QRadar Network Insights Delivers Real-time Insights Like Nothing Else

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

March 2017

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

QRadar Network Insights Delivers Real-time Insights Like Nothing Else

Table of Contents

QRadar Network Insights Delivers Real-time Insights Like Nothing Else

Executive Summary

Today, detecting and resolving security incidents requires a faster pace and more data than ever. Traditionally, meeting these two challenges puts the security teams at odds. To resolve incidents with enough clarity and detail to be assured that the incident was not a false positive, and that the analyst had sufficient details for a satisfactory resolution, meant having a specialist dive into the incident to retrieve the necessary data. The investigation process could take hours to days to complete, while responding faster meant curtailing or even foregoing a deep investigation to deal with the problem at hand.

Security operations teams are faced with the paradox of time vs. detailed context on a daily basis and often find they have to make a choice of which is more important. IBM is addressing this very problem with the release of QRadar Network Insights (QNI). QNI addresses the paradox of being able to accelerate incident response to shorten dwell time and overall incident impact, versus gathering enough context to ensure that the analyst is chasing a real incident and has the required information to address it appropriately. QNI delivers the ability to capture packet streams, dissecting them for suspicious content in real-time and then augment data in QRadar with that enriched content.

This paper discusses the relevancy of QNI's approach, the benefits of its technology, its technological differentiation, and ultimately several primary use cases surrounding the need for its capabilities.

The Value of QNI for Identifying Attacks and Breaches

The first thing to teach the inexperienced security professional is that regardless of what happened where, over 99% of attacks leave traces on the network. The question is, "Were the security and/or network teams prepared to catch it?" Aside from an internal attacker collecting local system data and copying it to removable media, taking screen shots, writing it down, or locally printing it, all other activities traverse the network. Attacks via email or web delivery, attack command and control, reconnaissance, and data collection across systems all leave network artifacts.

This is why IBM® developed QRadar Network Insights® (QNI™). IBM recognized the need to collect network telemetry continuously at high speed and provide analysis on that data so it can be combined with other log artifacts on the fly. QNI solved several consistent problems to achieve this approach.

Enhancing Context and Visibility

The factors listed in the section above are exacerbated by several common tool insufficiencies. Security personnel indicate they are impacted in their ability to gain context, and therefore visibility, into their environments due to a number of factors:

1. Sixty-five percent (65%) denote that their tools have a lack of integrations or APIs to couple data for correlation and analysis.
2. Thirty-eight percent (38%) indicate their management consoles provide insufficient information.
3. Thirty-seven percent (37%) identify their reporting tools provide insufficient information.

The majority of alerts are created as severe and critical, so actual critical alerts are lost in the in the sea of overall alerts due to the lack of upfront analysis. This exemplifies the old saying, "If everything is critical, then nothing is" and is directly caused by the lack of good, timely data and proper upfront analysis.

Detailed Packet Dissection at Line Speed

Though this may seem like a problem solved long ago by various IDS and IDP technologies, such is not the case when comparing them feature by feature. Though IDS and IDP sensors can tear packets apart, what they can do with information in the allotted time is significantly different. First, IDS and IDP deployed inline have only a few milliseconds to make a pass or decision, so they cannot dissect and analyze each packet to the same level as QNI. Since QNI is deployed in passive mode to merely sniff packets, not intercept them, it allows significantly greater time to evaluate the content and the context of the packet. Beyond the basic and common features like protocol identification, IP header breakout, byte and packet counts, session timing, VLAN information, and attack exploit evaluation of the packet, the features that make QNI stand out are:

1. Real-time application-level insights applied to the context of the session and the data.
2. Real-time deep content analysis (not performed by most IDS/IPS).
3. Real-time multi-session artifact analysis, correlation, and creation of comprehensive relevant metadata on the frontend to reduce false positives and enhance incident classification.
4. Operator customizable suspect data feeds to enhance monitoring, ongoing investigations, and retrospective analysis (configured via YARA rules).
5. Identification of malicious content with the context of the assets, applications, and users.
6. Out-of-the-box content that allows QRadar to leverage data from QNI for advanced detection for key use cases, including phishing, lateral movement, and data exfiltration, among others.
7. Insights into user and application behavior based on real-time network activity that enables deeper levels of insider threat detection.

This data is used to augment the QRadar prioritization of relevant alerts for the operator's attention and the data added to the incidents to accelerate alert-handling research and resolution.

QNI Delivers Extensive Enriched Metadata at Time of Incident Creation

Metadata is critical to success with breach investigations. EMA research asked security professionals how valuable they felt metadata was to their investigations. Seventy-four percent (74%) responded that it was either very valuable or invaluable to them for security investigations.

QNI not only delivers primary data extracted from the protocol, packet, session, and application information; it creates a plethora of metadata to add to the data repository in QRadar. QNI produces literally dozens of pieces of metadata. Below, EMA listed some of the most interesting and useful data that QNI delivers for the initial evaluation of an incident:

1. Host- and session-related DNS information
2. HTTP metadata, URLs, and redirects involved in the session
3. File data, file hashes, file entropy (image and audio files especially)
4. Email sever usage, senders and receivers, subject lines, and file attachments by type
5. Detected PII and confidential data based on defined criteria
6. Detected embedded scripts
7. Identification of known assets

Once this metadata is analyzed and fed into QRadar, analysts have the deep network data they need to detect advanced threats, perform historical analysis, and leverage even more of IBM's analytics to improve their security posture.

QNI Changes the Defense Paradigm from Reactive to Proactive

EMA identified that only 14% of organizations use full packet data for all investigations. This stems from two issues. First, full DPI tools can be very expensive, not just for the capture capability but for the analytics tools needed to gain full value. Second, even for small organizations, the cost of storing full packet inspection information collected continuously can become astronomical.

Another issue faced in most full packet inspection implementations, even if they are running at the time of the event, is that full packet inspection systems do not contribute information to the case in real-time. The analyst has to access the system separately to import the data. In cases where the data is automatically imported into a central data repository, it is done in batches, not streamed, and/or the analyst has to create and execute queries to stitch the data together with other log information. Again, this supports only the post incident/breach forensic approach. It also brings to light another impediment to operations. If the full packet inspection system is separate or requires a manual data import, this takes valuable time away from the investigation.

Bringing the enriched, context-enhancing data into the incident investigation creates numerous operational advantages for the SOC. First, it accelerates incident detection and response. The increased visibility sheds light on low and slow, multi-phase, and other forms of attacks previously unseen. Threats that were formerly hiding in normal application traffic such as web, email, and file transfers are now more easily identifiable. Attacks that used polymorphic code, rotating payloads, and other means of avoiding signature-based detection no longer go undetected. Attacks that abuse DNS and HTTP traffic to avoid detection are no longer a threat.

Because operations receive more telemetry faster, attacks are neutralized at earlier phases such as the reconnaissance or early breach phases, thus removing or severely shorting the attacker dwell time. This in turn means that if a breach does occur, the opportunity to expand their footprint through lateral movement, even in fully-automated attacks, is nonexistent to severely reduced. The reduced scope of breach means less manpower is spent on investigation and remediation. The combination of all these factors reduces both the opportunity cost and the real cost of a breach.

QNI acquires data, preprocessing or pre-analyzing it, and injecting it into QRadar in near real-time. Rendered metadata includes the network components of an attack combined with the application, system, and user-related information already in QRadar. This information provides the SOC with the advantage of having an enhanced level of detail at the *start* of the incident rather than the end!

Where QNI Provides Value to Operations

Getting the Right Data in a Timely Manner

Another significant issue security teams face is getting the right data at the right time. Breach detection requires accurate contextual data at the beginning of an incident. Providing that data at the beginning drives a more accurate incident classification and a faster, more efficient resolution. The timeliness of data can vary significantly between different tools, data processing, and delivery architectures. This often means that data is delivered much later in the incident lifecycle. Though data can be useful on the backend of the process for post-breach forensics, the lack of frontend integrated analysis of the collected data limits its usefulness up front. Fifty-eight percent (58%) of security personnel indicated to EMA that they do not have sufficient analysis capability in their toolset to provide the proper data relevance; thus, they must spend a significant amount of man hours in human research and analysis.

QNI operates at line speed, scaling horizontally to meet greater processing need.

SOC Challenges

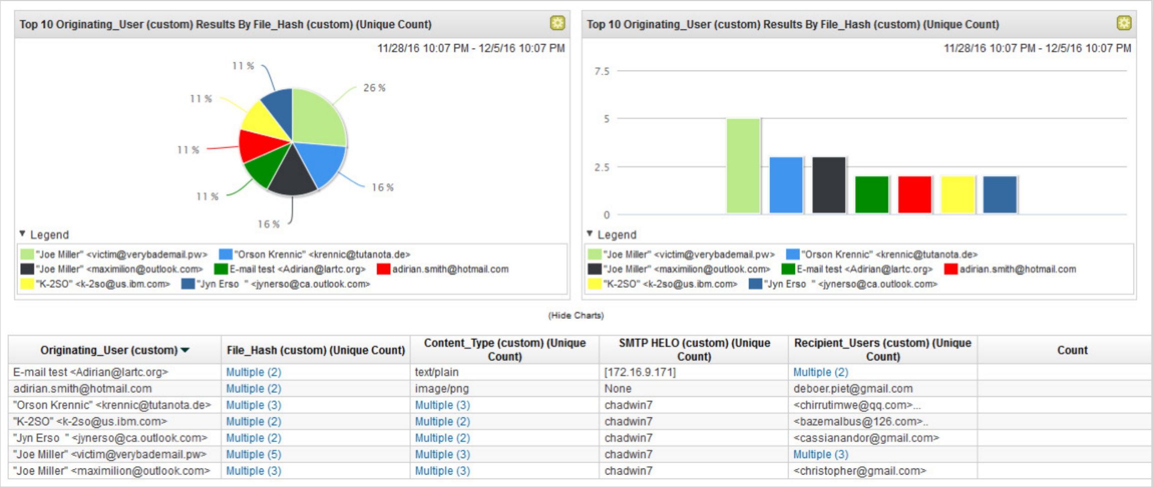
QNI has value across the entire SOC. Every operational role can and should leverage it. Both the tier 1 operator generally responsible for initial incident triage and the tier 4 advanced analyst who is assigned threat hunting can receive value.

For tier 1 operators, the early analysis and data enrichment means they receive fewer false positives and the alerts they do receive have better prioritization/classification. Having better data in the incident also means the analyst has faster access to critical data. Improvements seen by tier 1 include reduced incident volumes, faster incident response, and more efficient incident handling.

Tier 2 and 3 personnel experience reduced handoffs. With the enhanced incident data, customizable data feeds, and automatable data collection, these valuable personnel can reduce the time they spend collecting the required data. This results in quicker and more accurate diagnosis of the complex incidents driving faster first-time resolution.

With the enriched data, tier 4 personnel can look deep inside files and content to distinguish between normal and suspect activity. They can also identify the who, when, and how relating to an incident or breach. This allows them to quickly relate data correlations, accelerating investigations, and "connect-the-dots" between events that were previously seen as unrelated because the data just was not available. By quickly relating data correlations, personnel can better identify stealthy breach attempts and quantify the scope of a breach. This drives reduced attacker opportunity.

Key QNI Use Cases


Top 10 Originating_User (custom) Results By File_Hash (custom) (Unique Count)
11/28/16 10:07 PM - 12/5/16 10:07 PM
11 %
26 %
11 %
11 %
16 %
11 %
16 %
Legend
🟩 "Joe Miller" <victim@verybademail.pw>
🟦 "Orson Krennic" <krennic@tutanota.de>
⬛ "Joe Miller" <maximilion@outlook.com>
🟩 E-mail test <Adirian@lartc.org>
🟥 adirian.smith@hotmail.com
🟨 "K-2SO" <k-2so@us.ibm.com>
🟦 "Jyn Erso " <jynerso@ca.outlook.com>
Top 10 Originating_User (custom) Results By File_Hash (custom) (Unique Count)
11/28/16 10:07 PM - 12/5/16 10:07 PM
7.5
5
2.5
0
Legend
🟩 "Joe Miller" <victim@verybademail.pw>
🟦 "Orson Krennic" <krennic@tutanota.de>
⬛ "Joe Miller" <maximilion@outlook.com>
🟩 E-mail test <Adirian@lartc.org>
🟥 adirian.smith@hotmail.com
🟨 "K-2SO" <k-2so@us.ibm.com>
🟦 "Jyn Erso " <jynerso@ca.outlook.com>
(Hide Charts)

Originating_User (custom) ▼	File_Hash (custom) (Unique Count)	Content_Type (custom) (Unique Count)	SMTP HELO (custom) (Unique Count)	Recipient_Users (custom) (Unique Count)	Count
E-mail test <Adirian@lartc.org>	Multiple (2)	text/plain	[172.16.9.171]	Multiple (2)	
adirian.smith@hotmail.com	Multiple (2)	image/png	None	deboer.piet@gmail.com	
"Orson Krennic" <krennic@tutanota.de>	Multiple (3)	Multiple (3)	chadwin7	<chirrutimwe@qq.com>...	
"K-2SO" <k-2so@us.ibm.com>	Multiple (2)	Multiple (2)	chadwin7	<bazemalbus@126.com>..	
"Jyn Erso " <jynerso@ca.outlook.com>	Multiple (2)	Multiple (2)	chadwin7	<cassianandor@gmail.com>	
"Joe Miller" <victim@verybademail.pw>	Multiple (5)	Multiple (3)	chadwin7	Multiple (3)	
"Joe Miller" <maximilion@outlook.com>	Multiple (3)	Multiple (3)	chadwin7	<christopher@gmail.com>	

Figure 1 QRadar Dashboard with Enhanced QNI Data

Phishing

95% of all attacks on enterprises come from successful spear phishing. Those emails containing malicious links and attachments entice the recipient to click on them. If the recipient does, the user is compromised and the attacker is well on his/her way.

By detecting, extracting, and analyzing information such as email sender domains, subject lines, embedded links, and attachment content and hashes, QNI provides QRadar the ability to detect phishing campaigns before users access their inbox.

Insider Threat

In the past several years, insider threat gained lot of attention as a threat vector. In reality, though insider threat is a serious issue, the number of dishonest employees is not growing. The larger issue is that insider identities are being compromised through various means, so external threat actors can masquerade as trusted insiders utilizing legitimate identities to perform reconnaissance, lateral movement, and ultimately data exfiltration.

To deal with this ever-looming problem, QNI collects data on network activities relating to individual activities, including unapproved web browsing or searches, access into risky or suspicious domains, resolving aliases and privileged identities triggered by suspicious content, and feeding activity details to QRadar for user behavior analysis that indicates anomalous behaviors. Once identified, these risky users can be placed on a dashboard to trace their activities until it is no longer necessary.

Lateral Attack Movement

Years ago, personnel judged the success of an attack on how fast the threat actor could escalate to administrator privilege and do "something" in or to the system. Now, many attacks focus more on staying below the radar and collecting information to maximize data collection once administrator level access is achieved, if it ever actually needs to be invoked. Most data in the environment is available to normal users, so attackers do not need to escalate privilege to obtain their goals.

Once in, they need to move to explore and understand more about the environment to increase their system's foothold and data gathering capability. QNI identifies and catalogues this behavior. It looks deep into the communication between devices to detect reconnaissance, pivoting, and transfers between devices indicative of malicious lateral movement. No matter how it starts, lateral movement has to cross the network where QNI's ever-vigilant analysis is waiting. The detailed information is sent to QRadar for creation of new events or to corroborate previously existing events so analysts can instantly respond.

Malware and Ransomware Detection and Analysis

As attackers deliver malware to target systems, QNI is watching and analyzing the data streams to identify the threat. QNI knows the details of every file from the file name, type, entropy, embedded scripts, and file hash, to where the file came from and where it was sent. By supplying that information to QRadar and leveraging threat intelligence from X-Force Exchange, it becomes clear when malware evaded other detection methods. The threat from all instances of the malicious file within the environment can then be mitigated.

Ransomware is most effective (drawing the greatest ransom payments) when it encrypts attached storage and then compromises other systems. To get to the other systems, it identifies them through reconnaissance and uses the entitlements of the compromised individual to attach and infect the other systems in the environment. QNI identifies ransomware activities by combining the methods of detection it uses for phishing, insider threat, lateral attack movement identification, and malware.

Data Exfiltration

The end goal of most attacks today is some form of monetization, which involves capturing data. Other than ransomware encrypting data where it sits, to monetize the data, ransomware must be extracted from the environment. QNI is watching. When dissecting the network conversations it uncovers sensitive data, leaving the network via emails, chat messages, file uploads, social media, etc. and does it in real-time. IT even detects data hidden in non-standard formats and protocols like abnormal DNS payloads. If attacks are given the proper access, IT can intercept and decrypt SSL tunnels.

EMA Perspective

No other "security intelligence" vendor is offering a similar technology that scans incoming and outgoing packet data for signs of malicious intent at the same level of detail and timeliness. QNI added 30 new fields to the "flow" data extending the protocol's defined metadata to include layer seven content serving as the early warning signal when packets carry anomalous material.

QNI is not a mere "bolt-on" technology. IBM created it as a comprehensive suite of capabilities for incident detection, prioritization, and analysis with the intent to change the way analysts operate. It brings more forensic quality data to analysts earlier in the event lifecycle. In relation to the cyber kill-chain, QNI data moves incident visibility from after the "Actions and Objective" phase, where it is normally used in support of post-breach forensics, to the "Reconnaissance," "Weaponization," and/or "Delivery" phases, facilitating earlier detection. This enables analysts to act earlier and thwart attacks, or at least reduce incursion time for breaches. Acting earlier reduces the incursion window and also decreases the cleanup timeframe and overall resources needed. The QRadar interface augments data streams to maintain streamlined operations. The data is then also leveraged within the reporting engines to support all of the various reporting that QRadar provides.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3534.030917