CEQUENCE SECURITY

Behind the API Sentinel Risk Score

In determining the Risk Score of an API resource, API Sentinel assesses several vulnerability categories and potential security gaps. The score for each category is determined by either the overall score indicated by the type of control in place, such as for the Access Control category, or the sum of points earned for each gap identified for the risk type. A score of 0 is low risk, and a score of 10 is high risk.

The overall Risk Score for the API resource is then determined by the highest score of the three categories. This indicates the level of risk for the "weakest link" in that API's security. For example, if a particular endpoint scored 10 for Access Control, scored 0 for Sensitive Data Exposure, and scored 4 for Schema Non-conformance, then the overall Risk Score for the endpoint would be 10, or high risk.

RISK CATEGORIES & CONTRIBUTING FACTORS	SCORE
Access Control What type of authentication is necessary to access the API?	**10 pts Max Score**
No Auth Detected	10
Basic Auth Detected	7
API Key based Auth Detected (api key used in query parameter)	5
API Key based Auth Detected (api key used in HTTP header)	4
OAuth 2.0/OIDC Auth Detected (access_token in query parameter)	1
OAuth 2.0/OIDC Auth Detected (access_token in header)	0
Sensitive Data Exposure Is there Credit Card Numbers (PCI), Social Security Numbers (PII), or Custom Customer-configured Expressions present?	**10 pts Max Score**
Unencrypted communication (non-TLS)	+2
Sensitive data in cleartext in response headers	+2
Sensitive data in error messages in cleartext	+2
Sensitive data in cleartext in URI	+2
Sensitive data in HTTP Referrer Header	+2
Schema Non-conformance If an API Specification has been added to API Sentinel, are there any ways in which the API does not conform to the specification?	**10 pts Max Score**
Undocumented response codes	+2
Undocumented schemes	+2
Undocumented query parameters	+2
Undocumented endpoint or method	+10
Input or Output not conforming to API definition	+2

100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai