verinext

Best Practices Briefing
API Security

It used to be that practicing data security meant securing individual machines and the networks they resided on. However, as applications have risen out of specific machines and into the cloud, so have security threats. Instead of the vulnerabilities existing solely at the network layer, they are now also at the broad API layer, the doorway into our modern, cloud-native applications in both public and private cloud environments.[1]

The use of APIs is on the rise[2], and so too is the number of API security breaches. According to Forbes in March 2022, over 40% of large organizations have 250+ APIs. And 71% plan to use even more APIs over the next year.[3] As APIs continue to grow, a recent Gartner report predicts that "by 2025, less than 50% of enterprise APIs will be managed." This means that less than half of all APIs that potentially have access to important data in applications will be known, secured and controlled.[3]

From banks, retail and transportation to IAPI, autonomous vehicles and smart cities, APIs are a critical part of modern mobile, SaaS and web applications and can be found in customer-facing, partner-facing and internal applications. By nature, APIs expose application logic and sensitive data. As a result, APIs have increasingly become a premium target for attackers. APIs are essential for rapid innovation. It is critical that all APIs allowed by an application are known and secured to eliminate an otherwise huge attack surface is just waiting to be exploited.

During the API Security briefing, participants are provided with an overview of the rapidly evolving API security frameworks including specific vulnerabilities related to APIs. Verinext will also provide recommendations for providing effective workflows to secure the environment without slowing the pace of innovation, key factors to consider in implementing policy and process controls, and how to effectively budget both time and resources to address this critical need. This interactive briefing aims to contextualize market capabilities with the needs of your enterprise.

DISCUSSION FRAMEWORK:

1. Introduction: Why are many APIs inherently insecure?

- Top API Vulnerabilities and Market Trends
- Evolving standards and frameworks including OWASP (Open Web Application Security Project) and various standards promoted by vendors in the space

2. Key Design practices for API Security

- API Discovery and Risk Identification
- The compounding risk of application integration via APIs
- Authorization, Integrity and Testing

3. Visibility and Architecture: The Cornerstones of Robust API Security

- How Development and Systems teams unknowingly introduce API vulnerabilities.
- Exploring methods and tools to enhance visibility & security across the entire API landscape (internal and external), ensuring timely detection and response to threats.
- The role of architecture in bolstering API security: best practices, redundancy, segmentation, and API architectural considerations.
- How to provide continuous monitoring of APIs

EXPECTED OUTCOMES:

The goal of this briefing is to enhance your API Security Posture with the following:

- Tailoring the high-level steps to suit specific organizational needs and scenarios.
- Recommending continuous improvement activities and processes.
- Setting a cadence to stay updated in a rapidly evolving API security landscape.
- Choosing the appropriate risk-based framework for your environment.
- Defining the next steps to develop a roadmap and implement quick wins in your enterprise.

RECOMMENDED PARTICIPANTS:

VP Application Development, Application Security Engineers & Architects, Data Architects, CIOs, CISOs, Operational Technology and Information Technology Leaders, Line of Business Owners, IT Architects, and Digital Transformation champions.

Expected time: 90 minutes.

References:
1 - https://techblog.cisco.com/blog/top-5-api-security-breaches-in-2022
2 - https://apiumhub.com/tech-blog-barcelona/rise-api-economy/
3 - API Stack: The Billion Dollar Opportunities Redefining Infrastructure, Services & Platforms (forbes.com)
4 - Predicts 2022: APIs Demand Improved Security and Management (gartner.com)