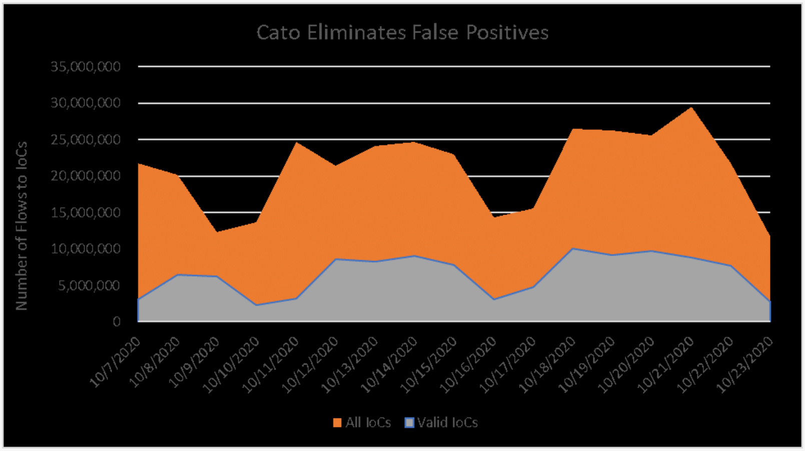
EINPRESSWIRE

CATO AUTOMATES THREAT INTELLIGENCE FEED ASSESSMENT, ELIMINATING FALSE POSITIVES

A three-month study of 400+ Cato customers shows a total of 7 false positives per month. Statistically, most Cato customers never experience a false positive.



By overlaying network information derived by real-time machine-learning models, Cato eliminates false positives in raw threat intelligence feeds leaving a cleaner, more accurate source and up-to-date security protection.

TEL AVIV, ISRAEL, November 3, 2020 /EINPresswire.com/ -- Cato Networks, provider of the world's first SASE platform, announced today the first purpose-built reputation assessment system to combine threat intelligence and real-time network information, practically eliminating the false positive (FP) alerts that have long crippled solutions. The system's unique algorithmic crowdsourcing technology continuously processes millions of reputation records and automatically updates Cato Cloud, delivering enterprises up-to-date protection without any overhead or intervention.

“Security analysts face a daily flood of security alerts most of which are simply irrelevant,” says Elad Menahem, Director of Security at Cato Networks. “These false positives result in alert fatigue that lead security professionals to block access to legitimate business resources or simply disable their defenses, increasing the risk of infection. Using artificial intelligence and machine learning algorithms, Cato's fully automated system solves this problem, allowing them to focus their efforts on stopping genuine threats.”

Machine Learning Models Leverage Deep SASE Context to Isolate False Positives

The lack of visibility into the broader attack landscape has long constrained the industry when identifying new attacks. Security providers only have access to security data, the Indicators of Compromise (IoCs), of threats stopped by their products. Traditional ISPs have network visibility, but they lack security insight. Enterprises remain constrained by both.

Threat intelligence services fill this gap, collecting IoCs of suspected malicious IP addresses,

> “Using artificial intelligence and machine learning algorithms, Cato’s fully automated reputation system eliminates false positives and solves the problem of alert fatigue. ”
>
> *Elad Menahem, Director of Security at Cato Networks*

URLs, and domains from across the Internet. However, the variability in the accuracy of threat intelligence feeds has left enterprises blocking legitimate destinations, interfering with the very business process defended by security systems. As one recent academic paper analyzing threat intelligence feeds concluded, “...[There are] questions on the coverage that services of these vendors actually provide.”(1)

Cato’s reputation assessment system eliminates false positives in threat intelligence feeds by leveraging the convergence of security and networking information in its SASE platform. Cato ingests more than 5 million IoCs from nearly 200 open source and commercial threat intelligence sources. IoCs are then scored, and false positives are identified and eliminated using real-time network intelligence gathered by machine-learning models mining Cato’s comprehensive data warehouse of SASE flow metadata.

More specifically, Cato’s proprietary machine-learning models crowdsource IoC verification by:
- Building a comprehensive reputation profile for each IoC. Cato builds a profile of each IoC from the record’s metadata, such as when the IoC was last reported, the number of user flows destined for this IoC, and the number of threat intelligence feeds reporting the same IoC.
- Predicting false positives. With a profile built for each IoC, Cato’s reputation assessment system simulates hits on the IoCs with the worst reputation, utilizing network traffic from its cloud-based network.
- Automatically removing false positives: Once identified, Cato automatically removes false positives from the security feeds and updates Cato’s global IPS, keeping the customer’s security posture current and free from false positives.

An internal study of more than 400 IPS customers over a three-month period shows a total of 7 false positives per month. Statistically, most Cato customers never experience a false positive.

The Cato reputation system is part of Cato security services and is currently available to all Cato customers. To learn more about Cato IPS and all of Cato’s security services, visit https://www.catonetworks.com/cato-cloud#security-as-a-service.

(1)Bouwman, Xander, et al. “A Different Cup of TI? The Added Value of Commercial Threat Intelligence.” www.usenix.org/system/files/sec20-bouwman.pdf. Accessed 26 Oct. 2020.

Dave Greenfield
Cato Networks
press@catonetworks.com
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/529822711