Security Analytics Tools Buyer's Guide

Your expert guide to security analytics

In this e-guide

Arbor Networks Pravail Security Analytics: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan examines the features of Arbor Networks' Pravail Security Analytics, which employs full packet capture to detect various signals of an attack for enterprises.

When it comes to network security, the old adage that a good offense is the best defense should be reframed as good analysis is the best defense. Attackers are continually adapting to the security controls enterprises put in place. In spite of all the technical controls an organization may deploy, humans are the perpetual weak link in security defenses. It takes just one rushed executive skimming email and clicking on a spear phishing lure to give an attacker a way into a company's systems. If we start with the assumption that our systems will be attacked -- and they will be compromised at some point -- then it logically follows that we need a means to detect such attacks and contain them as quickly as possible.

Pravail Security Analytics from Arbor Networks is designed for the way attackers function. Deployed as an appliance or a cloud service, the monitoring and security analytics platform employs full packet capture to detect various

In this e-guide

signals of an attack. For example, an attacker may use a phishing attack to trick a user into downloading a remote control program, which is then used to gather data on an organization's network and devices. The initial attack and the subsequent information collection stage leave different traces in the history of network traffic.

Full packet capture enables the analytics programs to detect and correlate these distinct patterns. This yields large volumes of data that lead to insight only with proper analysis, reporting and visualization tools.

Integrated view of events

The Pravail Security Analytics platform, for example, creates a timeline of events so analysts can correlate multiple steps in a single attack. Analysts can also use timelines to recreate the sequence of events in an attack to help understand how the attack unfolded. Visualization is a must-have feature when dealing with large volumes of data that lends itself to analysis from different perspectives. Analysts may want to view some data based on target or location at some times, and in other cases they may need to view data on multiple attacks from the attacker or attack type dimension.

Another benefit of full packet capture is the ability to analyze historical data for signs of an earlier attack. Major security vendors continually collect global intelligence about the state of cyberthreats; the Pravail Security Analytics

product leverages threat intelligence data from Arbor Network's Active Threat Level Analysis System. Information about a new mode of attack may come to light only after it has been in use for some time. The product uses processes to analyze previously collected data and search for new attack patterns.

Deployment

Pravail Security Analytics uses a collector and controller approach. Enterprises can deploy multiple collectors to multiple locations to ensure high speed collection of data and scale up storage to meet network demands. Collectors perform real-time analysis on data streams to search for known attack signatures. Controller appliances centralize management of collectors and analysis of data provided by collectors. The controller also supports the user interface to the application, and allows for querying of metadata and storage of deep packet analysis results. Pravail Security Analytics can be deployed three different ways: as a combination of controller and collector appliances for on-premises environments, as a cloud service (Pravail Security Analytics in the Cloud), or with an on-premises collector and a cloud-based controller.

In this e-guide

Pricing and support

Pravail Security Analytics is available for a free demo or 30-day trial; more information on enterprise pricing can be obtained by contacting the company. Support services include access to professional services that can provide dedicated support engineers, resident engineers as well as staging and implementation assistance. Support contracts offer 24/7 access to technical support, a customer support portal and software updates. Arbor Networks works with service delivery partners, that can provide additional information on cost, licensing and related services.

Conclusion

Constant and comprehensive monitoring of network traffic is an increasingly important tool for security analysts. Pravail Security Analytics uses a distributed set of collectors and controllers to accumulate, analyze and store network data. It also provides real-time analysis as well as visualization and analysis from multiple dimensions. The ability to loop through previously collected data and review for newly discovered attack signatures is especially important for applying the latest intelligence to events, even those that happened in the past.

Organizations that need the benefits of security analytics but may not have sufficient staff in house can benefit from working with Arbor Networks and its partners. Companies in regulated industries that need to protect private and confidential information may also benefit from a comprehensive security analytics platform such as Arbor Networks' offering.

Next article

In this e-guide

Blue Coat Security Analytics Platform: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan takes a look at the Blue Coat Security Analytics Platform, which is designed to capture comprehensive network information and apply targeted security analytics.

Information security is more than just *block and tackle* operations to stop malicious activity. As attacks become more sophisticated, it is important to have security analytics tools that can collect information about activities on an organization's network, servers and other devices. The Blue Coat Security Analytics Platform is designed to capture comprehensive network information and apply targeted security analytics and analysis on that traffic. Blue Coat describes it as a security camera for your network. The apt analogy highlights the fact that if malicious traffic traverses an organization's network, it will be recorded.

Analytics features

The Blue Coat Analytics Platform functions with the assumption that all network data is potentially valuable. IT collects data from the data link layer -- Layer 2 in the OSI network model -- which addresses data movement over a physical

In this e-guide

network, up to the application layer -- Layer 7. This comprehensive approach to data collection means that regardless of the layer used in malicious activity, traces of that activity will be captured. The Blue Coat Security Analytics Platform also offers visibility into SSL encrypted traffic.

The product classifies and stores data to enables both real-time analysis and after-the-fact forensics -- the analytics platform integrates with Blue Coat's Incident Response and Forensics product. The platform also used deep packet inspection to perform application classification services for more than 2,500 recognized applications, which allows admins to search for and identify programs based on various types of metadata.

Some of the newer features added to the Blue Coat Security Analytics Platform include anomaly detection, which conducts a statistical analysis on data related to anomalous and potentially threatening behavior; dynamic filtering, which allows admins to separate and prioritize different types of network traffic that are deemed less likely to carry threats, such as video conferencing streams; and SCADA support for industrial control systems.

Dashboard and alerts

Collecting too much data can be as bad as not collecting enough if an organization cannot find the information it needs when it needs it. The Blue Coat Security Analtyics Platform includes a dashboard for displaying current activity

and status information. It's also used for some configuration management operations. The dashboard is useful for getting a quick, high-level overview of the status of the analytics platform.

The system also generates alerts that can be delivered to system administrators using multiple delivery methods, including SNMP, syslog or SMTP. In addition to the main product dashboard, Blue Coat recently added a new alerts dashboard; the platform's web interface defaults the Alerts Management Dashboard and offers administrators contextual history of alerts along with their respective threat scores.

Deployment

The Blue Coat Security Analytics Platform may be deployed as a software application, a virtual appliance or preconfigured appliance. Customers can select necessary storage according to their needs. Since all network traffic is captured, it is important to have a data retention policy in place. Some organizations may want to preserve virtually all data for extended periods of time, but that is not a viable option for everyone.

Organizations can contact Blue Coat for more information on enterprise licensing and support plans. Enterprises looking for dedicated support services should review information on Blue Coat's Proactive Services, which provides a single point of contact for support needs.

Conclusion

Network traffic carries the traces of virtually all malicious activity, from malware infection to data theft. Blue Coat Security Analytics Platform targets network traffic and collects and classifies this valuable data. Customers can choose from three types of analytics tools for web, mail and file-specific threat analysis. Comprehensive data collection is essential to enable detailed forensic studies and real-time detection, but it can also lead to long-term storage challenges. Before deploying a tool like Blue Coat Security Analytics Platform, carefully analyze your storage requirements, budget and data retention policies.

With the flexibility to choose only the modules you need, Blue Coat Security Analytics will meet the needs of a wide range of organizations, especially those that have other security or management tools that provide some web, email and file controls. The Proactive Services offering may be especially helpful for businesses that want continuity in support personnel.

Next article

In this e-guide

Click Security Analytics: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan takes a look at Click Security's collection of tools focused on key areas of security analytics, including profiling, investigating and analyzing threats.

Information security is no longer just about implementing a set of best practices or point products like antimalware, network configurations and authentication mechanisms. All of those things are still required, of course, but they are no longer the end of the story. Organizations need the ability to analyze what is happening on their networks in real time.

This starts with assuming that some element of their security controls will be compromised. Enterprises today need to be looking for signs of that compromise. This is where security analytics comes in. Click Security is a company that provides a set of analytics tools focused on areas of security analytics, including profiling, investigating, responding and analyzing actor behaviors within an organization's network.

These tools allow infosec professionals to collect and analyze information about events on the network, identify particularly suspicious activity and then take action to mitigate potential risk of those activities. Here's a closer look at the tools within the Click Security Analytics suite.

In this e-guide

Click Security Profiler

Click Security Profiler provides an interface for analyzing both actors and events within an infrastructure. These tools collect data from multiple sources, including network traffic, logs and file events. The Profiler uses event correlation to group discrete events into higher level logical collections. It also provides a risk ranking of actors and events to help front line security analysts assess the relative importance and priority in the face of multiple threats.

Click Stream Security Investigator

Click Stream Security Investigator is a tool for viewing attacker activity at a higher level of aggregation than provided by the Profiler. With the Investigator, events are consolidated and visualized at a level that allows analysts to better assess the key events in the attacker's progress. This sequence of events, known as the kill chain, identifies key events in the progression on an attack. Attacks typically start with reconnaissance, followed by delivery of some kind of attack vector, installation of command and control tools and eventually exploitation of the capabilities that attacker has established. Understanding this typical course of events in an attack, and being able to identify them from network, log and other data is a key to deploying countermeasures to mitigate the risks of an attack.

In this e-guide

The Responder

The Responder is an application that applies lockdown policies in response to events. The application includes a graphical user interface displaying key metrics about the number of times policies have been triggered.

Actor Analytics Framework

The Actor Analytics Framework is a central hub for collecting and analyzing security related event data. The framework is designed to collect data on security events, analyze those events with emphasis on actor-oriented activities and incorporates threat intelligence to create a broad view of the actors and event contexts.

Click Security's Actor Analytics Framework also implements kill chain profiling and intelligence management. It utilizes in-memory analytics techniques to examine incoming events and links them to previous events by the same actor. Third-party intelligence data is added to context information collected from Click Security tools.

In this e-guide

Prior to being acquired by Alert Logic, Click Security introduced new functionality for its analytics suite, including Actor Context Graph, an interactive visualization feature designed to help admins correlate events with related data.

Pricing and support

Click Security offers support services online and over the phone. For those looking for direct support, Click Security works with partners as well. Contact parent company Alert Logic for additional details on pricing, licenses and support.

Conclusion

The Click Security Analytics tools address key information gathering and analysis stages needed to detect, understand and respond to a cyberattack. In spite of security best practices, the state of today's information security landscape leaves many with the feeling it is only a matter of time before our systems are attacked, if they have not been attacked already. Security analytics tools such as Click Security's Actors Analytics Framework are needed to respond to the kinds of attacks that are all too common today.

Security analytics tools, such as Click Stream, generate valuable information but are not standalone tools, such as malware scanners. Organizations with dedicated information security professionals who understand attack strategies and methods will get the most from Click Security. The combination of tools, such as Profiler, Responder and the Actor Analytics Framework, create a complete security analytics solution. It's important to note that Click Security was acquired by Alert Logic last spring, and Alert Logic said its intention was to "quickly integrate the Click Security employees and technology" into its Cloud Defender platform. This could change how Click Security Analytics is sold and supported in the future.

Next article

In this e-guide

FireEye Threat Analytics Platform: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan takes a look at the FireEye Threat Analytics Platform, a cloud-based security analytics product that offers threat detection and contextual intelligence.

Information security professionals could easily suffer information overload from the network, device and application event data that is generated in today's IT operations. They can't avoid or prune the volume of data either. Why? Because advanced attacks often require data from multiple sources to detect. As a result, InfoSec professionals are turning to security analytics platforms, such as the FireEye's Threat Analytics Platform, to help collect, analyze and prioritize security event data.

Real-time threat detection

The FireEye Threat Analytics Platform applies real-time analysis to streams of network and log data to identify potentially malicious activity. The system uses a combination of expert rules, analytics and threat intelligence data to classify security events. When a potential problem is identified, the security analytics platform generates an alert to notify security administrators.

In this e-guide

The FireEye Threat Analytics Platform is designed to process and analyze up to 80,000 events per second. By analyzing low level security events and correlating activities, the threat analysis platform can help identify users and devices involved in the attack. The product offers what FireEye calls a "Sub-Second Search" capability, which allows analysts to quickly search billions of events.

Security analytics as a service

Security analytics is an increasingly important challenge, and the market for threat analytics is growing as one would expect. FireEye, however, does not take the common approach of selling software or appliances. Instead, it sells its security analytics platform as a cloud service. This has a number of advantages. There is no need to purchase, install and maintain hardware on premises. This minimizes additional demands on your network and security operations teams. It also avoids capital expenditures.

Delivering security analytics also means FireEye can have customers enrolled and using the service in a matter of hours, instead of weeks that might be needed by some hardware procurement cycles.

In this e-guide

Prioritizing security events

Given the nature of cyberthreats today, it is not surprising that security administrators are often inundated with alerts. Finding a common malware file en route to a user's email inbox is not a surprising event. It is such a common event that it, along with other common but low risk events, could distract infosec professionals from higher risk threats that demand their immediate attention.

FireEye Threat Analytics platform prioritizes alerts so security incident responders can focus on the most threatening incident at any time. It also addresses the need for workflow support, as the platform includes tools for assigning tasks and monitoring the outcome of those tasks. Responders can add their own notes and attach relevant files to an incident record to help consolidate incident information in a single source. Search tools are provided to enable retrieval.

FireEye offers four support programs: Platinum, Platinum Priority Plus, Government and Government Priority Plus. All programs offer 24/7 email, phone and live chat support while the Priority Plus offerings include direct access to senior support engineers. FireEye also provides online community forums, technical education and access to a network or partners. For additional information on pricing, contact FireEye directly.

Conclusion

Many organizations can benefit from security analytics tools, but may be held back by the need to support additional infrastructure or lack of capital funds to buy additional hardware and application licenses. FireEye Threat Analytics Platform moves security analytics to the cloud, thereby creating an option for those who would rather enter in a pay-as-you-go arrangement than invest in security software and hardware up front. Its combination of threat analytics prioritized alerting and a cloud-based service, meanwhile, is a compelling differentiator in an increasingly important market segment.

Next article

In this e-guide

Hexis Cyber Solutions' NetBeat MON: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan checks out Hexis Cyber Solutions' NetBeat MON, a security analytics monitoring appliance that leverages several open source network monitoring tools.

Businesses and government agencies are at risk of an increasing array of information security threats such data theft, malware, denial-of-service attacks and even compromise by insiders. No single security control or policy can address all threats. Instead, IT needs to deploy multiple measures. A key challenge for InfoSec professionals is to collect and integrate data on security events from the array of security controls deployed to protect assets. This is where security analytics comes in.

NetBeat MON from Hexis Cyber Solutions, is a security analytics product designed to help protect medium-sized businesses, specifically ones with multiple locations.

In a nutshell, NetBeat MON is a monitoring appliance that observes network activity within any network and its devices. Hexis presents the benefits of the product as supporting "network hygiene." That is, understanding and managing

the contents of network traffic using tools such as packet capture and analysis, network flow analysis and intrusion detection.

Combining open source tools

Hexis Cyber Solutions did not reinvent the proverbial wheel when it comes to network monitoring, but it did combine well-established open source tools to bring cost-effective, consolidated monitoring to a broader market. NetBeat MON combines the features of five open source network monitoring tools: ntop, Wireshark, Suricata, Snorby and dumpcap.

- **Ntop** is a network traffic sorting tool that supports IPv4 and IPv6. The tool allows you to sort IP traffic using multiple criteria, including source, destination and protocol.
- **Wireshark** is a network protocol analysis tool that allows for both live traffic capture and offline analysis, including voice over IP. Information captures with Wireshark can be viewed in either a GUI or the TTY-mode TShark utility, and packet lists can be assigned a color scheme to help with sorting and analysis.
- **Suricata** is a tool developed by the Open Information Security Foundation. The tool is used for monitoring network traffic, as well as providing combined intrusion detection system/intrusion prevention system functionality. Admins can also write rules to specific protocols, as opposed to receiving ports.

- **Snorby** is a network security monitoring tool built using Ruby on Rails. Reporting features include the ability to classify events into predefined or custom categories for future reports. Additionally, the tool can integrate with OpenFPC, a packet capture tool.

- Lastly, **dumpcap** is a tool for network traffic dumping. Dumpcap captures packet data in pcap-ng files, although libpcap formatting is also available. Features include customizable UIs, automated patching and remote management, as well as analysis, NetFlow and packet capture capabilities.

Deployment options

The deployment of NetBeat MON is dependent upon an organization's operation. The product requires the deployment of individual appliances at each of its locations. These appliances are either configured as a Master or a Minion unit upon setup -- the capabilities and duties of each unit follow. The Master unit will most likely be deployed at an organization's central office, allowing for centralized management of the Minions.

Each unit offers 8x DIMM RAM slots, 4 x 3.5-inch hard drive bays (hot-swappable), and an Intel i350 Dual Port GB Ethernet port. The NetBeat MON racks are built on Intel Xeon processors. See here for a full specification list.

As for purchasing and support, the NetBeat MON appliance is available only through channel partners. Single-call support is provided for one year after

purchase, after that it is $1,500 per unit per year. The Hexis support team can answer questions regarding the open source tools that make up NetBeat MON, but does not provide direct support. Hardware issues are solved by sending the malfunctioning device back for repair.

Conclusion

No business or organization is too small to be the target of malicious cyber activities. Small and midsize business with limited resources can leverage open source security analytics tools without breaking their capital expenditure budgets.

Unfortunately, unless someone on staff is familiar with the implementation details of the range of open source tools in use, then deploying and maintaining a set of well integrated applications is difficult. NetBeat MON relieves some of that burden with a consolidated package of security analytics tools that does not demand an enterprise-scale budget to pay for it.

Editor's note: *Hexis Cyber Solutions was recently acquired by WatchGuard, which may impact the NetBeat MON security analytics product line*.

Next article

In this e-guide

Juniper Networks' JSA Series Secure Analytics: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan examines the Juniper Networks JSA Series Secure Analytics product family, which provides log analysis, threat analysis and compliance reporting for larger enterprises.

All organizations face cyberthreats, but large enterprises face a particularly challenging set of problems. By their nature, larger organizations have many more devices and network points of access to secure. This creates an often unwieldy attack surface to protect.

In addition, larger organizations are often subject to regulatory compliance that requires data and systems controls across their infrastructure. They must also deal with the issue of scale. IT products and services that work well for small and midsize companies may not scale to meet the volumes of data and equipment that must be protected in a large enterprise.

Enter Juniper Networks' JSA Series Secure Analytics, a security analytics and analysis platform designed to meet the needs of larger enterprises.

In this e-guide

Analysis for multiple security domains

The JSA Series includes modules to support multiple types of security analytics and analysis. These include models to handle log analysis, threat analysis and compliance reporting.

Log analytics provides tools to collect logs from across an organization and centrally store and analyze their content. This enables both real-time alerting and forensic analysis of events that have occurred in the past.

The threat analytics module spans areas typically covered by network operations and security analytics. By collecting and analyzing information from multiple sources, the module can identify suspicious activities across a range of event types. This kind of broad analytics capability is essential for detecting advanced threats that can occur as a series of steps over extended periods of time. Threat analytics builds on the Secure Analytics platform's capabilities with regard to collecting security logs, host and application logs as well as network application flow logs.

The compliance module helps infosec professionals demonstrate enforcement of policies and procedures required by various regulations. The platform supports reporting for Payment Card Industry Data Security Standard, HIPAA and other broadly applicable regulations.

In this e-guide

Analyzing enterprise scale security data

Large enterprises must address the needs of multiple sites of various sizes and with varying types of security requirements. The JSA Series spans a range of deployment options to meet those needs. The product family is available in four different versions.

The JSA3800 and JSA5800 are appliances designed for larger enterprises, while the JSA7500 is designed for carriers and other enterprises with exceptionally large volumes of data. For lightweight deployments, the virtual appliance version may be sufficient, for example.

Because the JSA Series platform employs a distributed architecture, it is possible to start with one appliance and add others as demand grows. In addition to meeting scalability demands, appliances can be configured in hot standby mode to enable rapid failover from a primary appliance to the hot standby.

The JSA Series can be purchased directly from Juniper Networks or through a channel partner. Juniper Networks offers professional services to help with planning, building and deploying the JSA Series.

Conclusion

Security analysis and analytics is challenging, and it becomes even more difficult at enterprise scales. Attackers, meanwhile, may be willing to work slowly in order to avoid detection. And since larger organizations tend to be geographically diverse, multiple data centers and offices require security controls -- such as security analytics and analysis -- to be available to local and remote networks. Enterprises also need continuous security protection from high availability controls that will scale to meet the demands of an enterprise.

Juniper's Secure Analytics platform is designed to meet all of these needs, with components to ingest and analyze a range of data as well as supporting additional compliance requirements. While it may be more than some organizations require -- particularly small and midsize enterprises -- the JSA Series is the kind of product that large enterprises could easily turn to for security analytics and analysis.

Next article

In this e-guide

Lancope's StealthWatch FlowCollector: Security analytics product overview

Dan Sullivan, Contributor

Expert Dan Sullivan examines the Lancope StealthWatch FlowCollector, a security analytics product that ingests large volumes of data to identify suspicious activity.

The vast majority of traffic traversing an organization's network is probably benign, but what about the small fraction of traffic that isn't? How can it tell benign from malicious before it's too late? This is the challenge that has driven the development of security analytics tools such as the Lancope StealWatch FlowCollector.

Analyzing network traffic

Security analytics products are designed to collect a variety of information types, and then integrate, analyze and classify content and events to enable security and system administrators to identify potentially malicious activity. Some security analytics tools tailor their analysis to network traffic, while others incorporate diverse data from server logs and endpoint devices. The common characteristic of all security analytics products, however, is the ability to ingest large volumes of data and quickly identify suspicious activity.

In this e-guide

Like other security analytics tools, the Lancope StealthWatch FlowCollector aims to consolidate data from across the network, such as routers, switches and firewalls. It uses NetFlow and IPFIX flow data collected from firewalls, routers and other network devices to achieve its mission.

Data collected at routers is used to analyze traffic entering or leaving the network. Lancope's StealthWatch FlowCollector also considers traffic between devices on the network. This is especially important for detecting malicious activity that occurs within the network boundaries. For example, a disgruntled employee might make a copy of a database backup to take to a competitor using a laptop and storage device connected to the network. This kind of event may not leave any traces in inter-network traffic flows.

Scalability is always a consideration when capturing network traffic. A single StealthWatch FlowCollector is designed to support up to 4,000 devices generating as many as 240,000 flows per second. At peak scalability, a properly configured StealthWatch FlowCollector system can process up to 50,000 sources and six million flows per second. StealthWatch FlowCollector includes the ability to detect duplicate flow data as well.

One company's anomaly is another's norm

The concept of anomalous behavior on a network is fairly easy to understand: it is something out of the ordinary. The first job of an anomaly detection system is

In this e-guide

to determine the baseline for a particular network. The StealthWatch FlowCollector creates a baseline of all IP traffic, which then supports analytics for detecting anomalies in either network traffic or host behavior.

The StealthWatch FlowCollector also includes host-centric analysis, such as host and application profiling and OS fingerprinting. This is useful for detecting outside of typical patterns of use on a host.

In addition, the analytics product provides reporting on device activity, such as host reporting, router interface tracking, and bandwidth accounting and reporting. There is also support for packet level performance metrics and quality of service reporting.

Lancope StealthWatch FlowCollector can go beyond base level network reporting to detect unauthorized hosts and web servers as well as misconfigured firewalls.

Lancope offers 24/7 customer support via phone and online portal. Enterprise premium support is also available for those organizations that want more proactive assistance with planning and deployments. A community portal offers access to documentation, knowledge base articles and training videos. For more information on pricing and licensing, contact Lancope.

Conclusion

Predicting malicious activity is difficult, even with large volumes of data and the most sophisticated analysis techniques. Baselines -- meanwhile -- change, sometimes slowly over time. This can impact the false positive rate of alerts, so care must be exercised when balancing the need to minimize false alarms with the desire to not miss a real threat because alert thresholds were too high.

If there is malicious activity on IT infrastructure, it is probably leaving a trace of some kind in network traffic, which tools like the Lancope StealthWatch FlowCollector can detect. This tool can profile a normal baseline of activity and then detect variations from that norm, and can alert administrators to potentially malicious activity.

StealthWatch FlowCollector is especially useful for network administrators and security professionals who need to monitor network-level activities across complex infrastructures.

Editor's Note: *Lancope was recently acquired by Cisco. While Lancope still operates as a separate company, the acquisition could impact the Lancope StealthWatch product line, including the FlowCollector series.*

Next article

In this e-guide

RSA NetWitness Logs and Packets: Security analytics product overview

Dan Sullivan, Contributor

Expert Dan Sullivan examines RSA's NetWitness Logs and Packets, security analytics tools that collect and review logs, packets and behavior to detect enterprise threats.

The state of information security is succinctly stated with the adage "InfoSec professionals have to be right all the time, and attackers only have to be right once." The idea behind this sentiment is that attackers can take their time to probe networks, assess security controls in place and find weaknesses to exploit. Meanwhile, security professionals have to constantly watch for unusual activity, assess vulnerabilities, and prepare to respond to a wide array of attack types. Security analytics tools such as the RSA NetWitness suite are designed to reduce the information overload burden on InfoSec professionals.

RSA NetWitness Logs and Packets

It is no longer a viable option in large enterprises to expect targeted controls, such centralized logging and vulnerability scanning, to provide information fast enough or sufficient enough to counter advanced threats. Security analytics emerged in response for the need to collect and integrate data from multiple

sources and evaluate that data looking for patterns of potentially malicious activity.

RSA this summer introduced its latest security, RSA NetWitness Suite, which builds on the company's previous offering, RSA Security Analytics. The suite includes NetWitness Logs and NetWitness Packets, which provide the bulk of the analytics capabilities for the suite -- the RSA NetWitness suite also includes EndPoint, SecOps Manager and other products.

The NetWitness Logs and Packets platform is designed to deliver advanced analytics, including real-time behavioral analysis, and visibility across enterprise endpoints, networks and cloud resources. This includes full packet capture and NetFlow logs, which allows the security analytics products to detect and reconstruct attacks.

Monitoring and forensics

RSA NetWitness Logs and Packets have several components for specialized operations, including a decoder, concentrator and broker.

The RSA NetWitness decoder is responsible for the real-time collection of network data. The decode captures data in real time and can normalize and reconstruct data for full session analysis. In addition, the decoder can collect flow and endpoint data. The concentrator collects information from multiple

decoders and provides the mechanisms needed to support the distributed decoders. There is a hybrid decoder/concentrator, specific to RSA NetWitness Logs and Packets, that comes in a single appliance designed for branch location monitoring.

The broker supports analytic services by enabling federated querying across the distributed system. The broker allows system administrators to work with a single device to collect information from across the network. Other components of the security analytics suite include an archiver for long-term storage and compression of log data for any compliance requirements, a virtual log collector or VLC for remote sites to send logs to the decoder and a security analytics server.

Behavior analytics

One of the key features of the RSA NetWitness suite is the advanced analytics engine's behavior analytics capability. Shortly before the RSA NetWitness suite was introduced, the company added real-time behavior analytics capabilities to the RSA Security Analytics platform, a feature that was then included in the NetWitness suite. The behavior analytics component uses machine learning to spot anomalous activities and behaviors of both users as well as systems. According to RSA, the behavior analytics engine is designed to detect lateral movements of threat actors.

In this e-guide

Data enrichment

In addition to collecting data, the RSA NetWitness platform also performs data enrichment and event stream analysis. Enrichment includes adding tags to highlight threat indicators or other relevant characteristics so analysts do not have to spend as much time on such low level data analysis tasks. This kind of analysis is the foundation for building real-time alerting mechanisms. RSA NetWitness includes tools to sift through large volumes of data to triage events and prioritize responses.

The suite also comes with an Event Stream Analysis (ESA) module, an analytics and alert engine designed to correlate data from a range of different events. The ESA module can take metadata from logs, NetFlow, packets and other sources and correlate the information. In addition, enterprises can create customer rules via the rule builder wizard for collecting and processing the data.

For customers already using other RSA products, you may be able to integrate those systems into RSA NetWitness Logs and Packets. For example, security managers can easily link RSA NetWitness Endpoint to NetWitness Logs and Packets. As with many enterprise applications, pricing is available through custom quotes. Customers can contact RSA for more information on licensing, support and free demos for RSA NetWitness Logs and Packets.

Conclusion

The RSA NetWitness Logs and Packets products are designed as federated, distributed tools that can scale to large networks and complex topologies. Analytic modules can perform real time analysis and well as incident analysis after the fact. Integration with the RSA security operations center is useful when consolidating and coordinating security monitoring and response around that platform.

The RSA NetWitness platform is well suited for enterprises with specialized information security teams that can take full advantage of the platforms capabilities. Smaller organizations may want to consider another security analytics platform.

Next article

In this e-guide

Sumo Logic Enterprise Security Analytics: Product overview

Dan Sullivan, Contributor

Expert Dan Sullivan examines Sumo Logic Enterprise Security Analytics, which uses a combination of rules, anomaly detection and predictive analytics to detect security threats.

The dynamic and persistent nature of cyberthreats requires a continual state of monitoring, blocking and -- potentially -- remediating. Security event and incident management platforms are designed to meet a number of important aspects of this continual monitor and response stance.

Sumo Logic is a cloud-based analytics vendor that focuses on security and compliance, but in the process addresses DevOps and infrastructure management issues as well. The Sumo Logic Enterprise Security Analytics platform is a security as a service offering that works with both on-premises and cloud-based enterprise infrastructure and applications.

Data collection

The Sumo Logic security analytics platform uses lightweight collectors to package and encrypt data that is then ingested in a centralized logging system.

In this e-guide

A search tool is provided so administrators and analysts can search through volumes of events. The system is designed to collect terabytes of data from on-premises applications, network infrastructure and devices as well as cloud resources.

The company's LogReduce tool is designed to take thousands of log events and group them into identifiable groups based on patterns. Sumo Logic also uses a specialized compression technique to find patterns across events, and enable the system to represent large number of events in a space-saving, efficient form for security analytics. The company's patented SumoLogic Elastic Log Processing engine is designed to scale as needed, depending on the computing, storage and processing resources available for each customer.

Analytics and altering

After collecting and ingesting data, the next logical step in the platform's workflow is analysis. Sumo Logic Enterprise Security Analytics employs a combination of rules, anomaly detection and predictive analytics to detect events of interest. Rules are useful for specifying well-known suspicious patterns, such as port scanning. Anomaly detection builds a baseline of typical activity and uses that to identify events that lie significantly outside the norm. Predictive analytics employs statistics and machine learning techniques to identity events that are likely precursors to security events of interest.

In this e-guide

Sumo Logic's security analytics platform can also provide insights into data pulled from third-party sources both in the cloud and on premises, including AWS CloudTrail and Cisco Adaptive Security Appliances.

Administrators and security analysts can monitor the state of events using the Sumo Logic customizable dashboard. They can also configure alerts to send notifications in the event anomalous activity is detected. The alert system can be customized to notify security team members where specific data deviates from the baselines or thresholds set by the organization. Alerts can also be sent through existing email systems or real-time communications platforms like Slack.

For businesses in regulated industries, Sumo Logic provides compliance reports to support Payment Card Industry Data Security Standard (PCI DSS), HIPAA, the Federal Information Processing Standard (FIPS), the Sarbanes-Oxley Act, ISO and COBIT. The vendor also holds attestations and certifications related to EU Safe Harbor, Service Organization Control 2 (SOC 2) and SOC 2 Type II, HIPAA, PCI DSS and FIPS.

Cost and support

The Sumo Logic security analytics platform is priced according to the volume of data analyzed. The company offers a free version of the platform for one to three users and up to 500 megabytes of data analyzed per day. This level

In this e-guide

includes data collection, analysis and event detection, search and dashboards. Data is retained for seven days. Support is available on the community forum.

The next level up is the Professional level service that includes analysis of up to one gigabyte of data per day and three to 20 users. In addition to the free service level features, the Professional level adds alerting, collector management API and up to a 30-day retention of data. Professional support is available during business hours.

Larger enterprises that require the full range of Sumo Logic features may want to consider the custom priced Enterprise service. It includes all the features of the Professional level as well as anomaly detection, enterprise application integration, single sign-on and multiyear retention. The Enterprise level support is extensive and includes help with proof of concepts, RFP development, a professional services trainer and optional 24/7 support.

Conclusion

Sumo Logic Enterprise Security Analytics addresses a range of security monitoring and incident response needs. The security as a service reduces administrative overhead of on-premises administrator, and offers a range of support and service levels to meet the needs of those organizations just exploring SIEM and security analytics analysis to those enterprises that are ready to deploy such as product in a production environment.

In this e-guide

About the author

Dan Sullivan, M.Sc., is an author, systems architect, and consultant with over 20 years of IT experience with engagements in advanced analytics, systems architecture, database design, enterprise security and business intelligence. He has worked in a broad range of industries, including financial services, manufacturing, pharmaceuticals, software development, government, retail, gas and oil production, power generation, life sciences, and education. Dan is a series editor and author with Realtime Publishers, a leading provider of expert, third-party content for the IT industry. Dan has written extensively about topics ranging from data warehousing, cloud computing and advanced analytics to security management, collaboration, and text mining. He has written sixteen books as well as numerous articles and custom white papers.