IBM Security

Thought Leadership White Paper

March 2015

Look deeper into risks and threats for improved enterprise security

Searching structured and unstructured data with IBM Security QRadar Incident Forensics

Threats to enterprise security are usually more diverse, often more subtle and sometimes even simpler than they're typically portrayed. That's because the risk is not always about hidden malware and mysterious cybercriminals. A malicious "bot" may indeed forward banking information to a command-and-control center that drains accounts, but a threat can also be as familiar as an employee naively clicking links in a cleverly disguised and infected email. Meanwhile, intellectual property may be leaving via ordinary email from malicious insiders, on its way to a competitor's engineering labs.

Although IT security teams know incidents are occurring, many organizations aren't able to learn much about how they take place. To do that, security teams need tools that can help them learn details such as when bad actors began communicating with one another about their plans, when and if unstructured documents were changed before sending, and even what information—from malware to confidential business data—was contained in any attached documents. And organizations need these abilities in easy-to-use tools that deliver rapid results.

This white paper will discuss cyber-forensics capabilities and describe how IBM® Security QRadar® Incident Forensics can provide the insight organizations require. QRadar Incident Forensics enables security teams to examine log source event and network flow data, and even unstructured data—including files created using business productivity tools such as word processing, spreadsheet applications or databases—to learn who last changed it and to gather packet capture (PCAP) data to reveal who's communicating with whom, and what information they're sharing.

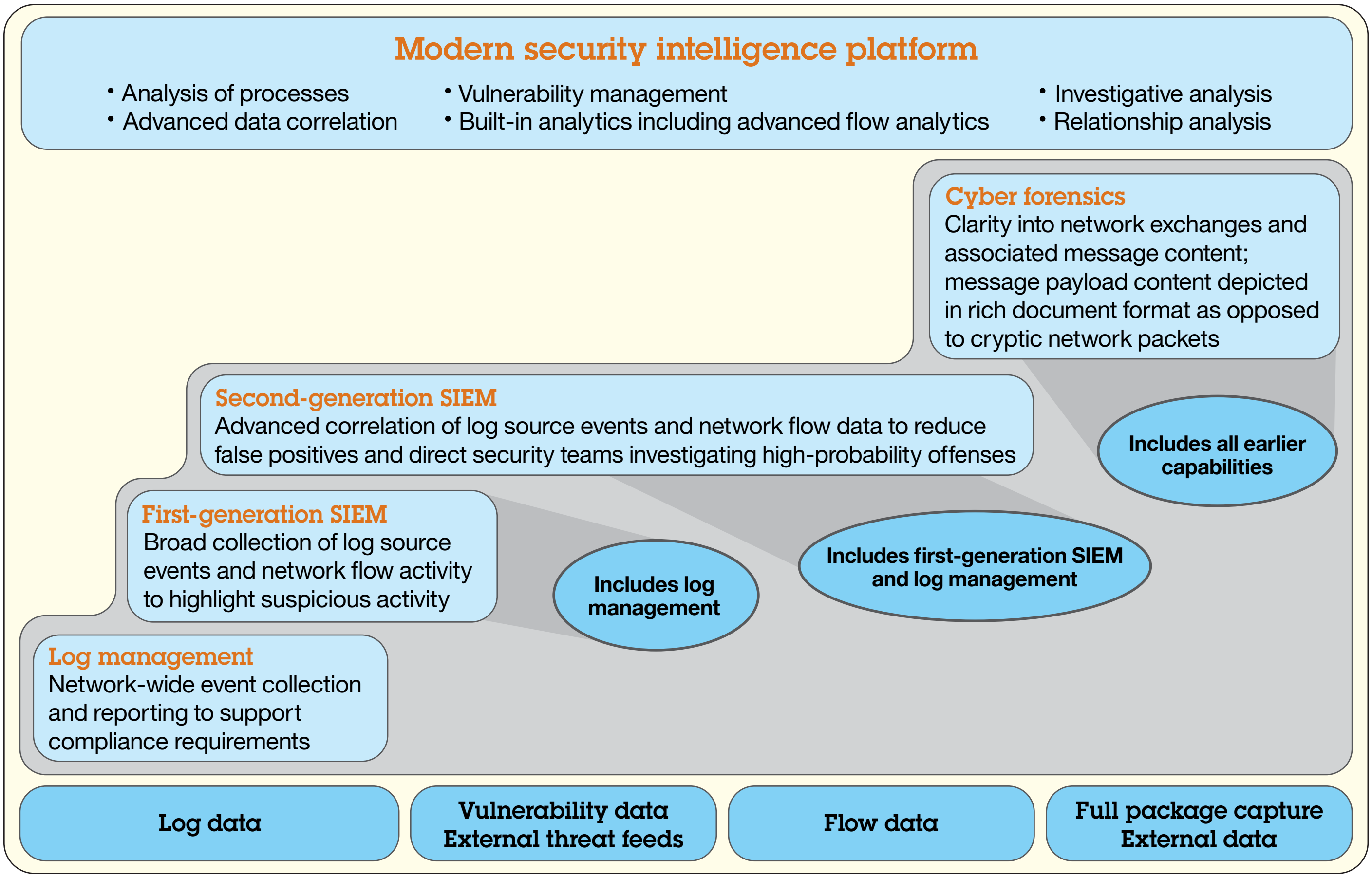
The evolution of threat investigations

Understanding risks and risky behavior—from advanced persistent threats (APTs) to insider fraud—is critical to protecting the enterprise today. But to gain that understanding, organizations need to rise above simple collection of log source data and make the transition to a robust cyber-forensics practice that looks at all data passing through the network wires. In order to make efficient security decisions, organizations need to use the full range of resources available for examining the detailed characteristics of messages as well as the basics associated with network flow traffic.

The security information and event management (SIEM) solutions many organizations deploy build on event collection and correlated network flow data to highlight suspicious activity and improve the investigation of high-probability offenses—helping identify changes in user behavior that may be related to identity theft or fraud. But they don't provide capabilities for fully understanding and dealing with these anomalies to the point where their investigations can supply evidence that will stand up in a court of law.

For more advanced security, organizations need cyber-forensics capabilities that can add definition to anomalistic network behaviors to more thoroughly investigate risk. To the core logs and flows that a SIEM solution collects, a cyber-forensics approach can add other meaningful data—from virtually any information, structured or unstructured, in motion or at rest, located anywhere on the network. Using defined criteria, it can search to uncover internal behavior that is risky to the business, dangerous external threats that have penetrated the network, or message content that can reveal information about the threat itself or the individuals perpetrating it.

Forensics capabilities build on security intelligence and diverse data



Modern security intelligence platform

- Analysis of processes
- Advanced data correlation
- Vulnerability management
- Built-in analytics including advanced flow analytics
- Investigative analysis
- Relationship analysis

Cyber forensics
Clarity into network exchanges and associated message content; message payload content depicted in rich document format as opposed to cryptic network packets

Second-generation SIEM
Advanced correlation of log source events and network flow data to reduce false positives and direct security teams investigating high-probability offenses

First-generation SIEM
Broad collection of log source events and network flow activity to highlight suspicious activity

Log management
Network-wide event collection and reporting to support compliance requirements

Includes all earlier capabilities

Includes first-generation SIEM and log management

Includes log management

Log data

Vulnerability data
External threat feeds

Flow data

Full package capture
External data

What's different about cyber forensics?

Cyber forensics can be described as an investigative analysis of all digital content—including full-packet data, documents and other artifacts—to reveal the presence, nature, impact and extent of a cyber threat. Until recently, however, cyber forensics remained more of a niche capability that was time-consuming, labor-intensive and difficult to use. It typically required specialized technical skills for operating multiple tools and solutions, each with a steep learning curve. As a result, it was generally employed only after a network breach had occurred and was often implemented by highly paid, external consultants. For everyday security, many organizations continued to rely on their longstanding SIEM capabilities, from which they gained an important core of security intelligence for responding to security incidents.

Today's advanced cyber-analytics solutions, such as QRadar Incident Forensics, however, amplify SIEM capabilities and integrate them with a broader array of data to yield more complete threat insights. The network flow revealed by a SIEM solution might be analogous to a call record in the telephone environment, revealing who communicated with whom, over what physical line and for what length of time. The log information also gathered by SIEM reveals information on activities such as authorized or unauthorized attempts to gain data access.

But these are views into network activity only. QRadar Incident Forensics can further replay the complete contents of the call and make use of anything that the call participants had electronically stored in the network for much deeper insight into potential threat activities.

Use case: Insider threat

An organization suspects that an employee, customer or partner is colluding with external parties to engage in detrimental activities.

Objectives

- Identify the colluding individual
- Understand the nature and patterns of interactions among collaborators
- Uncover the content that underlies the scheme
- Reveal the duration of the scheme to understand the scope of the risk

Applying QRadar Incident Forensics

- Search for the identities of the individuals involved
- Identify suspicious relationships using digital impressions
- Trace the activities of individuals to find the content of interactions
- Discover the likely motivations of the collusion
- Find the beginning of the colluding activities

The ability to leverage rich content, including the information contained in message attachments, can provide a more detailed view than was previously possible into employee, partner, supplier and customer network activity. QRadar Incident Forensics can help uncover information such as the identities of people who have sent messages, applications those people have used, documents they have created or edited, websites they've visited, or other activities they have engaged in on the network.

Significantly, QRadar Incident Forensics provides fast, simple, integrated search capabilities that the security team can use to look behind an attack or breach to identify its cause, help prevent damage and support actions that can reduce risk or prevent additional attacks in the future.

What happens in a QRadar Incident Forensics search?

A QRadar Incident Forensics search is typically prompted by an alert or a suspicion—perhaps a QRadar offense record, a notice of a trending method of attack issued by an organization such as IBM X-Force®, a correlation of event logs and flows that reveal a known pattern of malicious behavior, or a business development such as proprietary information appearing on a competitor's website. QRadar capabilities not only enable security teams to see suspicious events but also to quickly screen out false-positive results and verify additional materials—including unstructured data—that is relevant to identifying the user, what the user is doing, and whether or not the activity is a security concern.

Twitter feeds, Facebook updates, human resources documents, emails, web searches, documents produced by business applications—all can be identified by QRadar Incident Forensics and made available for search and inspection. Packets associated with Voice over Internet Protocol (VoIP) can be used to replay an entire conversation. QRadar Incident Forensics can search for malware embedded in files. And it can search for associated activities. For example, was information that's suspected in the theft of intellectual property recently emailed? And who were the recipients of that email? Similarly, was a file that contains erroneous information that might sabotage a business initiative recently altered? And if so, who made those alterations?

Use case: Fraud and abuse

An organization suspects that unauthorized transactions are being executed, with a negative financial impact on the business.

Objectives

- Locate unauthorized transactions
- Identify the individuals involved in and responsible for unauthorized transactions
- Understand the nature and the frequency of the transactions
- Assess the scope of the risk

Applying QRadar Incident Forensics

- Search for inconsistent or suspicious transactions
- Search for repeated transactions using data visualization
- Uncover the individuals associated with suspicious transactions
- Discover the content of transactions to reveal value and damage

Forensics, then, is about searching for the cause of a known or suspected event. And in its searching, QRadar Incident Forensics goes beyond the conventional ability to gather log and flow data to reconstruct the details of an event. Unlike other solutions that can require an hour or more to return results because they are slowed by retrieval of unrelated materials, QRadar Incident forensics speeds processing of PCAP data by limiting packet capture reconstructions to related content such as IP addresses and timestamps. This helps the security team to quickly discover otherwise hidden information, from motives to future plans to destructive scenarios such as theft that may be in their very early stages and can be stopped before they have any impact on the organization.

How the QRadar solution works

How does QRadar Incident Forensics do this? QRadar collects network information in real time using specialized appliances strategically located throughout an enterprise network. Then, when the security team receives an alert of an incident and submits an investigation query defined by source and destination IP addresses, QRadar retrieves all associated raw packet data and converts it into a highly indexed collection of rich documents saved in a case file. The results are fast because the investigation is directed, and only the data related to a specific QRadar offense is included in the resulting case file.

Using map reduce technology similarly employed in popular Internet search engines, QRadar indexes every document involved in the search. It records, for example, individual words in the text, author name and media access control (MAC) address of the network interface controller (NIC) in a network endpoint. Then, it provides searches of the indexed information on demand, giving the security team information they can use to track down threats and better understand attack vectors. For example: While conventional solutions investigating an Internet relay chat might provide metadata such as the time of day, names of individuals communicating and locations of parties sending messages, the ability of QRadar Incident Forensics to index the content of the message itself, known as the “payload,” can reveal what the conversation was about—such as whether people were conspiring to sabotage the business, steal information or infect systems with malware.

Use case: Network attack

An organization suspects that systems are being compromised by a cyber-attack technique such as a brute force login or SQL injection.

Objectives

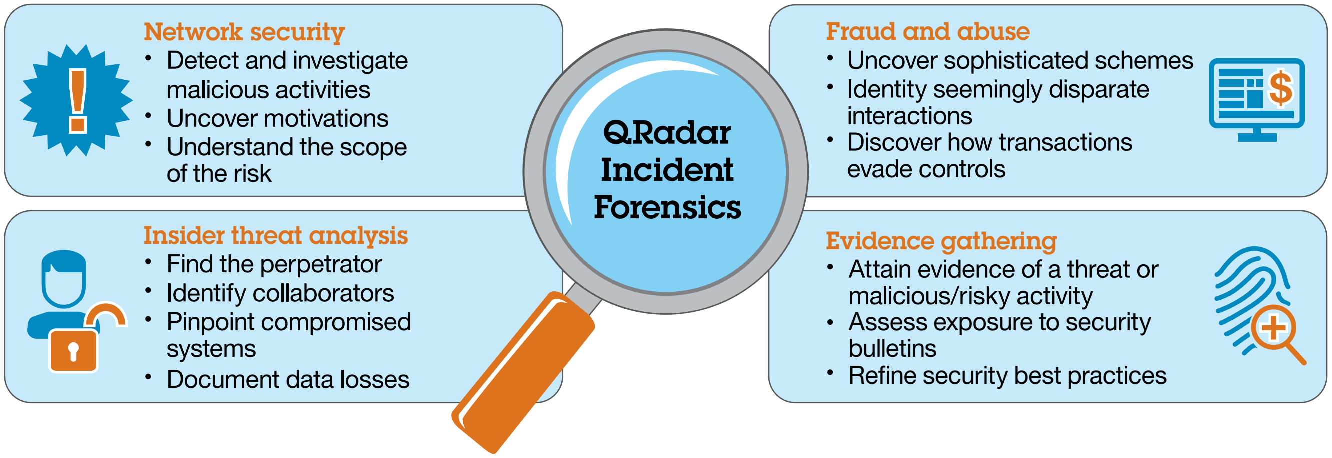
- Determine how many and which systems have been compromised
- Understand the risk to each system
- Uncover actions the attack took to circumvent detection
- Eliminate the code embedded within a system file

Applying QRadar Incident Forensics

- Search for malicious payload or a compromised asset
- Add a "suspect content" filter to refine an existing search
- Trace the interactions of a perpetrator, unaware carrier or compromised asset
- Discover inconsistencies or suspicious interactions

In the case of a brute force or SQL injection attack, an out-of-the-box rule in the QRadar solution develops an offense record and prompts forensics search activity that defines suspect content, data models that use patterns of words, numbers or even malicious code. A search based on suspect content could be looking for easily identifiable number patterns such as Social Security or credit card numbers, or even street names, for example. But it also could be looking for content that does not match the file's extension—a file labeled as an innocent JPG image, for instance, that in reality is an executable file that can launch a malware attack. QRadar Incident Forensics complements SIEM capabilities for deriving security intelligence from flow and log data with capabilities for revealing payload content, enabling a broad approach to identifying, investigating and helping stop risks and threats.

IBM Security QRadar Incident Forensics delivers clarity to security investigations



QRadar Incident Forensics

Network security
- Detect and investigate malicious activities
- Uncover motivations
- Understand the scope of the risk

Fraud and abuse
- Uncover sophisticated schemes
- Identity seemingly disparate interactions
- Discover how transactions evade controls

Insider threat analysis
- Find the perpetrator
- Identify collaborators
- Pinpoint compromised systems
- Document data losses

Evidence gathering
- Attain evidence of a threat or malicious/risky activity
- Assess exposure to security bulletins
- Refine security best practices

Results and benefits using QRadar

Importantly, QRadar Incident Forensics can enhance security, lower operational cost and reduce the security team workload by making it easy to conduct deep analytical searches. With QRadar, it is no longer necessary for the team to have advanced technical knowledge and significant forensics experience. Neither is it necessary to manually mine huge volumes of rich data searching for nuggets of knowledge about a security incident.

Instead, QRadar Incident Forensics provides a powerful but simplified interface that delivers search capabilities in the same familiar way as an Internet search engine. A familiar, free-form search environment reduces the security team's learning curve, enabling them to begin gathering insights sooner with less effort for a rapid return on investment.

By indexing network packet payload data as well as syslog, netflow and file metadata, the QRadar solution enables staff to enter a document name or bits of information contained in the document—in any format, from HTML to JavaScript, DOC, PDF or other—and gather information in the same way an Internet engine searches multiple formats. Once it locates information, QRadar can correlate the payload information to transactions revealed by associated log and flow data. A search might begin, for example, with numbers contained in a spreadsheet, locate that spreadsheet and, through its advanced correlation capabilities, discover which person sent a file containing the identified information to which other person.

Use case: Evidence gathering

Alerted by an X-Force security bulletin, an organization needs to perform a risk assessment to determine if it is at risk or already compromised.

Objectives

- Perform an assessment of the presence of identified vulnerabilities
- Detect the malicious presence of external parties
- Assess evidence of compromise
- Determine if the organization has become a victim of an exploit

Applying QRadar Incident Forensics

- Search for the threat, exploit or vulnerability, starting with individuals who may have been targeted
- Compile a list of incidents and their occurrences
- Cross-reference the incident list with data that may reveal an incident's impact
- Identify the affected individuals and systems
- Analyze the activities associated with the threat or perpetrator

Conclusion

Conventional SIEM solutions that are limited to collecting and examining log source and, potentially, netflow data do not provide the deep insights and clarity organizations need to identify, investigate and understand the cyber threats that abound today. Third-party forensics solutions that attempt to go further typically require specialized, hard-to-find security skills to operate and are slow to act—leaving threats uncovered while cybercriminals or malicious insiders do their dirty work.

IBM Security QRadar Incident Forensics, by contrast, builds on core full-packet capture technology with fast, easy-to-use, integrated capabilities that deliver the broad threat and risk insights organizations need. Utilizing simplified, fast search capabilities across all network content, both in motion and at rest, the QRadar solution delivers intelligence that reveals relationships between users and systems—and highlights suspicious content to reveal not only attack vectors that are already in place but also collusion and planning of theft, sabotage or other malicious actions that can damage the business.

For more information

To learn more about combatting threats and risk with IBM Security QRadar Incident Forensics, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/software/products/en/qradar-incident-forensics

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle