CEQUENCE

Datasheet

API Security Assessment Services

Industry-leading technology and expertise applied where you need it most

APIs Offer Threat Actors a Large and Growing Attack Surface

Digital transformation efforts have driven rapid proliferation of applications and APIs in every organization, leading to a growing and less visible attack surface along with a very real financial dependence on the smooth operation of this infrastructure.

With increasing usage of API-first development methodologies, every organization deals with an ever-growing collection of internal, external, and third-party APIs. Sadly, it is all too common to find that many, if not most of these APIs, are undocumented or unknown to security teams. And unfortunately it is easy for threat actors to discover and target APIs that are unprotected by security infrastructure designed for production applications, like CDNs, WAFs, and API gateways.

Cequence enables organizations to protect their applications and APIs by first discovering and inventorying all APIs. Where needed, OpenAPI specifications can be automatically created, allowing them to then be examined for adherence to internal governance and as well as external compliance requirements. Successful organizations typically implement a pre-production API testing regimen, where it's easier to remediate issues than it would be if they were already in production. Last, examining the traffic going to applications, looking critically at API interactions for signs of malicious activity using machine learning (ML), and using that knowledge to construct appropriate mitigation policies offers valuable protection against attacks.

Key Benefits

- ✓ **Quick, time-bound assessment** of key API security aspects
- ✓ **SaaS-based onboarding** requires no software deployed on customer premises
- ✓ **Executive summary report** generated at the end of each assessment
- ✓ **Visibility and remediation insights** into applications used for assessment service

API Security Assessment Services

Many organizations simply don't have the staffing or expertise to tackle these critical tasks. Cequence offers a complete collection of API Security Assessment Services that enable teams to make fast progress on assessing the current state of their APIs and the applications that depend on them. We provide real-world visibility into the threat actors probing your applications and APIs and their subsequent attacks, responding by creating the rules and polices needed to mitigate them, ultimately giving you an understanding of the elements required for an effective API security program.

Cequence API Security Assessment Services leverage the Cequence Unified API Protection platform to provide an array of valuable offerings, including insight into an organization's API attack surface, how APIs align with internal governance and external compliance, identify where APIs potentially expose sensitive data, and detecting threats and attacks against applications and APIs. These focused assessment services deliver actionable recommendations and include a readout from Cequence threat research experts.

Engagements typically run 2-3 weeks, except for the API Attack Surface Discovery service which runs approximately one week.

API Attack Surface Discovery

- Discovers API attack surface for one selected domain, providing visibility into externally-accessible API hosts, including a breakdown of where APIs are deployed (e.g., cloud IaaS), if and how they are protected (by CDNs, Gateways, WAFs, etc.), and their security dispositions
- Identifies edge, infrastructure, and application providers
- Documents recommendations to mitigate high-risk findings such as weak TLS usage

API Inventory & Risk

- Inventories all your known and unknown, internal, external, and third-party APIs using simple integrations with API gateways, load balancers or internal microservices APIs
- Generates OpenAPI specifications for APIs where none exist
- Analyzes OWASP API Top 10 findings
- Documents recommendations to mitigate high-risk findings

API Sensitive Data Exposure

- Discovers and assesses API vulnerabilities to help ensure compliance with relevant data protection regulations and improve overall API security posture
- Identifies sensitive unencrypted data using ML-based rules with predefined (e.g., credit card and social security numbers) and customizable data patterns
- Documents recommendations to mitigate high-risk data exposure

API Security Testing

- Comprehensive testing is performed to quickly uncover API coding errors and vulnerabilities such as Broken Authentication and Authorization, Insufficient Logging and Monitoring, Insecure Data Exposure, and Broken Object-Level Authorization
- Test plan generation for up to 3 high-value, non-production APIs
- Documents recommendations to mitigate high-risk test failures

API Threat Protection

- Detects and assesses potential threats to your applications and APIs, regardless of existing in-place infrastructure
- Easy, passive deployment doesn't impact existing infrastructure
- Choose up to three hosts to monitor; benefit from threat detection using 200+ out-of-the-box ML models and rules
- Documents threat findings with recommendations for mitigation

Why Choose Cequence?

Complete Unified API Protection platform

The Cequence platform easily integrates with your existing API gateway, CDN, or service mesh, allowing quick passive onboarding of the application being assessed, with no software needing to be deployed on customer premises.

CQ Prime threat research team augments our technology

Cequence not only provides an industry-leading SaaS solution, but is augmented by our CQ Prime threat research team, a dedicated group of highly-skilled security engineers, data scientists, and machine learning experts who actively apply insights gained from attack analysis and threat research into our solutions. This process ensures that the knowledge gained from handling specific incidents benefits all customers across industry verticals.

Advanced use of machine learning powers real-time detection and prevention

Cequence's machine learning models analyze user behavior, heighten attack detection, minimize false positives, generate rules, and suggest policies – all in real time.