GETTING REAL ABOUT SECURITY MANAGEMENT AND "BIG DATA"

A Roadmap for "Big Data" in Security Analytics

ESSENTIALS

This paper examines:

- Escalating complexity of the security management environment, from threats to IT environments to compliance mandates
- How to get more meaning from data already collected, by "eliminating the hay from the haystack" rather than "looking for the needles"
- The combination of infrastructure, analytic tools, and threat intelligence needed to drive business value from Big Data

It's an exciting yet daunting time to be a security professional. Security threats are becoming more aggressive and voracious. Governments and industry bodies are getting more prescriptive around compliance. Combined with exponentially more complex IT environments, security management is increasingly challenging. Moreover, new "Big Data" technologies purport bringing advanced analytic techniques like predictive analysis and advanced statistical techniques close to the security professional.

Given the state of today's security systems, most organizations are a long way from using these types of advanced technologies for security management. Security professionals need to get more value from the data already collected and analyzed. They also need a better understanding of both current issues and impending challenges related to data. Starting with a foundational set of data management and analytic capabilities enables organizations to effectively build and scale security management as the enterprise evolves to meet Big Data challenges.

TODAY'S SECURITY LANDSCAPE LEAVES NO ROOM FOR AD HOC SECURITY

When dealing with "Big Data," the volume and types of data about IT and the business are too great to process in an ad hoc manner. Moreover, it has become increasingly difficult to secure meaningful information from the data being collected.

Despite significant investment in information security, attackers appear to be getting the upper hand. According to the Verizon Data Breach Investigations report (2012), 91 percent of breaches led to data compromise within "days" or less, whereas 79 percent of breaches took "weeks" or more to discover.

There are a number of factors that explain this:

- Attackers are becoming more organized and better funded. But while attacks have become dynamic, defenses have remained static. Today's attacks are designed to exploit the weaknesses of our user-centric, hyper-connected infrastructures.
- IT-enabled organizations continue to grow more complex. Organizations now demand much more open and agile systems, creating incredible new opportunities for collaboration, communication, and innovation. This also results in new vulnerabilities that cyber criminals, "hacktivist" groups, and nation states have learned to exploit.
- Compliance is even more far reaching. Regulators and legislators are getting more prescriptive. Companies, particularly those with multiple lines of business or international operations, have an increasingly hard time keeping track of current controls that are in place, controls that are needed, and how to ensure controls are being managed properly.

The combined effect of these factors in IT environments makes security management much more complex, with many more interdependencies and a wider scope of responsibility. As more business processes become digitized, security teams have both the opportunity and the challenge to collect and manage more data. Investments are increasingly made in log management, vulnerability management, identity management, and configuration management tools. However, breaches continue to happen, causing more disruption and expense than ever.

THE THREE FOUNDATIONAL CONCEPTS OF BIG DATA IN SECURITY MANAGEMENT

A true "Big Data" strategy for security management must encompass all of three aspects – the infrastructure, the analytic tools and intelligence – to properly address the issues at hand.

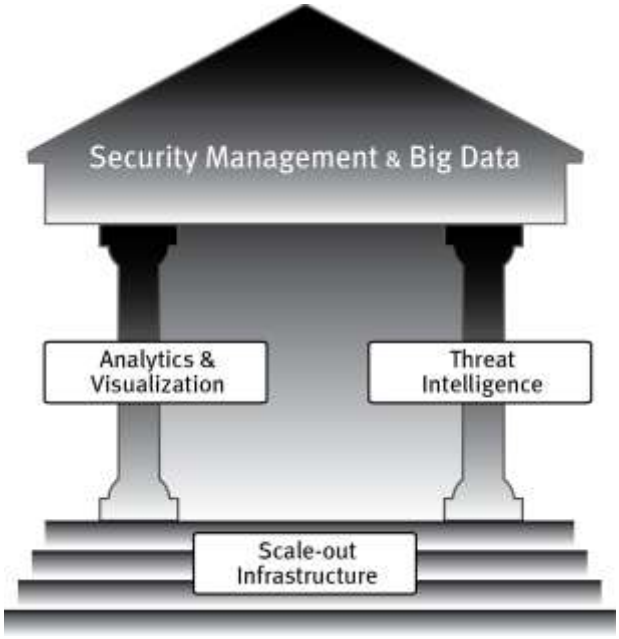

Figure 1. The pillars of Big Data in security management

To extract value from data being gathered, drive efficiency into threat management activities, and use compliance activities to drive decision making, security teams need a to take "Big Data" approach to security management. This means having:

- An agile "scale out" infrastructure to respond to the changing IT environment and evolving threats. Security management needs to support new business initiatives that impact IT, from new applications to new delivery models like mobility, virtualization, cloud computing, and outsourcing. The security management infrastructure must be able to collect and manage security data on an enterprise scale, scale to what today's enterprises demand, both physically and economically. This means "scaling out" rather than "scaling up", since centralizing all this data will be practically impossible. Also, the infrastructure needs to extend easily to adapt to new environments and readily evolve to support the analysis of evolving threats.
- Analytics and visualization tools that support security analyst specialties. Security professionals require specialized analytic tools to support their work. Some analysts require tools to facilitate basic event identification with some supporting detail. Managers may require only high-level visualization and trending of key metrics. Malware analysts need reconstructed suspect files and tools to automate testing of those files. Network forensics analysts need full reconstruction of all log and network information about a session to determine precisely what happened.
- Threat intelligence to apply data analytic techniques to the information collected. Organizations require a view of the current external threat environment in order to correlate with information gathered from within the organization itself. This correlation is key for analysts to gain a clear understanding of current threat indicators and what to look for.

"Big Data" does not equate simply to "lots of data." It demands significantly more intelligent analytics to spot security threats early on, with the infrastructure to collect and process data at scale.

"BIG DATA" DRIVES EFFICIENT, PRODUCTIVE SECURITY

Successful security management for "Big Data" requires a system that can extract and present key data for analysis in the quickest and most effective manner.

Figure 2. Requirements for a security management Big Data system

Security organizations today need to take a "Big Data" approach, including understanding adversaries, determining what data they need to support decisions, and building and operationalizing a model to support these activities. When referencing "Big Data" in this context, this is about building a foundation for useful analytics, rather than running headlong into an advanced data science project. Successful "Big Data" systems for security organizations need to:

- Eliminate tedious manual tasks in routine response or assessment activities. The system needs to reduce the number of manual, repetitive tasks associated with investigating an issue – like toggling between consoles and executing the same search in five different tools. While these tasks will not be eliminated overnight, the system should consistently reduce the number of steps per incidents
- Use business context to point analysts toward highest impact issues. Security teams need to be able to map the systems they monitor and manage back to the critical applications and business processes they support. They need to understand the dependencies between these systems and third parties, like service providers, and understand the current state of their environment from a vulnerability and compliance standpoint.
- Present only the most relevant data to analysts. Security professionals often refer to "reducing false positives." In reality, issues are usually more nuanced than false versus true. Rather, the system needs to eliminate "noise," and provide pointers for analysts to hone in on the most high-impact issues. The system also needs to provide supporting data in a way that highlights what are likely the biggest problems and why.

- Augment human knowledge. The system can help the analyst spend time analyzing the most critical items. This includes providing built-in techniques for identifying the most high priority issues, as well as current threat intelligence that uses those techniques to identify the latest tools, techniques, and procedures in use by the attacker community.
- See 'over the horizon.' Defense against modern threats is a race against time. The system needs to provide early warning –and eventually predictive model - marrying external threat intelligence with internal situational awareness to move the security team from passive defense to active defense and prevention.

SECURITY ANALYTICS: A STAGED APPROACH FOR "BIG DATA"

While advanced techniques like predictive analytics and statistical inference will likely prove important techniques in the future, it is important for security teams to begin by focusing on the basics, taking a staged approach.

- Start by implementing a security data infrastructure that can grow with you. This involves implementing an architecture that can not only collect detailed information about logs, network sessions, vulnerabilities, configurations, and identities, but also human intelligence about what systems do and how they work. Although you may start small, the system needs to be based on a robust, distributed architecture to ensure scalability as your requirements evolve. The system must support logical domains of trust including legal jurisdictions, as well as data for business units or different projects. The system needs to be able to manipulate and pivot on this data quickly and easily (e.g., show all logs, network sessions and scan results from a given IP address and its communication to a production financial system).
- Deploy basic analytic tools to automate repetitive human interactions. A nearer-term goal is often to create a model that correlates information visually to reduce the number of steps a human would need to take to gather all that information into one view (e.g., show all the logs and network sessions involving systems that support credit card transaction processing, and that are vulnerable to an attack seen in other parts of the business).
- Create visualizations and outputs that support major security functions. Some analysts will only need to see the most suspicious events with some supporting detail. Malware analysts will need a prioritized list of suspect files and the reasons why they are suspect. Network forensics analysts will need detailed results of complex queries. Others will need to review scheduled compliance reports, or general reports used to spot trends or areas for improvement in the system. The system also needs to be open to enable another system to access data and use it to take an action against an attacker, like quarantine them or step up monitoring of what they are doing.

Figure 3. Steps for implementing Big Data in security management

- Add more additional intelligent analytic methods. Only at this point should more complex analytics can be applied to the data in support of these roles. These analytics might include a combination of analytic techniques, such as defined rules to identify likely bad/known good behavior. It may also incorporate more advanced behavioral profiling and baselining techniques that deploy more advanced statistical techniques, like Bayesian Inference or predictive modeling. These analytic techniques can be used together to create an "influence model" – a model that combines different indicators to "score" issues the system has identified to lead the analyst to the areas that require the most urgent attention.
- Improve the model on an ongoing basis. Once the system is up and running, it will need to be fine-tuned on an ongoing basis to respond to evolving threat vectors and changes to the organization. The system will need the ability to tweak rules tweaked and adjust models to eliminate noise, consume additional data both from inside and outside the organization, and incorporate self-learning functions to improve the overall success of the system.

The system will need to evolve and expand to respond to changes in the IT environment as new IT services and applications come online, creating a cycle of constant evolution and improvement. At each point, the system will need to leverage external intelligence as inputs to the model.

That means the system will need to have an automated way to consume external feeds from threat intelligence sources; structured information including blacklists, rule or queries; unstructured intelligence including pastebins, Twitter feeds or IRC chats; and intelligence from internal message boards or notes from internal calls or meetings. The system must also be able to facilitate collaboration around shared knowledge. The system should share query results or unstructured intelligence either publicly, or in a controlled fashion with mutually trusted communities of interest or on a "need-to-know" basis.

FOUNDATIONAL INFRASTRUCTURE PAVES THE WAY FOR MORE SOPHISTICATED TECHNIQUES

Security teams will greatly increase their likelihood of success in implementing "Big Data" in security by focusing on first creating a scalable architecture and deploying tools eliminating non-value added tasks. This will give "quick wins," provide a solid platform and free up staff to concentrate on deploying and managing more complex analytic tools. Done properly this will:

- Increase the efficiency of security analysts. The number of "issues per shift" analysts can deal with can be increased from a few to a dozen and beyond.
- Reduce attacker free time and thus the impact of threats on the business. Analysts will be more automatically drawn to those issues which are most likely to cause problems and shut them down before they affect the business adversely.

Without this foundation or a clear, concrete objective in mind, a Big Data initiative could easily flounder and not bring any of the expected gains.

RSA SECURITY MANAGEMENT: A FIRM FOUNDATION FOR INFRASTRUCTURE, ANALYTICS, AND INTELLIGENCE

RSAs Security Management portfolio provides customers with:

- Comprehensive infrastructure visibility. RSA provides a proven infrastructure with the ability to collect all types of security data, at scale and from all types of data sources. This gives analysts a single place to view data about advanced threats and user activity from data gathered directly from the network or from key systems. RSA's infrastructure also provides a unified architecture for real time analytics as well as near time and historical query. This provides a comprehensive approach to real-time alerting, investigative analysis, metrics and trending and historical retention and archiving.

- Agile analytics. The RSA platform gives analysts the tools to perform rapid investigations – including intuitive tools for investigation presented for rapid analysis, with detailed drill down and incorporation of business context to better inform the decision making process. RSA's approach provides the ability to hone in on the most suspicious users and endpoints connected to your infrastructure and tell-tale signs of malicious activity through signature-free analytics. Full session replace provides the Ability to recreate and replay exactly what happened.
- Actionable intelligence. Threat intelligence provided by RSA helps security analysts get the most value from RSA products by incorporating feeds of current threat information. RSA's threat research team provides proprietary intelligence from a community of security experts, automatically built into our tools through rules, reports, parsers and watchlists. This allows analysts to gain insight into threats from data collected from the enterprise, and prioritize response actions by incorporating information from the business showing relationship between the systems involved and the business functions they support.
- Optimized incident management. RSA products help security teams streamline the diverse set of activities related to preparedness and response, by providing a workflow system to define and activate response processes, plus tools to track current open issues, trends and lessons learned. Industry leading services to help prepare, detect and respond to incidents. The platform integrates with the RSA portfolio and third party tools to exchange information with the wide range of tools needed to identify and handle incidents and streaming compliance management.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

RSA EMC²