Processing massive amounts of DNS and security data is simpler and faster with integration of open big data tools

A large service provider in Western Europe offers DNS-based security services across fixed and mobile networks serving millions of consumer and business customers. Their customers and the devices they use are protected from web threats like phishing, bots, and malware without any software installation or administration. This provider monitors the service and gathers large amounts of data so they can understand how the service is performing, and the threats their customers face.

The Challenge

Maintaining the highest level of customer satisfaction is always a priority for the network and security staff. They want to be aware of changes in the threat landscape and provide their customers with useful data and details when they request them. Their DNS-based security solution streams massive amounts of telemetry data 24/7 into log files. However, baseline reporting and extracting customer-specific insights using basic tools like grep was consuming valuable staff hours and wouldn't scale as the need for reporting grew. They wanted a way to maintain customer responsiveness without disrupting essential network operations.

The Solution

Security services implemented by this provider offer web protections for their subscribers, as well as network protections using Akamai's SPS ThreatAvert. The protections work by examining DNS queries received by their Akamai DNSi CacheServe resolvers and matching them against continuously updated threat intelligence. In some cases, the DNS query itself is not sufficient to identify malicious activity – so the resolver will return the IP address of a proxy, which then looks at URLs to determine if the destination is malicious. The provider chose to implement Akamai DNSi Big Data Connector (BDC) to integrate livestreamed data from these systems with Elastic Stack: Elasticsearch, Logstash, and Kibana (ELK). ELK is an economical, open solution that's widely used for processing and visualizing very large data sets. BDC transforms the data into a JSON format that can be used by ELK.

INDUSTRY

Communications Service Providers

SOLUTION

- Akamai SPS ThreatAvert
- Akamai DNSi CacheServe
- Akamai DNSi Big Data Connector

KEY IMPACTS

- Streamlined access to data across systems
- Ability to quickly see and understand threats

The Results

ELK has been implemented to generate reports for business customers and management, as well as for operations and security teams. BDC is the connecting element that enables easy access to the data. As a result, the provider gained the ability to look at the data in any way that they want. For example, they can access traffic for a specific customer that's directed to a proxy so they can better understand which threats a customer is facing. Kibana's simple, powerful interface displays highly informative graphs and charts in minutes, rather than hours. The provider is considering deployment of a role-based authentication system in the future so they can offer customers fully customized, self-service reporting.

Using Akamai solutions, the provider can offer customers detailed insights about threats they are facing.