By 2016, 25 Per Cent of Large Global Companies Will Have Adopted Big Data Analytics For At Least One Security or Fraud Detection Use Case

Criminals are rapidly evolving their hacking techniques, and are attacking quickly, making timely security and fraud analytics more critical than ever. Big data analytics give organisations faster access to their own and relevant external information.

In today's blog post, Avivah Litan, vice president and distinguished analyst at Gartner, said organisations can achieve significant savings in time and money when using big data analytics to stop crime and security infractions, by stopping losses and increasing productivity.

Ahead of the Gartner Business Intelligence & Analytics Summit 2014, being held on 10-11 March in London, Gartner predicts that by 2016, 25 per cent of large global companies will have adopted big data analytics for at least one security or fraud detection use case, up from 8 per cent today, and will achieve a positive return on investment within the first six months of implementation.

Ms Litan said:

Big data analytics gives organisations faster access to their own data than ever before. Big data analytics enables organisations to combine and correlate external and internal information to see a bigger picture of threats against them. It is applicable in many security and fraud use cases such as detection of advanced threats, insider threats and account takeover.

Information needed to uncover security events loses value over time, and timely intelligent data analysis is critical as criminals and bad actors move much more quickly to commit their crimes. For example, a year or two ago, hackers would look around, conduct extensive cyberespionage on their targets, and then go in for the theft — whether it was for money or information. Now, hackers — aware of more effective security and fraud prevention measures erected by their target victim organisations — simply go directly to the theft without a drawn-out reconnaissance phase.

To address these issues in the past, organisations relied on various siloed monitoring or detection systems that were optimised for various use cases, such as data loss, financial fraud, or privileged user monitoring.

Now, with big data analytics, organisations can:

- Cut down on the noise and false alerts in existing monitoring systems by enriching them with contextual data and applying smarter analytics. This is especially important as the number of security events increase substantially year over year.

- Correlate the resulting high-priority alerts across monitoring systems to detect patterns of abuse and fraud, and to get the big picture on the security state of the organisation.

- Pool their internal data and relevant external data into one logical place, and look for known patterns of security violations or fraud.

- Profile accounts, users or other entities, and look for anomalous transactions against those profiles.

- Remain agile, and stay ahead of malicious actors and activities, via faster tuning of rules and models tested against data streaming in near real time.

Big data analytics is ahead of most organisations' ability to successfully adopt them, and most vendors have barely begun to prove their software's effectiveness, so it's still early days for this market. Organisations are recommended to start small, but think big, and develop a road map that encompasses multiple use cases and applications across the organisation. The return on investment on big data analytics is typically too big to ignore.

More information is available in the Gartner report "Reality Check on Big Data Analytics for Cybersecurity and Fraud." Additional information on big data analytics will be presented at the Gartner Business Intelligence & Analytics Summit 2014 in Las Vegas, as well as the Gartner Business Intelligence & Information Management Summit 2014, 24-25 February in Sydney, Australia and the Gartner Business Intelligence & Analytics Summit 2014, 10-11 March in London.