Data Capture and Network Forensics, State-of-the-Market: IBM Security QRadar Incident Forensics vs. Other Industry Tools

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

July 2014

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Data Capture and Network Forensics, State-of-the-Market: IBM Security QRadar Incident Forensics vs. Other Industry Tools

Executive Summary

The ability to capture, consume and correlate multifaceted data from all over the enterprise is a growing need. No single data source or type can provide sufficient forensic capabilities to solve all of today's security problems. ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) end-user research demonstrates that the data needs of security organizations are growing at breakneck speeds reaching volumes associated with big data. Log information from network and server infrastructure is no longer sufficient to provide a full picture. Security needs to process a broader and richer data set including network and big data repositories. Additionally, the security technology has to be able to correlate commonalities within those variant data streams to produce meaningful data trails and do it in as near to real time as possible. A 2013 study by Ponemon Institute identified that if a security incident can be resolved in less than 60 seconds, the remediation costs could be reduced by as much as 40%.

Traditional log management tools do not contain the range of data or data mining and analysis capabilities to deliver true security analytics and forensics. Security Incident Event Management (SIEM) tools provide more capabilities but are also insufficient for full forensic analysis. Fifty-three percent of EMA research respondents understood that security analytics and forensics tools augmented their SIEM tools and 46% understood that security analytics and forensics tools were a natural evolution of the traditional SIEM. A good rule to follow is that a SIEM should provide correlation, normalization and alerts on key events and have the ability to query the data to retrieve answers to complex questions about the specific environment. A security analytics solution is able to adapt to the activities and behaviors within its monitored environment providing improved visibility into activities and why they should be investigated. It can ingest non-standard log data types at big data proportions to provide visibility into abstract data relationships bringing attention to problems that operators and administrators hadn't even thought of.

The introduction of a forensics solution will provide the increased capabilities to reduce false positives and time spent per case, thereby increasing the incident response team's ability to process the key highest risk incidents first and faster, and create a proper case file to manage all of the required data.

Having the capability of doubling the number of incidents the response team can resolve in minutes makes choosing the right solution imperative. This EMA report evaluates security forensics tools from an operations standpoint and identifies IBM Security QRadar as a leader among those evaluated. The investigation discusses the evaluation criteria for six tools widely recognized for their support in forensics data gathering and processing, and provides evaluation input on several other tools. *QRadar best met the operations evaluation criteria of all of the reviewed solutions.*

Data Capture and Network Forensics, State-of-the-Market: IBM Security QRadar Incident Forensics vs. Other Industry Tools

Table of Contents

EMA

Introduction

There is an increasing number of security tools that profess to deliver "actionable intelligence" or "actionable insights" to operators and analysts to improve security response. While many of them are out of scope for this evaluation, it is important to note that "Buzzword Bingo" is proliferated by vendors of diverse technology to gain attention in the security space. This approach confuses consumers and is frequently exacerbated in areas of emerging technology like security analytics and forensics. This paper attempts to reduce the confusion on what should qualify as a forensics solution and comparatively evaluate some of the products in the space.

One foundational note is that traditional log management tools do not qualify as forensics tools. Though they collect logs, they do not have full packet capture capability and therefore do not contain the breadth of data or data mining and analysis capabilities to deliver true security analytics and forensics. Security Incident Event Management (SIEM) tools, provide more capabilities than log management tools but are also insufficient for full forensic analysis. In the latest EMA security research, it was clear that security professionals get this. Only 1% of the respondents thought that security analytics as a function or toolset was a rebranding of SIEM. Fifty three percent understood that security analytics and forensics tools could augment their SIEM tools and 46% had the understanding that security analytics and forensics tools were a natural evolution of the traditional SIEM. That perspective can be seen in the marketplace with many vendors trying to rebrand their SIEM as security analytics tools without the change in capabilities necessary to substantiate it. A good rule to follow is that a SIEM should provide correlation, normalization and alerts on key events and the ability to query the data to retrieve answers to complex questions about the specific environment. A security analytics solution is able to adapt to the activities and behaviors within its monitored environment providing improved visibility into activities and why they should be investigated.

Ninety-five percent of the organizations that implemented an analytics or forensics solution indicated that they received "expected or greater than expected value" from the solution. This was the highest combined value statement of any of the 13 technologies evaluated in the research. Additionally, EMA research showed that a significant contributor to that value statement came from the ability of those tools to gather, reveal and analyze forensic data. Operations teams using these solutions moved the volume of cases they could resolve in minutes from an average of 12% of their case load to an average of 24% of their case load. The ability of the tool to use more data to come to a better conclusion also reduced false positives, aided alert prioritization, drove a decrease in staff burdens and case backlog, reduced per case cost of resolution and ultimately lowered cost of resolution for incidents.

Ninety-five percent of the organizations that implemented an analytics or forensics solution indicated that they received "expected or greater than expected value" from the solution.

Forty-five percent of the organizations that had a security analytics solution in place said they were confident that they could detect and remediate a security incident prior to it having a significant impact. This was the highest level of confidence among 13 different security technologies investigated. In addition to higher confidence levels for response, 90% of the respondents said that the introduction of the solution had reduced false positives and improved their actionable alerts.

Tools Reviewed

Given the numerous tools available in the market place that will support forensics to one degree or another, it is impossible to review all of them in the scope of this paper. Several of the more commonly known and/or used tools that provide forensic capabilities have been chosen. The tools chosen were billed by their respective companies as being created to provide forensics capabilities. The paper also identifies other tools that compete in the space but does not go into detail on those tools. The listing is more to make the reader aware of them.

Operations teams using these solutions moved the volume of cases they could resolve in minutes from an average of 12% of their case load to an average of 24% of their case load.

The tools that are reviewed in this paper in conjunction with IBM Security QRadar Incident Forensics are:

1. RSA Security Analytics – Originally named NetWitness, acquired by EMC in April 2011, and rebranded RSA Security Analytics.
2. Bluecoat Security Analytics Platform – Previously Solera DeepSee, it was acquired by Bluecoat Systems in May 2013 and rebranded.
3. LogRhythm Network Monitor – Introduced by LogRhythm as part of its 5.1 release in July 2011.
4. Niksun NetDetector – Created in 1997 by Dr. Parag Pruthi as a network monitoring solution to capture and analyze network traffic.
5. Wireshark – Network packet captures software released by Gerald Combs in 1998. Originally named Ethereal and rebranded in 2006 to Wireshark.
6. TCPdump (for Linux/UNIX) – Originally created in 1987 by Van Jocobson, Craig Leres and Steven McCane for network packet capture in Linux/Unix systems. Ported to Windows as WinDump about 2000.
7. Splunk[1] and HP ArcSight ESM[2] were not evaluated in this paper because they do not directly process real-time network captures.

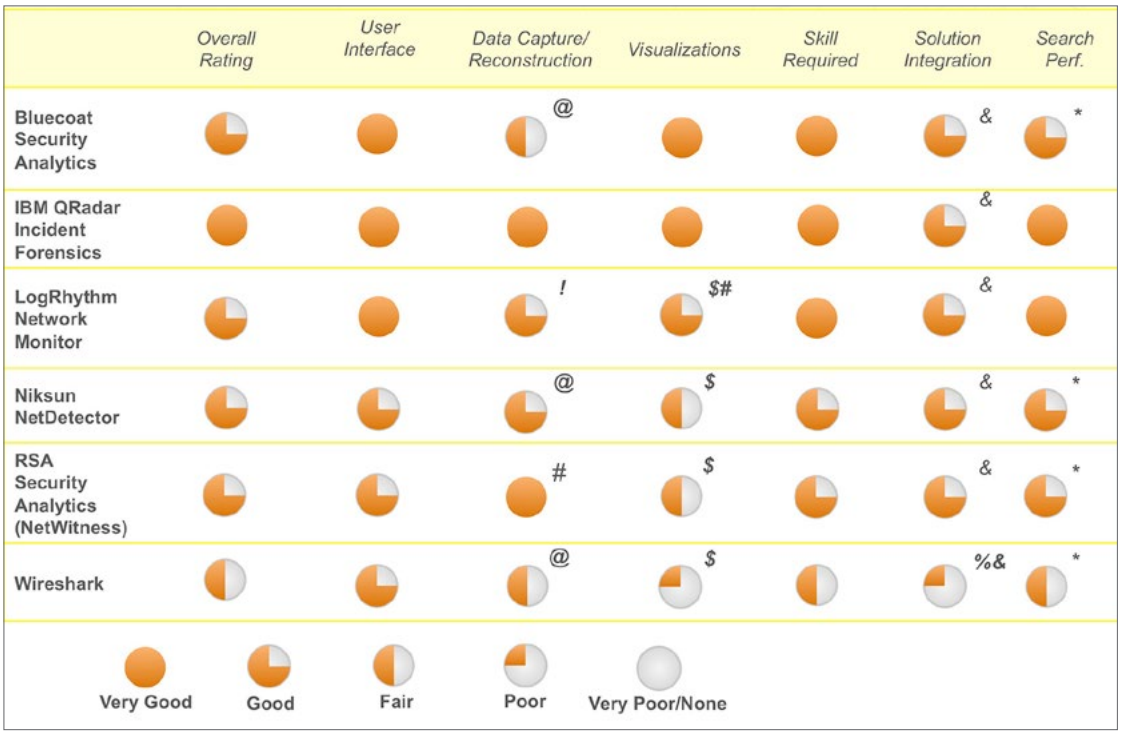
EMA Perspective

Networks, network connected systems, and the underlying data are under constant reconnaissance and/or attack from both within and without. Hacktivists, organized crime, and corrupt or disgruntled insiders seem to be everywhere. The current state of being is for companies to assume they have been or will be compromised. Security organizations must be vigilant in identifying threats and dealing with them. Because of the sophistication of many attacks, security needs tools that can peel back the layers of activities, revealing their true nature. Traditional Security Information and Event Management (SIEM) are only so good and do not have the full range of capabilities necessary to provide the complete picture. Security analytics and forensics solutions are the best means of making the correlations and responding in a timely manner. Advances in machine learning and user interface design mean forensic capabilities are no longer tools only for law enforcement or post event consultants.

Each tool reviewed was evaluated against each of the 6 criteria. Each tool and the evaluation criteria are documented below with commentary of the rating and why that rating was given. The ratings for each category are 0–4. A zero indicates *very poor* to *no support for a given criteria*. A four indicates *very good support for the criteria*.

[1] http://answers.splunk.com/answers/41740/splunk-and-port-mirroring
[2] http://www.youtube.com/watch?v=McNfhVJLqUs

Product Comparative Summary



[3]

TCPdump/Windump – Overall Rating 0.5

TCPdump/Windump and similar tools have been around for years. They were included in this paper because they have withstood the test of time. Being free tools, many practitioners have used them and can therefore relate to the comparison with the other tools in the list. TCPdump and Windump are considered first- generation tools.

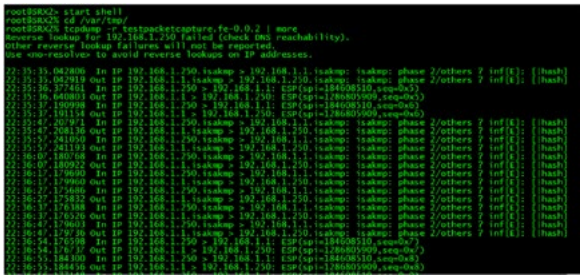


Figure 1: TCPdump interface

User Interface – 0

The user interface is a no-frills, command-line, switch driven view providing output from the packets intercepted broken down by field. The data scrolls up the screen and can be redirected into a packet capture (Pcap) file for later review. Being command line rather than graphical (GUI), the interface has no modularity, user customizability, or data pivoting. Getting to the raw data requires accessing the Pcap file.

Data Visualization – 0

TCPdump and Windump are not designed for any data visualization. To get any flow visualizations, the Pcap file must be exported into other tools like Wireshark.

[3] ! LogRhythm requires Pcap export to Wireshark or other tool for document reconstruction
* Search limited due to lack of metadata and/or endpoint data
$ Does not provide bubble flows
@ Does not collect machine/endpoint data
% Though it can consume and create Pcap files, Wireshark is meant to operate as a standalone tool.
& Requires some additional integration to maximize benefit.
# This figure was updated post webinar due to additional information made available

Data Capture and Reconstruction – 1

Designed for use on a single system, TCPdump and Windump only capture network traffic on a single interface card at a time. This limits the scope of the total data captured. If a network tap or span port is available, it can be used to capture traffic from that port, which widens the scope of its data capture.

TCPdump and Windump do not provide data reconstruction. All data is in the individual packets in which it was captured. They also have no application (layer 7) context to aid in understanding application misuse.

TCPdump and Windump are purely network centric and cannot provide context for end host and other non-packet centric data.

Forty-five percent of organizations that had a Security Analytics or Forensics solution said they were confident that they could detect and remediate a security incident prior to it having a significant impact.

Solution Integration – 1

TCPdump and Windump are meant to work as standalone tools. They can create Pcap files for use in other tools like Wireshark.

Data Search Capabilities and Performance – 0

These tools require use of systems tools such as grep or awk or customized scripts to be written to locate and extract data on UNIX systems. On Windows, it requires either DOS tools like findstr or text editors (Notepad/WordPad) using the built in search function.

Skill Required – 1

These tools are easy to set up and gather data, but to maximize results, the analyst must fully understand the switches that can be used. To process and extract data, the user must understand ASCII, hex, binary, uuencoding, and other text formats. The tools do no preprocessing to aid the analyst.

Wireshark – Overall Rating 1.83

Wireshark was created because TCPdump did not provide enough usability. Wireshark is considered a second-generation network troubleshooting tool due to its limited forensics capabilities.

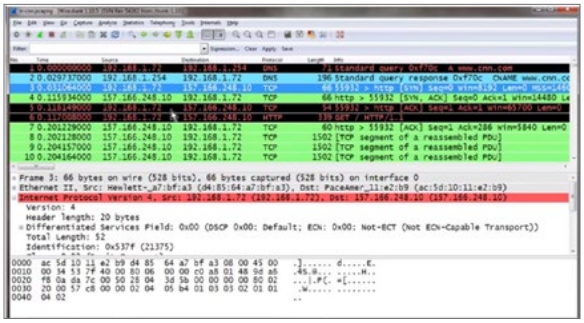


Figure 2: Wireshark interface

User Interface – 3[4]

As of 2014, Wireshark released a new interface based upon QT to improve its flexibility and improve performance on MacOS. Users can add, remove and rearrange columns to isolate data in the capture. Data filters can be applied on single or multiple columns. The current version also has the ability to create user profiles allowing different setups to be used by one or more users. Data can be captured from a single interface live, or a Pcap file can be fed in to review data historically.

The interface has no modularity, but profiles and columnar changes provide a reasonable amount of customizability within the scope of what it delivers. Rudimentary data pivoting can be accomplished with the filtering system. Getting to the raw data requires accessing the Pcap file.

[4] The user interface does not have the same breadth of abilities that the tools rated later in this report have. It is simple. It has few bells and whistles but what it does have, it uses well which is why it was rated a 3 out of 4.

Nintey percent of survey respondents said the introduction of an Analytics solution had reduced false positives and improved their actionable alerts.

Data Visualization – 1

Data visualization is provided by use of line coloring to represent various characteristics within the packet structure and data flows. This is a significant improvement over TCPdump but not sufficient for performing any advanced analytics.

Data Capture and Reconstruction – 2

Wireshark is designed for use on a single system and only captures network traffic on a single interface card, limiting the total scope of captured data. If a network tap or span port is available, it can be used to capture traffic from that port, which widens the scope of its data capture. It can also import previously captured data from a Pcap file.

Wireshark does provide file reconstruction. Multiple file types such as text[5] and graphics[6] documents can be reconstructed if the entire conversation was captured; however, accomplishing this can be labor intensive. Document reconstruction may require searching for key hex strings outside of Wireshark, depending upon the document file type, significantly impeding the time to resolve an incident.

Solution Integration – 1

Wireshark works primarily as a standalone tool. However, given that it can import Pcap files from other tools it does provide a limited sort of integration with tools that generate Pcap output.

Data Search Capabilities and Performance – 2

The columnar/field data filtering can be useful if you know the data string or the field name containing the associated data to locate the target. It's a far step up from TCPdump, but the impediment is having to know the specific details.

The speed of the search is usually very fast, but can be significantly dependent upon the size of the Pcap and the system resources.

Skill Required – 2

Wireshark is easy to download, install, and begin using, but requires a significant amount of network packet disassembly knowledge. The user will need to have other tools at his/her disposal to extract, decode, and utilize packet contents such as ASCII code, hex code, binary, Unicode, and others.

NOTE to the Reader:

Arguments may be made outside the scope of this paper which generation they are, but all of the tools discussed from this point farther are at least third-generation tools.

[5] http://www.youtube.com/watch?v=Nwi2rM4Syno
[6] http://www.youtube.com/watch?v=u-fMLIphj5o

Niksun NetDetector – Overall Rating 2.83

Niksun, operating for over 15 years, has evolved well beyond the traditional IDS in terms of its packet monitoring capabilities and performance. It's a multi-part platform with a collection and indexing engine (NetDetector), management appliance (NetOmni), and a back-end database appliance (Mercury).

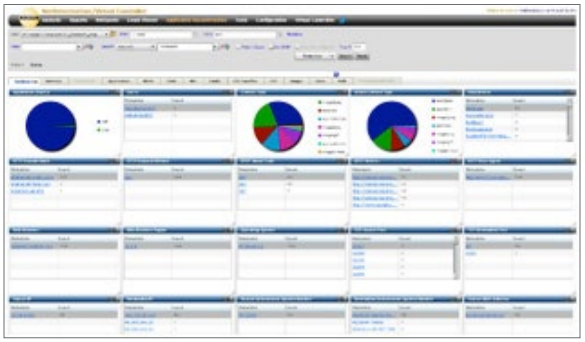


Figure 3: Niksun NetOmni interface

User Interface – 3

Using a highly modular, web-based GUI, the solution compartmentalizes data, alerts, and tasks into functional areas; however, each of the tab units seem to provide more of a montage or collage of data rather than a unified message or story. And because the data is compartmentalized, quickly identifying subtle issues like low and slow compromise activity is not terribly intuitive.

Niksun produces a lot of data and intelligence around numerous aspects of the packet flows, but not much in the way of advanced analysis. It allows drill downs providing the contextual information to create a hypothesis and either support or refute it, but does not seem to create much up-front analysis.

The interface's heavy utilization of embedded hypertext makes access to the metadata and underlying data easy for a chosen investigation, and from that point, the analyst can pivot on data to see other data points related to the case before rendering a decision.

Data Visualization – 2

Data visualization dashboards and flows are provided via pie charts and single dimensional line graphs. Data flows are also depicted in the widgets in the form of tables. Though functional, they do not provide a highly advanced holistic view of the data and attack flows. Analysts are given details in hyperlinks, text lists, and text based activity paragraphs, but information such as geolocation is not highly leveraged.

When asked about how analytics tool had impacted the frequency and duration of security investigations, 50% said the solution reduced both duration and frequency of investigations.

Data Capture and Reconstruction – 2.5

Niksun captures all packet transfer information at wire speeds up to 100Gbps making it the highest line speed capacity network packet capture solution reviewed, but it doesn't capture any log data from network, system, or application logs, nor does it ingest historical Pcap files. If operating at the time of an event, Niksun maintains the full packet capture in accessible storage, for a configurable period of time.

Niksun can also reconstruct any data transmitted across a monitored communications. It is OSI layer 7 application aware so it can identify application misuse as a threat indicator to help identify misconduct or compromise. Niksun also provides SSL inspection capabilities provided proper SSL certificates.

Solution Integration – 2.5

Components used for the Niksun solution are well integrated and purpose built so deployment is easy; however, Niksun suffers from its inability to integrate network, system, and application logs to create the larger, richer context of activities. For example, it can't identify things like configuration changes on host systems, and requires integration with a SIEM or other analytics tool to gain full contextual awareness.

Data Search Capabilities and Performance – 3.5

Niksun has exceptional search speed. The appliances are optimized for indexing, creating metadata and returning data quickly. It was the fastest of all of the third-generation systems tested; users don't have to know any heavy or specialized query languages to execute a search. Though flexible and robust, offering filtering fields to narrow the search results, the interface still requires an analyst to indicate a context via a dropdown box next to the text box.

Skill Required – 3

With modules and various aspects of the data so compartmentalized, looking at the dashboard and identifying an issue was not highly intuitive; however, the greater knowledge of the environment and network troubleshooting the analyst has, the quicker he or she will be able to use the tool.

RSA Security Analytics – Overall Rating 3.08

RSA Security Analytics, formerly NetWitness, provides analytics capabilities significantly advanced over TCPdump and Wireshark, and unlike packet analysis tools (which evaluate network events and incidents only in the context of network packet information) it significantly advances capabilities in many of the six areas by ingesting and processing other logs to provide a richer context for analysis.

Figure 4: RSA Security Analytics interface

User Interface – 3

The console can be configured by group/team/role, and the interface relies upon four tabs across the top for *Investigation, Navigation, Events,* and *Malware Analysis.* Each of the tabs has subsequent menus to aid in drill down or context pivots on data relating to the particular case. Having the context menus across the top is not quite as convenient as using right mouse click on context sensitive menus.

Very investigation oriented, which is both good and bad, it allows the operator to follow an alert to the underlying data, yet it's not as flexible for investigative branching and tangential data pivoting capabilities. For example, if an issue is detected and an investigation begins, the analyst can move through activities surrounding that event, but it is not easy to shift direction to look at other contexts.

Data Visualization – 2.25

Data visualization dashboards and flows are provided by use of RPM style gauges, single dimensional line graphs, bar, column and pie graphs – from that perspective, not highly advanced. Though analysts are given much of the detail in hyperlink and text lists, a significant amount of information about the data flows, such as geolocation, is not highly leveraged. As a related item, however, RSA Security Analytics does support multi-touch monitors to zoom in and out of collected traffic visualizations.

Data Capture and Reconstruction – 4

RSA Security Analytics can capture network packet and log traffic, correlate and normalize network, system and application data to provide a richer picture than simpler packet capture solutions. It can also import previously captured data from a Pcap file and is OSI layer 7 application aware, facilitating identification of application tunneling or misuse associated with malicious activity.

RSA Security Analytics can extract and reconstruct not only network conversations, but any transferred documents providing valuable evidence against malicious users. The Event Stream Analyzer (ESA) provides advanced analytics and cross correlation of all ingested events reducing false positives.

Solution Integration – 3.25

RSA provides a solid array of analysis capabilities out of the box. It also has integration hooks for other RSA Services such as RSA Live Feed Service for sharing and distributing threat and attack information, and RSA Archer for asset information and case management. It integrates with many other security solutions SIEM, threat intelligence and other vendors either as a data miner or in a bi-directional fashion.

Not having a built-in case management system negatively impacted RSA Security Analytics.[7]

Data Search Capabilities and Performance – 3

RSA has various sized appliances for security analytics. Organizations that properly size their data requirements will see good search performance. Though the metadata framework used for context and search is extensive, it is not the most robust evaluated. This impacts search because metadata is generally more highly indexed for search than raw data. It is also kept longer because it is more compact and descriptive than the raw data.

Investigator and dashboard widgets are more focused around drill down on incidents/events or structured investigations than on freeform searches.

Skill Required – 3

Dashboards and alerts are designed to present a lot of information to the analyst. With the customizations and solid drilldown capabilities, RSA Security Analytics facilitates analysis. It can deliver results to medium skilled employees and above (solid tier 2 to tier 3). Tier 1 personnel and less experienced tier 2 personnel may have some trouble with the investigations, getting lost in the drilldowns because they don't have the experience to know what the next step is.

Bluecoat Security Analytics Platform – Overall Rating 3.16

Formerly Solera Networks, Bluecoat Security Analytics is a solid platform for network packet analysis and investigation. Its high rating in four of the criteria somewhat skews the overall result if the solution requirements include the ability to process data other than network packet captures.

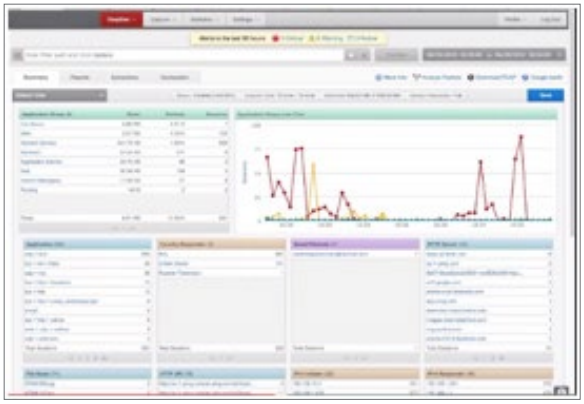


Figure 5a: Bluecoat Security Analytics Dashboard

User Interface – 3.5

Bluecoat Security Analytics utilizes a layered tab and menu structure to facilitate analyst access to information. The interface relies upon four tabs across the top of the user space focusing on *Dashboard/Capture/Statistics* and *Settings* with sub-tabs and drop-down boxes depending upon the primary tab. It's highly modular allowing either a standardized or user customized display of various types of table, pie, bar,

[7] https://community.emc.com/community/connect/rsaxchange/netwitness/content?filterID=contentstatus%5Bpublished%5D~objecttype~objecttype%5Bidea%5D

or column formatted data feeds. Many of the widgets in the dashboard allow mouse hovering and right click context menus for further investigation.

Bluecoat is also very investigation oriented; it allows the operator to follow an alert to the underlying data, but it is not as flexible in the investigative branching, and tangential data pivoting capabilities. For example, if an issue is detected and an investigation begins, the analyst can move through activities surrounding that event, but it's not easy to shift to other contexts.

Figure 5b: Bluecoat Security Analytics Data Geolocation

Users can quickly and efficiently scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object either via the direct data or through a solid array of metadata.

Data Visualization – 3.75

Bluecoat uses the standard line, bar, column and pie charts for data and attack visualization. A differentiating feature is the addition of the geolocation tab and Google Maps integration for showing packet flows. The tab aids in quickly visualizing where data is moving and directs analysts toward events with the largest flows but does not indicate directionality. The Google Earth integration shows the data locations and flows, but since it requires both an export of a kmz/kml file and importation into Google Earth, it's a little cumbersome and not as useful for real-time work.

Data Capture and Reconstruction – 2.25

The network data processed is OSI layer 7 application aware to identify misuse and tunneling used to obfuscate malicious activity. Aside from capturing live network data, the Bluecoat solution will also process and analyze historical Pcap files.

Integrating with its Web Security Gateways (WSGs) and proxy technologies, the analytics solution is able to perform SSL inspection; however, it suffered in this category because it does not process or provide analysis of standard network, systems, and application log data. For example, it won't detect activity carried out on local systems, like data theft via USB, or other end point malicious activity.

Solution Integration – 2.75

Bluecoat offers various appliance sizes and a virtual machine image. It integrates with many network solutions including Advanced Persistent Threat (APT) detection solutions, Next Generation Firewalls (NGFW), Intrusion Detection Sensors (IDS), and common SIEM vendors. Many of these integrations allow modification of rules and policies to update those defenses more quickly.

The solution does have a case management system.

Data Search Capabilities and Performance – 3

Organizations that properly size their data requirements will see good search performance. Due to metadata creation capabilities, it has a similar search capacity as RSA.

Bluecoat Security Analytics is structured to focus event/incident alerts and drilldown investigations more than freeform searches.

Skill Required – 3.75

Data layout and compartmentalization is well balanced and supports the less experienced analyst provided by a well laid-out drilldown capability. It supports the concept of a force multiplier for personnel. Analysts of any level can get value out of the system very quickly, but just as with any advanced solution, there are advanced features and techniques that will take time to master.

LogRhythm Network Monitor – Overall Rating 3.21

LogRhythm is widely known for its SIEM platform, which it has been evolving for a number of years and is now billed as a Security Intelligence Platform. To meet that billing, LogRhythm has been expanding the SIEM capability by creating/integrating functional modules. One of these modules is Network Monitor. This evaluation focuses on the Network Monitor module and its specific capabilities and performance.

Figure 6a: LogRhythm Network Monitor Interface

User Interface – 4

Network Monitor's dashboards are highly modular and customizable by group/team or user. The user interface is well laid-out making movement through investigations fluid, and facilitating transition and pivoting on data items. It uses a top-level menu that persists as each is selected, functioning similar to a tab structure without the graphics delineating a tab. The top-level menus consist of *Dashboard/Analyze/Capture/Configuration/Diagnostics/Logs* and *About*. Each contains events, or data pertaining to the topic. Data filtering can be conducted by any field or metadata, or by policy matches to more easily get to the data germane to the investigation.

Data Visualization – 3

Data visualization is presented in pie, line, column bar format. It does not have geolocation or bubble graph data flow visualizations; however, it uses additional color contexts to improve the stacked line and column charts' ability to convey information.

Data Capture and Reconstruction – 2.25

Being a network capture system, it does not ingest any logs from networks, systems or applications. This however, is to be expected. As was mentioned in this solutions introduction, it was designed post the LogRhythm SIEM so that functionality was not needed internally to Network Monitor.

Network Monitor does not appear to allow the ingestion of PCAP files from other tools.

It is OSI layer 7 application aware facilitating identification of application tunneling or misuse associated with malicious activity.

Using the software installation, data capture speed is highly susceptible to system processing load, especially when installed on shared infrastructure.

Though it can reproduce network communication streams and data flows, Network Monitor intentionally lacks the ability to provide document reconstruction as a precaution to avoid malicious documents from infecting the system, and suggests using Wireshark. This choice definitely impeded the investigation.

Solution Integration – 3

Network Monitor integrates seamlessly with the other LogRhythm Security Intelligence components. It also integrates with SIEM tools from other vendors making it an attractive option for consumers that already have a SIEM in house.

Network Monitor does not have any sort of integration with Wireshark for accessing documents. That must be conducted manually after exporting the Pcap file, and since it was designed for use with a SIEM, Network Monitor does not have an internal case management system.

Data Search Capabilities and Performance – 3

Network Monitor has a single size appliance and a software installation so consumers must follow the recommended guidance for which to use in their environments to provide adequate search capabilities. Though difficult to entirely quantify, it appears that Network Monitor generates one of the largest metadata sets that can be fully used for searching. The search engine is very flexible offering many options for getting to key information.

Skill Required – 4

For the analysts, the solution is easy to use. Investigations seem to flow very well and information is easy to retrieve. Dashboards and alerts are designed to present a lot of information to the analysts. It can deliver results to low tier 1 analysts and above in short order.

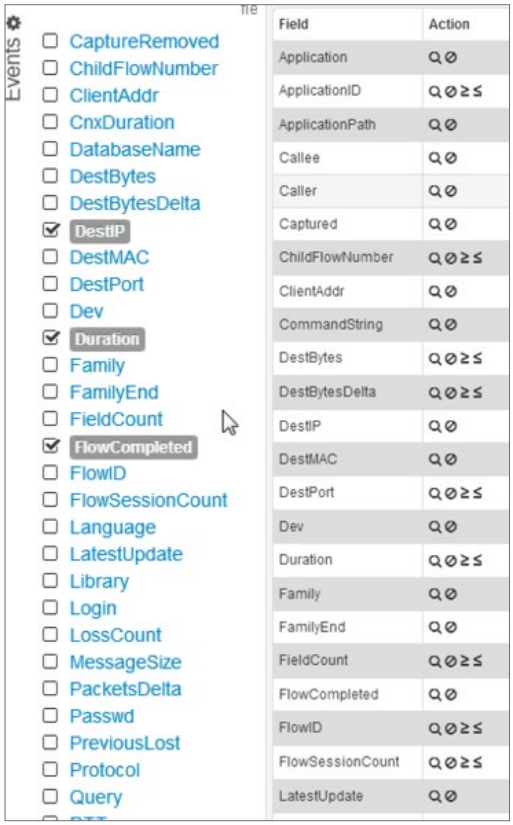


Figure 6b: Select Network Monitor Search Options

IBM Security QRadar Incident Forensics – Overall Rating 3.92

IBM acquired QRadar in 2011 as a SIEM and has since invested tens of millions of dollars into the system to evolve it beyond a traditional SIEM into a forensic analysis solution designed to meet the most demanding analyst's needs. QRadar was engineered to scale to the performance and investigative needs of analysts working in the medium sized enterprise to the fortune 10.[8]

Figure 7a: Sample QRadar Dashboard

User Interface – 4

The user interface offers a top tab structure with tab specific menus below. It organizes the data by functional area using the following tabs: *Dashboard, Offenses, Log Activity, Network Activity, Assets, Forensics, Reports, Ricks, Vulnerabilities,* and *Administration*.

The *Dashboard* is modular and highly customizable by the analyst to represent data as is intuitive to him or her enabling a high level of productivity. From a work standpoint, the tab structure does a good job of combining relevant information and much of the data is also available in one or more drilldowns so the analyst does not have to jump back and forth to get it.

[8] http://securityintelligence.com/events/attain-clarity-of-your-security-posture-with-new-qradar-incident-forensics/#.U7wZiBDRrEw Register for Webinar

This user interface is the only one to include asset[9], risk and vulnerability detail tied to the assets involved in the event or incident further improving the analyst capability to render better decisions on the situation.

During an investigation within the interface, an analyst can easily pivot between data threads to redirect focus from one line of investigation to another. An example would be seeing anomalous activity from one server, drilling down to see the user involved, and then pivoting on that user to see what else the user has been doing or pivoting on the data flow to identify possible attack collaborators.[10]

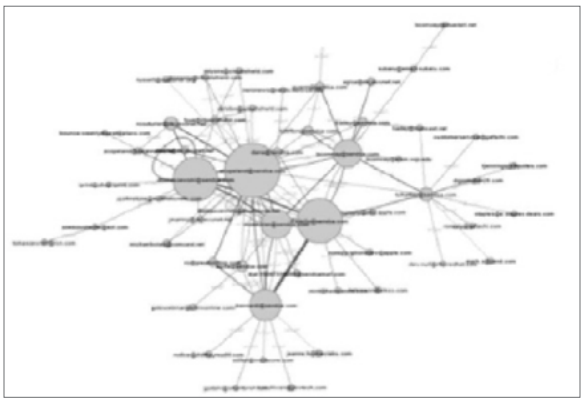


Figure 7b: Sample QRadar Data Visualization

Data Visualization – 3.75

QRadar uses all of the standard visualization like dials, pie charts, bar and column charts and line graphs. It also uses a style of flow visualization not seen in the other products. The flow mapping and visualization using bubbles indicating flow size so an attack or data exfiltration or malware infection can be mapped from beginning to end.

Though provided in the underlying metadata, QRadar does not currently display a geolocation graph or context. This would be a very useful overlay to the bubble visualization for quick understanding of where the data is coming from and going.

Data Capture and Reconstruction – 4

QRadar is the only solution reviewed that supports both packet capture and network system, and application log collection in a single analysis engine. The full log and packet integration along with OSI layer 7 application awareness provide the broadest context for investigations available in the single package.

QRadar is not only activity, anomaly, and behaviorally based but provides over 800 policies out of the box to support identifying issues like sensitive data movement, threat actor correlation and more.

Solution Integration – 3.75

QRadar integrates with all standard logging sources and can be configured to receive and process custom log formats as well. The QRadar Incident Forensics module supports standard packet capture formats accepting packet data from existing packet capture solutions.

QRadar also integrates with internal (X-Force) and external Threat Intelligence feeds (Norse Corp., Etc.) to augment the data it gathers internally. It also has an integrated case management system that is designed with the requirements of the legal system.

Data Search Capabilities and Performance – 4

The system is dual purposed for data search. Users can quickly and efficiently drill down on events and anomalies to find the relevant details pivoting on data and creating context searches. The system also facilitates open search, similar to that found in a web browser. Using only common verbiage like anyone would in a major search engine, data can be easily located to begin an investigation or report.

[9] RSA Security Analytics, if integrated with RSA Archer GRC, can also present similar data.
[10] http://www.youtube.com/user/IBMSecuritySolutions

Analysts can search through visual timelines of an event, deeply interrogating activities returned in the search to understand the context associated with each object either via the direct data or through a wide array of rich metadata. The metadata is one of the most – if not the most – comprehensive seen in this space.

Skill Required – 4

For the analyst, the solution is easy to use. Investigations seem to flow very well and information is easy to retrieve. Dashboards and alerts are designed to present a lot of information to the analyst. It can deliver results to low tier 1 analysts and above in short order.

Summary

Though there is no silver bullet for security, organizations looking for a better way to identify threats and reduce risks within their environments should strongly consider a security analytics and forensics solution. These solutions have the broadest capabilities of any of the newest threat identification technologies. Whether the threat is a malicious actor internal or external to the environment, human or malware, creating faults or exfiltrating data, these newest-generation tools have access to enough data to significantly improve detection, reduce false positives and focus valuable staff on the right problems at the right time.

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

2918.071114