exabeam

June 11, 2021

5 Questions on the Future of SIEM and Cloud Answered

Featuring Insights from Joseph Blankenship, VP, Research Director, Forrester

Contents

Exabeam recently hosted a **webcast** “A Discussion of Security Analytics Market Trends with Forrester Research” with guest speaker, Forrester VP, research Director Joseph Blankenship to answer questions on the future of SIEM and cloud.

Joseph has 12+ years of prior security experience encompassing roles at Solutionary (NTT Security), McAfee (Intel Security), Vigilar, and IBM Internet Security Systems. He held earlier positions in IT, telecommunications, and consulting with Nextel, IBM, Philips Electronics, and KPMG. He presents at industry events, is quoted in the media, and writes on a variety of security topics.

We are delighted to present his perspectives in this e-book that offer answers to five of the most-asked questions about current SIEM technologies and cloud security.

Joseph Blankenship’s research focuses on security monitoring, threat detection, insider threat, phishing prevention, operations, and management.

1. Exabeam: You've said security information and event management (SIEM) technology is becoming outdated and less effective. How so?

Joseph Blankenship: Legacy SIEMs suffered from their inability to ingest data at scale and from the number of false positives they provided to the SOC. Because of this, SIEM vendors architected their solutions so that they could consume more data and began using analytics for data analysis, instead of being tied solely to ineffective rules. This ability to consume more and more data, however, has led to other issues.

The main complaint from SIEM customers now is this – it's too expensive at scale. Security teams are pumping more and more data into their SIEMs, looking for "needles in haystacks." This model leaves security teams with a large SIEM bill to ingest, analyze, and store all this data. The amount of data coming from the business is not going to decrease; in fact, it will only continue to grow. With current SIEM technology and pricing models, this is unsustainable for most organizations.

Beyond the cost, security teams are under more pressure from the business and the board to give assurances and stop attempted security breaches. With that in mind, security teams are looking for solutions that are purpose-built for high efficacy threat detection and response. SIEM providers have the opportunity to evolve in this direction, but need to make significant strides in incident automation and response capabilities in order to keep up with competing solutions.

2. Exabeam: Have analytics assumed primacy when it comes to detecting treats? Are all analytics created equal?

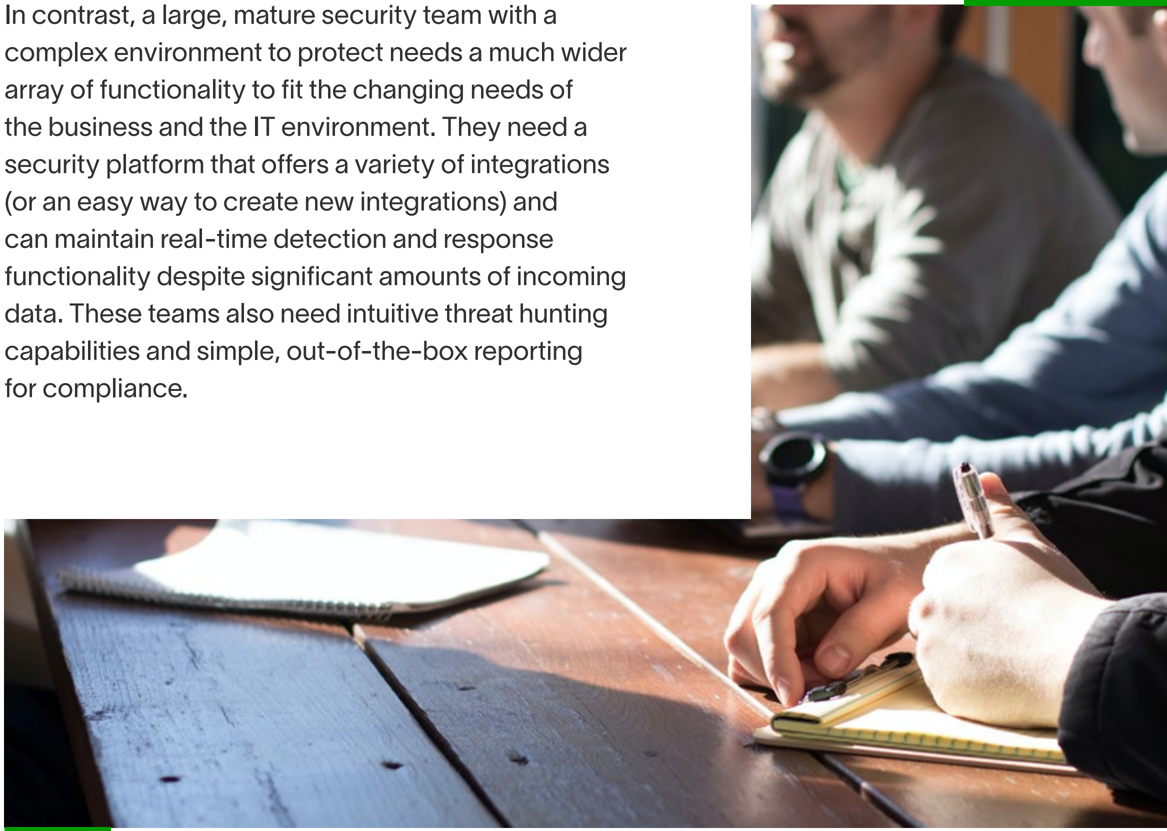
Joseph Blankenship: Analytics are of critical importance when it comes to detecting and defending against attacks given the massive amount of data flowing through the enterprise. There is simply too much information and too many evasive threats for security teams to consistently build all their own rules for detection, thus security analytics must take over.

Critically, all security analytics are not created equal. Every aspect, from the data types ingested to the precision of the analysis, can have an impact on the quality of the end result. Security analytics must be designed with specific use cases in mind, both from the standpoint of the attacks they are trying to surface and the way they aid the analyst. Though not directly security analytics themselves, the output of security analytics and the way it is presented play a key role in its value. The findings of security analytics must be presented to the analyst so they can take immediate action, without having to work through a complex narrative or user experience.

3. Exabeam: What do security analytics vendors need to do to meet customer needs for customization?

Joseph Blankenship: Customer needs for security analytics customization come in a few flavors, depending on the size and security maturity of an organization. Less mature and small security teams need a solution that is easy to use and requires minimal integrations and little expertise to get up and running. They need, at times, a single analyst to be able to address the majority of threats in the environment without burning out. This requires a significant amount of automation to be built into the security analytics platform so that the analyst can focus on the most dangerous and pressing threats, without having to worry about repetitive processes and mass false positives. Further, this type of solution needs to give the security team a path to grow and add on functionality as the business and the security team mature.

In contrast, a large, mature security team with a complex environment to protect needs a much wider array of functionality to fit the changing needs of the business and the IT environment. They need a security platform that offers a variety of integrations (or an easy way to create new integrations) and can maintain real-time detection and response functionality despite significant amounts of incoming data. These teams also need intuitive threat hunting capabilities and simple, out-of-the-box reporting for compliance.



4. Exabeam: The rise of the MITRE ATT&CK framework over the past couple of years has been astonishing. The hard part is operationalizing MITRE into the day-to-day workflow. Do you agree and do you have advice for folks?

Joseph Blankenship: The MITRE ATT&CK framework is exciting because it gives security teams and the larger community a language by which to communicate threats they are seeing in the wild. Security teams have widely recognized the benefits of this approach and have quickly embraced MITRE ATT&CK.

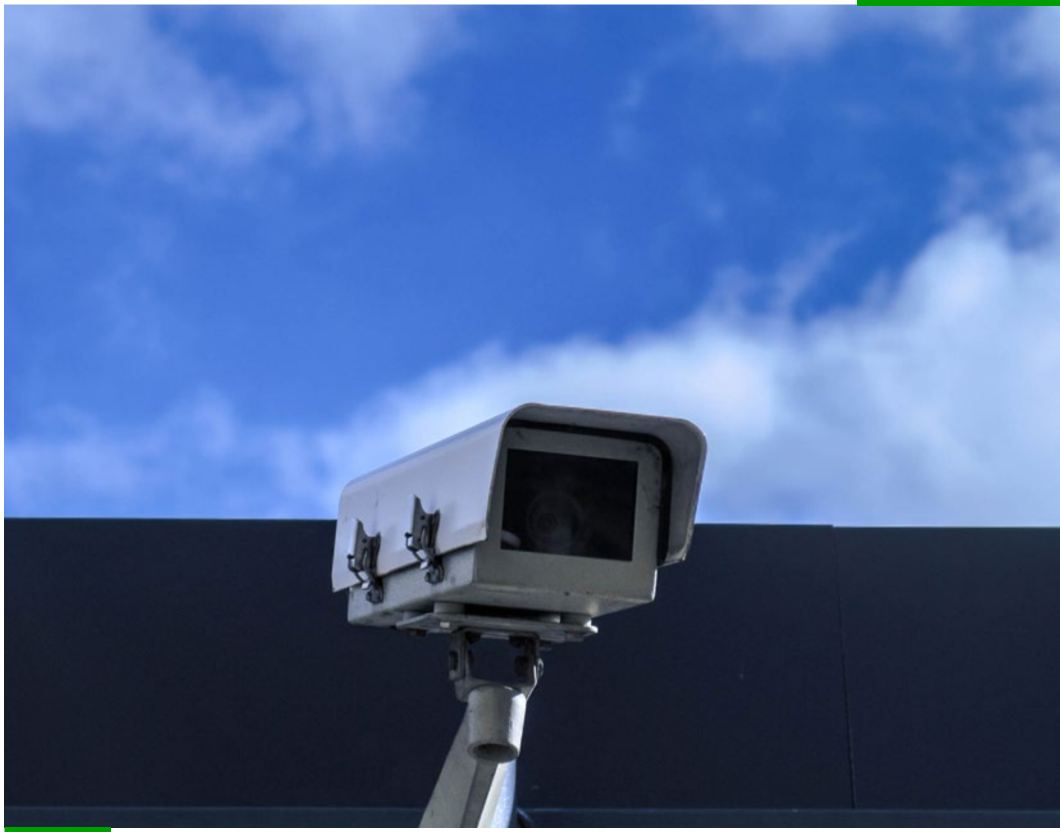
A first look at the MITRE ATT&CK matrix can be daunting, especially for those who assume they need to check off every single box for success. I recommend security teams start by reviewing and learning about how other security teams are using MITRE ATT&CK. A great way to start is by reading security research that maps to MITRE ATT&CK, which gives a sense of how it can be shared and applied in your own environment. From there, a great way to use MITRE ATT&CK is in the context of red teaming.

Identify specific attacks that affect your industry or size organization and execute a red team exercise based around those TTPs to find where you are successfully detecting or missing parts of the attack. By using the MITRE ATT&CK framework to classify the actions your red team is taking, you can then share that information with the blue team so they can improve your defenses against the most common threats facing your organization.

5. Exabeam: What are the benefits of moving security to the cloud? Why have security operations lagged other functions?

Joseph Blankenship: Security operations constantly lag behind other business functions, but there's a good reason why. When the business makes a decision to use new technology, it's the job of security to prepare for and allow that to happen in a secure way. This leaves security functions needing agility in the face of a constantly changing environment.

That said, there have been concerns around data privacy and compliance that have made security teams hesitant to move to the cloud. Over time, cloud security vendors have added capabilities to manage and report on compliance. Security vendors are also giving customers greater control over their cloud data, which has made the move to the cloud more appealing. In addition, the cloud is an attractive option for IT and security teams looking to lower costs and allow for flexibility and scalability. The cloud is now the preferred option for consuming security analytics capabilities for most firms as it allows for increased scalability of compute and storage, without the need to manage on-premises hardware and software.



exabeam

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Management Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users, and malicious adversaries, minimize false positives and make security success the norm. For more information, visit www.exabeam.com.

To learn more about how Exabeam can help you visit **exabeam.com** today.