AKAMAI CASE STUDY

Integration of live streamed DNS query data into Elastic Stack improves security, operations, and business outcomes.

The Canadian Internet Registration Authority (CIRA) is responsible for managing the registry for 2.8 million ".CA" domains. In addition to keeping the DNS safe and reliable, they offer a secondary anycast and recursive firewall DNS service. CIRA uses DNS query data to support Security as a Cloud Service, monitor the cyberthreat landscape in Canada, and enhance ongoing security research.

The Challenge

The operations team at CIRA needed to take advantage of data insights from the infrastructure that supports their D-zone DNS Firewall Security as a Service offering. With more than 100 customers and 500,000 seats covered by the product, massive amounts of data are generated. A policy and data architecture allows the system to scale as service uptake increases. CIRA wanted a way to implement analytics on the data stream so they could make better decisions faster, and make more accurate appraisals of their network and security requirements.

The Solution

Akamai DNSi Big Data Connector (BDC) was used to integrate DNS query data gathered from the Akamai DNSi CacheServe resolvers deployed to support D-Zone Firewall. BDC transforms data gathered from DNSi servers into a JSON format for use by Big Data systems. Data from BDC was integrated with the "Elastic Stack," also known as "ELK," which consists of the Elasticsearch search and analytics engine, a data-collection and log-parsing engine called Logstash, and an analytics and visualization platform called Kibana. Together, these components allowed CIRA to search and display all kinds of DNS and security-related data collected across their network.

The Results

With the integration of Big Data Connector and the Elastic Stack, CIRA can illustrate the value of the DNS layer for cyber-security by understanding and displaying important aspects of the threat landscape. They are able to observe threats seen across Canada, within individual sectors of the economy and within a customer. They can also look for suspicious variations of customer domains used in DNS lookups, such as names with variations like cirä.ca, that use alternative character sets to try and trick users into believing the domain name is legitimate.

CIRA plans to add value to security services they offer by providing additional information such as block data by geography, and new malicious domains observed locally or across the service. Gathering operational data will assist customer support with troubleshooting issues like domains being blocked unexpectedly, or unusually high volume of SERVFAIL queries responses that reflect adverse conditions. Finally, it's their goal to conduct pure data research to illustrate trends and highlight problems for infographics, sales presentations, and conference talks.

Akamai *Experience the Edge*