The Resource Centre

Express Computer

Date: 01/09/2015 Page No: 22 Location: Main Circulation: 61000

Edition: National

SECURITY ANALYTICS SYMBIOSIS

We live in a complex digital world where the organisations face rapidly changing risk landscape. The exponential growth in the number of sophisticated cyber attacks means that even the best security system can now be breached

BY JASMINE DESAI

The Data Breach Investigations Report (DBIR) 2015 by Verizon shows that in 60% of the cases, attackers manage to compromise the organisation within minutes. As the "detection deficit" is critically high in most organisations, many of the attacks are successful. The growing sophistication of the attacks is now forcing the businesses to deploy security analytics solutions.

According to Ionut Ionescu, Director, Cyber Threat Management, Wipro, security tools can detect only the known vulnerabilities—this is primarily because these tools operate on the basis of what is already known. They can only offer defence against attacks that are similar to the attacks that have occurred in the past. But in case of security analytics, Machine Learning Algorithms are deployed. These Algorithms can detect vulnerabilities and attacks that are mostly unknown.

Sonit Jain, CEO, GajShield, says, "Analytics-driven security enables real-time monitoring of network traffic, it also helps in consolidating and coordinating event data from applications and network logs. This helps enterprises set up intelligent security models rather than just rely on IPs and usernames that often are without any context." He is of the view that security analytics can bring in-depth information to the network flow and security incidents.

Analytics-driven security can give a definite form to the data flowing through the enterprise and by doing that the technology can help in preventing breaches. Context-based deep inspection technologies help identify threat vectors and the type of information, external identity and risk level. All this can help in identifying the source of data breaches and data leaks.

Michael Smith, APJ Security CTO, Akamai Technologies, says, "Most security tools are built around individual log events. What you get out of SIEM, Big Data platforms and related operational processes is the ability to correlate different events into a bigger picture, which I refer to as a meta-event. When you go into a data analytics platform and teach it to recognise the traffic pattern, then you are essentially mining for the information on the attacker."

Elaborating on the issue from the perspective of users, Leela Krishna Munnangi – Head IT, Broadridge Financial Solutions, India, says, "Security analytics offers significant enhancement in security breach detection capabilities. It provides the much needed value add." He is of the view that security analytics has greater accuracy in real-time breach detection (primarily in external malware threats). It can lead to improved TAT on detection and the prioritising of the action plan. It results in low false positives, which is relatively higher in most security intelligence and SIEM systems.

Execution of Security Analytics Framework

The driving of such technologies within the organisations requires a certain roadmap. Avinash Kadam, Advisor – ISACA India Cybersecurity Initiative, says, "Integrating security analytics into governance, risk and compliance (GRC) processes allow security and business teams to build a common language and discussion framework around risk scenarios. When framed in the GRC taxonomy, analytics provides the context, which the businesses can understand and use while making decisions in areas ranging from improving business processes to making necessary security investments. It is this fundamental need to mature from risk identification to risk analysis and, finally to risk intelligence that drives the maturity of security analytics programs."

In the enterprise models, where users access applications, development platforms and network infrastructure as a service over the Internet, a successful deployment can happen only when a holistic view is taken of the existing infrastructure and the needs. All the factors may not be in the direct control of the IT departments, but if anything goes wrong they are expected to fix it. Therefore, it is important that IT and the business work together to establish a process and methodology that orchestrates the adoption of SaaS applications into the enterprise.

> It is this fundamental need to mature from risk identification to risk analysis and, finally to risk intelligence that drives the maturity of security analytics programs

Avinash Kadam
Advisor – ISACA India Cybersecurity Initiative

> Quite a few organisations have invested in security data analytics but they are yet to realise the value of their investment

Michael Smith
APJ Security CTO, Akamai Technologies

> The deployment of security analytics solutions has the effect of moving the security analyst to a forward position in the attack lifecycle

Vivek Chennamaneni
CTO, Netxcell Ltd

> It is important to enhance scope of security analytics to include more data points, which can further improve the accuracy of detecting a breach

Leela Krishna Munnangi
Head IT, Broadridge Financial Solutions, India

According to Ionescu of Wipro shares the details of a case where Wipro has provided security analytics services to a large energy company. He informs that Wipro used Big Data Analytics to perform an off-line analysis of the energy company's access and identity management systems. After the analysis, Wipro identified patterns of behaviour in ICT infrastructure use that necessitated a deeper investigation, which, in turn, yielded some interesting DLP protection use-cases and insights. The client could fine tune their existing security system to ensure that there was overall reduction in the misuse of data or data leakage.

Getting the Best from Security Analytics

The most effective way of getting the best out of security analytics is to fully utilise its capabilities of real time breach detection. Says Munnangi of Broadridge Financial Solutions, India, "It is important to enhance scope of security analytics to include more data points, which can further improve the accuracy of detecting a breach."

Vivek Chennamaneni, CTO, Netxcell Ltd., says, "The deployment of security analytics solutions has the effect of moving the security analyst to a forward position in the attack lifecycle. Proactive analysis becomes part of the security operations. In my view, CIOs should start by focusing on proactive analytics; based on the insights that are gained, they can device a better risk management strategy."

It is also vital that CIOs understand how and where investments can be applied to strengthen security and mitigate risks. Jain of Gajshield says, "CIOs should focus on deploying context-based security. It should be a comprehensive adaptive platform and the organisation should secure business information using risk management with context-based security."

Yuvraj Pradhan, Sales Engineering Manager, India & SAARC, Intel Security, is of the view that it is important to ensure that while the enterprise solution is being deployed, the adaptive platform of security analytics must also be put in place so that the system works well with other business security applications. They should ensure that the security solution has the right tools like analytics, encryption, etc., at each layer of data transfer. This will make it easier for the IT teams to identify attacks and reduce risks.

As enterprises increasingly rely on mobile, internet and the connected ecosystem for productivity and competitive edge, they generate huge volume of complex data. With the right set of security big data analytics, enterprises can take advantage of valuable insights into business risks far beyond the realm of IT.

Smith of Akamai says, "Organisations need to start small, by planning goals that are achievable. Quite a few organisations have invested in security data analytics with big ideas, but they are yet to realise the value of their investment. What they are facing is essentially the classic CIO problem of properly deploying people, processes, and technology. The best strategy is to start mall and then keep adding resources as you learn."

At Akamai, they have a WAF (Web Application Firewall) that is sold as a service. During the last two years, the company created a Big Data solution known as Cloud Security Intelligence (CSI) to consume all the events from the WAF as unstructured data in "attribute:value" pairs. This leads to the ability of analysing 30+ days of events.

Role of CIO

Ajay Dubey, Regional Sales Manager, Websense says, "The scope for CIOs in context of security analytics is broad and it can help them identify information breaches and reduce the impact of cyber attacks. Innovations within security software have automated many of the tasks that are related to detection and blocking. There is better protection from next-generation firewalls and intrusion-prevention systems." He is of the view that the security analytics platforms are most suited for bringing awareness about security events by gathering and conducting analysis. Such solutions can ensure that the events that can be a security threat to the organisation are detected and neutralised with better accuracy.

CIOs have to develop a security program that addresses the organisation's unique security risks and requirements. By developing a unified security analytics framework, the organisations can analyse massive amounts of behavioural data and other indicators to distinguish between malicious and legitimate business activities. Essentially, the security analytics solutions have to generate the ability for correlating the events based on time and user behaviour across networks and devices in the organisation.

Dubey explains the idea by giving the example of the issue being faced by one of Websense's clients. He says, "Recently one of our clients received an infected email from a recognised sender. It later came to light that the sender's email ID had been compromised by a hacker who then used the account to send the email to our customer. When our customer clicked the link that he received in his email, he got redirected to a malicious site from where a zero-day malware got installed into his machine. All this happened while the customer was waiting for some information to download."

"Our customer closed the window but the malware was already installed. Next day when the customer was in his corporate office, the malware encrypted some critical data (like Intellectual property) and tried to send it to someone outside. As the customer was using DLP, this was blocked and our engineers found that there was an infected machine. They immediately swung into action and neutralised the malaware."

Annie Mathew, Director, Alliance and Business Development, BlackBerry, says, "CIOs are responsible for choosing and deploying the security solution, which is most suitable for meeting the needs of the enterprise. During the deployment of enterprise solutions, adaptive platform of security analytics should be put in place so that it works and coordinates well with other business security applications."

Skill-set is another parameter which is tied closely with the success of the solution. According to Sid Deshpande, Principal Research Analyst, Gartner, the CIOs must be aware that the effectiveness of any analytics backed security technology can only be as good as the skill of the analysts or operators who are managing the tool. "The issue of skills is of primary importance in case of security analytics deployment," he says. He is of the view that we can expect better implementation of security analytics by a broad range of enterprises in India when the vendors of such solutions start aligning their solution to the business requirements of their customers.

jasmine.desai@expressindia.com

> The issue of skills is of primary importance for ensuring fruitful security analytics deployment

Sid Deshpande
Principal Research Analyst
Gartner

> While the enterprise solution is being deployed, the adaptive platform of security analytics must also be put in place

Yuvraj Pradhan
Sales Engineering Manager
Intel Security