Build a powerful APIM security strategy with Tyk

Understanding the security threats your APIs face is the first step in safeguarding your organisation against them. APIs are the foundation of modern digital transformation. Still, you need to find the right balance of using them to grow your business while keeping a tight grip on governance and security.

Tyk's API Management platform comes to the rescue by addressing the top challenges from different vantage points to increase your API security. Here are 10 of the top API security threats and how Tyk can mitigate against them:

01. **Broken object-level authorization**
Using object identifiers to retrieve and manipulate data via API endpoints can risk unauthorised access through its lack of client verification.

Tyk Solution
We implement object-level authorization using direct integration and third-party identity providers.

02. **Broken user authentication**
Failure to correctly authenticate users is a threat to API providers and the users whose data lives within it.

Tyk Solution
Our API Gateway supports many authentication methods, from simplistic to advanced.

03. **Excessive data exposure**
When an API returns sensitive data in its response, an attacker will use this data, such as email addresses or other valuable personally identifiable information.

Tyk Solution
Tyk has body transformation plugins which are used to remove sensitive data from the response.

04. **Lack of resources and rate-limiting**
APIs will become overwhelmed if the resources they rely on are consumed to the point that they can no longer operate.

Tyk Solution
Our APIM Gateway is configurable to use multiple plugins to support and manage API traffic through various threats.

05. **Broken function level authorization**
Clients can access functionality beyond their intended access level, such as administrative functions.

Tyk Solution
Tyk's policies and access control plugins grant and deny access to API paths and methods.

Tyk

06. **Mass assignment**

The mass assignment vulnerability is a lack of data input validation which allows attackers to modify data or elevate privileges by manipulating payload data.

Tyk Solution

Payload validation is implemented through JSON schema validation, body transformation, custom plugins and request method transformation.

07. **Security misconfiguration**

Security misconfiguration vulnerabilities cover a range of common security mistakes made when exposing services over the internet.

Tyk Solution

Various Tyk features limit the scope of information returned by an API to ensure the security of published services.

08. **Injection**

An Injection vulnerability is caused by a lack of validating user input, where that input is later used verbatim without any protection mechanisms.

Tyk Solution

Validation of input is achieved with Tyk features such as JSON schema validation, body transformation and custom plugins.

09. **Improper assets management**

A lack of a technical overview of deployed API assets where they are vulnerable to exploits due to stagnation and lack of oversight and ownership.

Tyk Solution

Tyk can play a valuable role in the enforcement of API asset management through versioning, sunsetting, key expiry, Tyk analytics, Tyk pump and secret storage.

10. **Insufficient logging and monitoring**

This is where an organization is blind to current active attacks, previous attacks, and the information needed in the forensics process to determine the attack's impact.

Tyk Solution

Various features of the Tyk platform can enhance data collection.

If you're looking for more on API security - we've got you covered! Check out our dedicated modern APIM security page at tyk.io/c/api-security, where you'll find everything you need to start building your most powerful APIM security strategy today.

Tyk