wib. | Whitepaper

Building an API-First security Program – the why and how

Throw the light onto APIs without casting shadows

Why illumination is the route to eliminating API blindspots and how Wib Fusion Platform's advanced incident detection, complete visibility into API interactions, and seamless integration with existing security tools enables organizations to proactively defend against API logic attacks.

Introduction

In today's digital landscape, organizations increasingly rely on microservice architectures to enable faster development and deployment of their applications. APIs (application programming interfaces) play a crucial role in these architectures, enabling communication and data exchange between various services. As a result, APIs have become an attractive target for attackers who seek to exploit vulnerabilities and gain unauthorized access to valuable company resources.

A significant challenge faced by organizations is the presence of API blind spots within their diverse security programs and tools. Development teams utilize development security programs, employing solutions such as SAST, SCA, and API management tools. The security programs of DevOps teams incorporate security tools like IAST and DAST. Security teams, meanwhile, implement security programs like SOC, vulnerability management, auditing, pen testing, and red teaming, utilizing vulnerability management tools, WAFs, and SIEMs. Traditional security tools employed by these various teams often lack the visibility into and understanding of API-specific logic, leaving organizations vulnerable to API and business logic attacks. These attacks manipulate the intended functionality of an API by bypassing security measures, mostly relying on field validation techniques.

To address this issue, we introduce the Wib Fusion Platform, a comprehensive API security solution designed to provide holistic protection across an organization's entire API ecosystem. It delivers API-focused automated visibility and security to enhance areas where current programs are blind to, empowering development, and security teams with the access, insights and tools to eliminate API blind spots and secure API threats starting from code, passed to testing and committed to production environments. In this paper, we will discuss the problem of API blind spots within organizations, the solution provided by the Wib Fusion Platform and how it integrates with various security programs and tools across the security pipeline.

API blind spots in security programs

API blind spots occur for many different reasons. What's important at the outset is to accept that blind spots exist. Many organizations believe they are protected as they have code analysis tools, WAFs, API gateways, or because they run pen testing and other such programs. This is the first problem; having a false sense of security – a sense that these specialized code, testing, and application tools will cover all aspects of API visibility and security.

They do not.

APIs are elusive. They are special. They are not just another piece of code or application, to be analyzed based on a specific field or for a CVE. They focus on business logic, and they are relied upon (in their secure implementation) in the wider context of the organization to enable its core business functions.

In this article, we examine each of the existing security programs of a typical organization, and their API blind spots.

Development teams

Development teams use static application security testing (SAST) and software composition analysis (SCA) to identify and remediate code-level vulnerabilities. While these tools can detect some API security issues, they are not designed to handle the specific challenges of API security.

- SAST tools analyze the source code for potential vulnerabilities but may miss runtime vulnerabilities or fail to understand the complex interactions between different API endpoints.
- SCA tools identify and manage risks associated with third-party dependencies but do not address API-specific vulnerabilities.

These examples demonstrate that existing security programs in development environments often lack the visibility and understanding needed to effectively defend against API-specific threats. This leaves organizations vulnerable to API logic attacks and other sophisticated exploits, necessitating a comprehensive API security solution capable of eliminating API blind spots.

DevOps teams

DevOps teams employ tools such as dynamic application security testing (DAST) and interactive application security testing (IAST) to pinpoint vulnerabilities in their applications. However, these tools may not effectively address API-specific vulnerabilities, as they typically focus on the broader application rather than the distinct features of APIs.

- A DevOps team using DAST tools may identify vulnerabilities in an application's external interfaces, but these tools may not catch the intricate internal API calls occurring between microservices. As a solution, implementing API-focused visibility and security can help DevOps teams better understand and secure these internal API interactions.
- In contrast, IAST tools monitor an application's runtime behavior. However, their dependence on instrumentation and code analysis may not offer enough insight into the complex nature of API interactions. By incorporating API-specific visibility and security, DevOps teams can gain a more comprehensive understanding of API behavior, enabling them to detect and resolve vulnerabilities more effectively.

Security Teams:

Vulnerability management team

The vulnerability management team identifies, assesses, and manages vulnerabilities in an organization's systems, applications, and infrastructure. It uses vulnerability management platforms and scanners to detect vulnerabilities and coordinate penetration testing and red team exercises.

However, vulnerability management scanners might not detect API-specific vulnerabilities, such as misconfigurations, weak authentication methods, or known and unknown APIs ('shadow' and 'zombie' APIs).

SOC team

The security operations center (SOC) team monitors, detects, and responds to security incidents. It collaborates with the WAF management team to ensure web application firewalls (WAFs) are properly managed and configured to protect web applications from common attacks.

WAFs, however, harbor API blind spots when they struggle to detect and prevent API logic attacks that exploit vulnerabilities in the API's design or implementation.

Incident response team

The incident response team manages and responds to security incidents within the organization. It focuses on minimizing the impact of breaches, recovering from incidents, and ensuring proper communication. It manages and uses security information and event management (SIEM) systems to identify and track incidents and prioritize responses.

SIEM tools can suffer from API blind spots, as they may fail to recognize API-specific anomalies like excessive access attempts or abnormal data transfers.

The solution: Wib Fusion Platform and Wib Fusion Defense

The Wib Fusion Platform, a comprehensive API security solution, is specifically designed to address API blind spots and shield organizations from API-specific threats. By providing all-encompassing protection across the entire API ecosystem, this platform enables security and development teams to bridge the gap and eliminate API blind spots effectively.

To maximize the effectiveness of the Wib Fusion Platform and Wib Fusion Defense, seamless integration with existing security programs is essential. By incorporating Wib Fusion Defense into an organization's security pipeline, it enhances the capabilities of various security tools and teams, creating a comprehensive and unified approach to API security.

Development security workflows: SAST, SCA, ticketing

Wib Fusion Defense complements the static and dependency analysis performed by SAST and SCA tools. It provides real-time feedback on API security issues, enabling developers to address vulnerabilities early in the development process. With the help of Wib Fusion Defense's API testing engine, developers can validate the efficacy of applied patches and ensure they address the root cause of the vulnerability. The platform also integrates with ticketing systems, streamlining communication between teams and automating the tracking of vulnerability remediation efforts.

DevOps security workflows: DAST, IAST

Wib Fusion Defense enhances the capabilities of DAST and IAST tools by providing additional visibility into API-specific vulnerabilities and runtime behavior. It identifies potential attack paths on vulnerable API endpoints, allowing DevOps teams to prioritize their efforts and focus on the most critical security issues. Moreover, Wib Fusion Defense's validation engine enables DevOps teams to track vulnerabilities that are deployed into testing and pre-production environments.

Security teams workflows

Wib Fusion Defense integrates with SOC security program tools such as SIEM systems, providing API-specific security event data that enhances its ability to detect and respond to threats. By incorporating API baselines and known attacker tactics, security teams can better identify anomalies and proactively defend against API logic attacks. Furthermore, Wib Fusion Defense's virtual patching feature integrates with existing WAFs to provide temporary security fixes while permanent solutions are developed. It also integrates with vulnerability management tools to enable security teams to track vulnerabilities that were streamlined and found in production environments.

The Wib Fusion Platfom also supports collaboration with red teams, providing valuable input for penetration testing exercises and helping to identify areas of improvement in an organization's API security posture.

By integrating Wib Fusion Platform and Wib Fusion Defense with existing security programs across the security pipeline, organizations can enhance their overall security posture and effectively eliminate API blind spots. This holistic approach ensures that API security is a top priority throughout the development lifecycle and provides a comprehensive defense against API-based attacks.

By offering a comprehensive API security solution that addresses the unique challenges of API protection, Wib Fusion Platform and Wib Fusion Defense effectively eliminate API blindspots in security programs. With advanced incident detection, complete visibility into API interactions, and seamless integration with existing security tools, organizations can now proactively defend against API logic attacks.

Key features of Wib Fusion Defense:

Incident management and response:

- Incident detection by actor, path, or general target: Identifies security events based on the originating source, specific API endpoint, or broader scope, providing comprehensive coverage.
- Affected assets and business impact assessment: Evaluates the potential ramifications of an incident on critical resources and overall business operations.
- Complete forensics, including incident/event timeline and call activity: Offers in-depth analysis of security events, including a detailed chronology and information about related API calls.
- Immediate response mitigation and recommended blocking rule creation: Provides actionable recommendations to prevent further damage and generates rules to block threats effectively, integrating seamlessly with the organization WAF.
- Incident validation using the comparison to code: Validates that the intended functionality coded by the developer matches the behaviour of the user.
- Blocking performance: Reviews vulnerabilities associated with incidents and assesses the effectiveness of implemented blocking rules.
- B2B detection and API consumer profiling: Discerns the endpoints utilized by applications and those accessed by human users, to better understand API usage patterns and optimize security measures accordingly.
- Fully integrates with the vulnerability detection of the Fusion platform, focusing on weak or vulnerable endpoints to detect possible attack paths: Enhances security by identifying and addressing potential avenues of attack on vulnerable API endpoints.

Vulnerability detection and management:

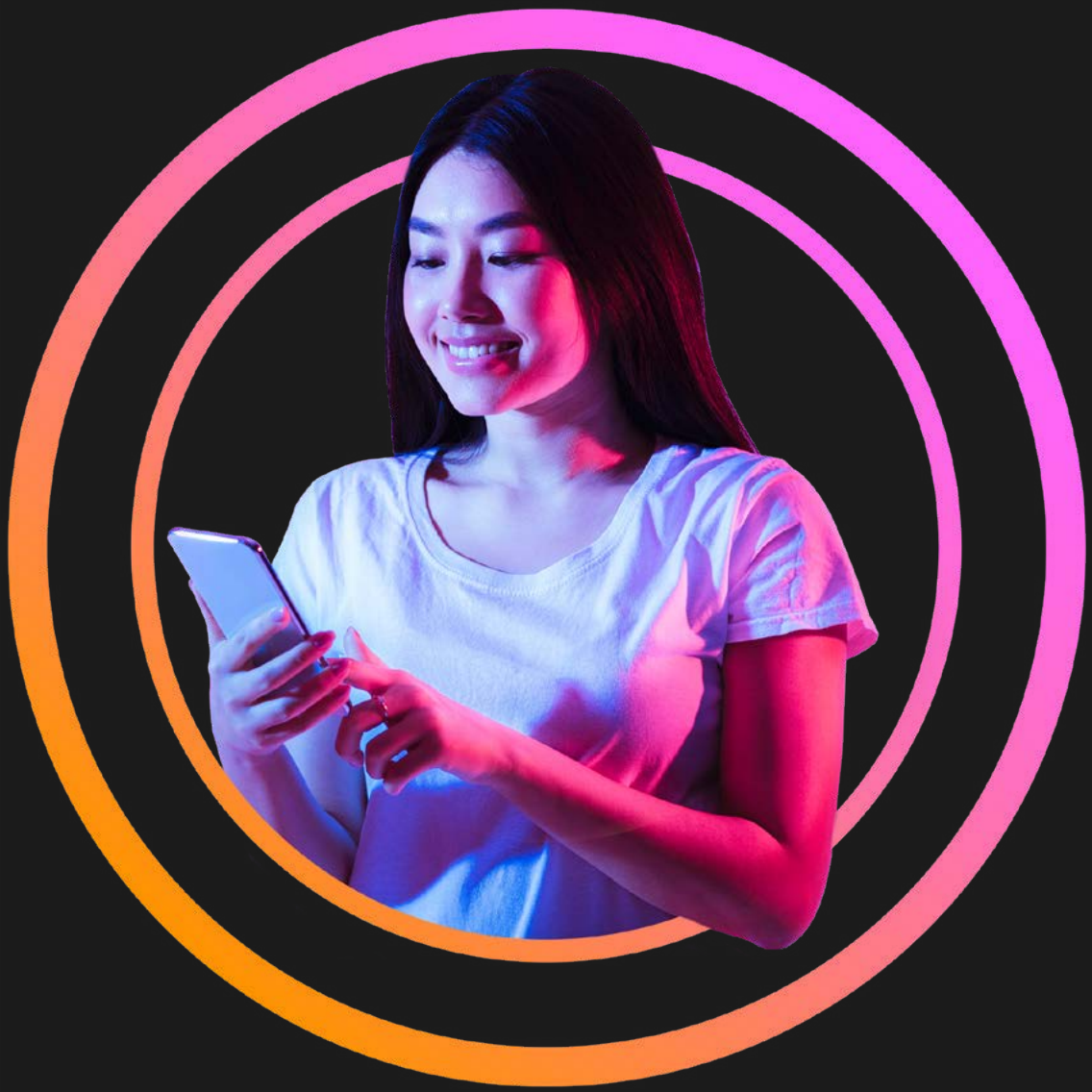
- Detection of OWASP API Security Top 10 vulnerabilities: Identifies and addresses the most critical API security risks, as defined by the OWASP foundation including Broken Object Level Authorization, Broken Authentication and others.
- Detection by path/vulnerability type: Scans APIs code for specific vulnerabilities or paths, allowing for targeted remediation efforts.
- Virtual patching via WAF: Employs web application firewalls to create temporary security fixes while permanent solutions are developed.
- Vulnerability validation using the API testing engine: Confirms the existence of identified vulnerabilities in pre-production or testing environments and ensures accurate remediation measures.
- Related incidents analysis: Examines incidents connected to identified vulnerabilities, providing additional context for response efforts.
- Patching performance assessment: Evaluates the effectiveness of applied patches, ensuring that vulnerabilities are adequately addressed.
- Ticket-based tracking to monitor remediation progress and recovery: Facilitates organized tracking of vulnerability remediation efforts and streamlines communication between teams.
- Validation of implemented fixes using the API testing engine: Verifies that applied patches effectively address vulnerabilities, ensuring long-term security improvements.

In conclusion

The Wib Fusion Platform and Wib Fusion Defense offer organizations a comprehensive solution to eliminate API blind spots and strengthen their overall security posture. By addressing the unique challenges associated with API security, these tools provide a holistic approach that aligns with industry best practices and ensures comprehensive protection against API-based attacks.

Wib Fusion Defense empowers security and development teams by integrating seamlessly with existing security programs across the security pipeline, enhancing the capabilities of various tools and teams. This integration ensures that API security is a top priority throughout the development lifecycle, enabling organizations to proactively defend against API logic attacks and other sophisticated exploits.

In summary, implementing the Wib Fusion Platform and Wib Fusion Defense enables organizations to fill the gaps in their security programs, effectively addressing API-specific threats and vulnerabilities. By adopting this comprehensive and unified approach to API security, organizations can confidently safeguard their valuable resources and reduce the risk of cyberattacks.



wib.com