

Challenges by Role

- **CISO** – Leveraging big data and advanced analytics to get ahead of threats is impossible with traditional systems.
- **Security Operations** – Operations must constantly offload data as budget constraints and system limits are reached.
- **Incident Responders** – It takes days or weeks to access complementary data they need in order to respond to flagged events.
- **Security Analytics** – Can't perform advanced analytics (e.g. machine learning) against TBs worth of data in short order.

Data Powered Cybersecurity With an Enterprise Data Hub

Cybersecurity has become the topic of conversation for organizations across every industry. With the average breach costing \$200 per lost customer record¹, and even more for lost intellectual property, organizations are looking for new solutions. Forward thinking organizations have discovered a new class of solutions that can detect sophisticated, novel threats designed to look like typical behavior by collecting and analyzing massive volumes of data. These solutions help combat rogue insiders and advanced persistent threats (APT) and have moved enterprise data hubs, powered by Apache Hadoop, to the forefront of the cybersecurity arms race.

Challenges

As attackers have become more sophisticated, attack surfaces have expanded, and the number of attacks increased, organizations find themselves exposed to an onslaught of novel, and previously unseen attacks. Combined with the threat of inside rogue users, it's clear organizations face an enormous challenge.

The tools available to the Security operations center (SOC) are not built for the modern world of always connected mobile computing, and criminal and state sponsored attackers. Indicators of compromise from external attackers and rogue insiders are buried in data streams that are coming off of countless systems and this information is either too large to keep, store and analyze, or not structured in a way that is suitable for traditional systems. The result is the SOC is limited to analyzing subsets of security data to detect only well known exploits using signature matching, correlation and swivel chair analytics

Can't Access Data - With traditional cybersecurity architectures, SOC's are only seeing a small percentage of security data. The reason is that today's data volumes and varieties exceed the limits of current technology. To meet the data volume challenge, security operations limits the data sources used for analytics and then archives this data typically after 60-90 days. In addition to the volume challenge SOC's have no effective means for storing and analyzing unstructured data e.g. emails and text messages, which can contain valuable indicators of potential threats using techniques like sentiment analysis.

Limited Analytics - As criminals leverage more advanced attack techniques, traditional security information and event management (SIEM) systems can't identify the attack because SIEMs are built to detect known threats using signatures and correlation. SOC's need to leverage advanced, behavior driven analytic techniques in order to discover small changes in user and system behaviors, the most reliable early indicators of compromise. This behavior analysis allows for detection of rogue insiders and APT but for this analysis to be effective terabytes of data are required. As a result, employing behavior driven analytics is still a dream for most SOC departments.

Long Time to Mitigation - Incident responders lack the direct access to detailed data needed for efficient event investigation and mitigation. With SIEMs only holding a small time period worth of information, incident responders have to request data from the operations team in order to get the information that they need. This is a back and forth process that takes days or even weeks before the responders eventually get the needed data.

Combating rogue insiders and APT requires a new type of full stack solution that can detect previously unseen attacks while they are unfolding. These challenges represent a massive opportunity for SOC's to augment their existing cybersecurity capabilities and become proactive in the fight against attackers

¹ Ponemon – 2014 Cost of Cyber Crime report

Benefits

Cloudera's enterprise data hub for Cybersecurity is a new solution designed to detect previously unseen threats early in the kill chain, helping organizations avoid financial and reputational damage. Unlike traditional solutions that provide signature and correlation analysis across subsets of security data, EDH for Cybersecurity can ingest, store and analyze any volume of cybersecurity data. This allows for behavior driven analytics that can detect the smallest changes in user or system behavior, traditionally the most reliable indicators of compromise. EDH for Cybersecurity works seamlessly with existing cyber defenses allowing organizations to quickly deploy and improve their security posture with no disruption.

Unify Security Data - Data and event information can only be a strategic asset if accompanied by a system that can store any volume or variety online. When SOCs implement an EDH for Cybersecurity they gain a single, comprehensive repository of security data that allows them to keep information online indefinitely. SOCs gain a single, scalable storage and analytics platform for complete access to endpoint, network, cloud, and user data, in addition to full support for non-traditional sources like email, text, social media, audio and video. With Hadoop acting as the foundational technology, organizations can store this data on an accessible platform at a lower cost per terabyte than traditional systems.

Detect Advanced Persistent Threats - Cloudera's EDH for Cybersecurity powers a new generation of security analytics designed to detect threats based on behavior analysis. These security analytics allow organizations to leverage advanced statistical and machine learning techniques in order to detect rogue actors, perimeter penetration, and advanced persistent threat. By quickly discovering atypical user and system behaviors, security analytics professionals are able to discover previously unknown and novel threats within their environment.

Accelerate Threat Mitigation - Incident responders require a single location to search, access, and visualize vast amounts of endpoint, network, cloud, and user data in order to mitigate flagged events as quickly and effectively as possible. Using EDH for Cybersecurity's search and query capabilities, as well as powerful partner applications for visualization and threat analysis, Cloudera greatly speeds investigation and shortens the time for breach mitigation. This allows responders to immediately access historic and real time data in order to quickly make it through their flagged events.

Conclusion

An enterprise data hub, powered by Apache Hadoop, has shifted the paradigm of cybersecurity data management and threat detection. Utilizing the power of Hadoop, organizations can now store unlimited volumes and varieties of security data, use powerful behavior analytics across terabytes of data to detect rogue insiders and APT, and provide immediate search, query and visualization across all historical data to speed investigation and mitigation. With Cloudera's enterprise data hub for cybersecurity, organization are able to benefit from the power of Hadoop while leveraging Cloudera's enterprise data hub features that are required for production deployments.

About Cloudera

Cloudera is revolutionizing enterprise data management by offering the first unified Platform for Big Data, an enterprise data hub built on Apache Hadoop. Cloudera offers enterprises one place to store, process and analyze all their data, empowering them to extend the value of existing investments while enabling fundamental new ways to derive value from their data. Only Cloudera offers everything needed on a journey to an enterprise data hub, including software for business critical data challenges such as storage, access, management, analysis, security and search. As the leading educator of Hadoop professionals, Cloudera has trained over 40,000 individuals worldwide. Over 1400 partners and a seasoned professional services team help deliver greater time to value. Finally, only Cloudera provides proactive and predictive support to run an enterprise data hub with confidence. Leading organizations in every industry plus top public sector organizations globally run Cloudera in production. www.cloudera.com.

cloudera.com

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

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

© 2015 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice.