INFORMATICA

Data Fusion for Cyber Intelligence

EXECUTIVE BRIEF

"Our Nation's cyber security strategy is twofold: (1) improve our resilience to cyber incidents and (2) reduce the cyber threat. Underlying all of these efforts is the need to acquire the best possible information about the state of our networks and the capabilities and intentions of our cyber adversaries."

– *President Barack Obama, February 13, 2013*

Mapping Cyber Indicators for Data Analysis, Protection, and Sharing

Today, even the most diverse industries are interconnected. This has given rise to a standard of on-demand access to the information contained in historically isolated services, such as banking, healthcare, telecommunications, and utilities. But this convenience has introduced vulnerabilities into our national infrastructure that have the potential to cause irreparable harm. Access that was once achievable only through on-premise systems or in a restricted capacity can now be attained remotely and globally by an advanced persistent threat (APT). This has blurred sovereign borders and enabled asymmetric cyberwarfare between adversaries old and new, including rogue individuals, terrorist cells, and national governments.

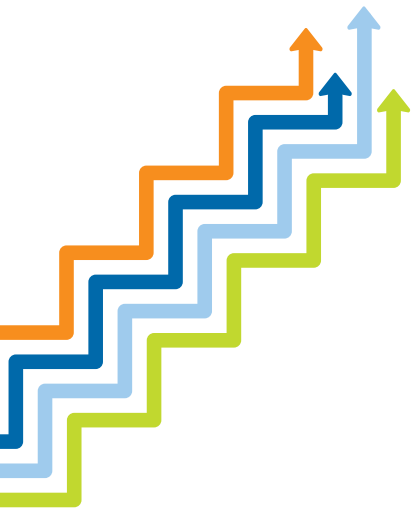
Although it is the responsibility of a country's government to safeguard its citizens from foreign and domestic cyber attacks, vulnerable systems are often not government owned. The onus then falls on computer incident response teams (CIRTs) in both the public and private sectors to protect data and systems while cooperating together to share information about cyber threats. Only then can we detect attack patterns, attribute sources of APTs, and take a truly holistic approach to vulnerability assessment of our nation's critical infrastructure.

The volume, velocity, variety, and complexity of these cyber attacks poses a daunting challenge to information management. As such, analyzing threats can quickly become a big data problem. The Ponemon Institute, a research think tank dedicated to advancing privacy and data protection practices, recently found that 61 percent of companies and government agencies believe that big data analytics are what will most effectively identify patterns and perpetrators, reduce vulnerabilities, and strengthen their organization's overall security posture. According to Dr. Larry Ponemon, chairman and founder of the institute, "While data growth and complexity are explosive factors in cyber defense, new big data tools and data management techniques are emerging that can efficiently handle the volume and complexity of IP network data."[1]

Big Data Provides Cyber Intelligence Insight

Enterprises constantly struggle to protect the integrity and privacy of data threatened by cyber attacks. Fusing intelligence-driven security data from multiple sources and processing it with big data analytics has the potential to solve this problem. But first, analysts need to identify relevant information and recognize its potential relationships to other data points. The sheer volume of data makes it very difficult to detect, analyze, and act on threats from any single source. Big data analytics rises to this challenge and presents an opportunity to garner intelligence collectively from all of the pieces.

This executive brief addresses how enterprise data integration and big data analytics meet the needs of intelligence analysts and computer incident response teams. The Informatica® Platform provides robust capabilities in these areas, supporting three pillars of cyber intelligence: data fusion and analysis; data privacy and security; and data collaboration and sharing. By using the platform to leverage big data analytics, government organizations can dramatically improve their prevention of cyber threats and their ability to respond to them.



[1] Ponemon Institute LLC, Big Data Analytics in Cyber Defense (February 2013).

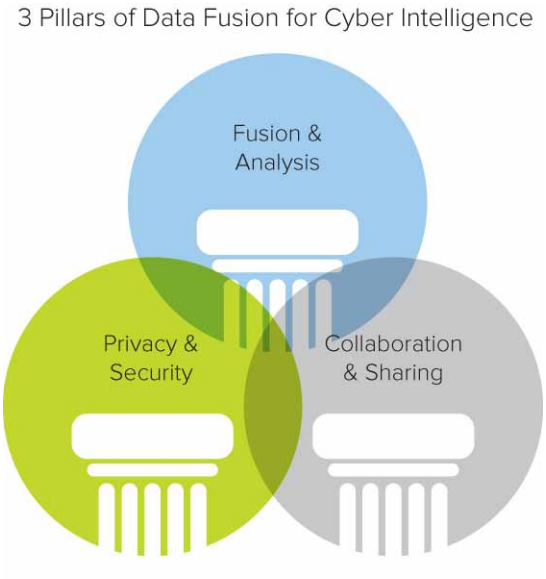
Enhancing an Agency's Cyber Posture with Data Fusion, Security, and Collaboration

Government agencies and private companies continuously face complex and malicious cyber threats. Whether these are threats of one-time infiltrations originating from a single source or of group-based attacks and APTs, organizations face constant pressure to protect themselves and the data for which they're responsible. As a result, they're increasingly looking beyond traditional defense capabilities—not only to stop attacks when they occur but also to gather intelligence to predict, prevent, and defend against these attacks in the future. To do so requires leveraging intelligence-driven methodologies to enhance organizational understanding of events, relationships, methods, perpetrators, and targets.

To master such advanced cyber intelligence capabilities, organizations are turning to big data to reveal previously obscure patterns and trends that can be used to mitigate attacks while securing critical information. A robust approach to ensuring success involves three important areas: fusion and analysis; security and privacy; and collaboration and information sharing.

Fusion and Analysis

Advanced cyber intelligence incorporates a multitude of datatypes and data sources. It includes log and sensor data, gateway activity, network traffic, and other security information and event management (SIEM) data. This data is often collected, stored, and analyzed independently, and its analysis frequently is preserved in unstructured formats such as spreadsheets or text documents in desktop environments. This fragmentation and lack of structure renders much of this data inaccessible to the enterprise. The ability to consolidate, cleanse,



The Informatica Platform supports the three pillars of cyber intelligence: data fusion and analysis; data privacy and security; and data collaboration and sharing. By leveraging big data analytics, government organizations are dramatically improving their prevention of cyber threats and capability of responding to them.

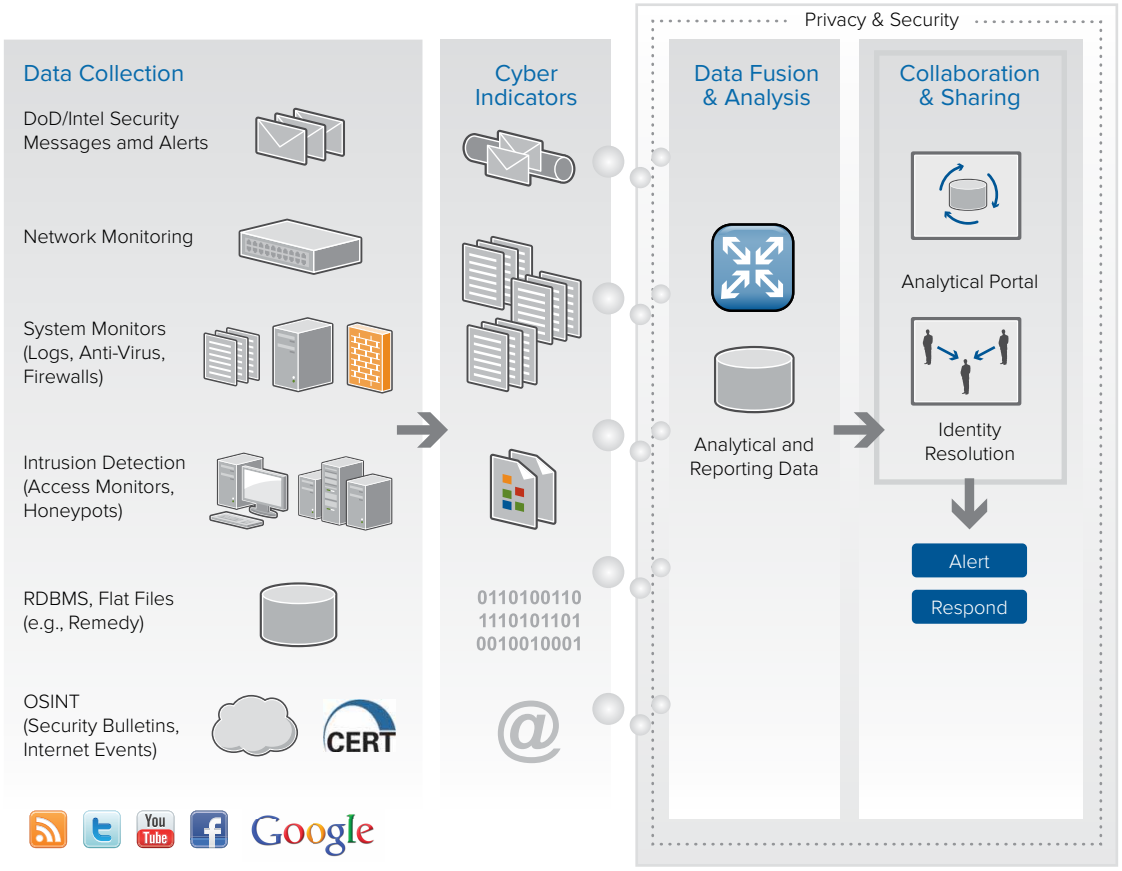
and correlate disparate data into a single operating entity that leverages shared analytical and business intelligence environments is essential to determining relationships and patterns, as well as identifying new tactics, techniques, and procedures (TTP). This type of analysis ultimately enhances an organization's security posture and increases its threat attribution. Fortunately, technology now offers the ability to utilize vast amounts of this new inbound data and augment it with legacy information to attain a deeper understanding of cyber threats.

Security and Privacy

Government agencies are required to maintain the highest standards of data governance and security. Because of this, they struggle to balance the demand for access to vital information with the need to protect it. Whether it be financial data, personal health information (PHI), classified state secrets, or sensitive information about critical infrastructure, network and perimeter security alone are not sufficient as the only line of defense. Data security must be designed with multiple layers of protection and then implemented from the inside out to prevent catastrophic damage from any single point of failure.

Collaboration and Sharing

By leveraging a high-performance, big data analytics platform, organizations can monitor or resolve advanced threats, attacks, and suspicious activities in real time. However, it is only when cyber incidents can be analyzed holistically that we can gain insight into their motives and detect their commonalities, increasing our protection from them. The ability to share threat information in an efficient, effective, and interoperable manner (as with well-known, high-fidelity sharing standards such as MAEC, OVAL, and CybOX) is critical for collaboration to increase the timeliness and quality of analysis.



Gathering, handling, storing, and analyzing cyber threat data is a daunting challenge with new data available every minute, coming from numerous sources, in many formats. Informatica technology facilitates the capture, integration, sharing, and security of this critical data.

Conclusion

Throughout today's landscape of increasingly interconnected industries, vast amounts of cyber indicators are collected continuously from perimeter and network security systems. Technology now offers an unparalleled opportunity to fuse, enhance, and transform this data into valuble and coherent cyber intelligence. Governments investing in software for data enrichment, integration, and analysis are better equipped to discover more threats, gain deeper insight, and reveal relationships in massive data volumes.

The Informatica Platform directly supports the gathering of intelligence by discovering, distilling, and delivering the information needed to detect and prevent new threats. Informatica's core capabilities for integrating, moving, and managing data enable CIRTs, cyber security teams, and organizations in IT, law enforcement, and intelligence to:

- Access and analyze large quantities of cyber indicators across systems, regardless of source or format
- Discover obscure relationships and patterns across threats and attacks
- Extract insights and deliver intelligence in real time within an organization and to external entities
- Increase collaboration by sharing information across portals
- Improve efficiencies in performing data analysis

Fusion and Analysis

- Data integration coordinates both structured and unstructured information managed within the enterprise.
- Data quality cleanses data to ensure that it's trustworthy.
- Complex event processing senses events as they occur and provides alerts in real time.
- Master data management and identity resolution discover potential relationships among people, organizations, events, and transactions.

Privacy and Security

- Persistent data masking securely manages complex, sensitive governmental data for privacy and regulatory compliance.
- Persistent data masking hides or blocks sensitive and confidential information from unauthorized access in both production and nonproduction environments.

Collaboration and Sharing

- B2B data exchange enables the sharing and management of data using any cyber sharing standard.
- Dynamic data masking allows for information to be appropriately secured according to role-based access controls.

With these core capabilities, the Informatica Platform meets the increasing demand by government organizations to gather, fuse, share, and interpret complex data to form meaningful cyber intelligence.

ABOUT INFORMATICA

Informatica Corporation (NASDAQ: INFA) is the world's number one independent provider of data integration software. Organizations around the world rely on Informatica for maximizing return on data to drive their top business imperatives. Worldwide, over 4,630 enterprises depend on Informatica to fully leverage their information assets residing on-premise, in the Cloud and across social networks.

INFORMATICA®

Worldwide Headquarters, 100 Cardinal Way, Redwood City, CA 94063, USA
phone: 650.385.5000 fax: 650.385.5500 toll-free in the US: 1.800.653.3871
informatica.com linkedin.com/company/informatica twitter.com/InformaticaCorp

IN08_0413_02435