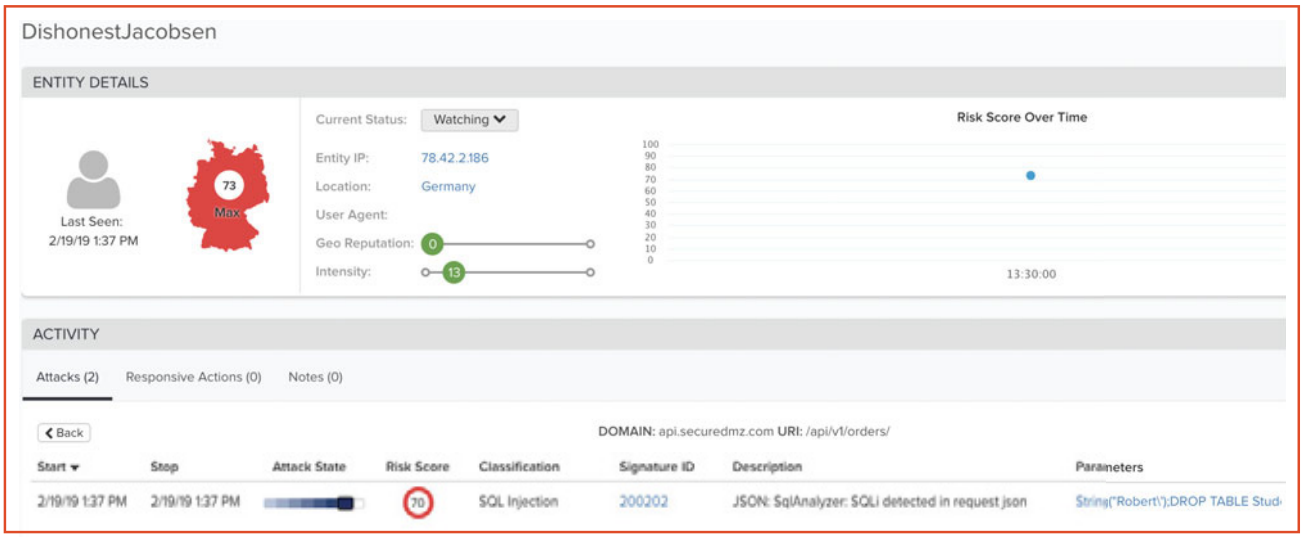
SRC CYBER SOLUTIONS LLP

THREATX

DATA SHEET

ThreatX API Security

APIs are integral pieces of modern applications, providing user-facing functionality, back-end connectivity, and enabling mobile applications. Securing these APIs can be a challenge for traditional security and **Gartner predicts that by 2022, the majority of breaches will occur due to attacks against APIs.** ThreatX brings a comprehensive approach to API security that ensures consistent visibility into all APIs and protection from both traditional and advanced threats.



API attack, as monitored and scored by the ThreatX WAF

API Protection Capabilities

Detection Designed for APIs

ThreatX natively analyzes the most common API protocols and data formats to reveal and block threats in the payloads of API traffic. This ensures that, unlike traditional WAFs, your API traffic gets the same level of protection as your web front-end.

- Native JSON and XML support
- JSON and XML analysis within WebSockets
- API code injection detection
- API Input validation

API Reconnaissance

ThreatX's behavioral analysis reveals a wide range of attacker behaviors early in the kill-chain and without the use of signatures.

- Scanning
- Mapping
- Fuzzing of endpoints
- Method enumeration

Denial-of-Service Protection

ThreatX protects APIs against both traditional DoS attacks as well as Layer 7 DoS attacks that wouldn't be detected based on attack volume alone.

- Block abnormally large requests or responses
- Rate-limiting for high-intensity requests
- Attacks attempting to tie up application resources (e.g queries that result in exceedingly long response times).

Custom API Policies

ThreatX's highly flexible Policy Engine enables teams to tie detection and enforcement policies to the unique needs of the application or business. Examples include:

- Set risk scores on a per-API endpoint basis to closely track sensitive API calls (e.g. 'changeAdminPassword')
- Monitor specific API response messages and codes
- Track requests with malformed IDs, incorrect version use, etc.
- Tarpitting API calls that have a high impact on performance

Geofencing

ThreatX enables policies based on a user's location. Policies can block users or raise their risk score based on the country they are connecting from. This is a standard feature of the ThreatX Platform and can be further customized using the Policy Engine.

API Brute Force

In addition to traditional brute force attacks, ThreatX detects brute force techniques that are unique to APIs, such as brute forcing API keys.

Coverage for Front-End and Back-End APIs

Containerized applications and microservice architectures typically rely heavily on APIs for internal and backend communication. This internal east-west traffic is often unseen by traditional appliance-based WAFs.

ThreatX easily deploys as a Kubernetes sidecar ensuring that security is built-in as modules spin up or down, while also retaining visibility into traffic between modules. Likewise, this internal visibility allows ThreatX's behavioral profiling to extend to internal APIs to reveal signs of abuse or progression of an attack.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

THREATX

SRC CYBER SOLUTIONS LLP