CybelAngel's API Threat Detection:

Your Definitive Guide

CybelAngel

Introduction by **Camille Charaudeau**

Chief Product Officer at CybelAngel

WHY IS API DISCOVERY SO CRITICAL?

APIs are key to contemporary IT strategies, with businesses across the spectrum leveraging them to integrate systems, collaborate with partners, and develop essential applications. Gartner's research supports this trend, with their 2024 CIO and Technology Executive Survey revealing that **67% of participants intend to increase their investment in API and integration technologies, marking a significant uptick from 2023.**

API discovery is a crucial process in the API lifecycle, and therefore critical to get right. It allows cybersecurity teams to gain full visibility on their API estate by uncovering unmonitored, shadow and vulnerable APIs. It means that your cyber team can stay ahead of the curve when it comes to proactive risk assessment and remediation. It is an important component of a solution employed to defend APIs against threats and vulnerabilities. This is why we have developed an "API Threat Detection" solution to defend against these critical exposures.

Within this ebook, we share why API threat detection should be a part of a robust cybersecurity strategy to safeguard against data exploitation and exposure.

We also review the following critical components of API threat detection within this ebook:

1 What CISOs need to know about APIs and API security

2 API threat detection: preventing data exposure

3 Compliance risks

4 CybelAngel's API Threat Detection

We hope that you will find our definitive guide to API threat detection a helpful and clearcut starting point as it frames a critical part of the success of your organization's API initiatives.

CONTENTS

WHAT CISOs NEED TO KNOW ABOUT APIs AND API SECURITY

API security is all about the measures used to protect APIs and the sensitive data they handle from cyber threats and API attacks.

WHY IS THIS IMPORTANT?

Having the right API protection in place will safeguard your brand and reduce the risk of API security attacks.

WHAT ARE THE SECURITY LAYERS OF API?

Any successful API security framework will cover these four main areas.

Service

Protecting the system from being flooded with traffic

Data

Avoiding any malicious code being injected into the API system

Identity

Ensuring that only the right people can use the API

Access

Being certain that each user only has a certain level of access to the system

With this in mind, let's explore the API security checklist that can help with securing APIs within each of these layers.

WHAT ARE THE FUNDAMENTALS OF API SECURITY?

There are lots of API security best practices, with the OWASP Top 10 API Security Risks being an excellent reference point for cybersecurity teams. The ability to access multiple credentials in an API is known as Broken Object Level Authorization (BOLA), and is ranked number one on the OWASP API Top 10 security risks.

HERE ARE THE FIVE FUNDAMENTALS OF API SECURITY:

1. Authentication mechanisms

This involves verifying the identity of anyone accessing the API. You can do this using a range of authentication methods, such as API keys, OAuth, and JSON Web Tokens (JWT). All of these authentication and validation tools let you restrict who has access to API resources and web services.

2. Access control

By regulating who can get access to the API, and to what extent, you can reduce your API attack surface (aka, the chances of being targeted by cybercriminals). For example, you can make the most of role-based access control (RBAC) or fine-grained access permissions.

3. Encryption

With encrypted data systems, it's much more difficult for hackers and cybercriminals to get access to API services and exploit them. For example, all web APIs should use "transport layer security" (TLS) to encrypt any messages while they're being transmitted.

4. Rate limiting or "throttling"

By controlling the amount of actions and automation that an API can do within a certain space of time, this can reduce the risk of Distributed Denial-of-Service (DDoS) attacks.

5. Regular monitoring

Tools such as web application firewalls (WAFs) can monitor traffic and highlight any anomalies that could indicate an API attack.

HOW DO I KNOW IF AN API IS SECURE?

There are several questions your IT team can ask to identify whether your own API network is safe and secure to use.

- [ ] Do they have strong encryption protocols, such as transport layer security (TLS) in their specification?
- [ ] Do they have secure authentication mechanisms?
- [ ] Do they adhere to well-known security standards, such as mobile API security, OpenID Connect, or OAuth 2.0?
- [ ] Do they run regular security testing and audits?

Before being able to secure your APIs, you need to first get an overview of your API estate. External-facing API discovery solutions are a fundamental piece of the puzzle to get your team's full visibility into all APIs you own and their risk status.

Uncovering all your external-facing APIs and endpoints is the starting point of a successful API Security strategy. It plays a vital role by facilitating smooth integration among systems and services. It empowers developers to easily locate and comprehend existing APIs, while also promoting innovation, collaboration, and the development of robust, interconnected applications.

API THREAT DETECTION: PREVENTING DATA EXPOSURE

API threat detection is a crucial process in the API lifecycle. It allows cybersecurity teams to gain full visibility on an organization's API estate by uncovering unmonitored, shadow and vulnerable APIs. What is more, is that it is an important component for proactive risk assessment and remediation. They are an important component of a solution employed to defend APIs againsts threats and vulnerabilities.

Now, let's explore everything about API threat detection.

WHAT IS API THREAT DETECTION?

It is the process of searching for and finding API resources, and it can refer to the discovery of both internal and external APIs. External facing APIs are particularly at risk as a preferred attack vector for hackers.

It is an essential aspect of application security and development. It empowers organizations to effectively manage their API ecosystem, ensure up-to-date API specifications, and structure APIs for optimal performance. Whether performed manually or automated, API threat detection is instrumental in accelerating development and achieving better outcomes in both internal and external programs.

There are four core reasons why API threat detection is so key for saving internal resources.

1. API threat detection finds rogue and zombie APIs: It helps identify and address rogue and outdated APIs, also known as zombie APIs, that may still be active due to personnel changes or oversight.
2. API threat detection means greater efficiency: API threat detection facilitates project efficiency by allowing teams in different departments to avoid duplicating efforts and reinventing the wheel. This helps large enterprises identify existing internal APIs that could be utilized by multiple teams, streamlining development processes.

3. API threat detection saves technical time and effort: External API discovery offers businesses the opportunity to enhance their website or app functionality with interactive map and route planning features. Instead of developing these functionalities from scratch, businesses can explore existing APIs that provide the desired capabilities. Discovering and utilizing these external APIs can result in significant time and effort savings.

4. API threat detection means costs benefits and savings: Zombie APIs can cut into profits, with the suggested costs of API vulnerabilities in 2022 set at upwards of $75 billion annually.

Let's take a closer look at the different functionalities when it comes to API threat detection tools who have internal and external programs.

API DISCOVERY: INTERNAL V EXTERNAL PROGRAMS

The functionality of API discovery varies slightly depending on the use cases and operational domain. usually split between internal and external programs." to "Solutions that uncover external-facing APIs can also be useful to ensure internal APIs are not misconfigured. Cloud security solutions can also help in monitoring internal APIs and are complementary to API Threat Detection solutions.

Here is what CISOs need to know.

INTERNAL PROGRAMS

In the context of internal programming, API discovery refers to defining innovations and capabilities for applications that grant access to third-party resources. API discovery plays a key role in accelerating app development by providing insights into API utility, predicting the outcome of API usage, reducing the likelihood of API duplication, and understanding the potential for API improvements.

WHY IS THIS RELEVANT FOR CISOS?

In terms of context, when you discuss"internal programs" in relation to API discovery, it refers to efforts within the organization to identify and manage APIs that are used internally. This might include APIs that facilitate communication between internal applications, microservices, or systems. For CISOs, this is critical for several reasons:

Security Posture:
Knowing what APIs exist internally helps in assessing security vulnerabilities or compliance issues.

Risk Management:
Understanding the internal API ecosystem allows for better risk assessment and mitigation strategies, protecting internal systems from potential security breaches or data leaks.

Operational Efficiency:
Proper API management can lead to more seamless integration and interaction between different parts of the organization, improving overall operational efficiency.

EXTERNAL PROGRAMS

In contrast, "external programs" relate to APIs that are exposed to or consumed by external entities, such as third-party developers, partners, or customers. In this instance, API discovery involves identifying the required APIs from a digital pool.

Users can access an API storefront that features multiple APIs and select the ones they need. During this type of discovery, users familiarize themselves with the core values associated with APIs and the necessary procedures to implement them. Popular platforms like GitHub, Postman, Google, and Rapid API, to name a few are commonly used for this type of API discovery.

WHY IS THIS RELEVANT FOR CISOS?

There are three main reasons why.

Security and Compliance:
External APIs present a direct interface with the outside world and are, therefore, a common target for attacks. It's vital to implement robust security measures and ensure regulatory compliance.

Security Posture:
Knowing what APIs exist internally helps in assessing security vulnerabilities or compliance issues.

Public and Partner APIs:
Different strategies may be required to manage APIs designed for public consumption versus those used for specific partners. Identifying and cataloging these helps in applying appropriate security policies and access controls.

Monitoring and Threat Detection:
Being aware of the entire external API portfolio allows for better monitoring of suspicious activity and quicker response to potential threats, safeguarding sensitive data and services.

Next, let's examine the overall importance of API threat detection for the overall tech ecosystem for businesses.

HOW DOES API THREAT DETECTION BENEFIT ORGANIZATIONS?

Until now we've briefly touched on the resources that can be saved when organizations deploy API Threat Detection tools, and for good reason. Gartner predicts that 50% of enterprise APIs will be "unmanaged" by 2025.

It is clear that APIs are vital for any technological architecture of the future. But some organizations continue to not understand how API threat detection can benefit them.

API threat detection serves several roles within an organization.

- **Cyber visibility:** API threat detection plays a crucial role in identifying all APIs being used within an organization, including identifying potential security risks. It optimizes resource allocation to enhance overall efficiency
- **Cost benefits:** API threat detection plays a crucial role in identifying all APIs being used within an organization, including identifying potential security risks. It optimizes resource allocation to enhance overall efficiency
- **Sensitive data:** Within the API ecosystem, API threat detection tools reduce sensitive data exposure concerns for organizations. Particularly when we see the explosive growth in API use, both externally and internally, with it is an ever expanding attack surface. We detail more about this explosive growth in CybelAngel's 2024 annual report.
- **Comprehensive documentation:** Discovered APIs that are thoroughly documented, provide developers with essential information such as functionality, endpoints, authentication requirements, and example responses. Well-documented APIs streamline the development process and ensure ease of use for developers.
- **Improved integration:** API threat detection facilitates seamless integration and smooth operations between various systems and applications by identifying the available Application Programming Interfaces. This enables organizations to leverage existing APIs efficiently and build robust, interconnected systems.

Now let's look at some important differentiators between API classifications.

WHAT ARE THE DIFFERENCES BETWEEN API DISCOVERY AND API MANAGEMENT

The growing complexity of IT infrastructures that companies manage, internal APIs now number in the hundreds or even thousands

According to a recent global survey on APIs in banking, by McKinsey and Company, 81% of participants saw them as a high priority for both business and IT functions. The same

survey found that major banks are dedicating an average of 14% of their IT budget towards API programs, showcasing the industry's recognition of their value.

API management platforms enable organizations to effectively develop, design, monitor, test, secure, and analyze APIs. These platforms offer a robust set of software and processes to make both public and private APIs consumable and scalable.

With full-lifecycle API management, organizations can easily discover and use APIs, control access, analyze usage, and enforce security and governance policies. In essence, API management platforms govern an enterprise's entire API ecosystem, managing the API lifecycle end-to-end.

API discovery is the process of finding internal and external API resources. It plays a crucial role in application security and development, allowing organizations to manage their API ecosystem effectively and ensure up-to-date specifications and optimal performance.

WHY IS API DISCOVERY SO CRITICAL TO OVERALL GOOD API MANAGEMENT?

So, what are the differences between API discovery and API management? This is a great question.

In essence, API discovery is essential for cyber teams whereas API management is more focused on the management of APIs by development teams.

1. **API discovery avoids duplicating functionality:** API discovery plays a vital role in helping developers and cyber teams understand what APIs and avoid duplicating functionality by using already available APIs.

2. **API discovery focuses on finding and cataloging available APIs:** Modern API discovery involves tools and platforms that automatically discover and create API documentation. API management, instead, closely follows the entire lifecycle, including creation, deployment, monitoring, and API documentation.

3 **API discovery plays a vital role in ensuring security and compliance:** By identifying all APIs, teams can ensure that each API meets security requirements for sensitive data. This conceals a massive chunk of your API ecosystem from security controls. API management reviews whether your APIs meet these standards. It also identifies what needs to be improved or fixed.

COMPLIANCE RISKS

In a world where cyberattacks and security threats are all too common, keeping all your systems and sensitive information safe is more important than ever.

For busy CISOs and SOC teams, slipping behind application security and API security best practices is not an option. Attackers are increasingly targeting APIs, exploiting weaknesses to access sensitive data, or to sabotage systems. What is more is that significant compliance risks are linked to API data exposure threats.

Let's examine what this entails for companies in 2024.

API ATTACKS AND REGULATORY ISSUES

The fallout of exposing user and client data is one API attack threat that CISOs lose sleep over. It's vital to implement robust security measures and ensure regulatory compliance.

Excessive data exposure API risk doesn't just affect brands—it can also lead to long-term legislative consequences. Here are some of the main data privacy laws that could be involved.

1. General Data Protection Regulation (GDPR): Known as 'the toughest privacy and security law in the world', the GDPR was created in 2018 for any organization that targets or collects people's data in the EU.

2. Health Insurance Portability and Accountability Act (HIPAA): A US law passed in 1996 intended for healthcare providers and organizations to protect patient data confidentiality.

3. California Consumer Privacy Act (CCPA): A US law passed in 2018 to 'give consumers more control over the personal information that businesses collect about them.'

Laws like these exist to keep people safe and to hold organizations accountable for how they use sensitive information. With the rise of API usage and the digitization of modern society, the risk of private data being leaked is only increasing, making these regulations more relevant than ever.

For example, in the E.U. GDPR compliance directly ties to web application and API security. Under Article 25, data protection must be “by design and default,” requiring data controllers to enforce technical measures that bolster data principles and rights. Ensuring these safeguards are embedded in their processing methods is essential to achieve GDPR compliance.

For brands who are concerned with both the cost and the reputational effects of sensitive data PII leaks, there are regulatory fines also in place.

In 2023, Rousseau, the digital voting platform utilized by Italy’s 5 Star Movement political party, incurred a €50,000 fine due to a lapse in security that left user data exposed to potential breaches.

CYBELANGEL'S API THREAT DETECTION

Regain control over your external-facing APIs with CybelAngel's API Threat Detection solution.

INTERESTED IN A DEMO?

DISCOVER UNKNOWN ENDPOINTS

Gain visibility into your entire API estate to prevent regulatory fines and identify emerging threats from unmonitored APIs with CybelAngel's API Threat Detection solution.

Uncover more relevant results through multiple discovery engines.

Focus scarce resources on critical threats first

Decrease time-to-resolution through pre-built integrations

AUTOMATED 24/7 DISCOVERY

- No manual input needed
- Discover GraphQL & REST API endpoints
- Non-invasive scanning

DETECT API RISKS

- Low false-positive rate
- OWASP Top 10 compatible
- On-demand human analysis

SEAMLESS INTEGRATION

- Dedicated API endpoint
- Connectors and no-code automation

24h

Scan frequency, enabling daily monitoring of exposed APIs.

Low False Positives

Less noise makes for more efficient teams.

<2h

Set-up time. No additional employee resources required.

DISCOVER WHAT CISOS THINK ABOUT CYBELANGEL'S API THREAT DETECTION SOLUTION

"The CybelAngel API Threat Detection solution has been a game-changer for our development and security teams. It's not just about identifying and securing shadow APIs; it is also about streamlining operational efficiency and fostering a culture of proactive security. The ability to monitor 24/7, detect and rectify issues before they escalate has saved us not only substantial financial resources but also time to focus on what really matters."

Thierry Auger
CISO at Lagardère Group

CONCLUSION

One core question remains. Can you mitigate the effects of API threats?

In short, the answer is **yes**.

Dedicating proper attention, resources, and a comprehensive strategy towards safeguarding APIs is essential. CISOs, with the right security measures in place for their organization, can absolutely navigate the myriad of security vulnerabilities that application programming interfaces are susceptible to.

Overall, an effective API security framework not only shields against data intrusions but also ensures adherence to stringent regulatory standards to protect the sensitive data of. The most critical aspect to consider is that API lifecycle solutions, such as CybelAngel's API Threat Detection, are essential for safeguarding your brand's integrity. These tools mitigate security threats and help to bolster the confidence of your customers and partners, who engage with your digital interfaces and apps.

Adding onto this, the dynamic landscape of cyber threats underscores the urgency for businesses to constantly refine and update their API security protocols.
It is clear that to offset cyber risk and cyber attacks a static approach to API security will no longer suffice.

In short, you can counter API threats via these 4 core areas.

- **Proactive identification** of potential vulnerabilities, e.g. sensitive data PII exposure
- **Implementation of cutting-edge security** measures and tools
- **Creating a security-first mindset** culture across your organization and especially for backend teams
- **Evolving your cybersecurity outlook** from a reactive to proactive approach.

At CybelAngel, we pride ourselves on our innovative approach to cybersecurity, and API threat detection.

We work with our clients to shape our technology to address and tackle today and tomorrow's threats.

INTERESTED IN A DEMO?

Scan, Prioritize, Resolve, External Threats

CybelAngel is the world's leading platform for External Attack Surface Management.

Secure your digital activities against cyberattacks and cyber breaches.

Learn more: https://cybelangel.com/
Dive deeper: https://cybelangel.com/blog/

Stay connected

CybelAngel