The Role of Domain Search and Monitoring in Enabling MDR and MSSP Teams

Posted on October 15, 2019

Based on findings by ESG, more than 80% of cybersecurity professionals today agree that their organizations are seeking to enhance their threat detection and response capabilities. In fact, 77% said their business managers are constantly pressuring them to do so.

The problem, however, is that enhancing threat detection and response is no mean feat. In fact, 76% of those surveyed mentioned that this has become more challenging compared to a couple of years back. Cybersecurity professionals are pointing to concerns such as the surge in the sophistication and volume of threats, a growing attack surface, and increasing workload. Additionally, many firms lack the right skills and staff to make significant changes in this area.

So rather than deploy new tools that they are not even sure to work, many CISOs are now turning their attention toward asking third-party service providers for help. This is where managed detection and response (MDR) and managed security service providers (MSSPs) come in.

But despite their growing demand and popularity, these services face some major challenges that can hinder many providers and have already done so.

In this post, we'll take a look at the hurdles these two are contending with right now and how domain search and monitoring tools can enhance their overall effectiveness.

Let's get started.

Challenges Faced by MDR and MSSPs

As providers of outsourced services, MDR and MSSPs are constantly pressured to provide the best in cybersecurity today. MDR and MSSPs are looked upon for proactive solutions in hunting down threats across an organization's network. This translates into searching for indicators of compromise (IoCs) that can help thwart malicious activity.

Besides that, there is a continuous need to leverage the latest research and threat intelligence as

they are expected to provide their customers with actionable insights into prompt threat identification and response. This is particularly important as analyzing threat data from various endpoints and networks can help paint a clearer picture of an attack.

MDR and MSSPs also have to know where the attacks come from, how infections spread, and if any of their systems have already been affected. And this can only be achieved when a range of data inputs from threat intelligence feeds, detection tools, and third-party data sources are combined.

Lastly, there is also a need for them to have global monitoring capabilities. This is essential as it can help provide specialists with the information they need to anticipate emerging threats.

How Does Domain Search and Monitoring Fit Into All This?

As you can already tell, up-to-date threat data is one of the key elements that both MDR and MSSPs should possess. Relevant search and monitoring capabilities allow users to obtain the latest information available on domains. This is particularly handy since many of the attack campaigns by threat actors begin and end with the use of websites.

With WHOIS data close at hand, these cybersecurity firms can get details such as the name and contact information of a domain registrant, the organization they are linked to, their location, the registrar hosting the domain, and more. All of these key data points add up so that specialists can use them for cybersecurity analysis, threat detection, and research purposes.

Here’s What WhoisXML API’s Service Has to Offer

Our Domain Research Suite can supply users with WHOIS records — including current and historic registrations — for both gTLDs and ccTLDs. Several thousand gTLDs are supported, including .com, .net, .us, .biz, and more including those that have been newly created. This means

that you can keep track of even the more unique extensions like .yoga, .country, and .business. We also offer details on thousands of ccTLDs like .uk, .cn, and .ru so MDR and MSSPs can perform WHOIS searches globally.

Cybersecurity experts can acquire accurate information on more than 300 million active domain names and can expect to get access to hundreds of thousands of additional records on a daily basis. This means that the service is able to track down even those domains that have been recently registered. Doing so can be quite useful in identifying cases of phishing as threat actors commonly employ numerous newly registered domains for this activity.

Apart from that, you can get both parsed and raw WHOIS data from downloads as database dumps, CSV files, or in the form of a variety of APIs. This allows for easy integration with existing systems or other cybersecurity processes as the information provided is all normalized.

By having access to such data, MDR and MSSPs can enrich their existing threat intelligence on domain information with global capabilities. This allows them to give their customers better threat monitoring and response moving forward.

MDR together with MSSPs can avail of a cost-effective means to address cybersecurity threats. With the help of domain research and monitoring, they can better meet their customers' cybersecurity needs.

If you're interested in learning more about what our service has to offer, send us a message at support@whoisxmlapi.com.