Exposing Cyberthreats with Predictive Analytics and Machine Learning

> "Implementing Cloudera Enterprise into the ClearSkies platform, we managed to deliver advanced statistical and behavioral analytics along with machine-learning capabilities. These capabilities enable our clients to quickly and effectively identify cyberthreats that otherwise will go undetected."
>
> —Christos Onoufriou, CEO, Odyssey

Overview

Odyssey is a leader in delivering cybersecurity solutions and services in Southeastern Europe and the Middle East, with offices in Cyprus, Greece, Serbia, and the United Arab Emirates.

Odyssey was founded in 2002 to help organizations effectively and efficiently manage their information security risk. The company is ISO 27001 certified, is a Qualified Security Assessor (QSA), and is an Approved Scanning Vendor (ASV) accredited by the Payment Card Industry Security Standards Council (PCI SSC).

ClearSkies SECaaS SIEM platform with Big Data Security Analytics, a homegrown product of Odyssey, is a full-featured, powerful, and flexible next-generation security information and event management (SIEM) solution that addresses the need of organizations of any size and industry to manage the wealth of log data generated by their mission-critical systems, applications, and communication links.

Impact

For Christos Onoufriou, CEO, Odyssey, migrating the ClearSkies platform onto Cloudera Enterprise has expanded the platform's functional capabilities and performance by making possible the delivery of security analytics through the fast, efficient collection of large volumes of heterogeneous data sets. "Cloudera with Apache Hadoop gave us unprecedented scale and analytics," said Onoufriou.

Added Eleftherios Antoniades, Founder and CTO, Odyssey, "It facilitates faster security investigation and remediation, which is pivotal to a next-generation SIEM solution, and improves our ability to detect emerging cyberthreats and trends, such as changes in user behavior."

Indicatively, during the investigation of a client incident, Odyssey rapidly analyzed and correlated, in real time, close to 15 billion log entries, which helped the client uncover an advanced, persistent threat in which confidential company information was being sent outside the network perimeter firewall. "Without Cloudera and Apache Hadoop, this wouldn't be possible," said Antoniades.

Business Drivers

Odyssey was facing collection and processing bottlenecks, limited search capabilities, and constraints in delivering real-time statistical and behavioral analytics because its legacy databases couldn't easily scale to support the increasing amount of log data from client mission-critical systems, applications, and communication links.

"We had billions of log data coming in and we were going to reach a point where we wouldn't be able to actually produce, in a reasonably quick way, the analytics customers wanted," said Onoufriou.

Added Antoniades, "We investigated ways to not only resolve the performance issues, but also to provide more capabilities to our clients. Our vision is to put everything together for our clients, including vulnerability data, threat intelligence, and security analytics."

cloudera®

Key Highlights

Industry

- Cybersecurity solutions and services

Location

- Headquartered in Nicosia, Cyprus

Business Application Supported

- Next-generation SECaaS security information and event management (SIEM) with Big Data Security Analytics

Impact

- Increased visibility into emerging cyberthreats, including zero-day attacks and insider threats
- Provided unprecedented scale and speed
- Enabled delivery of powerful operational analytics

Technologies in Use

- Apache Hadoop Platform: Cloudera Enterprise, Data Hub Edition
- Apache Hadoop Components: Apache Flume, Apache Impala (incubating), Apache Spark, Cloudera Manager, Cloudera Navigator, Cloudera Search, HDFS

Solution

To integrate big data analytics into its ClearSkies platform, Odyssey implemented Apache Hadoop using Cloudera Enterprise. With Cloudera, the company can now collect and combine any volume or type of log data in its original fidelity, and deliver real-time security analytics capabilities, all within a single, enterprise-grade platform.

For example, Odyssey has implemented predictive models that leverage streaming data and data at rest to enhance the detection of cyberthreats, including botnets, malware, and zero-day exploits. In addition, behavioral models help expose abnormal user activity that may be related to potential malicious activity or insider threats.

Through the statistical capabilities of such models, Odyssey's clients can customize the sensitivity of the models based on their operational needs, simply by adjusting a predefined threshold. This is vital in helping reduce the number of false-positive alerts, allowing security analysts to focus their efforts on the investigation of real threats.

"For one business, it may be acceptable to see 1,000 failed authentication requests each hour; however, for another, five failed authentication requests in a minute would be considered a high number," said Antoniades. "Using machine-learning techniques, our predictive models are customized by being trained according to each customer's environment, adjusting on that specific environment's characteristics. This can minimize the number of false positives by 95 percent."

Modernizing the Data Architecture

Using Apache Flume, it is now possible to inject more log data for processing in real time, which helped the company eliminate the processing bottlenecks and data latency issues it previously experienced. Apache Spark delivers the processing performance required to integrate threat intelligence with log data. Apache Impala (incubating) enables the organization to perform daily, hourly, and, even, seconds-based aggregations on log data generated over the course of a year—a critical capability in understanding user behavior and uncovering anomalies. It also accelerated reporting, with reports delivered in seconds instead of hours.

Using Cloudera Search, clients can perform complex search queries across billions of log data in a matter of seconds. "With Cloudera Search, our clients can identify in real time potential threats and attacks," said Onoufriou.

Why Cloudera

Odyssey evaluated several Hadoop vendors before selecting Cloudera.

"We prepared a POV [Proof of Value] document asking vendors to demonstrate their technology and technical skills for helping us in resolving the bottlenecks that we were facing for collecting, processing, and analyzing log data, and sharing with us their knowledge and understanding to support our vision," said Antoniades. "Only Cloudera was able to demonstrate that they had the product, expertise, and knowledge to help us understand how we would be able to overcome the limitations we were facing. Moreover, they shared their knowledge and understanding to support our vision, and, most importantly, they delivered."

He added, "Cloudera also helped us in simplifying the management, administration, and scalability across the Hadoop clusters using Cloudera Manager and Cloudera Navigator."

About Cloudera

Cloudera delivers the modern platform for data management and analytics. The world's leading organizations trust Cloudera to help solve their most challenging business problems with Cloudera Enterprise, the fastest, easiest, and most secure data platform built on Apache Hadoop.

cloudera.com

1-888-789-1488 or 1-650-362-0488

Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA