SECURITY ANALYTICS FOR THREAT DETECTION AND BREACH RESOLUTION IN 2019

EMA Top 3 Report and Decision Guide
Focus Vendor: Awake Security

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) REPORT
WRITTEN BY DAVID MONAHAN

Q1 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

CONTENTS

INTRODUCTION

Understanding Security Analytics

The need for better analysis at the front of an incident inspired the creation of security analytics. Over the past five to seven years, lag times in identifying and remediating threats created not only dissatisfaction with the commercially available systems, but also stemmed significant creativity. Much of the advancements evolved from applying the concepts that have been driving advancements in business processes and IT analytics for a significantly longer period of time. Both the algorithms and the models had to be adjusted to form security analytics.

Security analytics were created to provide advanced data analysis using multiple analysis techniques, the most popular of which is a class of adaptive outcome algorithms called machine learning (ML), also now being dubbed artificial intelligence (AI). These algorithms and models supply individual and community behavioral analysis combined with protocol, packet stream, and big data interrogation and risk profiling techniques. Combined, they identify, prioritize, and aid in containing threat actors.

To deliver increased detection and accelerated response and containment, security analytics can ingest data from packet streams and flows, perimeter defense, authentication, application, endpoints, and any other of the myriad of IT and security technologies. Security analytics also interface with other monitoring and alerting systems, like security incident and event management systems (SIEM). This data, along with the good algorithms and the proper application thereof, can produce extremely high-fidelity intelligence for rendering the context of an event, provide a previously unobtained level of visibility into activities in the environment, and supply excellent prioritization of incidents.

EMA TOP 3:
EMA PRESENTS ITS TOP 3 AWARD TO VENDORS THAT ARE BEST ALIGNED WITH TODAY'S CUSTOMER PRIORITIES AND PAIN POINTS

Each vendor uses publicly available ML and has its own intellectual property and proprietary approach that, when combined, create a unique solution. The combination of their integrations for data collection, the back-office analysis approach, and the user interface make each product different, thus making it imperative for each organization to understand their requirements and discuss them with prospective vendors prior to purchasing a solution of this type.

A crucial aspect of this whole genre is that these technologies look for patterns and anomalies within those patterns. Not all anomalies are bad and not all seemingly normal actives are good. That is why the quality and volume of data and the means of modeling and analysis are so crucial. Each environment has different systems that provide the data, and each vendor has different ways of analyzing that data, so different vendors may perform with somewhat different degrees of efficacy between those dissimilar environments.

Security analytics tools are not a silver bullet. Though they all create a myriad of metadata to aid analysis, all of them also rely on other technologies to provide them with relevant source data for that analysis. If an organization is missing the technologies that provide that source data, tools silos, or a pathway to get that data to the analytics engine and data silos, then security analytics will be hampered and simultaneously provide a false sense of security.

Security Analytics and SIEM

SIEM evolved over twenty years. Some people felt it was unable to adapt, which is why disruptive technologies that are now labeled as security analytics burst onto the scene.

Some of the vendors that provide security analytics are trying to take over the role of the central interface for security operations, thus also identifying as SIEM 2.0 or Next-Gen SIEM. At the same time, some of the traditional SIEM vendors have been working diligently to incorporate ML/AI and new models into their SIEM technology to provide equal capability and defend their market share. Many of the traditional SIEM vendors did very well in addressing use cases, and many of the new vendors did as well. Given this, setting aside preconceived notions and biases is important for identifying the best tool for the organization.

INTRODUCTION

Why You Should Read This Research Report

This report is a time-saving guide. It is designed to help decision-makers who have identified problematic security use cases to select analytics tools that best address those use cases to aid in narrowing selection choices for proof of concept testing or other interviews.

If the security team has invested in the proper tools and still is not able to render a solid defense, and reaches a point where they have been able to break down data silos and address the political silos that impede information flow and cooperation, then this report can aid in choosing a vendor to take the security practice to the next level.

Evaluation Methodology

This report comes from hundreds of man hours of data collection and review based on vendor interviews, product demos, customer interviews, and documentation review.

It is also important to note that while these vendors all provide security analytics, many of them compete in different solution spaces, so not all use cases are applicable to all vendors and therefore not all vendors were evaluated against all use cases.

Evaluated Vendors

Awake	Huntsman Security	SecBI
Balbix	IBM QRadar	Seceon
Barac	IronNet	Securonix
Bay Dynamics	Lastline	Splunk Phantom
Corvil	LogRhythm	SS8
Dtex	Mantix4	STEALTHbits
empow	ObserveIT	Sumo Logic
ExtraHop	Preempt	Teramind
Gigamon	ProtectWise	Vectra
Gurucul	Palo Alto Networks (RedLock)	Versive
HPE Niara	RSA	

About the Use Cases

The use cases in the report were gathered from management and frontline security professionals of current customers, non-customers, and vendors. Current customers and non-customers indicated their perceived needs from analytics, while the customers also provided details on use cases that they discovered they could address once they started using their chosen solution. Vendors provided insights on advanced use cases they address. Over sixty use cases were identified, with just over 40 published in the report.

The evaluated solutions focus on security analytics in different ways. The approaches to data collection and the types of data they collect affect not only the applicability, but the efficacy of the solutions in the various use cases. Given this variance, it is conceivable that more than one solution meets the organization's needs or that given a wide breadth of needs, multiple solutions could be warranted.

WHAT ARE THE EMA TOP 3 REPORTS?

EMA Top 3 reports identify the leading priorities organizations face with resolving challenges and meeting enterprise requirements in particular IT management focus areas. The intent of this report is to inform and inspire influencers and decision makers in their project planning and vendor selection process.

While EMA internally conducted a detailed analysis of solutions that help support the identified IT management priorities, this report is not designed to provide a feature-by-feature comparison. In certain cases, EMA recognized products for their innovative approach rather than their ability to meet a predetermined checklist of features. Additionally, some popularly adopted approaches may not be represented in this report because EMA's analysis did not indicate that they fully address emerging market requirements. This guide was developed as a resource for organizations to gain insights from EMA's extensive experience conducting hundreds of product briefings, case studies, and demonstrations.

Solution Qualifications

In order for a product to be considered for recognition as an EMA Top 3 secure access enablement solution, all evaluated features and capabilities were required to conform to the following rules:

- Reported features must be generally available on or before December 1, 2018. Features that are in beta testing or are scheduled for inclusion in later releases do not qualify.
- Reported features must be self-contained within the included package sets. Any features that are not natively included in the evaluated package sets, but available separately from the same vendor or a third-party vendor, do not qualify (except where explicitly noted as points of integration).
- Reported features must be either clearly documented in publicly-available resources (such as user manuals or technical papers) or be demonstrative to confirm their existence and ensure they are officially supported.

How to Use This Document

It is important to recognize that every organization is different, with a unique set of IT and business requirements. As such, EMA strongly recommends that when using this guide to create a shortlist, each organization conduct its own evaluation to confirm that other aspects of the solutions will best match its business needs or that the disclosed use cases also meet other requirements, like business workflows and full reporting necessities. This guide will assist with the process by providing information on key use cases common to many prospective buyers to review during the selection process, and an associated shortlist of vendors with solutions that meet them.

For each use case, EMA provides the following sections offering insights for use in the platform selection process:

- **Quick Take** – This is an overview of the use case, why it is important, and how the solutions address it.
- **Buyer's Note** – Key considerations prospective buyers should be aware of, and questions they should ask during the evaluation process.
- **Top 3 Solution Providers** – By identifying and recognizing the most innovative vendor solutions that address the greatest business priorities for secure access enablement, the table in this section provides a brief overview of each platform and the respective capabilities. Within the Top 3, the solutions are listed alphabetically by vendor, so the order in which they appear is not an indication of EMA's preference. It is highly recommended that organizations seeking to adopt solutions addressing a particular priority investigate each of the corresponding Top 3 vendors to determine which best meet their full and unique requirements.

USE CASE: DETECTING LATERAL MOVEMENT

Note: Solution providers are listed alphabetically without other preference assigned.

Awake

Lastline

Versive

82% of respondents believe that security technologies exist that will consistently detect stealthy threats, APTs, or ATAs.

One of those technologies is security analytics.

EMA "Data-Driven Security Unleashed" research

QUICK TAKE

Lateral movement is a fundamental stage of an attack desiring to remove data or convert hosts into servants of a botnet. Once inside, the attacker has to perform reconnaissance and will then move to other susceptible hosts. During this process, the attacker's control within the environment expands and data can either begin flowing from each host or be moved to a central internal hoard to be trickled out. This is particularly useful if the attacker can identify and compromise a system with legitimate Internet communications. If detected early in this stage, the scope of damage and extent of investigation are decreased, cleanup is comparatively reduced, and losses are curtailed. Limiting lateral movement reduces data exposures and therefore can significantly reduce or even eliminate external notification requirements.

BUYER'S NOTE

Detecting lateral movement requires a combination of detection of reconnaissance activities, communications, and connections between internal machines. When these involve machines that do not normally communicate, it is a much less difficult task and can be handled with appropriate premade policies and rules because those communications are a known quantity. When attempting to detect undesirable touches, communications, and connections between machines that are normally in contact, the difficulty of early detection and delineation within common or authorized communications is drastically more difficult. Lateral movement can be arrested by a number of techniques that can be applied both pre- and post- detection. Changes to host, workload, and network firewalls as well as network access lists can be used as a best practice to isolate systems and network communications before any operations begin and can be updated at any time as needs change. For situations where the affected systems need to communicate, DNS and ARP cache manipulation are also very common after detection techniques are used for isolating compromised hosts.

Lateral movement detection can result in high numbers of false positives and negatives. Awake Security deals with this challenge by tracking behaviors and attributing those to the entities rather than ephemeral characteristics, like IP addresses. It then presents this information in a forensic timeline for the entity and uses machine learning algorithms, like belief propagation, to score the risk for each entity.

USE CASE: IDENTIFYING CREDENTIAL ABUSE

Note: Solution providers are listed alphabetically without other preference assigned.

Awake

Huntsman

Vectra

74% of organizations stated that events generated by their IAM solution were very valuable to extremely valuable for security analysis.

EMA "Data-Driven Security Unleashed" research

QUICK TAKE

Credential abuse is a serious threat, whether it comes from an insider or an external threat entity. This use case was aimed more at the abusive insider than the external threat entity that compromises and then misuses an identity. In these scenarios, people that have authority to access systems or data misuse that authority in some manner. The classic case is an IT admin accessing payroll or HR data, or a database admin accessing content in the database that does not pertain to the execution of his or her job, or an executive admin or a nurse accessing sensitive files out of personal curiosity for which he or she has permissions for business purposes. This also extends to people who are over- or under-provisioned.

In these scenarios, security analytics rely on several aspects of behavior. A person in a particular job tends to have a relatively narrow set of tasks and system of file access throughout a day or week. Unless some aspect of the job or management of the job changes significantly, their patterns of behavior will stay in that band. People in the same role or functional group tend to also have the same patterns of behavior. Analytics solutions track those behaviors and monitor them for deviance. When a deviance occurs, the solutions alert the company.

It is important to get early warning of these activities because they can indicate credential compromise or sharing as well as a duped, misguided, overly curious, or malicious person in the environment. In cases of overly curious personnel or someone who is weighing the options of malicious behavior, knowing they can be detected is sufficient deterrence for continuing action. For others who are either duped, misguided, or have serious intent, SecOps can get to the situation faster and thwart much of the possible threat.

BUYER'S NOTE

Most of these systems rely on having sufficient, accurate user data. To use group relationships, many of the solutions rely on having access to an accurately maintained identity and access management (IAM) system, such as Active Directory. Having an accurate IAM system helps associate the various identities to a single user, making it imperative that the IAM system be well-maintained.

Interestingly, Awake Security handles this differently. Their solution automatically determines identities based on parsing E-W protocols like Kerberos, SMB, etc. to gather the credentials. It then automatically tracks those entities as they move across the network and uses behavioral fingerprinting and clustering to identify similar entities (akin to the group relationships mentioned earlier). This approach is useful to handling unmanaged infrastructure (not in IAM systems) and in avoiding the need for integrations with those data sources.

USE CASE: THREAT HUNTING WITH MITIGATION/CONTAINMENT

Note: Solution providers are listed alphabetically without other preference assigned.

Awake

Seceon

Vectra

28% of respondents have outsourced threat hunting to a managed security services provider because they lack the technical capability that security analytics could provide to perform the function.

EMA "Security Megatrends" research

QUICK TAKE

Threat hunting is a little different because it is proactively looking for threats that are already inside the monitored perimeter. No technology is infallible. Current security analytics solutions are far ahead of their predecessors when it comes to threat detection, but they are learning systems and sometimes new attacks can be used to infiltrate the environment before the system learns to automatically detect them. If this happens, analysts are using their own skills, augmented by the analytics system searching for the trail of clues that will indicate the threat. Once found, mitigation/containment of the threat is of the utmost imperative. At that point, mitigations can be enacted through the system interface to mitigate the threat in one way or another.

BUYER'S NOTE

With proactive threat hunting, the user interface has to be extremely adept at capturing information and arranging it in a manner that creates a history of the relevant events and helps move the other irrelevant data and hunting paths out of the way. With these tools, dead ends in investigations can be reduced and investigations made more efficient.

All vendors in the analytics space are developing partner integrations and native capabilities for mitigating threats. These integrations most often manifest in the use of APIs created by the defensive system's vendors. Since business disruption is unacceptable, regardless of what mitigations and remediation vendors support out-of-the-box, a conservative approach dictates that prior to fully automating, remediation and mitigation actions be manually initiated and tested until a high degree of certainty is attained with their efficacy and correctness. Evaluate the vendors' current technology partnerships, integrations, and roadmaps to ensure the product can utilize the solutions currently in use and the one the company is planning to use in the next couple of years.

Awake Security lets users build and save his or her own hunting rules through a powerful query language, and then automates future hunts for the security team. This allows senior analysts to save their hunts and junior analysts to follow up on any threats identified through this process.

CONCLUSION

Security analytics tools are a significant strategic and tactical investment. They are significant both from the potential costs and from the potential benefits. The ability to identify a myriad of threats earlier in the attack process is a crucial part of the security arsenal. Each of the tools listed in this report can provide a great deal of value for the organization provided it is adopted while evaluating the larger picture. Below are the top considerations when investigating a security analytics tool:

1. Identify the use cases most pertinent to your organization, both presently and for the next 3-5 years.
2. Evaluate current workflow processes and the tool's ability to adjust to work within those processes or the organization's ability to adapt to the tool, whichever is more appropriate.
3. Consider the organization's ability to collect and centralize the necessary data so the tool can do its job.
4. Asses the ability to retain the necessary data for a sufficient length of time if forensics is part of the operations plan.

While there is no security silver bullet, security analytics is a great step forward for any organization to improve its ability to detect threats. When purchased without the proper research, these tools can create unnecessary overhead and actually impede performance by creating a false sense of security. However, security analytics is the perfect operational example of prior planning averting negative performance. When the proper tool is selected, customers will see great benefits.

VENDOR PROFILE: AWAKE SECURITY

Awake Security delivers a software platform powered by the expertise and real-world investigations of hundreds of the world's foremost investigators. Awake's network detection and response platform applies artificial intelligence to bring these human skills to all customers, instantly analyzing billions of packets to immediately discover every device, user, and application on the network. Through autonomous hunting and investigation, Awake uncovers malicious intent from insiders and external attackers alike.

AWAKE

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com.

Please follow EMA on:

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3796-Awake.011619