Selecting a Threat and Vulnerability Management Solution

Key criteria to guide evaluation

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Written by David Monahan
Prepared for RiskSense

August 2018

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Selecting a Threat and Vulnerability Management Solution

Table of Contents

Executive Summary

Risk is managed through the evaluation and reduction of its primary components, threats, and vulnerabilities. Probabilities of likelihood and occurrence are applied, along with understanding both hard and soft values of assets and the costs of prevention investments in people, processes, and tools versus the cost of post-breach remediation, mitigation, and cleanup activities.

To make appropriate investment decisions for determining to pursue a proactive prevention strategy versus a possible breach recovery strategy, context is king. Gaining more accurate and timely information is a core requirement for this vital decision making. Therefore, identifying a threat and vulnerability management system that can collect, manage, analyze, prioritize, and disseminate information at the pace of business is a crucial business requirement. This paper discusses ten key criteria for addressing the need for better threat and vulnerability management information to improve risk management.

Manage Threats and Vulnerabilities as Risk Components

For organizations operating in firefighting mode, finding the time to identify and address threats and vulnerabilities seems like a daunting and even impossible task. It is truly a catch-22. While fighting fires, there seems to be no spare time to identify and get ahead of threats and vulnerabilities. However, by not programmatically managing threats and vulnerabilities, problems abound, prioritization of redress activities does not happen, and more fires erupt. Managing threats and vulnerabilities requires a proactive approach to information gathering and analysis so they can be addressed before they are exploited. These activities have their challenges, but when executed appropriately, they are far less costly than dealing with the aftermath of a breach.

Top 10 Criteria

Though each plays a critical role in the tool or platform selection process, the most important criteria will depend on the organization's operational requirements. Only after properly documenting those requirements should the organization move forward in the selection and trial process. The following points are provided in alphabetical order.

1. Allow Access to Underlying Information

SecOps, ITOps, and DevOps each support threat and risk management reduction in their own domain. Those different responsibilities drive the need for access to different information for verification of the threat or vulnerability and whether or not mitigation and remediation efforts are successful. The system must offer different means to access the underlying data through context-sensitive menus, ad hoc data searches, and custom dashboards.

2. Assist Operational Flexibility

Provided the operational processes are not flawed or otherwise inadequate, the tool should bend to the needs of the organization and its processes, not the other way around. Whether for threat and vulnerability discovery, investigations, lifecycle management, or change control and remediation, the tool must be flexible enough to support the required processes.

3. Deliver a Living Knowledgebase

Assets, threats, and vulnerabilities should not be evaluated in a vacuum. The chosen system should maintain a history of the state of the assets with relation to threats and vulnerabilities. This must be done to understand how the risk profile of the asset changed over time to measure improvement.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

4. Enhance Context to Improve Security

EMA research[1] identified that 52 percent of threats were improperly prioritized by external systems, such as NVD, and internal alerting systems that require manual reprioritization. These misclassifications were due to poor context due to the classification system having insufficient information about the environment. Thus, more relevant data points for analysis are better for determining context that will drive severity classification, derived risk level, and ultimately rank in the prioritization of mitigation or remediation.

5. Facilitate Integration and Automation

Before a company starts automation, they must ensure that they have a good functioning process. Without that, the organization will continue to suffer from poor outcomes, only there will be more of them delivered faster.

With the demands placed on IT and SecOps, more automation is necessary. There are more incidents, requests, tickets, vulnerabilities, and threats. Figure 1 shows the relationship of the growth of vulnerabilities to assets in various-sized organizations in relation to the size of their security teams.[2] Though larger organizations have more money and larger security teams, they also have a disproportionally larger number of assets and vulnerabilities.

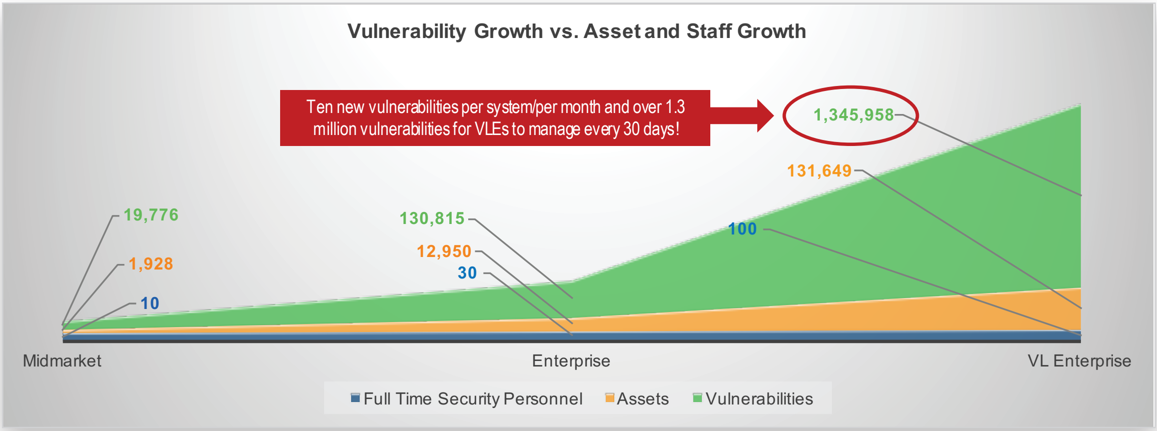

Figure 1: Growth of vulnerabilities versus assets and staff in midmarket to very large enterprises

This creates a much larger attack surface for ITOps, DevOps, and SecOps to maintain. In addition, the same research identified that 79 percent of organizations were overwhelmed with the volume of threat alerts they received.

It is unlikely that the number of threats or vulnerabilities will go down. Everyone is still being expected to do more with less. Budgets are currently healthy, but there are not enough people to do the work. The only way to successfully compensate for a lack of personnel is through improved automation.

Automation and integration go hand-in-hand. To fully automate a process, various technologies must be integrated. Be sure to delineate the technologies and systems used in IT and compare those with the out-of-the-box integrations and the vendor roadmap for the future to determine how well the system matches for an imbedded technology base.

[1] EMA, “A Day in the Life of a Security Pro”
[2] EMA, “A Day in the Life of a Security Pro”

6. Operate as a Force Multiplier

Human capital is often a gating factor in security today. The tool selected should be able to deliver pertinent information to create context for effective prioritization, thus empowering lesser-skilled team members to make decisions at a functional level higher than their skill level would otherwise dictate. This also sets the foundation for an operational best practice. The analysts will learn faster while becoming more accurate, more productive, having fewer false starts and delays on investigations, requiring fewer escalations, and delivering faster remediation and mitigation.

7. Produce Appropriate Metrics and Reporting

Working in a programmatic fashion, each level of the business—from frontline techie to board-level executive—requires different information to effectively do their job. Executives are strategic and need a high-level view to make decisions on the program status to reduce cyber risk. Middle management spans tactical and strategic processes. They need clarity on issues to judge their effect on organizational risk, determine how to assess recommendations, and assign resources needed to address those issues. Techies need details by asset to determine prioritization and approaches for remediation/mitigation strategies and make recommendations based thereon.

Given all of these requirements, it is imperative that the tool has an in-depth scoring model that provides high accuracy for creating and maintaining the proper metrics and reporting. Rating systems like NVD, CERT, vulnerability management tools, and even CVSS make severity and prioritization decisions with only pieces of the valuable information available. To make a well-informed decision, each piece of information those tools have should be merged with other pertinent information into a single foundational record. Other examples of data points include threat data like overall activity using the threat, active exploits, and available weaponization. The layer on top of that includes the proliferation of a vulnerability in the environment, the business criticality of susceptible systems and applications, and the accessibility of those from the Internet and by anonymous internal or external users, as well as any other compensating controls and detection systems in place.

8. Provide Platform Scalability and Performance

As shown in Figure 1, the larger the organization, the larger the number of threats and vulnerabilities operation teams must deal with. This would also intuitively reveal that the tools the teams need to manage that program would have to scale to meet the greater number of assets, inputs, queries, and issues to be tracked. Risk management systems tend to be in place for many years. When looking at a platform, evaluate it for not only what a company has today, but for what they expect in five years or more.

9. Support Data Compartmentalization

Whether for compliance, privacy, least privilege, or other organizational controls or requirements, the tools chosen must offer the ability to control and mange access to data. This should include role-based access controls for different functional activities and underlying data controls in case the organization needs to actually control the underlying data. This could be necessitated by compartmentalization needs by customer/client, agency, department, or team. If the capability is there, the organization can meet any future internal restructuring or client delivery changes.

10. Simplify Collaboration

Collaboration is key to effective and efficient problem identification and remediation/mitigation. SecOps, ITOps, and DevOps are often siloed in their operations. They fail to collaborate because their tools, data, and management chains are also often siloed. EMA research[3] identified that only 47 percent of ITOps and SecOps teams work together, only 36 percent of DevOps and SecOps teams work together, and all three work together only 18 percent of the time. These teams need tools that will facilitate collaboration through tool and data aggregation, creating a central unified repository.

[3] "Integrating SecOps with IT Operations, Development, and ITSM in the Age of Cloud and Agile"

Getting all of the information to the same place allows teams creating a single workflow to address multi-team collaboration required to improve threat identification and prioritization and accelerate remediation or implementation of mitigation strategies for compensating controls. Creating a closed-loop validation system as part of collaboration will ensure each action is completed accurately and in a timely manner.

EMA Perspective

Threat and vulnerability management forms the basis of risk management, which is a crucial tool for organizations to manage resources and control losses. To be successful, management teams need the right data in a timely fashion. Having too little information or getting it too late for the decision-making process can have catastrophic results.

Though tool selection for any purpose is an important process, tool selection for threat and vulnerability management not only affects short-term business decisions, but also the long-term business outcomes. Managers must be engaged to understand how new tools will affect workflows. The more teams that can use a tool, the more budgets can be used to support its purchase and the greater the company value. Thoroughly investigating, documenting, and understanding business and operational requirements prior to making an investment of both money and time is crucial for optimal performance.

About RiskSense

RiskSense, Inc., is the pioneer and market leader in proactive cyber risk management. The company enables enterprises and governments to reveal cyber risk, quickly orchestrate remediation, and monitor the results. This is done by unifying and contextualizing internal security intelligence, external threat data, and business criticality across a growing attack surface. The company's software as a service (SaaS) platform transforms cyber risk management into a more proactive, collaborative, and real-time discipline.

The RiskSense platform embodies the expertise and intimate knowledge gained from real-world experience in defending critical networks from the world's most dangerous cyber adversaries. As part of a team that collaborated with the U.S. Department of Defense and U.S. Intelligence Community, RiskSense founders developed Computational Analysis of Cyber Terrorism against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program.

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. You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

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

3761.083018