CYBER SECURITY INSIGHTS · 7 MIN READ

Big Data and Cyber Security Analytics

DAVID WHITE AND ANNIE TU · MARCH 21, 2016

Current state of play

Despite the best efforts of cyber security teams to secure their technology environment, security breaches continue to plague corporations worldwide. In 2015 alone there were at least 79,000 reported security incidents and 2,122 confirmed breaches. The sheer number of attacks is troubling, but what raises greater concerns is that many of the world's largest companies, which support well-funded, sophisticated security teams, were among last year's security breach victims. The traditional paradigm of building walls around our networks in an attempt to keep bad actors completely outside corporate perimeters is no longer a viable tactic. Even the most technically advanced organisations will be – and likely already may have been – breached at some point.

We must accept this new reality and begin to develop our defence models not only to stop hackers from getting in, but to better identify and respond to their malicious activities once they do. Encouragingly, a new generation of tools for cyber security analytics based on big data technology offers expanded help for companies seeking to improve their proactive and reactive cyber-defence capabilities.

The limitations of traditional security approaches

One reason that current approaches to network security often fall short is that they tend to be fundamentally reactive. They focus on stopping known threats based on identifiable fingerprints and catalogued artefacts. Yet minor changes to malware by assailants can often easily make the crumbs of data left behind virtually undetectable. Today's attackers often deploy customised malware whose footprints and payloads are unique enough that even heuristic-based scanners often look right past them.

Traditional security tools are also often deployed in a fragmented and disjointed manner. Firewalls, antivirus and malware scanners, web and mail server gateways, intrusion prevention systems, data loss prevention systems, endpoint scanners, and access control management tools all work in isolation. They were not designed to communicate with one another or to share information with each other. While these tools tend to remain vital to any security arsenal, their piecemeal utility makes it difficult for security teams to develop a clear picture of what is actually transpiring on their network at any given point in time. And when malicious code does slip by, it can possibly remain undetected for months or even years.

Another major drawback of typical current cyber security models is their inability to reconstruct history after an identified security incident. A breach investigation can take weeks or even months to conduct and often concludes with many key facts left unknown. One major constraint is the capture and integration of time sensitive information required for an investigation. When the alarm sounds security incident response teams are forced to scramble trying to build a picture of what transpired using fragments of information from a vast array of diverse sources. Much of this information is ephemeral, and at best may only cover a few days of network history. This may not be enough to understand several months or years of cyber attack activities. This data tends to be siloed in separate specialised systems which can be difficult to link to directly, and sometimes it is not stored at all. Event log files may need to be copied off hundreds of different virtual servers, for instance.

This patchwork of ephemeral data makes the journey from incident alert through the identification of impacted machines, and on to the isolation and elimination of the threat very precarious. It could potentially have a seriously detrimental effect and hamper investigations. The end result is an ever-evolving and changing story that slowly unfolds over time, often troubling company management and shareholders with conflicting reports of findings over time.

How can big data and cyber security analytics help?

Big data cyber security analytics solutions can help companies better manage these issues. Big data technology, from operating systems to analytics and reporting layers, is specifically designed to address the need to rapidly process massive amounts of data from a vast array of sources, very quickly. These platforms are also designed to hold many different forms of data without the need to transform, cleanse, normalise, or validate their content in advance. Users can consolidate all their data feeds onto one platform quickly and proactively, regardless of their size or complexity.

A properly built platform can allow companies to stream all of their network traffic through a cyber security analytics portal in real time, allowing them to shine a light on all network activity, as if they were watching it with a video camera. For added value this data stream can also be combined with other data points such as system logs, VM-to-VM IP traffic, network flow records, user account directories, and the fragmented outputs from traditional security tools. A good deal of third-party information can also be piped in through an on-premises feed or cloud service subscriptions like geolocation services, cyber threat and reputation feeds. Some examples examples include Emerging Threats, Google Safe Browsing, Malware Domain List, SANS Internet Storm Center, SORBS (Spam and Open-Relay Blocking System), VirusTotal, and other spam or IP address blacklists.

Supplementary website intelligence services, such as DomainTools, Robtex, and the global domain registry database, may also be integrated for improved cyber security analytics.

Companies that create a single platform that proactively collects the data required for cyber security analytics and makes it available instantly for real time and historic analysis may improve their cyber security defence and response programs dramatically. This approach can eliminate the time required to rebuild history after a security incident and drastically reduce response and investigation times from months to just days, or even a few hours. Centralising this data also provides teams with a holistic view of each of the various stages in the response life cycle providing a significant edge over their adversaries and allowing for much earlier detection and containment of adverse activities.

Using the cyber-kill chain stages for system assessment

Are big data cyber security analytics right for you? A good place to start to answer this is by using the kill chain framework to benchmark your organization's response procedures and identify weaknesses. First pioneered by defence contractors, the cyber-kill chain is a widely used mapping technique that describes the process an attacker goes through to achieve an objective, whether it is data theft or a disruption of service. Breaking the kill chain at any stage stops the attack. The earlier in the kill chain an incident is detected and contained, the more efficient the defence mechanism is. Leveraging big data for cyber security could potentially result in exponential increases to the availability of and access to information when it is most needed, affording a better chance to respond to threats earlier. A centralized high-speed response platform that is calibrated to these kill chain stages – reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and action – may increase a company's cyber defense effectiveness, making it more likely to detect and block an attack as early as possible (figure 1).

An assessment using this framework considers the types of information available at each stage and ascertains the stage at which your company would typically be able to detect breaches. Consider the reliability of your current cyber-defence tools, catalog the information they provide, and assess how the effort that would be needed to rebuild a complete and accurate picture of actions on your network for the past six to nine months. Then consider how a real-time camera feed with record and playback features for all your network traffic might help address any shortcoming you could identify.

> New generation of #cybersecurity #bigdata analytics can improve your proactive and reactive defence capabilities.
>
> Click to Tweet

One of the greatest benefits of big data architecture is its infinite scalability. This means companies don't need to take a scorched earth approach when building and deploying solutions. They can start small with their most critical gaps, systems, or locations, and grow in scope as returns on investments and value become realised and demonstrable. Just ensure you wrap a data governance program around these and any other big data program you deploy, else you may be creating more security, privacy, and data retention problems than you are solving.

Disclaimer

The opinions expressed are those of the author and do not necessarily reflect the views of AlixPartners, LLP, its affiliates, or any of its or their respective professionals or clients.

This article is the property of AlixPartners, and neither the article nor any of its contents may be copied, used, or distributed to any third party without the prior written consent of AlixPartners.

This article regarding Big Data and Cyber Security Analytics ("Article") was prepared by AlixPartners, LLP ("AlixPartners") for general information and distribution on a strictly confidential and non-reliance basis. No one in possession of this Article may rely on any portion of this Article. This Article may be based, in whole or in part, on projections or forecasts of future events. A forecast, by its nature, is speculative and includes estimates and assumptions which may prove to be wrong. Actual results may, and frequently do, differ from those projected or forecast. The information in this Article reflects conditions and our views as of this date, all of which are subject to change. We undertake no obligation to update or provide any revisions to the Article.

TAGS #BIG DATA #DATA BREACH RESPONSE

CLOSE

David White

Director at AlixPartners

David White specialises in information lifecycle governance with a particular focus on data security, privacy, analytics, and regulatory compliance. He is a former AmlLaw100 Attorney and has more than 20 years of experience assisting companies in complex regulatory compliance and investigations, including electronic discovery, compliance audits, data breaches, and forensic investigations.

in

CLOSE

Annie Tu

Vice President at AlixPartners

Annie Tu is a bilingual industry recognised cyber security mentor with over 10 years' experience covering cyber incident response, forensic investigations, eDiscovery, FCPA review and business consulting. Annie has managed and coordinated numerous international projects involving multiple territories in Asia Pacific and Europe. Having resided and worked in the UK, Hong Kong and mainland China, Annie has a unique insight into the challenges faced by businesses with diverse cultures. She is a SANS GIAC Certified Forensic Analyst (Silver), an Encase Certified Examiner, a Certified Ethical Hacker and a SANs mentor for the forensic course "Advanced Computer Forensics and Incident Response".

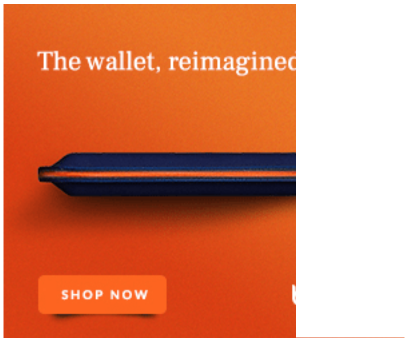
LATEST

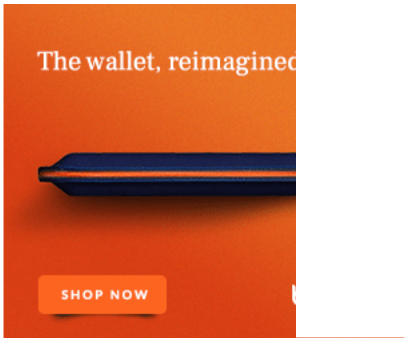
GriftHorse Android Malware Present in 200 Scam Apps Affects 10 Million Devices Stealing Hundreds of Millions

Twitch Data Breach Exposes “Everything”: Source Code, Confidential Company Information and User Payouts, CLOSE r Promises More Is on the Way

Privacy Principles for Implementing Digital Contact Tracing

Ransomware Attack on Springhill Medical Center Leads to a Negligent Homicide Investigation After a Baby Dies





STAY UPDATED

Get notified of new articles and relevant events.

Type your email

□ I agree to the privacy policy

SUBMIT

LEARN MORE

About
Contact
Our Advertising
Privacy Policy
Cookie Policy
Terms of Use
Do Not Sell My Data

News, insights and resources for data protection, privacy and cyber security professionals.

STAY UPDATED

Get notified of new articles and relevant events.

Type your email

□ I agree to the privacy policy

SUBMIT

FOLLOW US

CLOSE