SECURITY ANALYTICS FOR THREAT DETECTION AND BREACH RESOLUTION IN 2019

EMA Top 3 Report and Decision Guide
Focus Vendor: Vectra AI

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 AI
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: IDENTIFYING CREDENTIAL ABUSE

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

Vectra AI

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

These systems rely on having sufficient user data. Talk to solutions vendors about the time it takes their solution to train the models for credential abuse or if that period can be accelerated in any manner. To use group relationships, these solutions rely on having access to an accurately maintained identity and role management system to determine who the associated people are to compare. This system must be cleaned and maintained before users will see any significant benefit.

USE CASE: IDENTIFYING NETWORK PROTOCOL MISUSE/ABUSE

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

Vectra AI

81% of major APT campaigns hide their command and control (C2) in common web ports.

Trend Micro infographic, "Connecting the APT Dots"

QUICK TAKE

To perform effectively on this use case, it is highly advantageous for the analytics system to be at least somewhat aware of OSI network layers three through seven. If it does not or cannot understand how a standard IP transport protocol, a custom Internet protocol, or application protocol is supposed to operate, there is no way for it to identify that something is amiss.

The data hidden with the transmission employing this type of technique would be analogous to a network protocol steganography. To attempt this type of attack, attackers can use protocol tunneling or other methods to try to fool perimeter and internal firewalls and other detection solutions into allowing or otherwise ignoring the communication stream because it looks benign. In reality, the attacker is hiding the actual nature of a communication.

This approach began gaining popularity in the last ten years or so, but recently hit a plateau as attackers began moving to more TLS. A popular attack method is to tunnel communication through common network communications ports like HTTP or DNS. These ports are commonly allowed through firewalls and other perimeter security devices because they provide business-critical functions. While unsuspecting monitoring devices believe the traffic is HTTP or DNS traffic, it is actually something else. The attacker is misusing the protocol because ports 80 and 53 that should be communicating HTTP and DNS, respectively, are actually being used to communicate in a different manner.

BUYER'S NOTE

In most environments, this may not be seen as a primary use case. However, ignoring it would be a mistake if the organization does not have a full application layer proxy in place.

USE CASE: INCIDENT RESPONSE WITH ATTACK BLOCKING

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

Vectra AI

68% of breaches took months or longer to discover.

24% of organizations identified advanced workflow integrated with automation as a top SecOps initiative.

2018 Verizon DBIR and EMA Report: "Integrating SecOps With Operations, Development, and ITSM in the Age of Cloud and Agile"

QUICK TAKE

In a security incident, time is essential. The most effective incident response requires a highly accurate and fast detection mechanism with an ability to streamline information gathering and operations workflows. It must also interact with defensive tools in the environment from within the context of the incident. The greatest time loss in an incident is the investigative process. It is also generally the most frustrating for analysts. The second-largest waste of time is having to manually log in to infrastructure and defensive systems to update policies after incident detection. The solutions in this category are excellent at gathering information for context. As a bonus, they all have a large number of integrations, with the most popular defensive technology solutions to accelerate attack blocking.

BUYER'S NOTE

First, buyers should be sure they know the list of current and solidly road-mapped integration targets. Vendor integration is a must, and the security analytics vendor and the partner should regularly update that integration. If the APIs and other scripts are only maintained by one or the other, connection paths can be changed, causing a break in the integration services. Make sure to talk to the prospective vendors to understand who owns and maintains the integrations and whether they ride on published APIs or middleware scripts.

Going with a smaller vendor may yield fewer integrations up front, but may also provide buyers with a generally more agile development process that includes customer input for supporting new integration vendors. On the other hand, smaller vendors are riskier from a company stability perspective. They may go out of business or be acquired, letting the product wither and die.

USE CASE: RISK PRIORITIZATION FOR ACTIVE SECURITY EVENTS

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

Vectra AI

Only **38%** of organizations identified that they are consistently successful in correlating security incidents to business risk.

EMA "Data-Driven Security Unleashed" research

QUICK TAKE

This is an extension of having good overall telemetry for context and prioritization. Security analytics were developed to exceed traditional SIEM capabilities for identifying and prioritizing events. This particular use case takes things to the next level in identifying the priorities not in batches or after some period of additional data collection and analysis, but in near-real time. During an active incident, the last thing analysts should need to do is "hurry up and wait" or spend time to figure out which of the active incidents should be dealt with first. Analysts need timely, highly accurate telemetry on what should be addressed immediately. This use case addresses the seemingly unending black holes that absorb analysts' time during the day while trying to solve urgent problems and address pressing issues.

This is a big use case for getting rid of what amounts to busy work or distractions by putting first things first. Properly installed and configured security analytics solutions produce fewer actionable events than traditional SIEM and log management tools. Going to the next level, these solutions also address current incident risk levels when they come in, and also adjust them as additional telemetry is received.

BUYER'S NOTE

This ability is not yet widely available in the market. It has serious positive impacts on analyst time and risk reduction, strongly supporting ROI arguments for investment. To create the ROI calculations, use current event volumes and time spent addressing incidents, especially false positives and incorrectly categorized events, to compare to tested outcomes.

USE CASE: THREAT DETECTION ACROSS ON-PREMISES AND CLOUD

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

Vectra AI

52% of respondents erroneously believe their public cloud provider owns most to all of the security responsibility for their data and applications.

EMA "Security Megatrends" research

QUICK TAKE

The cloud is an important resource to a rapidly-growing number of companies. Though the cloud offers many advantages and opportunities, it also comes with some risks and difficulties in relation to security. The challenge is getting sufficient data back from the cloud to run effective analytics. There are variations in the security controls and means of passing data for security that, if unaccounted for, may prove to create significant and unexpected blind spots in security visibility.

The cloud is a significant target for attackers because of its data richness. Due to differing lines of demarcation for cloud PaaS, IaaS, and SaaS, common confusions about who owns which aspects of security create common security gaps for threat actors to exploit. Security analytics in the cloud provide early detection of those threats as well as useful information so the gaps can be closed.

BUYER'S NOTE

Threat detection in the cloud is highly reliant on which APIs the cloud vendor exposes for interrogation by security. The Tier 1 cloud providers all have some form of access, but the API handles vary. If a user is not currently partnered with a cloud vendor, then the choice of analytics vendor is very open. If a user is already partnered with a provider, ask the solutions vendors to discuss which cloud providers they support and which one(s) they feel they support best to identify alignment. If an organization has a cloud architect who understands a cloud provider's APIs, it could be advantageous to try to set up a discussion between that person and one of the analytics solutions developers, the technical product architect, or CTO to ensure that the solution is fully compatible with the cloud provider. This conversation is also useful if someone is considering expanding into multiple cloud partners.

USE CASE: THREAT HUNTING WITH MITIGATION/CONTAINMENT

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

Vectra AI

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.

VENDOR PROFILE: VECTRA AI

Vectra AI launched in 2011, first shipped its product, then named the X-Series, in April 2014. Vectra AI has stong venture backing raising $122.5 million through multiple rounds. Over that time, the AIdriven detection and threat hunting platform was rebranded to Cognito. Industry veterans with a common background in Juniper Networks lead the company. Among its customers are Pinterest and Ticketmaster.

Cognito is made up of Cognito Detect, which automates detection of advanced threats in real time, and Cognito Recall, which applies machine learning to help human analysts with deeper threat hunting and incident response. Its combination of AI, machine learning, and vbehavioral traffic analysis of network data is used to gain a basic understanding of attacker behavior (even with encrypted traffic). Key to the advances Vectra made to the platform is the company's Vectra Threat Labs threat research team, which provides the company's data scientists with new insights into previously unseen threat behaviors to improve machine learning models. Cognito Detect sits on a SPAN port and performs analysis on network traffic, as well as logs gathered from security and authentication systems and SaaS applications. Cognito Recall is a cloud service that uses the network metadata, logs, and cloud events gathered from Cognito Detect to assist human analysts in deeper investigations.

Vectra AI is able to link current events to historical events to identify low and slow attacks. Cognito makes exceptional use of Bayesian networks to identify connections between a range of events, hosts, and detection methods to surface coordinated attacks automatically. This allows it to prioritize behaviors that represent the most serious threats. Reporting is also a strong suit for Cognito. As a dedicated, privately-held company, Vectra stands out as on par with much larger rivals due to several factors, including its extremely high growth rates, healthy number of patents, and an unusual amount of market recognition for a small company.

Cognito is highly effective and has gained numerous industry accolades, but also has one of the highest costs of the platforms in this evaluation. Vectra tied with one other company for the number of analysis techniques used to identify threats. Cognito does not provide an internal case management system, but prefers to integrate with the in-use ticketing system. Cognito reporting capabilities were rated as one of the highest in the comparisons.

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.

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-Vectra.020619