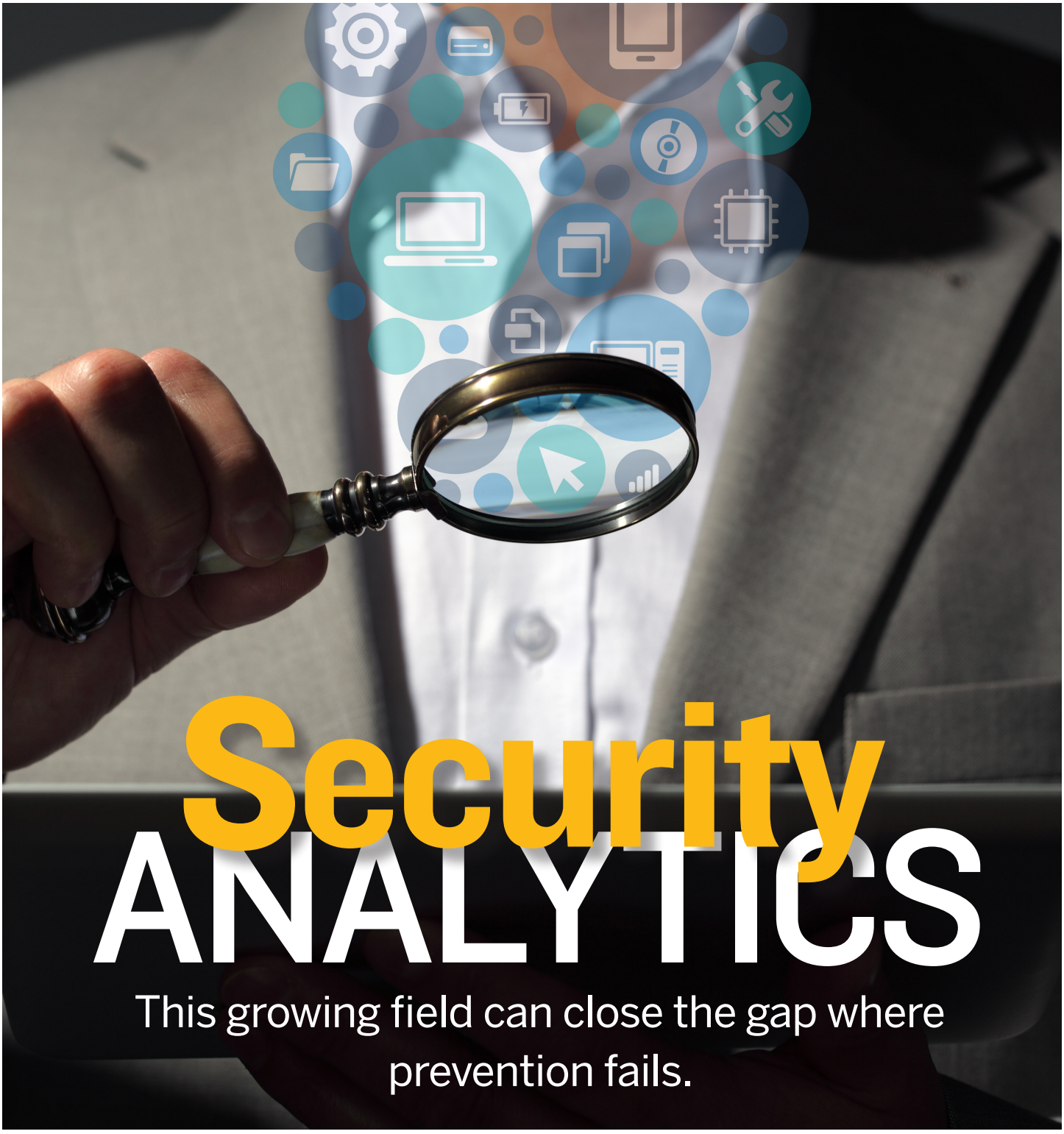

Security ANALYTICS

This growing field can close the gap where prevention fails.

ebook

An SC Magazine publication

Sponsored by

LogRhythm®

The Security Intelligence Company

Analyzing analytics

Security analytics has gone from buzzword to obligatory application in a very short time. Esther Shein investigates.

Since the dawn of the computer industry, jargon has been a key sales driver. Whether it was speeds and feeds or some obscure secret-sauce feature, jargon has been the white sugar that feeds tech. In today's enterprise, security analytics are an integral part of that sweet tooth – but perhaps this time there is more meat than just empty technobabble calories.

Security services are an integral part of the offerings at BT Group, a multinational telecommunications company based in London, where executives have long been aware that "the range and complexity of security-related data is considerable, and continues to grow at a dramatic rate," says Oliver Newbury, chief technology officer for BT Security.

As a result, a core part of BT's strategy has become "the ability to automate key security controls and provide appropriate analytics," he says. Several years ago, BT began working with a security tools vendor whose tools are designed to give the corporate data security team access to modeling, attack simulation and advanced analytics.

The idea behind security analytics is to enable security teams to extract relevant and actionable intelligence from their data to gain visibility and context-aware intelligence of their entire attack surface – physical, virtual and in the cloud.

The function of security analytics is at its best when provided with contextually rich data relating to the business assets and people, allowing more accurate conclusions to be reached regarding the risk of any observed activity, explains Newbury. "Enriched security event data can be analyzed both by analytic software and human analysts to identify a wider range of threats with improved levels of confidence than raw event data by itself."

BT is far from alone when it comes to a desire for greater insights and visibility into the activities inside an organization's network that might indicate breaches have occurred. Security experts say they are seeing organizations falling behind daily in addressing their critical alerts, so they need a capability to identify where the true severities are.

That's where security analytics comes in. The software uses advanced analysis algorithms, including machine learning, to "close the gap where prevention fails," and provide that visibility in order to accelerate incident response, according to David Monahan, research director of security and risk management at Enterprise Management Associates, a market research and consulting firm based in Boulder, Colo.

When effectively deployed, security analytics software prompts an early warning to stop lateral movement of a threat and prevent data exfiltration, he says. You can think of security analytics as looking for threats in the proverbial haystack *of* needles – it will help determine "which is the worst one that's going to poke you first," he says.

This is critical for businesses with limited IT and security resources even as the

OUR EXPERTS: Analytics

Eric Ahlm, research director, Gartner
David Monahan, research director, Enterprise Management Associates
Oliver Newbury, CTO, BT Security
Angela Orebaugh, assistant professor and director of cybersecurity and IT programs, School of Continuing and Professional Studies, University of Virginia
John Pescatore, director of emerging security trends, SANS Institute

99%

Percentage of breaches that led to compromises within days or less

– RSA

infrastructure becomes more complex and threats more sophisticated and organized. Couple that with a changing technology landscape that now includes more Internet of Things (IoT) and bring-your-own-device (BYOD) policies in corporate environments, along with traditional networks and perimeter security transitioning to cloud and virtualization environments and, some observers say, security gatekeepers are losing direct control over their own IT environments.

"Security analytics are helping companies prepare for and respond to attacks that aren't detected by typical IT security infrastructure," says Angela Orebaugh, an assistant professor and director of cybersecurity and IT programs at the University of Virginia's School of Continuing and Professional Studies. These include low-and-slow attacks that fly below the radar and advanced persistent threats (APTs),

> "Security analytics are helping companies prepare for and respond to attacks that aren't detected by typical IT security infrastructure."
>
> *– Angela Orebaugh, University of Virginia*

she says. For example, companies are using security analytics to perform threat detection, attacker profiling and digital forensics.

The goal of security analytics platforms is to bring "situational awareness to security events by gathering and analyzing a broader set of data," so that the events that pose the greatest harm are found and prioritized by IT with greater accuracy, says Eric Ahlm, a research director at Gartner.

That broader set of data can include sandbox execution of code, packet stream and protocol interrogation, content interrogation and activity anomaly detection, according to the 2015 EMA report "Data-Driven Security Reloaded." The software might also take in data from other log sources and interface with other monitoring and alerting systems, like security incident and event management (SIEM) systems. This produces "the highest level of visibility possible into activities in the environment and produces the highest fidelity intelligence for rendering the context of an event, thus providing as few false positives as possible," the EMA report states.

Another significant driver for security analytics, according to recent research conducted by Monahan, is that 80 percent of organizations he surveyed that are receiving more than 500 critical/severe alerts per day don't have the analysis capabilities to prioritize them. Additionally, 88 percent of organizations indicated they are able to investigate less than 25 critical/severe alerts per day.

"This means that 44 percent of organizations have a daily surplus of severe/critical alerts to investigate and are therefore perpetually behind," Monahan says. "This extends attacker dwell time, increases potential for losses and increases cleanup costs. As the number of severe alerts grows, this percentage grows as well." Sixty percent of the organizations that generate over 500 critical/severe alerts are in the same daily deficit situation, he adds.

Ahlm refers to the use of security analytics platforms as "adversary hunting using analytics" and says the impetus for them is data overload, alert overload and a shortage of people to deal with events. Echoing Monahan, he says, "There's too much security data and the value of that data has been diminished with false positives and, simply, event overload."

Enterprises turn to security analytics to find the most persistent adversaries in their environment that have been missed, he adds. The biggest trigger is when a company realizes it has been breached and had no advanced warning, he says, "so visibility or the means to detect [a breach] is huge."

The personnel shortage too is a big

#1

Mobile devices are the top security risk in enterprises

– LogRhythm 2016 Cyberthreat Defense Report

challenge, especially when it comes to investigating attacks. "This is a real problem when I talk to buyers, especially when they get into investigations," says Ahlm. "There's not enough people to go around [and] they are hard to find and expensive."

Gartner classifies security analytics into submarkets. These include user behavior entity analytics (UBEA), which is also sometimes referred to as user behavior analytics (UBA); endpoint detect and respond, which monitors abnormal behaviors on a user's computer; and network traffic analytics, which addresses patterns of communications. There is a lot of crossover among them, Ahlm notes.

Oliver Newbury, CTO, BT Security

These submarkets have evolved "because of their ability to find the unknown," says Monahan. "SIEM might give you the severity or critical alerts, but you don't know which is the worst and you can't focus on all of those in a day."

As a result, one interesting trend is that some SIEM vendors are adapting their products to meet the market need for better analytics with Big Data engines, says Monahan. "Security analytics will mine all the data in a SIEM repository and as it identifies issues, like an event or ticket that exists, it will inject more information," as opposed to just gathering data. "SIEM is not gaining more market share, they've capped out," he maintains. So vendors are "either creating new capabilities around machine learning and analytics or making acquisitions to get into that space and enhance their [product's] capability."

When threats are internal

BT serves approximately 1,000 major global multinational and public sector organizations in more than 180 countries around the world. Newbury says it focuses on all aspects of security analytics, although its key offerings are centered on network traffic and the movement of information in and out of networks. The company also uses identity analytics, which "plays a significant part in understanding who is accessing what and when to ensure inappropriate access is mitigated," he says.

The firm uses a combination of off-the-shelf security analytics technology with a lot of in-house customization for integration for a particular customer's needs, Newbury says. "The aim is not to re-invent the wheel, but to enhance it through visualization as well as plugging the capability gaps around specific customer use cases. Integration and context is key, whatever the analytic solution as every customer has different needs."

Security analytics can also be used to address insider threats, when employees unwittingly or maliciously render a corporate network vulnerable to attack. Newbury says that is a significant area of interest for BT. "We have developed a number of attack scenarios and use cases for identifying and remediating the potential impact of an insider breach," he says. By applying advanced analytics against event data relating to access or removal of highly sensitive data from within the estate, he says BT can identify users who are abusing their privileges and attempting to take sensitive business documents across the corporate boundary in a number of different ways.

Analytics can also be used to look at outliers and profile deviations. It can simulate attacks from any threat origin and exploit vulnerabilities, network misconfigurations, risky access paths or lax security controls that IT discovers, industry observers say. The simulations and analysis yield risks

#2

Phishing and spear-phishing attacks were rated as the second-greatest security concern in enterprises

– LogRhythm 2016 Cyberthreat Defense Report

are prioritized by their potential business impact with corresponding remediation recommendations to improve network segmentation, IPS signatures and other compensating controls.

Companies should use security analytics systems to deal with inside threats, which have increased significantly, says Monahan. There are external entities that compromise the identities of insiders that make it look like insider threats are occurring. "The bad guy, in many cases, wants to look like an insider and poke around and find data."

It used to be that external threats would come in and get out and very few companies captured significant log data "around Joe Blow in the company," Monahan says. Now the methodology has changed and an attacker's goal is to "come in and look like Joe or Bob and poke around and get out." UBEA is good at detecting this type of behavior and does anomaly detection as well, he says. "Suddenly, Joe is doing something way outside of what he normally does." Insider threats "seem to be more significant now than in the past, and these solutions are good at identifying that."

John Pescatore, director of emerging security trends, SANS Institute

Managed security providers

But in order for security analytics tools to provide value, you need to have skilled people and the right processes in place. Often, however, smaller companies can't afford both the tools and the skilled people, so they will turn to managed security providers, which have invested in both and offer security as a service. "For a lot of people, a managed service makes the most sense," says John Pescatore, director of emerging security trends at the SANS Institute.

One trend he is seeing within vertical industries – such as banking, health care, retail and automotive – is the growth of Information Sharing and Analysis Centers (ISACs), which are industry groups that get together and, for a fee, share information about attacks. Some of that information includes which analytics tools they are using.

"I've seen the true power of security analytics emerge when multiple organizations share data to develop advanced threat intelligence and proactively mitigate today's evolving threats," says UVA's Orebaugh.

Security analytics changed the way BT manages data now. Having a centralized platform lets IT merge and correlate large amounts of disparate information into a contextualized view of risk with a "big picture" view of the attack surface. That view and context helps IT understand attack vectors and enables security teams to prioritize the alerts they receive and what needs to be addressed first.

In addition to security analytics, the company also uses traditional defensive measures, such as firewalls and IDS devices, segmentation techniques to ensure networks are accessible only by users with legitimate access privileges and multifactor authentication.

What to look for in a platform

Organizations need to be eyeing security analytics in order to sort through all of the environments where their data resides and "identify the priority issues from all the other noise," says Monahan. "We need better technology to sort through the data to get the information. Data is raw bits and bytes." Security analytics makes better use of information by identifying patterns and behaviors in all of that data.

People tend to think of security analytics

>45%

More than 45 percent of respondents said today they do manual network-enabled analytics

– IDG

as a magic bullet, but you have to make sure you understand what your basic requirements are when evaluating a platform, he warns.

> "There are personnel and personnel cost issues that make many of these technologies attractive to buyers."
>
> – Eric Ahlm, research director, Gartner

The system also needs to have the right data to make a decision. "Some [companies] rely on their own data feeds and some rely on SIEM. The biggest mistake companies are making is if you have garbage in, you're getting garbage out." The system can only analyze the data it has, so the faster you can get data into it, the faster it can give you useful results, Monahan says.

"If you're missing a set around a particular network segment or particular endpoint or application or set of applications, then as far as security analytics is concerned, it's not there," he adds.

Pescatore believes there is a lot of wiggle room around how security analytics works. "The real-world use cases we've seen where security analytics provide value are where the tools provide essentially low false positive ranking of alerts, enabling the security analyst staff to start with the most important items first," he notes. All too often, however, security analytics marketing babble promises that "we find things no one else finds," which Pescatore says often means "we find everything, including every possible permutation of false positives."

There is no one way to define whether one security analytics tool is better than another, he believes. For Pescatore, the key is that the person using the tool is spending their time more productively because they are focusing on the critical alerts rather than the false positives.

Security analytics tools "can really act as force multipliers" when used in tandem with skilled analysts, good data, good processes and connections between security teams and operations to focus on what is important to the business, he says.

"If you have those processes, these tools can be really powerful in keeping up with and maybe staying ahead of bad guys," Pescatore says. But, he adds, if you just have a few people running around, just buying tools, this isn't going to change the equation at all.

At the end of the day, like other technologies, it's not just about having a good security tool. Analytics platforms "can make your security team of 10 people act like a big team," says Ahlm. "There are personnel and personnel cost issues that make many of these technologies attractive to buyers."

That is because security analytics platforms "can reduce the mean time between detect and respond," he says. Big Data is just a huge pile of data and there is nothing analytics can do that a security professional can't do manually, he says, but the value is in making connections and correlations and linking disparate things together more quickly in a pattern that is more apparent.

Ahlm sees definite potential for growth in the security analytics realm. He believes there will be a lot of convergence in the UBEA and SIEM markets as acquisitions continue to be made. "I think we'll see lot more activity across those submarkets, meaning buying interest and investment and acquisition interest is there, and that's exciting to me." ■

For more information about ebooks from SC Magazine, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

62%

Company directors who cited cybersecurity and IT risks as important concerns

– EisenAmper

Sponsor

The Security Intelligence Company

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, and advanced security analytics.

For more info, please visit us at logrhythm.com

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
CUSTOM MANAGER Kelly Heismeyer
kelly.heismeyer @haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*