ArcSight

How to Select a SIM Vendor:

A Guide to Evaluating Security Information Management Solutions

top10

The Importance of a Security Information Management (SIM) Solution

- Security Information Management (SIM) is the centerpiece of any strong security management program. With the number of worms, viruses, hackers and malicious insiders growing each day, organizations are adopting best-of-breed security infrastructures to protect themselves. But by pouring millions of dollars into a wide array of security solutions like antivirus gateways, firewalls and intrusion detection systems, organizations have exposed themselves to a new problem: crippling complexity.
- Without intelligent centralized management and automated correlation, many enterprises have found that their security programs have evolved into a complex patchwork of disparate systems that generate an overwhelming flood of data but offer little visibility into true threats and attacks. While this was acceptable in the past, due to increasing regulatory compliance pressures and an ever-evolving threat landscape companies now are adopting SIM technology to centrally manage information risk and protect critical IT assets.
- When researching the SIM market, however, security professionals may find it difficult to wade through vendor marketing messages and pinpoint significant differentiation. This should come as no surprise, especially as there are no standard definitions for such terms as “events per second,” “vulnerability correlation” and “asset criticality.” This allows some vendors to boast performance numbers that may be inaccurate or misleading. As a result, organizations are finding that their SIM implementation may not achieve the value originally promised.
- **ArcSight has developed the following list of evaluation best practices to assist organizations in making the right SIM choice for their environment. This list has been compiled directly from the experiences of customers who have implemented SIM solutions. These practices should be used as an integral part of your evaluation and selection process.**

10

When in Doubt, Engage in a Proof of Concept

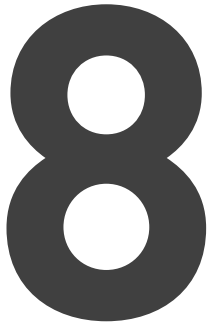
SIM vendors can provide a dizzying array of features during product demonstrations that sound and look great, but the big “Aha!” only happens when you can use the product with live information coming in from your own security infrastructure. A live trial helps organizations avoid serious pitfalls that can arise from relying on canned demonstrations to determine the effectiveness of the product. As a customer, it's your right to ask for a trial, typically something that takes only a few days, and in the end it is well worth the extra effort.

Research Vendor Viability

The SIM market has grown significantly over the past three years. Beyond basic company viability, look for a vendor that has a technology built specifically for the enterprise SIM market, has a proven track record with partners and can address your changing business needs. In addition, check to make sure that the SIM vendor has customers in your market and that they understand your unique business needs.

Know the Importance of Vendor Independence

Vendor independence is critical to effectively manage and gain value from a best-of-breed infrastructure and to avoid conflicts of interest. Security device vendors that also offer SIM products may not be able to maintain the required partnership with competitors and ensure up-to-date, workable integration support.



7

Demand a Flexible and Agile SIM Solution

Security is about staying ahead of the game, so your SIM solution needs to be very flexible in order to grow with your organization. A universal reason for purchasing a SIM solution is to tame the data overload problem. But as organizations gain a consolidated view of their logs, true management use cases emerge. These include the ability to customize multiple areas in the product-such as data collection policies, correlation rules and associated actions, workflow, dashboards, reporting and investigation tools-to drive maximum efficiency. For example, when a new policy is drafted or a new threat emerges, organizations will derive strong benefit from immediately tuning their SIM to identify policy violations or occurrences of the new threat. During the proof of concept, work with vendors to gain a strong understanding of how to customize each resource.

6

Understand the EPS Argument

Because there is no standardization in SIM terminology, the often argued "events-per-second" (EPS) number means very little as to the true performance, effectiveness and extensibility of the product. These numbers are sometimes based on simple collection of raw logs, especially when the SIM solutions provide little or no intelligence or pre-processing by the agents and event collectors before these events reach the SIM manager. A truly effective enterprise SIM will be able to demonstrate effective collection and processing of data at highly scalable enterprise-class rates. These enterprise class rates are directly dependent on a number of factors including: event rate pre and post filtering and aggregation; extension and use of analytic capabilities; real time and historical information management requirements; and the breadth of the user base. Based on these factors, qualifying enterprise scalability does not take the form of a simple EPS number, but rather is derived from a set of factors based on the operational requirements, data inputs and usage of the SIM technology.

five

Understand the Difference between a Security Appliance and an Enterprise Security Management System

SIM appliances have been lauded for their ease of deployment. SIM software solutions have been praised for their enterprise feature sets, including workflow, customization and extensive threat identification capabilities. Ease of deployment requirements should be balanced with the requirements of an extensible feature set to obtain a solution that can continually grow with your organization.

4

Know the Meaning of Correlation

Like many SIM terms, the word correlation lacks a standard definition. SIM technologies that claim to perform asset, vulnerability and event correlation achieve this with varying methodologies and degrees of success. Issues to research include:

How does the product perform cross-device correlation? Cross-device correlation is key to deriving true analytic value from a SIM solution. Products that do not offer a central categorization language to map device events to a common taxonomy cannot be used in extensive cross-device categorization. Without a categorization language, users must remember the input language for each device type, leading to lack of efficiency and overly complex correlation rules.

How does the product derive priorities? All SIM products derive priorities differently. Make sure prioritization can be determined by the severity of the attack, the criticality of the asset and the vulnerability status of the target relative to the specified attack. It is also important to determine if priorities are adjustable. After implementing a SIM, organizations will need to tune prioritizations based on unique factors such as known false positives and high-risk attacks.

How does the product process vulnerability information? Most SIM vendors claim to support vulnerability data, but the breadth, depth and applicability of integration can vary. Key aspects in determining the value of integration include automated population of assets with discovered vulnerabilities, the ability to use vulnerabilities in correlation rules for real-time risk management and application of the system's vulnerability status into each event's priority score.

How does the product incorporate asset value? Incorporation of asset value-the business and technical characteristics of a system, such as Sarbanes-Oxley, mission critical, confidential-is performed with varying degrees of extensibility. Determine how the vendor populates and leverages business and technical asset categories in its correlation and prioritization capabilities. Extensibility is also important to melding the product's analytics to your organization. Ask your vendor to create a custom asset category and associate risk-relevant actions for attacks against that asset.

How does the product track and escalate threat levels? With millions of events per day, the ability of a SIM to track activity and escalate based on successive attacks is critical to identifying the most dangerous threats.

Can the product perform correlation on both real-time and historical data? While many SIMs provide the ability to correlate information in real time, it is also important to correlate historical information. This allows you to easily identify newly discovered threats that may have unknowingly occurred in the past. Additionally, one feature for historical correlation capability should allow you to test the accuracy of newly created correlation rules.

Can the product automatically discover unknown threats? While correlation rules can find known threats, SIM customers should inquire about additional analytics that can analyze the incoming data and build new rules for the automatic discovery of unknown threats.

How does the product deal with time in the correlation process? Time is an important aspect of effective correlation. Ensure that your vendor correlates information based on the time the event was generated and also provides the ability to correlate based on the time sequence of events. This will ensure that no attacks are missed due to transmission latency and will also allow the SIM to deliver accurate threat identification for multi-stage sequenced attacks.

How easy is it to alter, tune and author new rules? Enterprise security teams will derive a long lifetime of value out of a SIM product if the interface allows for intuitive, customized tuning and authoring of correlation rules. Conversely, the lack of a robust authoring system will lead to significant roadblocks.

three

Look Carefully at Product Support Programs

SIM users typically face serious limitations including the need to integrate data that is not supported by the SIM vendor. Be wary of vendors that support only a limited number of products or that list support as “under development.” This is a sure sign the vendor does not have an agile agent support process. Ask vendors for information about their agent development process, strength of partnerships with supported product vendors and number of supported products. Also evaluate the vendor's custom agent development capabilities. Ask about custom agents that are being used at customer sites and the number of customers that are currently developing their own agents with the provided toolkit. In addition, validate that traditional agent features are available for custom developed agents. Some vendors only offer simple parsers under the guise of a complete agent development environment. This simplification has been known to severely degrade custom developed agent performance and features.

two

Capture and Normalize All Event Data

Simply put, normalization is the process of rearranging data relationships so the data will be easier to store and retrieve. This allows your data to be used for high-performance, real-time correlation and effectively queried for reporting. Most SIM products do not capture and normalize all relevant information. Rather, they only provide you with the most commonly used data, such as source IP, destination IP and time and event description. The remaining event data is truncated or wrapped into a string that cannot be efficiently used in correlation. This is a serious problem since data is not available for audit and real-time threat management—massively limiting the value of the SIM.

1

Define Operational Requirements

The value of any SIM product is directly related to the data that is input into the system; the meaning the system can derive from the data; and the actions the system is programmed to take. Checklists can be useful, but they must be tailored to reflect the operational requirements of the organization. To effectively refine checklists, you must first determine the primary use cases for the product. Common use cases include:

Support for 24x7 security operations center. To ensure effective prioritization and response to issues, security operations must have continuous, 24x7 situational awareness with concrete workflow. SIM systems for the SOC need to provide best-in-class flexibility and customization features to ensure the organization can shift focus to address emerging threats. In addition, because a significant cost of maintaining a SOC involves staffing expenses, the system that provides the greatest accuracy for threat identification will produce the largest return on investment. In addition, validating the systems ability to continuously monitor and troubleshoot performance is critical to maintaining seamless 24x7 support for the SOC.

Using the SIM as a "virtual SOC." This option is for organizations whose budgets do not allow for the implementation of a 24x7 security operations center or organizations that have a more tolerant risk profile. These organizations choose to use their SIM as a virtual SOC to provide accurate threat identification and alert staff to any pressing issues. Virtual SOCs generally have a small staff, which means their SIM solution needs to be highly customizable to avoid late- night pages from false alarms. Since virtual SOCs are not a 24x7 operations, companies need a product that offers both real-time analysis for instant threat identification and historical analysis capabilities for review of historical logs during normal business hours.

Audit and compliance capabilities. Audit and compliance requires the integration of a largely different set of data sources, such as operating systems, mainframes, databases and identity management applications. Ensure that your vendor offers the ability to build customized agents for devices to collect from non-traditional sources such as proprietary applications that are not immediately supported. While some SIM products offer templates for compliance reporting, it is even more critical for the product to categorize relevant assets that should be audited, and offer significant customization and correlation capabilities to draw out information relevant to your defined compliance program.

Insider threat. This use case requires internal devices to monitor trusted user activity and identify suspicious or unauthorized use of confidential information. Even more than audit and compliance, this scenario demands comprehensive analytics and the integration of non-traditional data sources. Key SIM requirements are the proven ability to integrate with applications, databases, operating systems, identity management and physical security systems that assist in profiling trusted user activity and the flexibility to baseline and analyze based on behavior.

Get Started Today

ArcSight offers an enterprise-class security information management solution that can cost-effectively address a broad range of requirements. We welcome you to test our product head-to-head against any on the market. Our account executives can provide details that address your specific criteria, show you a product demo and provide a trial for an in-depth look into our solution. It's no coincidence that leading publications recognize ArcSight ESM for its superior flexibility, functionality, scalability and ease of use. For help with your enterprise security management needs, contact ArcSight at info@arcsight.com, call (408) 864 2600 or visit us online at www.arcsight.com.

now

About ArcSight

ArcSight, the recognized leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading global companies across all verticals—and more than 20 of the top 30 U.S. federal agencies.

ArcSight, Inc.
5 Results Way, Cupertino,
CA 95014, USA
Email: info@arcsight.com
Phone: 408 864 2600