Cloudera's Cybersecurity Solution in Financial Services

Introduction

The threat of cyberattacks on financial institutions has increased significantly in the past few years. Nine in 10 global cybersecurity and risk experts believe that cyber risk is systemic and that simultaneous attacks on multiple companies are likely in 2017, according to a study by American International Group.

A majority of respondents (85 percent) think that certain industry sectors are more susceptible to systemic attacks than others.

The financial services (19 percent), power/energy (15 percent), telecommunications/utilities (14 percent), health care (13 percent), and information technology sectors (12 percent) ranked as those most likely to be part of a systemic attack in the next twelve months.

Forward-thinking organizations have discovered a community-based approach to fighting cyberattacks leveraging Cloudera's open platform. Cloudera's cybersecurity solution, based on Apache Spot, enables anomaly detection, behavior analytics, and comprehensive access across all enterprise data using an open, scalable platform. Using the diverse open source community to accelerate shared innovations, while changing the economics of cybersecurity, allows organizations to come together to fight back against cyber threats.

Cybersecurity Challenges

As the threat surface expands the increased number of sophisticated attacks continues to expose organizational vulnerabilities. The tools available to security operations centers (SOCs) are not built for the modern adversary operating in the hyper connected world. Challenges range from responding to suspicious activity with limited context, discovering advanced threats buried in billions of events, and understanding the true business risk associated with a user or entity.

Long Investigation & Response Time

Reducing the mean time to incident resolution (MTTR) is a key performance indicator of the efficiency of any SOC and incident response team. Factors pushing the MTTR up can be attributed to the fact that historic data is made unreachable due to archives, necessary data is scattered amongst multiple applications, and important contextual data is not even being collected in the first place. This limited enterprise visibility not only pushes the MTTR up, but also makes it impossible for incident responders to have complete confidence in their classification of suspicious activity.

Detecting Unknown Threats

Traditional cybersecurity applications, like security information event management systems (SIEMs), are notorious for their high false positive rates due to their signature and correlation based techniques (if<A>and<B>then<C>). The detection capabilities are fantastic for known threats, but as the threat landscape gets more complex, hackers find ways around these rules. Even if SOCs want to deploy large scale anomaly detection or behavior analytics via machine learning on enriched data, it's impossible to run these analytics due to the processing limitation of traditional technology.

Understanding the True Business Risk

CISOs have the critical and highly difficult job of balancing risks with the current resource constraints of their enterprise. As the compliance landscape continues to change, and the next major attack always around the corner, security operations centers need to truly understand the risk associated with every user and entity. Understanding this risk to properly invest resources prior and even during an attack will allow enterprises to better mitigate overall cyber risk.

A Modern Cybersecurity Platform for Machine Learning and Advanced Analytics

Today, leading organizations worldwide are adopting Cloudera Enterprise as the data management and analytics platform for storing, managing, processing, and, more importantly, driving analytics for their cyber security needs. Cloudera's cybersecurity solution, based on Apache Spot, empowers security operations centers to reduce the mean time to incident response with complete enterprise visibility, detect advanced threats faster via machine learning, and change the economics of cybersecurity by building on an open source platform.

Working with the Apache Spot community, Cloudera's solution leverages the community driven network, user, and endpoint open data models (ODM). This creates a standard community defined schema for critical security data that is usually siloed across multiple applications. Accessing the open data model provides complete enterprise visibility and enriched data sets for faster investigation and advanced detection. Furthermore, storing the security data in the ODM and on Cloudera's open source platform breaks vendor lock-in by disconnecting the data from the application.

Financial institutions can buy or build applications on top of Cloudera's platform and the ODM to address new use cases while still leveraging the same enriched data set and infrastructure. With multiple Cloudera partners integrating with the ODM, SOCs can now leverage packaged visualizations and machine learning for accelerated detection, investigation, and response. When organizations partner with Cloudera, they get components like Data Science Workbench in order to do advanced threat hunting and model development in Python, R, or Scala. This allows organizations to get additional machine learning value from the Cloudera partnership without having to make additional investments.

Customer Use Cases Examples

Complete Enterprise Visibility

One customer has built a cybersecurity data hub to aggregate various data such as logs, emails, texts, at petabyte scale. This provides a single pane of glass into enriched data for faster incident response and smarter detection models.

Splunk and SIEM Optimization

Optimizing the existing Splunk environment with Cloudera's Cybersecurity solution this customer was able to create an analytical foundation to support current and future needs. By using Cloudera's platform paired with Apache Spot's ODM, the customer was able to reduce their Splunk cost while increasing data and analytic flexibility. They can now execute large scale advanced analytics across multiple years worth of data for advanced threat detection.

Detecting Insider Threats in the Cloud

In order to roll-out a large scale, secure, distributed service, this customer adopted an insider threat solution that uses Cloudera both as its distributed security analytics engine and long term data retention engine. By placing this solution in the AWS cloud, on Cloudera, the customer is able to minimize the implementation timeframe, achieve the desired scale, and use machine learning for insider threat detection.

Conclusion

With Cloudera's cybersecurity solution enterprises don't get a single vendor supporting them, they get an entire community. Experts in the big data, analytics, and cybersecurity community are rallying around the Apache Spot project and open data models to collectively fight back against cyber threats. With multiple SOCs adopting Apache Spot's open data models, enterprise can begin to share machine learning algorithms with one another in order to keep pace with the fast moving hacker community.

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. Our customers can efficiently capture, store, process, and analyze vast amounts of data—empowering them to use advanced analytics to drive business decisions quickly, flexibly, and at lower cost than has been possible before. To ensure our customers are successful, we offer comprehensive support, training, and professional services.
Learn more at cloudera.com.

cloudera.com

1-888-789-1488 or 1-650-362-0488
Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA