Whois XML API Launches Whois App for Splunk

Posted on May 2, 2019

You asked, we delivered!

We are now thrilled to offer our hallmark Whois data in the form of a new app which will be available in Spunk Enterprise's Splunkbase. Now without leaving the Splunk environment security teams can directly access Whois XML API's largest Whois database for proactive threat hunting and cyber crime investigations.

Our new app helps Splunk customers uncover domain profile data for over 5 billion historic Whois records, 300 million domain names and over 2850 gTLDs (including .com, .org, .net, .biz and more) and ccTLDs (including .uk, .us, .ru and more). And not to forget, hundreds and thousands of domains names are being added to our ever growing database each day. The crucial information from Whois records enables cyber security researchers to access key data points for domains including who registered it along with their contact information, the registrar, expiry dates, last update date, who to contact about the domain name & much more.

Key features of WhoisXmlApi's new Splunk app:

- Easily conduct Whois search for domain names or IP addresses
- Access well parsed & normalized Whois data
- Filter data-sets by setting up custom rules and triggers
- Select the time-frame for the data
- Perform instant look-ups

With today's threat landscape, it's critical to quickly identify & respond to threats that continue to increase in complexity & magnitude. Our efforts, in combination with Splunk software, can be leveraged by security teams for identifying malicious entities & help bolster their security intelligence operations.

We'd like to invite you to download our new WhoisXmlApi app for Splunkbase at no additional cost here: https://splunkbase.splunk.com/app/4404

For information on how to configure & use the Whois App check out our tutorial here: https://whoisapi.whoisxmlapi.com/blog/whois-api-splunk-application-tutorial