THREATQ™ AND CrowdSec

Supercharging the Rhino with actionable Crowdsourced threat intelligence

Technology Segment: Enrichment and Analysis

CrowdSec data is now available directly in the Threat Quotient platform. Those data are gathered at an unprecedented scale, based on the detections of hundreds of thousands of online workloads hunting unwanted behaviors in their logs. They are highly curated and false positive free, hence can directly be integrated as blocklists into appliances & firewalls.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond to take the right actions faster.

CROWDSEC CTI

CrowdSec's unique Threat Intelligence is a community-driven and adaptive cybersecurity approach that leverages the power of crowdsourcing to identify and mitigate threats in real time. By harnessing collective intelligence from its user community, CrowdSec can effectively recognize new attack patterns, trends, and potential threats, providing a continuously evolving security solution. This collaborative model allows users to share information and expertise, creating a strong and proactive defense network even against the latest threats.

INTEGRATION HIGHLIGHTS

Crowd Sourced

Crowd curated

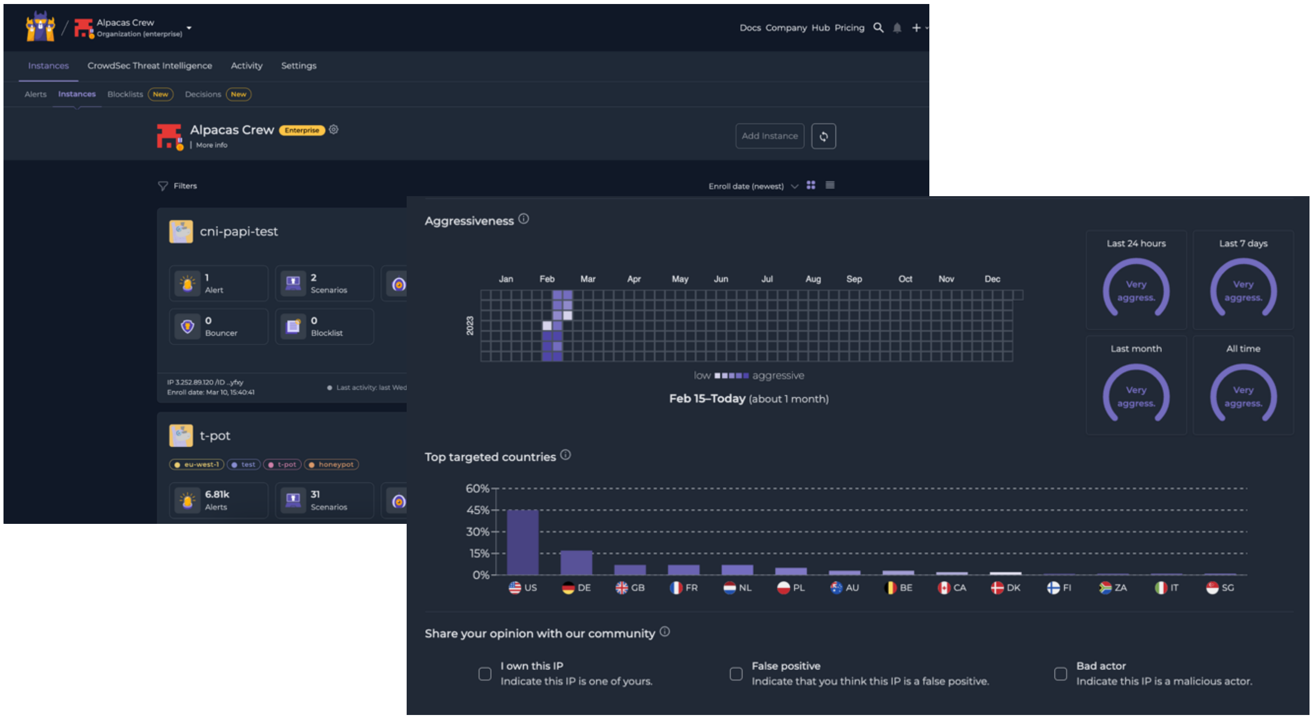
Behavior-based detection

Actionable blocklist

INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- The set FIRE contains around 60K ultra curated, 0 false positive bad IP addresses that can be used as blocklist
- The global set SMOKE contains around 35M IP addresses CrowdSec network identified and can be used for CTI and threat hunting



□ I own this IP
Indicate this IP is one of yours.

□ False positive
Indicate that you think this IP is a false positive.

□ Bad actor
Indicate this IP is a malicious actor.

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents, enables more focused decision-making, and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high-fidelity data. ThreatQuotient's industry-leading data management, orchestration, and automation capabilities support multiple use cases, including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization, and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations in Europe and APAC.

For more information, visit www.threatquotient.com.

ABOUT CROWDSEC

CrowdSec is a dual security engine designed to protect Internet-exposed workloads, whatever their type, task, or OS. It detects IP having bad behaviors in the logs and remedies the threat they pose in the most adapted way, using your existing network components. On top of that, when an IP is flagged, it's shared with CrowdSec network and as long as enough trusted peers keep reporting it, the IP is maintained in our global real-time blocklist. That way, everyone in the network is further protected by this network effect.