SECURITY ANALYTICS FOR THREAT DETECTION AND BREACH RESOLUTION IN 2019

EMA Top 3 Report and Decision Guide
Focus Vendor: Balbix

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

Q1 2019

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

CONTENTS

Introduction 1
What are the EMA Top 3 Reports? 3
Use Case: Asset Inventory/Classification 4
Use Case: Breach Avoidance Through Predictive Analytics 5
Use Case: Real-Time Threat Visualization 6
Use Case: Risk Prioritization for Active Security Events 7
Conclusion 8

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: ASSET INVENTORY/CLASSIFICATION

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

Balbix

Corvil

ExtraHop

During asset discovery, in any given organization there are at least **25%** more assets connected to the network than are cataloged.

ForeScout Technologies research

QUICK TAKE

Virtually every environment has more assets on the network than they have accounted for in their asset databases or network diagrams. IT and business personnel are constantly adding and removing end-user devices and new systems to support business needs. Virtual computing and cloud, with pressures from shadow IT, agile delivery models and emerging IoT deployments, have exacerbated this problem.

Accurately identifying everything that is connected to the infrastructure should be a critical concern since each application and system is part of the potential attack surface that can be leveraged as a beachhead for incursion or data exfiltration.

BUYER'S NOTE

There are numerous specialized systems that provide asset inventory or classification services, such as CMDB and NAC tools. Identifying a security analytics tool that will double up to provide this feature can deliver cost avoidance by alleviating the need for the adoption of a separate system or a cost reduction. It does this by allowing the discontinuation of the purpose-built solution. Do a thorough analysis of the business requirements to determine the features used within the organization now and those that may be needed in the next three to five years prior to discontinuing an existing solution.

USE CASE: BREACH AVOIDANCE THROUGH PREDICTIVE ANALYTICS

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

Balbix

IBM QRadar

Preempt

46% of organizations said predictive security analytics were one of their top three use cases. Use case: Identifying attack surfaces and the likelihood they will be exploited.

EMA "Security Megatrends" research

QUICK TAKE

The current state of mind assumes that all companies have been breached, or inevitably will be, and they should accept that as a fact. The issue with that idea is, while preparation is good, pessimism can be detrimental to being proactive. It is true that no one can stop attacks, but part of risk management is identifying where weaknesses are and then strengthening them, preferably before they are exploited.

Predictive analytics can be applied in several ways to address this undesirable situation. By analyzing patterns of behavior before and during attacks, as well as context and business impact for all assets, AI algorithms and other engines can make educated guesses of the systems and informational assets that may be targeted. Depending on the system, it can be augmented with data from vulnerability scanners and threat intelligence to identify the vulnerabilities that are most likely to be exploited to get through the perimeter to critical assets.

BUYER'S NOTE

The solutions listed here are different in scope of functions and overall cost. Be aware of current and future operational needs to select the most applicable solution or platform for integration into the existing architecture. Prospective buyers should have in-depth discussions about how the award winners create and disseminate their predictive analytics to ensure the delivery methods are, or can be, compatible with the existing and desired processes, procedures, and workflows.

USE CASE: REAL-TIME THREAT VISUALIZATION

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

Balbix

ProtectWise

STEALTHbits

30% of organizations identified enhanced data visualizations as a top five capability for accelerating detection of malicious threat actors in their environment.

See the Lockheed Martin – Cyber Attack Kill chain or the MITRE ATT&CK matrix for more details

QUICK TAKE

One of the questions that should come to mind when choosing a security analytics solution is, "Is a graphical user interface (GUI) an appropriate criterion for evaluating a security tool?" With many solutions the answer may be arguable, but with security analytics, the answer is a resounding, "YES!" Data visualizations allow human analysts to find and study data relationships that would be far more difficult, even impossible, for them to find just combing through data. Visualizations in the GUI lead analysts to faster, more accurate decisions and a deeper and broader understanding of where threats are in the monitored environment and within their own lifecycle.

BUYER'S NOTE

There are a variety of threat visualizations. These leaders have very different strategies on how they deliver threat information. In fact, each solution in this category uses variations to create a proprietary screen for analysts. Because different people process visual information differently, and there are workflow variations between organizations, be sure to involve the people who will be using the solution on the frontlines in the testing, preferably in a live proof of concept test.

USE CASE: RISK PRIORITIZATION FOR ACTIVE SECURITY EVENTS

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

Balbix

Preempt

Vectra

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 of difficult to complete tasks or after some period of additional data collection and analysis, but in clearly priroritized lists and in near-real time. With an active incident, or imminent breach prediction, the last thing analysts should need to do is "hurry up and wait" or spend time figuring out which of the many active incidents and related security tasks should be dealt with first. Analysts need timely, highly accurate telemetry to determine and present 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 and predicted incident risk levels when they come in, and also adjust them dynamically 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 and SecOps efficiency arguments for investment. To create the ROI calculations, use current event volumes and time spent addressing selected events and incidents, especially false positives and incorrectly categorized events, to compare to tested outcomes.

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-Balbix.011619