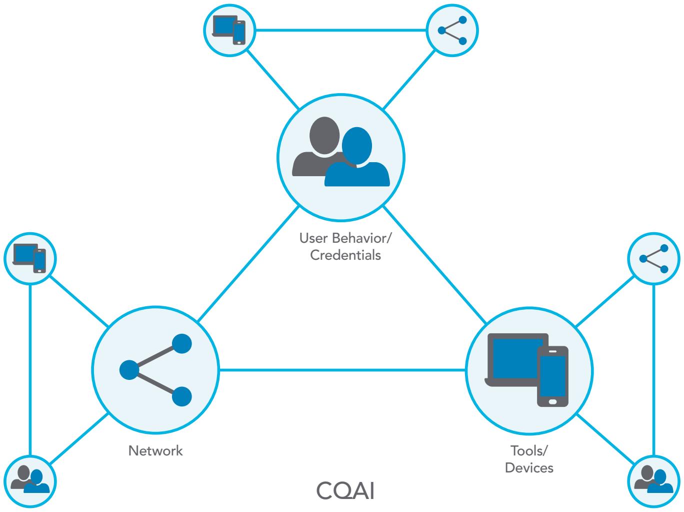
CQAI Tech Brief

Cequence Security takes a platform-based approach to protecting web, mobile and API-based applications from business logic abuse and vulnerabilities that may lead to infrastructure compromise and data loss.

The intelligence of Cequence Application Security Platform lies in CQAI, an analytics engine that uses multiple techniques operating in unison to first understand your applications and then detect attack attributes and characteristics within the transactions. Each incoming web, mobile and API-based application transaction request is fully analyzed across multiple dimensions by CQAI resulting in an indicator of intent and confidence score.



CQAI is extensible, benefitting from threat analysis done by the Cequence Security Team, from in-field intelligence generated by customers and new features added in the form of scheduled updates. The analysis techniques used by CQAI to detect and stop business logic abuse are described below.

Machine Learning

CQAI includes a library of "machine learned" attack models, which can differentiate with very high accuracy, malicious automation requests from legitimate requests. These models are trained and refreshed based on data generated from legitimate browsers and mobile applications, as well as the large library of automation attack tools obtained from the dark web. The behaviors are analyzed on an ever-increasing set of characteristics that include network layer, application layer and user behavior layer characteristics.

Behavioral Heuristics

Behavioral Heuristics are indicators of malicious behavior, based on certain network attributes. In malicious automation attacks, bad actors will frequently change their (fake) identity and mask their location. This means that traditional identification techniques like user ID and IP address are unreliable when measuring velocity. Heuristics will compare normal user behavior like speed, time of day and location of login attempts with common malicious automation characteristics.

As a result, when any malicious automation tool tries to send requests masquerading as a popular web browser or mobile application, the CQAI engine detects them as such with high degree of accuracy.

Network Analytics

Attackers continually attempt to hide their identity and location using common tools such as open proxy servers, compromised home routers from residential ISPs, VPN servers, favorable ISPs, and favorable web hosting providers. This knowledge of open and favorable services is collected from known cyber-crime forums and translated into Network Analytics as a detection mechanism. Network Analytics not only benefits from Cequence Security Research Team contributions, it gains intelligence as CQAI analyzes more and more customer traffic. For example, if customer A, B, and C were targeted with a malicious automation attack using an open proxy X in country Y, customer D and E can benefit from this observation and will treat traffic coming from open proxy X in country Y as suspicious. In order to benefit from the community effect of Network Analytics, customers should opt in the intelligence sharing option from CQ Insight.

Statistical Analytics

Statistical Analytics calculates statistics of different network attributes and their combinations, across a variety of rolling time windows. Statistical Analytics maintains statistics on normal pattern of behavior across a set of network and application layer attributes. If in a given time window, a certain attribute exceeds its normal pattern by a certain factor, it then considers that to be a malicious automated attack. This feature takes into account time of the day usage patterns that are common for most web properties.

Compromised Credentials Checker

There are billions of compromised credentials available from the breaches that happened in the past few years. Attackers use these credentials to test against new sites as people tend to reuse the same username and password across multiple sites. Compromised Credentials Checker does real time validation of login attempts against compromised credential lists.

Fingerprint

CQAI generates a fingerprint for every transaction it sees and, as the most powerful analysis element, the fingerprint is a true differentiator. A fingerprint takes into account the behaviors and the transaction intent, the combines that information with the users, network, organization, and application sources. The result is an in-depth set of data points that are independent of the origin IP addresses and are invaluable in identifying large distributed attacks.

Summary

Cequence Application Security Platform uses a variety of AI-powered analytics techniques to catch malicious automation attacks in real-time, with very high accuracy. It comes pre-packaged with a set of rules, heuristics, and models which are effective from the moment the solution is deployed. Once deployed, the Cequence Application Security Platform observes network traffic and builds further models and heuristics, thereby increasing its efficacy over time. Our customers can customize the platform to solve their specific security problems using the signal and intelligence available at the network layer.