New intelligence analytics uncover hidden criminal activity in just seconds

October 28 2014, by Sean Audet

IBM today announced new high-speed analysis and criminal investigation software that is designed to uncover hidden criminal threats buried deep inside massive volumes of disparate corporate data. IBM i2 Enterprise Insight Analysis (EIA) can find non-obvious relationships masked within hundreds of terabytes of data and trillions of objects in just seconds. By fusing together these multiple data sources, organizations can gain complete visibility into threats across the enterprise, giving companies the ability to transform how they protect themselves from increasingly sophisticated attacks.

Organizations across industries face endless threats from cybercrime and other criminals in pursuit of private customer information, employee records, financial data and intellectual property. The Center for Strategic and International Studies (CSIS) estimates that cybercrime costs the global economy $445 billion each year. But companies are overwhelmed with an increasing volume and diversity of data to protect, giving cybercriminals the ability to hide their covert activity for months after an attack. The proliferation of connected devices and machines – from mobile phones to smart cars to remote oil rigs – only compounds the problem by opening new avenues for criminals to penetrate the enterprise.

Operating at high speeds and massive scale, i2 Enterprise Insight Analysis accelerates the data-to-decision process by uncovering new insights into criminal threats against the enterprise that intelligence and security analysts might otherwise not have realized for days, weeks or

months later. EIA analyzes huge amounts of disparate data to discover weak-signal relationships that reveal the true nature and source of an attack. The solution unravels these hidden connections that can be divided by as many as six degrees of separation between disparate sources – from corporate records and social media chatter to data accessed by remote sensors and third-party applications. As developments unfold, EIA provides always-on recommendations that proactively alert analysts to new related abnormalities at the speed of attack.

For example, consider a national retailer that hasn't yet realized hundreds of its customers' credit card account numbers have been stolen and sold on the black market. Any illegal transactions can be easily lost in the noise of typical day-to-day activity – such as a transaction denial, a billing dispute or multiple purchases at the same store. But when connected together, EIA can immediately spot commonalities that reveal the specific store branches that were breached. This insight allows the retailer to take action before millions of accounts are compromised and any significant damage is done.

"Organizations can't afford to take a reactive approach to cyber defense, nor can they do it alone. The speed of threat is too great, and today's attackers are far more technically advanced, proficient and organized than ever," said Maria Vello, President and CEO of The National Cyber-Forensics & Training Alliance (NCFTA), a non-profit role model organization for collaboration, information and resource sharing between public and private organizations in the fight against cybercrime. "Threat analysts and investigators need the ability to look at every possible data set and relationship – no matter how distant or unrelated they may seem – and be able to make key associations and correlations in seconds. The new IBM i2 offering is an impressive tool in its ability to quickly analyze these massive data sets in near real time to paint a complete picture of the threat."

Built on IBM Power Systems, IBM i2 Enterprise Insight Analysis can complement existing security or fraud solutions with additional features, such as:

- Enhanced visualization capabilities: With multi-dimensional visual analytics, investigators can gain a better understanding of an attack by visualizing a comprehensive situational overview of all possible related elements for a more easily digestible viewpoint.
- Open, modular architecture that scales as needs change: IBM i2 Enterprise Insight Analysis is fully customizable with fast integration with third-party applications and features, such as natural language processing and complementary analytics at the tactical, operational and strategic levels.
- Interoperability inside and outside the organization: The open design not only integrates with existing infrastructure and other apps but also allows users to easily share critical threat information across the company and with partners, customers and other organizations.
- Out-of-the-box functionality: Out-of-box functionality reduces the training, maintenance and deployment costs while allowing organizations to quickly begin protecting their infrastructure.

"While most organizations understand how big data can help prevent the ever increasing threat of cybercrime, they are so overwhelmed by massive data volumes that they can't act fast enough to turn it into meaningful intelligence to stop criminals," said Bob Griffin, General Manager, i2, Threat and Counter Fraud, IBM. "With IBM i2 Enterprise Insight Analysis, we've changed the ability of investigators to find that illusive needle in a haystack that helps them detect a cyber attack. This provides any organization with always-on analytics that turns massive amounts of data into real-time insights in a way that simply wasn't possible before."

Provided by IBM