IBM Security QRadar Incident Forensics

Network visibility to help rapidly and thoroughly investigate malicious activity

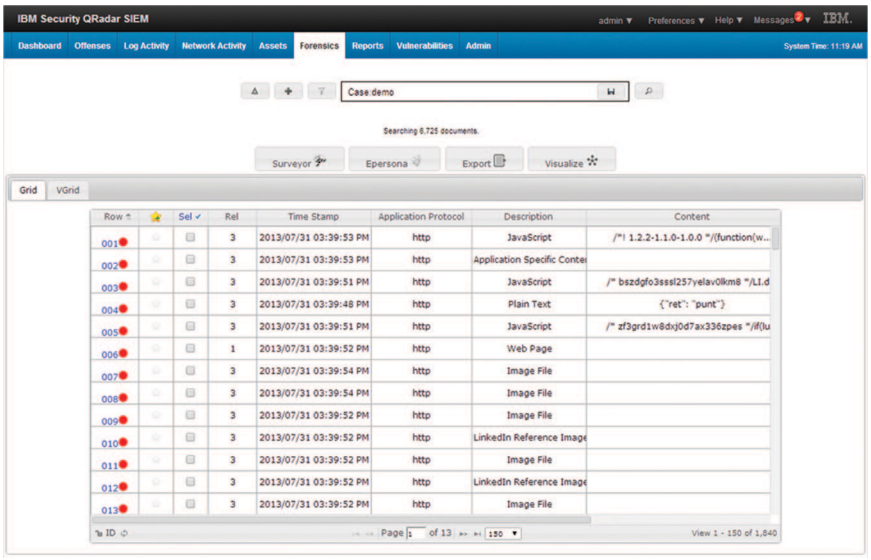
Highlights

- Investigate security incidents using packets captured from across an enterprise network
- Simplify the query process with an Internet search engine-like interface
- Integrate with IBM® Security QRadar® solutions and existing packet capture (PCAP) formats to decode, index, reconstruct and analyze data
- Generate multiple views of data including relationships, timelines, source and threat category
- Build new intelligence by labeling suspected content, adding URL categorizations and visually displaying digital impressions of users or applications
- Help resolve identified incidents, in most cases in minutes or hours instead of days or weeks

IBM Security QRadar Incident Forensics is a software- and appliance-based solution designed to give enterprise IT security teams better visibility and clarity into security incident-related network activities. This insight can then be used to help discover the full extent of a network security incident, remediate damage, and reduce the chances of data exfiltration or the recurrence of past breaches.

In today's enterprise environments, where too many vulnerabilities exist and too few staff hours are available to manually investigate and remediate incidents, QRadar Incident Forensics delivers insight and analysis that cannot be achieved using only log source events and network flow details. The solution provides powerful indexing, searching, data pivoting and reporting capabilities that support smarter, faster decisions by the IT security team.

A simple, search engine-like interface allows for intuitive searches for data related to a security incident—including data at rest (documents) or in motion (packet captures), structured or unstructured data, and documents and files ranging from email messages, voice-over-IP (VoIP) phone calls, website visits, blog posts and even message attachments such as files or pictures. QRadar Incident Forensics indexes and correlates all of this data, prioritizing search performance to help quickly distinguish true threats from false positive results generated by an existing SIEM correlation rule. By reconstructing raw network data back into its original form and retracing a security incident, the solution provides valuable information to help support network security, analyze and help prevent external attacks and insider threats, and document incident-related evidence.



IBM Security QRadar Incident Forensics search results appear as a prioritized list based on the relevance to a Boolean, free-text query.

Investigations that reach beyond pure packet captures

QRadar Incident Forensics seamlessly integrates with IBM QRadar Security Intelligence Platform using its one-console management interface. Compatible with standard PCAP formats, the solution enables directed analyses investigating QRadar offenses or possible attack conditions identified by external threat intelligence sources such as IBM X-Force®. It delivers visibility and investigation for security incidents across the entire network infrastructure.

QRadar Incident Forensics, unlike less comprehensive solutions, not only extracts more usable data from PCAPs, it can also import related documents and files and make all of these materials available for search-driven data exploration. The solution enhances search performance with its powerful indexing capability, which indexes the metadata and the actual payload of PCAPs or file documents. This enables the analyst to perform text-based searches that may involve numbers, dates or keywords. The solution supports both real-time investigations of suspicious activity and reconstruction of previous actions, returning search results in seconds, in most cases.

A comprehensive process for identifying and analyzing incident-related data

Used in a security incident investigation, QRadar Incident Forensics returns information on data and network relationships, event timelines, event sources and threat categories via steps and capabilities that include:

- **Index**—The solution indexes all available network data, file data, metadata and even the textual characters in each recovered file; it then stores everything using a scalable search engine indexing system.
- **Reconstructions**—By recognizing IP sessions embedded in PCAP data, the solution collects all associated raw PCAP data and reassembles the content into its natural form, retaining and reconstructing the full content of each file in each session; it then saves information in the appropriate format, such as DOC, PDF, PPT, HTML or MPEG3.
- **Search engine**—When it receives a query via the search interface, the solution responds with a list of activities and assets ordered by relevance to the query. These may include chat conversations, file transfers, web pages visited, spreadsheets or similar.
- **Surveyor mode**—In answering a query, QRadar Incident Forensics presents interactions in a chronological order.
- **Presentation**—When a result is returned by the search engine and is opened, assets contained in the result are displayed in their native format. Websites, including social networking and photo- and file-exchange sites, are shown as the reassembled elements would appear online.
- **Data storage**—The solution retains only the information created during an investigation case rather than huge volumes of raw PCAP data past a user-defined expiration date, reducing storage capacity growth and enabling longer-term security incident analyses.
- **Visual exploration**—The solution empowers the security analyst to view associations and relationships visually across multiple attributes and to navigate efficiently from one data category to the next based on the needs of the investigation.

Critical insights and information from big-data analytics

QRadar Incident Forensics is designed to help IT security teams identify suspected content, define new correlation rules, categorize content by URL reputations and build digital impressions that show network relationships. Its powerful data-pivoting capability can reveal extended and sometimes hard-to-find relationships for searchable variables such as IP, MAC and email addresses; application protocols; user queries; and SSL certificates.

The solution's big-data analytics capabilities return critical insights and information in three key areas:

- **Digital impressions**—QRadar Incident Forensics visually reconstructs network relationships to help reveal what or who an attacking entity is, how it communicates, and what it communicates with.
- **Suspect content**—A set of pre-built rules can use data patterns or known behaviors to identify reconstructed content as suspicious.
- **Content categorization**—The solution enables investigators to dynamically categorize PCAP content based on metadata and automatically filter it using intelligence feeds from organizations such as X-Force. Filtering by categories also helps improve productivity and performance.

Why IBM?

The rapid response and information provided by QRadar Incident Forensics can help IT security teams reduce the time it takes to investigate QRadar SIEM offense records, in most cases from days to hours or even minutes. Once an incident is identified as a legitimate threat, security teams can retrace the step-by-step actions of an intruder, helping them remediate activities associated with successful breaches and reverse actions to prevent recurrences.

In defending against advanced persistent or internal threats and fraud, QRadar Incident Forensics can help IT teams document their regulatory compliance. Security teams can benefit from a dramatic improvement in their ability to rapidly distinguish true threats and attacks from false positive results, and can begin to formulate proactive security best-practice approaches based on a clearer understanding of network security incidents.

For more information

To learn more about IBM Security QRadar Incident Forensics, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/services/us/en/it-services/security-intelligence.html

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2014

Please Recycle

WGD03033-USEN-00