Easing Threat Intelligence Contextualization with Domain Reputation API

Posted on March 2, 2020

We see about 500 new threats emerge every minute, and most of them come with unique or enhanced techniques. The rise of new technologies and trends in the way we do things, which include the adoption of the bring-your-own-device (BYOD) concept, cloud services, and the ubiquity of Internet of Things (IoT) devices, among others, are also posing more dangers. All these changes have widened the perimeter that businesses need to protect.

In response, a majority of companies have started using threat intelligence to bolster their cybersecurity measures. They believe their threat intelligence investments have generated an estimated $2.26 million in cost savings, higher than the returns they got from investing in other technologies like artificial intelligence (AI) and automation.

That said, we can conclude how beneficial and crucial the need for reliable threat intelligence is. Threat intelligence helps organizations identify and understand threats better and alert them to potential perils or attacks. With it, companies can create tailor-fit security measures and policies.

Perhaps, the only remaining question is how users can maximize the full potential and benefits of threat intelligence?

This post discusses the challenges that come with collecting, analyzing, and using threat intelligence to make the most out of it. We'll also give users an idea as to how they can prioritize threat alerts using Domain Reputation API, which can be a challenge amid the ensuing lack of skilled cybersecurity specialists and budgets.

Too Much Threat Intelligence Can Be a Problem

Organizations know how vital threat intelligence is to maintain a secure network. And so they've made it part of their process to gather threat intelligence from various sources that include:

- **Open source feeds:** These are typically maintained by government institutions (e.g., Department of Homeland Security

, the Federal Bureau of Investigation [FBI], etc.) and nonprofit organizations. They are publicly accessible and free to use.

- **In-house threat intelligence:** This refers to information gathered by a company's internal threat response team or security operations center (SOC). It generally comes from network logs and records of past security incidents.

- **Community feeds** are publicly available feeds that cybersecurity practitioners contribute to regularly. They typically upload malicious file samples and indicators of compromise (IoCs) that peers can use in their investigations. Examples include Virus Total, PhishTank, and Stop Forum Spam.

- **Commercial services** are maintained by cybersecurity companies and thus require payment or subscription to their products.

- **Dark Web forums** are not indexed by Google and other search engines but can provide in-depth information on emerging threats from the attackers themselves. Cybercriminals and threat actors are known to sell their exploit kits, malware creations, and other cybercrime tools on the Dark Web.

With the proliferation of available threat intelligence sources, gathering it is easy. Analyzing it and determining which alerts need to be addressed immediately is a different matter altogether. The process can be cumbersome and unmanageable, especially given the cybersecurity skills gap.

How Screening a Domain's Reputation Can Ease Threat Intelligence Contextualization

When it comes to cybersecurity, time is of the essence. The earlier a threat is discovered, the better. The key to that is a preventive, proactive approach that can be achieved through threat intelligence gathering. Threat intelligence can:

- Allow users to block malicious domains or IP addresses from their networks
- Add context to ongoing investigations or compromise assessments
- Let users compare Domain Name System (DNS) logs with data from malicious domain and malware repositories
- Enable users to hunt for risk indicators proactively
- Arm users with emerging threat trends for their reports to management

However, for threat intelligence to be useful, it requires context so cybersecurity staff can take the necessary action. That context varies from company to company, depending on business requirements and priorities.

To properly secure online assets, an organization needs to deal with the most significant threats first, which can be a nightmare with tons of data to sift through, thus requiring a means to automatically gauge the severity of a threat. One possible way to do that is by integrating a domain reputation API determining the risk score of a domain or an IP address into existing systems and solutions.

The API generates a domain's or an IP address's reputation score based on several parameters, including the site content, connections to other domains, Secure Sockets Layer (SSL) certificate configurations and vulnerabilities, and others. It can help configure a firewall, for instance, to automatically block connections coming from or going to domains or IP addresses that have low scores (an indication of ties to malicious activity). In essence, **Domain Reputation API** can act as a gatekeeper for users.

While it may not be possible for any cybersecurity team to analyze the thousands of newly registered domains on a daily basis, Domain Reputation API can instantly provide insight into any domain's or IP address's reputation. It can help security experts speed up the discovery of ongoing attacks or threats lying hidden within their networks, making threat intelligence not just insightful but, more importantly, actionable.

Want to speed up threat intelligence contextualization with domain intelligence? Contact us at support@whoisxmlapi.com.