Shift-Left: Security is a Part of all Phases in Software Development

Published 18 March 2021

Team8
Global venture group

Developing and managing software is more agile and faster than ever. Security can't come after the fact, but needs to be shifted-left to the developers, embedding security considerations from the start in a DevSecOps model.

Drivers

Time to market is often prioritized over security. Developers are measured by how fast they can code, rather than on how securely. And business leaders are measured on how quickly they can provide new products and services to the market. With no time to fix insecure code at the source, security is often "bolted on" once the application is fully developed -- a risky approach. As a result, 42% of organizations that experienced an external attack blame the incident on a software security flaw and 35% blamed a buggy web application.[1] In today's dynamic environment of micro-releases and daily or weekly software updates, software developers need to maintain a security mindset and rely on controls throughout the coding process in order to get ahead of security issues. Despite this, the migration of a developer-driven security paradigm has been slow; Google reports only 20% of firms are considered "elite performers" with DevOps.[2] 'Shift-left' highlights the need for security teams to work with developers from the very beginning of the development lifecycle to build-in information security and security automation. Ideally, developers are empowered to embed security while creating a product or service, with tools that not only make code more secure but also codify intent.

Impact - The farther left the shift, the more deeply security is integrated into the application development process. To achieve this, security professionals should hone their coding skills, and developers must be able to code with security in mind.

Solutions - Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Software Composition Analysis (SCA), Secure Development Lifecycle, Developer Security Training, Container Security

Perspectives:

- **Defender's Perspective -** "One way to measure the speed of business is developer velocity. Developers are constantly adding features to applications, and if companies wish to remain competitive, modern day security has to move at the speed of business." - Stephen Garcia, VP of Cybersecurity, FanDuel

- **Team8's Attacker Perspective -** "Shift-left creates several problems for the attacker. As software becomes more security robust, the chance of zero days is getting slim. However, sophisticated attackers can also shift left, adding malicious code or backdoors early in the development cycle before or after the source code is compiled. An example of this is the attack on the build system of SolarWinds. Instead of waiting for or finding a vulnerability, attackers changed the system just like a coder would, and created their own vulnerability."

In our next blog, we will cover Smarter Security.

Related blogs

+ Introducing cybersecurity, the megatrend of the 2020s

+ Cloud security: A necessary component in digital transition planning

+ Security of Things: Dealing properly with the explosion of connected devices

+ Perimeterless world: Networks are becoming less tied to physical locations

+ Privacy & Digital Trust: 2010' s were about Data Collection, 2020' s will be about Data Protection

1 https://www.forrester.com/report/The+State+Of+Application+Security+2020/-/E-RES159057

2 https://services.google.com/fh/files/misc/state-of-devops-2019.pdf

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can offen lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.