CEQUENCE SECURITY

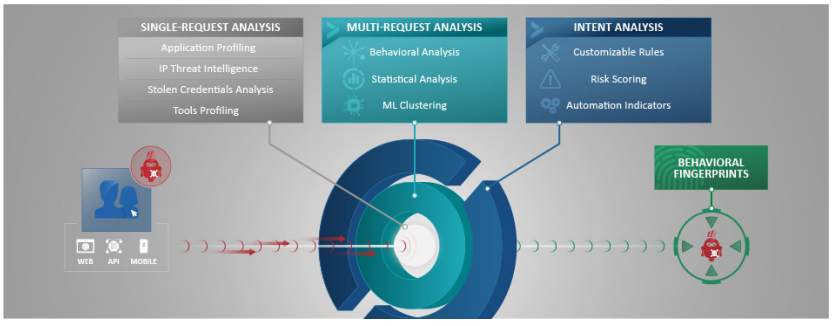
CQAI

AI-Powered Intelligence for Stronger Application Security

Cequence Security takes a platform-based approach to protecting API and web-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, a patented ML-based analytics engine that uses multiple techniques operating in unison to first analyze your applications and then detect attack attributes and characteristics within the respective transactions. Each incoming API and web application transaction request is fully analyzed across multiple dimensions by CQAI resulting in an indicator of intent and confidence score.

CQAI includes a library of Machine Learning-based 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 network, application and user characteristics.

CQAI is extensible, benefitting from threat analysis done by the CQ Prime Threat Research 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.

- **Application Source Profiling:** Automated ML-based profiling of incoming requests to validate that the application sources – the browser or mobile application are genuine. A common attack technique is to spoof or impersonate the browser, user agent or the mobile application itself.

CQAI

ML-based analytics engine that powers the Cequence Application Security Platform. Key benefits include:

- No App Development Impact: CQAI eliminates cumbersome JavaScript and SDK integration and QA efforts, allowing your teams to automatically protect newly deployed and constantly updating applications from automated threats.
- Security Policy Consistency: Agentless approach provides you with the same, consistent telemetry and policy response options for your API and web application traffic, ensuring both APIs and web applications are protected.
- Faster Remediation Through Rich Automation Insights: Integration of rich automation insights with your SIEM and SOC provides your team with up-to-the minute visibility into automation indicators and behavioral insights into bot behavior, reducing investigative efforts and allowing for faster policy enforcement.

- **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.
- **Source IP Reputation Analysis:** 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, commonly referred to as Bulletproof Proxies. This knowledge of open and favorable services is collected from known cyber-crime forums and translated by this detection technique.
- **Source Tools Profiling:** Comparison of attack characteristics with those found in commercially available toolkit configurations. Attackers will create predefined attack configurations to simplify and monetize their attack techniques.
- **Behavioral Fingerprinting:** ML-based behavioral analytics detects evasive techniques often missed by client-based JavaScript and SDK techniques. 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 and tracking their activity.
- **Rule Validation and Risk Scoring:** Risk scoring by analyzing behavioral profiles against more than 150 predefined and custom automation indicators. Findings can be translated into Bot Defense or App Firewall policies.

Summary

CQAI uses a variety of ML-based 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.

© 2021 Cequence Security, Inc. All rights reserved. Part#EN01202-1