CLOUDERA

WHITEPAPER

Cybersecurity requires real time monitoring and long-term analytics

To counter Advance Persistent Threats and other rising cyber perils, government needs a simple, effective solution that marries real-time threat detection with massive data storage, powered by machine learning.

GOVERNMENT DATA IS INCREASINGLY UNDER ATTACK. Adversarial states and state-sponsored actors leverage an ever-expanding range of cyber exploits, with an emphasis on Advance Persistent Threats, to steal sensitive data, conduct covert surveillance, and interrupt vital services.

As government migrates to the cloud, cyber must support a heterogenous infrastructure, with vast volumes of data potentially exposed on both legacy and modernized frameworks. Existing Security Information Events Management (SIEM) applications were not designed with such a hybrid state in mind. They generally cannot support the speed and scalability needed to secure data in the cloud; nor are they able to effectively monitor the growing number of data generators at the edge—the rising tide of IoT.

A new solution is needed, one that marries real-time threat detection with massive data storage, giving analysts a common workbench to simultaneously detect anomalies in real time and also execute long-term analytics, using machine learning and other innovations to leverage historic data for investigation and remediation.

The rising threat

Cyber threats pose a rising national security risk. State and non-state actors view government systems as especially ripe for exploits, targeting state secrets, intellectual property and the vast wealth of personally identifiable citizen data that resides in government hands.

Advance Persistent Threats, or APTs, present an especially high-risk category of cyber incursion. In this prolonged and targeted form of attack, bad actors sniff out vulnerabilities and insert malware that may lie dormant for a long period—hence "persistent." Threat actors may use sophisticated code to remain undetected in the system.

CLOUDERA

WHY CLOUDERA

- **Hybrid and Multi-Cloud** - Run your analytics on the clouds you choose. Easily and securely move data and metadata between on-premises file systems and cloud object stores.
- **Analytics from Edge to AI** - Apply real-time stream processing, data warehousing, data science and iterative machine learning across shared data, securely, at scale on data anywhere
- **Security and Governance** - Use a common security model, role and attribute based access policies and sophisticated schema, lineage and provenance controls on any cloud.
- **100% Open** - Open source, open compute, open storage, open architecture and open clouds. Open for developers, partners, and open for business. No lock-in. Ever.

At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. We deliver the modern platform for machine learning and analytics optimized for the cloud. The world's largest enterprises trust Cloudera to help solve their most challenging business problems.

Learn more at **cloudera.com.**

Government entities that rely on conventional SIEM applications are especially at risk. Resource-constrained agencies typically lack the human capital to tackle the APT threat, and while SIEM is generally adept at real-time threat detection, such systems generally lack the ability to correlate present-day data against historic trends. As traditional SIEM ecosystems struggle to leverage advanced analytics in order to discover such sophisticated threats, government is hard-pressed to identify potential vulnerabilities until it is too late.

Cloudera Cybersecurity Platform (CCP)

Cloudera presents a new way of solving the problem. A suite of high-end capabilities, Cloudera Cybersecurity Platform (CCP) makes available a common workbench where analysts can gain insight into both real-time and historic information, supported by machine learning and artificial intelligence.

As an open source solution, CCP frees government from the fiscal trap of vendor lock-in, while ensuring there are many capable eyes from a range of disciplines reviewing the code. Open source likewise offers a future-proofed solution, one that will continue to evolve as new threats and new defensive stratagems emerge.

CCP's shared workbench recognizes virtually all commonly used cyber machine system source and application protocols. It can ingest telemetry data from a range of sources including both legacy and cloud applications, as well as the growing galaxy of edge data sources. By storing logs over the long term—literally billions of rows of transaction and petabytes of storage—Cloudera is able to leverage machine learning to seek out long-term trends.

The platform shifts cybersecurity from reactive to proactive mode, enabling analysts to better identify potential chinks in the armor before the enemy can exploit those vulnerabilities. This empowers resource-constrained government agencies to make the most effective use of their human capital.

As a common framework underlying the SIEM environment, CCP is able to put big data to work as a critical tool in the cybersecurity arsenal. Long-term analytics in turn enable the system to more readily identify potential anomalies—suspicious instances that might otherwise go undetected.

Seamless transition

Government agencies have invested heavily in a wide array of security solutions, and it makes little financial sense to scrap those in favor of something new. Understandably risk-averse, IT leaders are loath to contemplate a rip-and-replace solution to their cyber woes.

Nor do they need to consider such drastic measures. Cloudera's solution works hand in glove with existing SIEM approaches, giving analysts a common framework supported by big data and key analytic tools. Adoption of CCP is invisible to the end users: All they notice is better, more timely information. The transition to CCP is both seamless and transparent, bringing to bear new tools and new efficiencies without disrupting the existing cyber workflow or introducing new risk.

As an open-source, platform-based solution, CCP solves a number of key problems for federal IT leaders. Unlike conventional SIEM solutions, it delivers the scalability needed to safeguard an ever-widening threat surface, along with the flexibility needed to adapt to the constantly changing landscape of data sources and network connections. Rather than add complexity to an already complex endeavor, the shared workbench approach simplifies the routine work of cyber hygiene, freeing key personnel to devote their attention to higher-level tasks going forward.