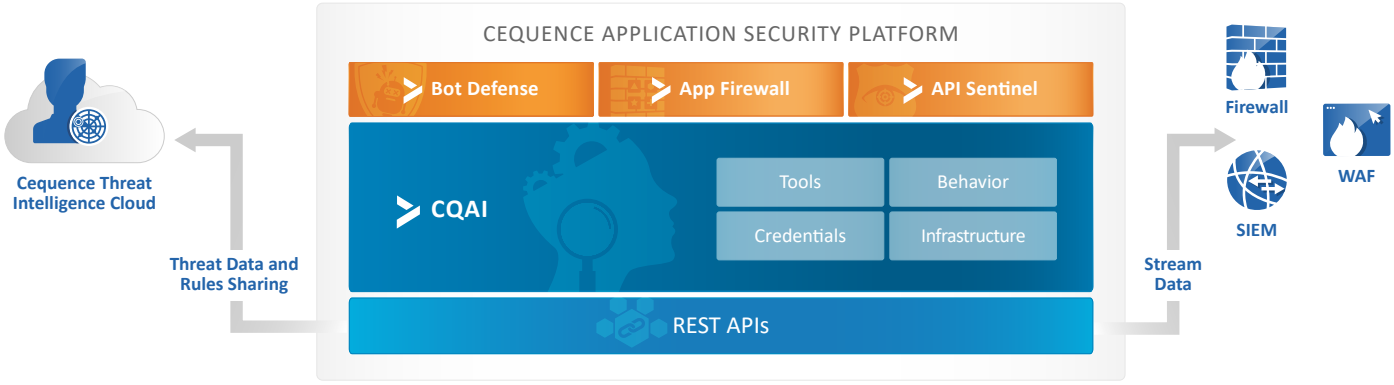
CEQUENCE SECURITY

The Benefits of Threat Intelligence Sharing

Overview

The heart of the Cequence Application Security platform is CQAI, a patented ML-based analytics engine that discovers automated bots targeting your web applications and APIs by evaluating each transaction to determine malicious or legitimate intent.



Therein lies the power of CQAI - its' ability to analyze your transactions in real-time to surface malicious signals that can then be used for mitigation. To amplify the power of CQAI for all customers, the CQAI findings can be sent to the Cequence Threat Intelligence Cloud for analysis by the CQ Prime Threat Research Team.

Threat Intelligence Sharing Benefits

The shared threat intelligence from customers in different industries and locations is collectively analyzed by the CQ Prime Threat Research Team to uncover unique attack patterns, techniques and trends resulting in enhanced rules, ML-models and policies that are pushed back into CQAI for all customers.

The benefit of threat intelligence sharing cannot be understated. Using the patterns and behaviors observed across a range of customers collectively benefits all users in the following ways:

- Exponentially improves the volume of attack indicators that can be used for prevention.
- Increases the cost economics of the attack, making the effort of little or no value.
- Automates prevention efforts to stop attacks in near real time, eliminating human intervention.

When combined with data from other customers, the analysis leads to threat detection and prevention enhancements which are then pushed back into CQAI in the form of an update. To ensure privacy and compliance guidelines are adhered to, customers can configure the threat intelligence data that they want to send to the Cequence Threat Intelligence Cloud for analysis.

Shared Threat Intelligence Examples

The threat intelligence collected by CQAI is based on the Four Pillars of Detection and includes browser behavior, tools in use and assets being targeted or accessed.

Tools

HTTP/SSL Fingerprints

Body/cookie/payload exploration, heuristics

The "code" to execute attack

Credentials

Data breaches

Username and anomaly detection

The account take over targets

Infrastructure

IP addresses, Orgs/ISPs used to anonymize attack

Bulletproof/data center Proxies

Cloud IQ customer attack DB

Behavior

Time of day, spike detection, ML models

Attacker strategies and methodologies

Examples of the threat intelligence that customers can chose to share include:

- **Transaction Metadata:** CQAI looks at transaction details such as geo-location, time, ISP of the originating request, correlating the IP address with the list of compromised IP addresses that form the Bulletproof Proxy Networks commonly used by threat actors to launch automated attacks.
- **Tool Attributes:** CQAI analyzes access patterns and behaviors across all transactions and endpoints. Sharing details of tool attributes that are used provides the CQ Prime Threat Research Team with valuable insight into the continuously evolving attack toolkits.
- **Browser Behavior Analytics:** Modifying the browser attributes is a common technique for threat actors to use as a means of evading mitigation. CQAI analyzes a wide range of attributes including user agent, and browser fingerprint to determine if the browser in use is real, or automated/fake.
- **Targeted and Accessed Assets:** Threat actors will target assets of value hidden behind login or registration applications. CQAI analyses and collects data on the assets targeted and accessed along with the interaction to help determine transactional intent.

Maintaining Data Privacy

The raw data sent to the Cequence Threat Intelligence Cloud is configurable and does not include any PII data, such as credentials, email addresses, and other such information. Moreover, the threat signature:

- Is encrypted in-transit using HTTPs and at rest when stored in the Cequence Threat Intelligence datastore.
- Is only accessible by the CQ Prime Threat Research Team with strict access, authorization and audit controls in place.
- Whenever possible, data is stored within the customer's country of origin, to address data residency requirements.
- The data is shared with a limited set of Cequence employees and is never shared with anyone outside of the company.

Conclusion

The threat intelligence data shared with the CQ Prime Threat Research Team who analyze bot attacks across all of their customers, taking what is learned, sharing it with our customers and using it to improve defenses. The end result is the creation or update of detection and prevention techniques that are delivered to all customers to help ensure they stay ahead of the evolving attack landscape.

CEQUENCE® SECURITY

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