Adapting Security to Cloud-native Development

Organizations are seeing increased security risk for cloud-native applications. With 69% of respondents saying they are experiencing an increase in IaC template misconfigurations, there is a pressing need for a platform approach. Most organizations believe that a platform approach will drive efficiency to enable security to scale with cloud-native development. The top 5 business drivers for cloud security posture management include improving security testing, detecting secrets that have been committed and stored in source code repositories, applying an issued patch, quick remediation, and automating security controls via integration.

Interpreting Security in DevOps

As organizations increasingly leverage cloud platforms to efficiently mitigate security risk as development scales, these platforms tie security in development processes to improving security posture, helping security teams effectively manage risk for cloud-native applications. Organizations are prioritizing developer-focused security strategies, including shifting some security responsibilities to IT or operations teams to set it up for them, which not only saves time but also increases security risk.

Cloud-native application development allows developers to quickly assemble applications from third-party code and templates. While this saves them time, it increases the chances of introducing mistakes and vulnerabilities that may be exploited. Organizations are concerned about hackers exploiting vulnerabilities in internally developed code. While utilizing IaC templates empowers developers to provision their own code repositories, it also increases security risk.

To better understand OSS usage risks so they can quickly respond when vulnerabilities are found, organizations are also investing in solutions that integrate security processes into developer workflows. About 85% of organizations are using or plan to use IaC, with 68% of respondents saying they are experiencing an increase in IaC template misconfigurations. About 69% of respondents believe that a high percentage of code composition is OSS, with 26% of organizations saying a high priority of them is open source software challenges and concerns.

Conclusion

To see how Cisco can address your cloud application security needs from development to runtime, please click the link below.