and agility, ensuring security in each phase of the DevOps pipeline. This focus on security and performance is particularly important in network service provider environments given the unique needs in providing wide-area communications services. Specifically, these networks are characterized by such factors as:

Complex Network Models: Unlike many IT environments and applications, service provider workloads generally exist in a complex and expansive network environment (the WAN) and may require sophisticated network models to support needed network capabilities.

Service Function Chaining: In IT environments, applications and services generally represent discrete and independent workloads. However, service provider applications are often comprised of complex combinations of services that may have interactions (e.g., policy, billing or legal intercept purposes) and must be configured together as an application through which traffic needs to be correctly steered based on dynamic information.