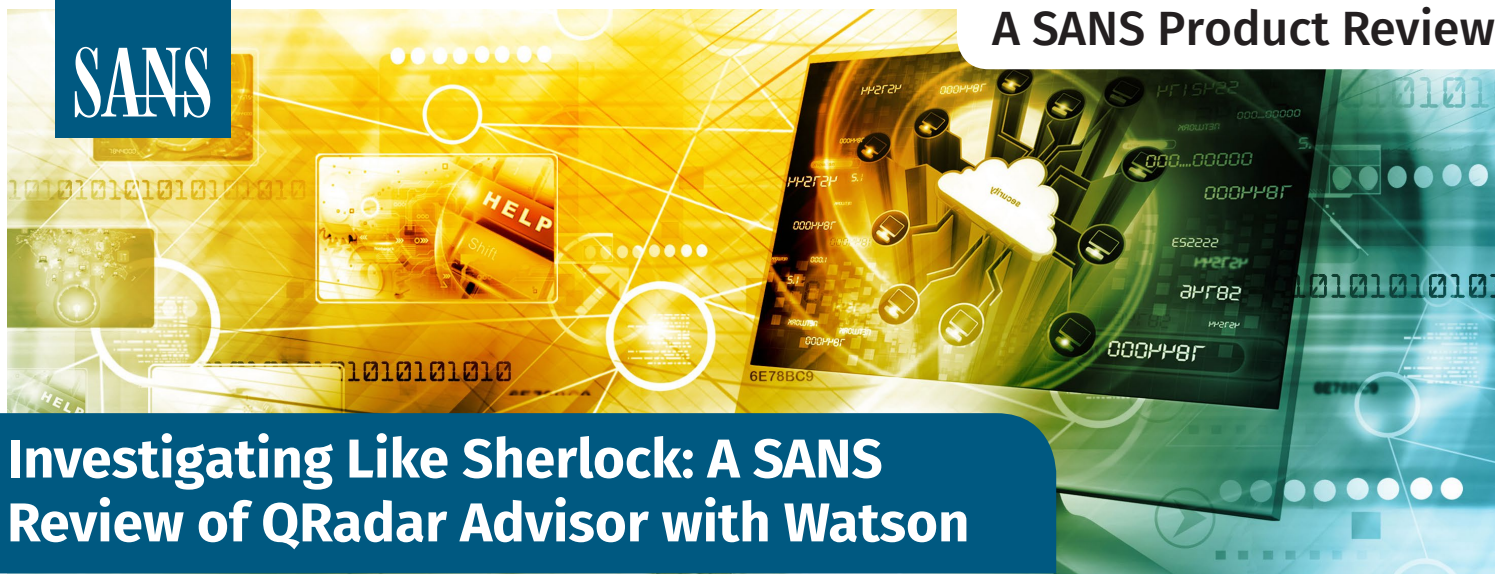
Investigating Like Sherlock: A SANS Review of QRadar Advisor with Watson

Matt Bromiley

SANS

A SANS Product Review



Investigating Like Sherlock: A SANS Review of QRadar Advisor with Watson

Written by **Matt Bromiley**

October 2019

Sponsored by:

IBM

Introduction

The role of a modern information security analyst is one that can be simultaneously scattered and daunting. Investigating threats to an environment often involves poring through gigabytes, if not terabytes, of data, trying to understand the differences among multiple evidence sources. Furthermore, analysts may need extra time to consult external data sources to vet and/or confirm their findings—yet another task that can result in unnecessary data point consumption. Because time is the most valuable asset to any responder, the more of it we can devote to neutralizing attackers, the better.

Automation is touted as one of the ways to help streamline analyst workflows. With it analysts can script out functionalities to help them contain or remediate threats faster. Improving the automation in one's environment is an additional technique that can combat the supposed skills shortage in cybersecurity. Unfortunately, these time-saving techniques are often unique to analysts or particular teams; not every member of an investigative team may have the same automation capabilities. This disparity can lead to a significant discrepancy in the consistency and/or confidence with which analysts report results.

In this paper, we examine QRadar Advisor with Watson (QRAW), a platform that combines IBM's famous Watson with QRadar. QRAW brings a unique vantage point that helps analysts streamline investigations, add crucial context and make faster, more confident decisions on suspicious traffic in their environments. We found QRAW to be a force multiplier for most modern security teams, primarily because we were able to triage, assess and act significantly faster with QRAW's input.

Time is your asset, until an attacker starts to take it away. Finding ways to analyze, correlate, automate and make confident decisions faster reduces dwell time and keeps time on your side.

Some of the highlights from our testing of QRAW included:

- Consistent investigative results and increased analyst confidence
- Mapping of key details and observables to Mitre's ATT&CK™ Matrix
- Automatic graphing and link analysis, allowing for easier intrusion data consumption
- Correlation between current and historical events and threats, allowing for a wider view across organizational history

While assessing QRAW, we constantly found ourselves armed with significant amounts of data, but consumption and correlation were easier. Threats were classified, and we found we were able to confidently assess threats with the data presented. As you read through this paper, ask: Can your analysts do the same?

Change Your Perspective

Before digging into our highlights of QRAW, we must discuss the need for a changed perspective in information security. Unfortunately, some security teams are forced to treat their environment in a piecemeal fashion, at least from an investigative perspective. This perspective tends to separate key components of the environment (such as endpoints, network, log sources, internal versus external, and the like) into individual pieces that analysts must work hard to correlate. This additional work is often a waste of time that provides a longer "runway" for attackers to utilize.

To help alleviate these concerns, some organizations will utilize central logging, aggregation, and/or SIEM platforms and simply "turn everything on." The result is a platform bloated with various data sources, the value of which may never be determined. Some data sources may be normalized; others may not. While log aggregation platforms do bring all the data points into one place, they do very little to assist the analyst if data points are not correlated, enriched and *providing value to the security team*. A changed perspective means your organization is utilizing tools and platforms that return value to the security team, making their lives easier and allowing for more confident decisions about incidents and intrusions.

Your tools and platforms should add value to the security team. If they don't, keep looking until you find those that do.

An easy way to return value to your security team is to break out of piecemeal visibility and investigations. One of our favorite takeaways when working with QRAW was the capability of viewing the environment *holistically*—seeing how all the data points work together. After all, when an attacker enters an environment, it will cross multiple lines, affecting both network- and host-based artifacts along the way. Any security team that voluntarily omits an evidence source simply due to difficulty of ingestion or correlation is likely never seeing the extent of threat actor activity. Holistic visibility is the first force multiplier for your security teams.

Lastly, when changing your organization's perspective, it is now impossible to ignore threat intelligence to enrich your data, add context and provide insight into the incidents you are experiencing. Threat intelligence has two primary sources: internal and

external. Internal threat intelligence is composed of the *institutional knowledge* of your organization; the incidents and intrusions you have previously suffered, and the attacks you have defended against. *External* intelligence helps you uncover what the rest of the world is experiencing—to help defend against or detect the unknown.

We found that when working with QRAW, much of the above has already been done for your security team. That work allowed us to focus on making decisions and protecting the organization. Incident detection and response became fun again.

Getting Smart with Watson

As we examined QRadar Advisor with Watson, we found ourselves with extra time almost immediately. Not because we had no intrusions—on the contrary, tasks that are typically done manually by analysts or scattered across multiple tools were done for us and provided in central investigation screens in QRAW. While a wealth of information can provide insight and visibility into the environment, this review focuses on performing investigations alongside QRAW.

Offenses and Investigations

One of our favorite features of any platform—and something that QRAW delivers on—is the capability of getting to the *data that matters* immediately. As shown in Figure 1, QRAW begins by categorizing "Investigations."

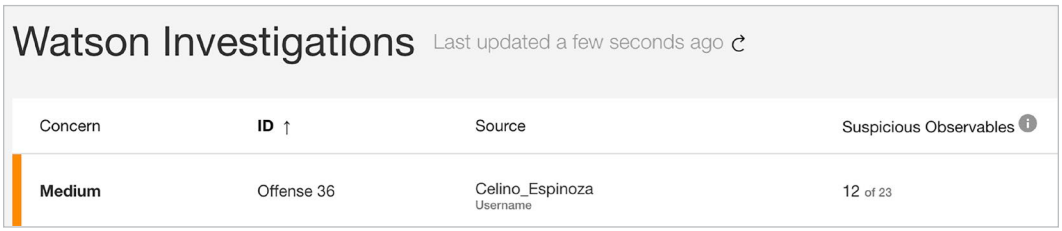


Figure 1. Example of How QRAW Categorizes Investigations

Note that a QRAW investigation is not a template to which an analyst adds results; instead, it is a collection of data points that QRAW has correlated into analysis. Investigations are typically associated with "Offenses," as shown in Figure 2, which provide insight into suspicious activity and anomalies within the environment.

While the metadata surrounding a particular Offense resembles what some analysts may refer to as an alert, there is a lot of important metadata present. One of our favorite key data points is the "magnitude" of a particular Offense. This visual representation helps analysts quickly determine what the top Offenses are so they can focus their time accordingly. It's amazing how a simple, visual assessment of a threat can boost analysts' confidence.

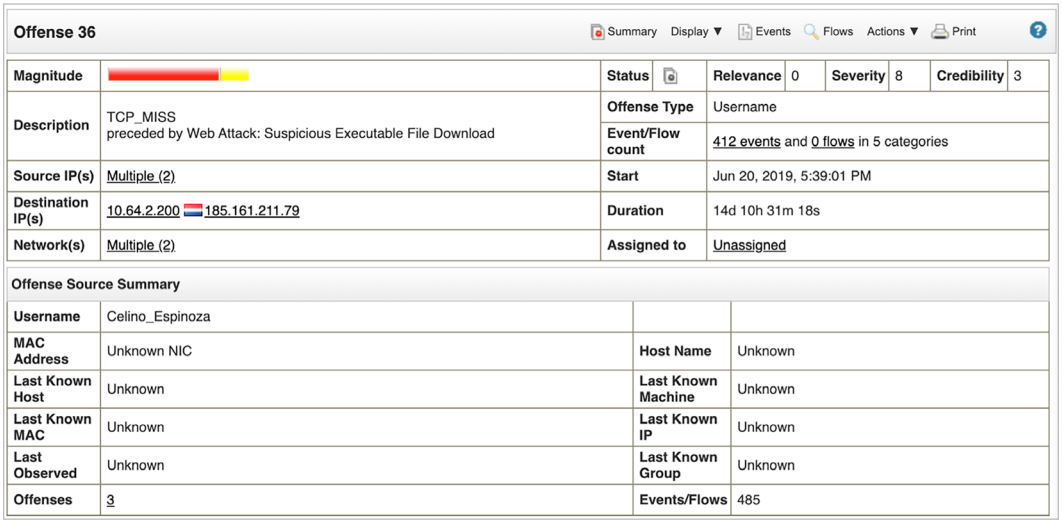


Figure 2. Offenses

Anything underlined in the Offense tab is interactive for the analyst. For example, there are two IP addresses represented within this Offense: one internal, one external. QRadar Advisor recognizes these data types and provides useful actions right from this screen. For example, simply hovering over the external IP address, as shown in Figure 3, displays automatic geolocation and mapping.

Figure 3. Screen Displaying Automatic Geolocation and Mapping

Furthermore, an analyst can also begin action against either IP address. As shown in Figure 4, right-clicking any IP address allows an analyst to perform DNS and WHOIS lookups, port scans, or view in the context of the network.

These actions would typically require an analyst to open a new browser tab or switch to a different tool. Any platform that provides context and insight into an investigation—while allowing for an analyst to take actions right *from the same screen*—is always going to save time during investigations.

Figure 4. Right-click on IP Address Enables Additional Functions

Typically, an analyst's next steps may be to take any observables, such as an IP address or technique, and begin performing lookups to identify any context or actors associated with available observables. Because we have Watson with this instance of QRadar, however, our analysts have even less work to do!

After an Offense has been investigated with QRAW, key metadata about the Investigation will be present in the Offense tab as well. Figure 5 displays a screenshot of the QRadar Advisor with Watson sub-tab that allows for a high-level snapshot of QRAW's key concerns about this Offense.

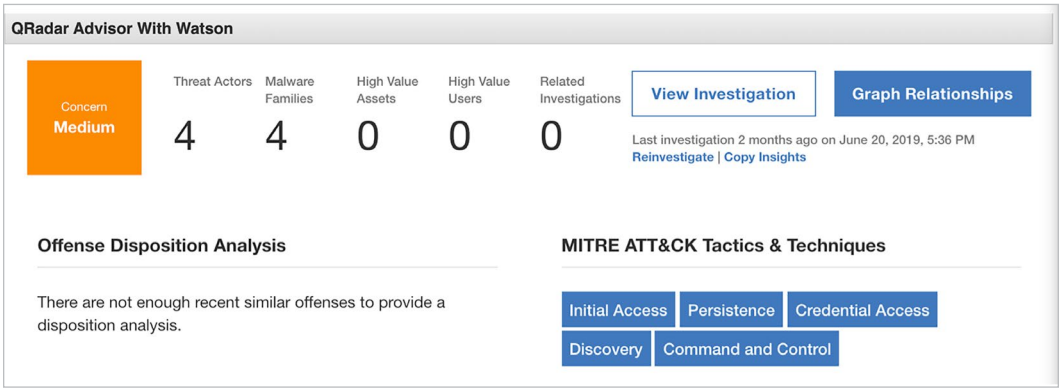


Figure 5. QRadar Advisor with QRAW Sub-tab Showing Key Concerns

Notice that in Figure 5, the analyst is provided with immediate context to help further assess the validity and importance of an alert. The key data points that can help influence this decision include:

- The number of associated threat actors and malware families
- The Offense Disposition Analysis, which analyzes similar and/or previous Offenses to make a rapid disposition for the analyst
- Techniques associated with this Offense, mapped to Mitre's ATT&CK Matrix
- The value of the assets and users involved with an Offense; QRAW immediately calls out any high-value items that may propel an investigation's importance.

Moving from an Offense into an associated Investigation begins to open up the power of QRAW. Viewing Investigations is one part that we enjoyed the most, primarily because information we're used to gathering manually was already captured and provided for us! Let's dig into this Investigation further.

From Observables to Context

Clicking into an Investigation allows QRAW to shine with rich metadata and context about an associated Offense. Figure 6 shows, for example, that our knowledge of this Offense has now been expanded to include two critical alerts, both of which are network artifacts. Furthermore, we can see associated threat actors and malware families related to this Offense.

Some additional—and extremely helpful—context tells us whether the particular observable has been found locally in our environment. Note that we didn't have to pull on any strings to find this additional context—QRAW did it for us.

One of our favorite parts of the entire platform was the automatic mapping of observables to known MITRE ATT&CK Tactics and Techniques, provided in Figure 7.

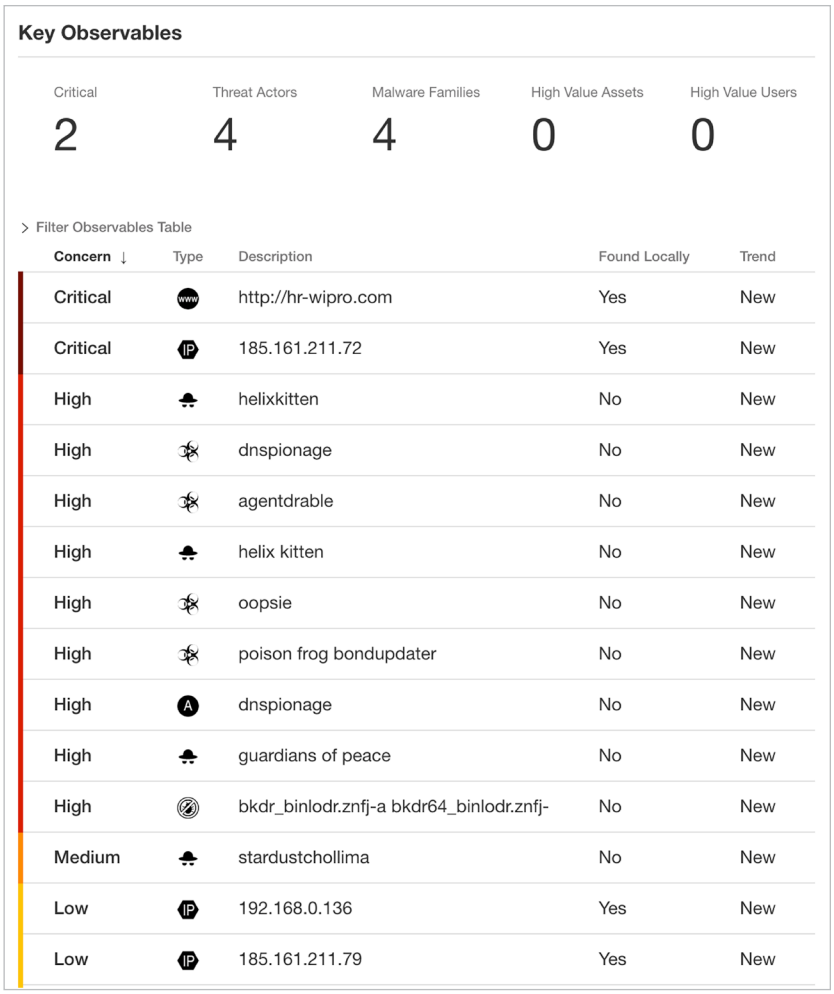


Figure 6. Key Observables

Information security analysts at all levels have come to know the MITRE ATT&CK Matrix as a way to build a common vocabulary when describing threat actors, techniques, campaigns and malware—to name just a few. By performing this automatic mapping for us, QRAW was able to speak a language that many investigators and responders are already used to speaking—*without having to perform manual correlation!*

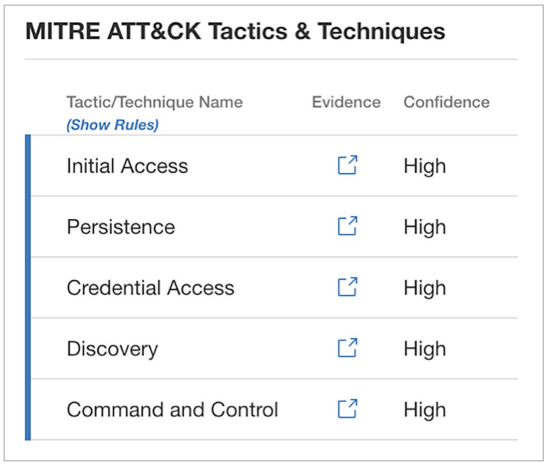


Figure 7. Automatic Mapping of Observables to Known MITRE ATT&CK Tactics and Techniques

Correlate All the Things

Another one of our favorite features in QRAW was the capability to graph relationships. Similar to the ATT&CK Matrix, link analysis is another skill and language that analysts speak easily. Often, however, graphing is done manually or is minimal to the point of questionable usefulness. QRAW reversed this position for us, by providing incredible link analysis and customization techniques. Figure 8 on the next page provides insight into an initial graph that was generated by this particular investigation.

Interestingly enough, we found ourselves resorting to the graph more often than not to help assess the severity of the Investigation QRAW had provided. For example, savvy investigators may have noticed in the Key Observables table (Figure 6), that multiple groups were represented, with clearly different state-nexus associations. This difference may seem confusing to some analysts; link analysis and graphing helped us solve that problem.

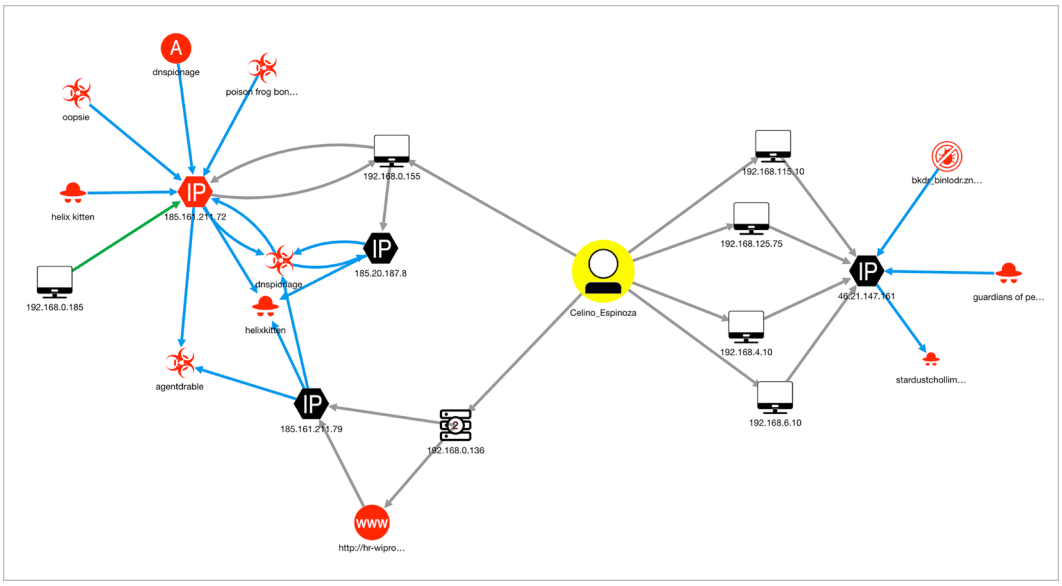


Figure 8. Insight into Initial Graph Generated by an Investigation

Furthermore, QRAW allowed us to customize the graph to remove data that may not be relevant to us. Figure 9 provides a screenshot of the exact same graph. The grayed-out areas of the graph represent QRAW's "Local" graphing feature, which highlights only observables that have been seen in our local environment.

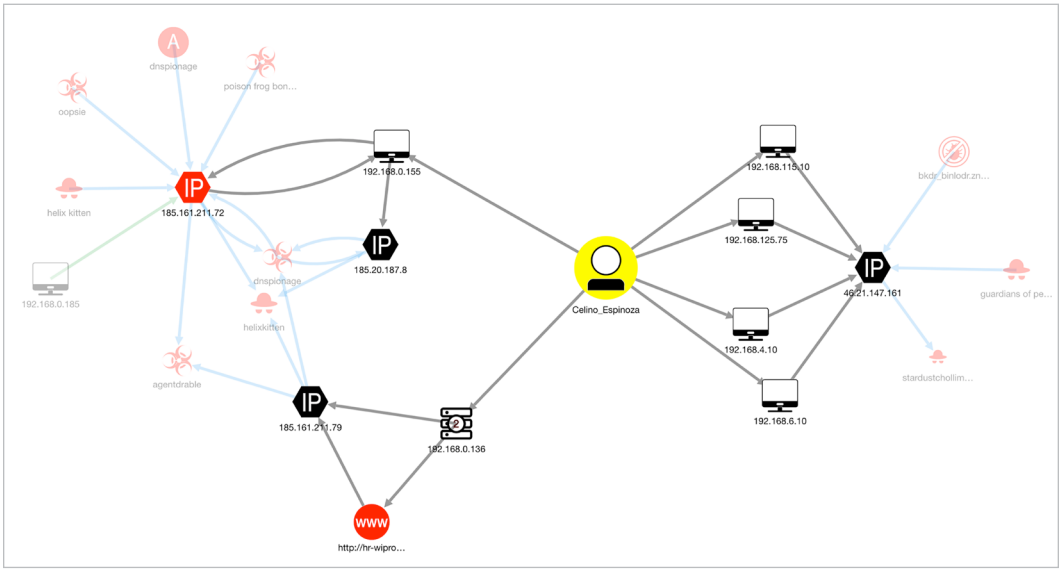


Figure 9. Link Analysis of Local Observables

This important distinction allows the analyst to pivot between what has actually been observed in the environment as part of this investigation and what QRAW has enriched. As shown in Figure 10, five options are available for manipulating graph data.

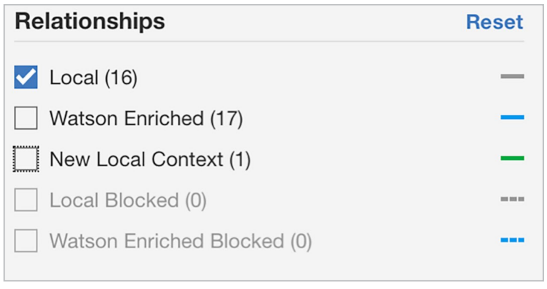


Figure 10. Five Options for Manipulating Graph Data

For this investigation, the three available relationship levels, and their relevance, were:

- **Local:** Displays items found in the local QRadar instance
- **QRAW Enriched:** Items discovered during enrichment via QRAW automated intel lookups
- **New Local Context:** Observables or techniques discovered by expanding on QRAW's enriched data points

We found the "New Local Context" graph to be especially insightful, as it actually provides new malicious activity that might not have previously been identified. Any investigator knows that attackers seldom attack or gain a foothold on only one system; typically, lengthy incident response has to be performed to find the extent and scope of an attack. With QRAW's ability to collect observables, enrich them and perform *additional internal lookups*, however, we were able to discover additional malicious activity without leaving this particular investigation. We were able to Scope and Identify, one of the more critical incident response phases, without changing our screens.

QRAW's link analysis and graphing also allows analysts to pivot between different observable severities or types, and map our key ATT&CK Matrix patterns. Figure 11 provides a screenshot of the various options available for graph manipulation.

Similar to the Offense tab, the graph itself is highly interactive and provides context immediately for the analyst. Pivoting on the "dnspionage" node, for example, provided the data displayed in Figure 12. Our analyst was able to track how QRAW had tied this observable into the investigation and could perform his or her own additional research if desired.

Selecting one of the malicious IP addresses, as shown in Figure 13 on the next page, provided even more insight and performed the typical activities an analyst might otherwise have to go elsewhere to do. Such activities include determining how an indicator is being utilized by an attacker, key WHOIS details and any associated threat intelligence (not shown in Figure 13).

At this moment in our assessment of QRAW, we realized a turning point in our investigation. We had not navigated through dozens of screens or data points but felt we had a good handle on what had happened in the environment. Furthermore, we understood the threat. By automatically correlating Offenses and Observables, QRAW had done a good deal of the work we were used to performing manually. At this point, we felt the way any analyst should: We had enriched data, a higher sense of confidence and were able to effectively discuss the next steps to be taken in the environment.

Figure 11. Options Available for Graph Manipulation

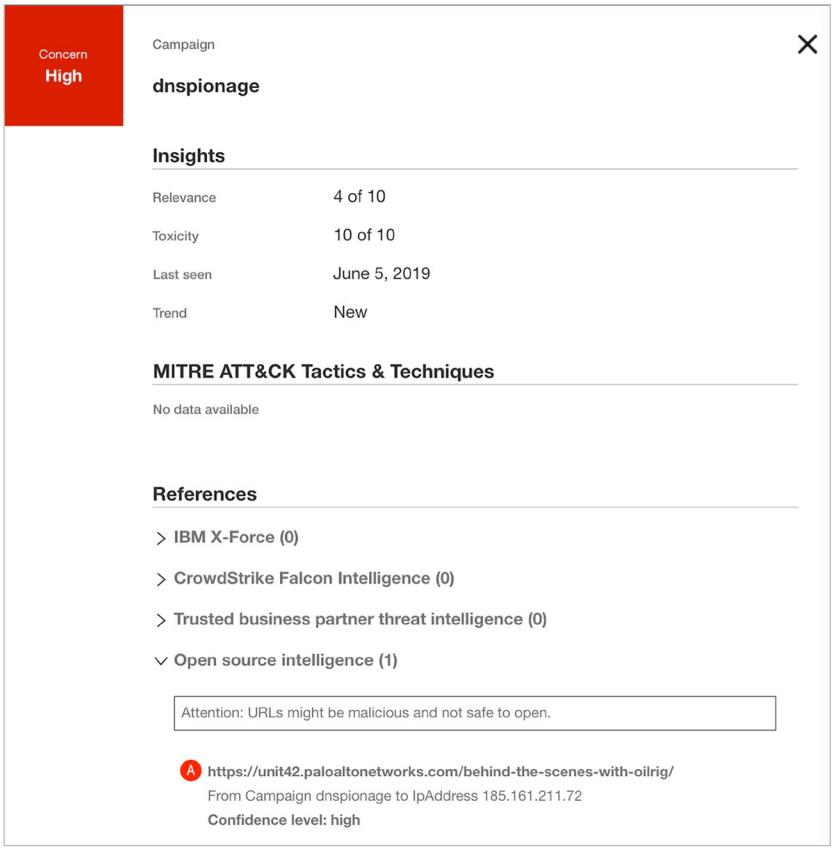


Figure 12. "Dnspionage" Node Display

Closing Thoughts

We found that working with IBM's QRadar Advisor with Watson provided a fun, unique investigative experience. We were able to quickly gain insight into suspicious activity and anomalies in the environment. The platform's assessment of magnitude and ability to act quickly on events allowed our analyst to make more confident decisions faster. And therein lies one of our key takeaways from utilizing QRAW: We found we were able to make more confident decisions and perform more consistent investigations.

When armed with QRAW, a lot of tasks that used to be spread across multiple tools or browser tabs are automatically curated and performed for the analyst. Threat intelligence sourcing, one of the more cumbersome and time-consuming tasks any analyst encounters, is something that serves as a force-multiplier from QRAW. By being able to quickly jump from Offense to informed, contextual decision, analysts can continue assessing the weight of activity, instead of trying to evaluate a potential threat intelligence source.

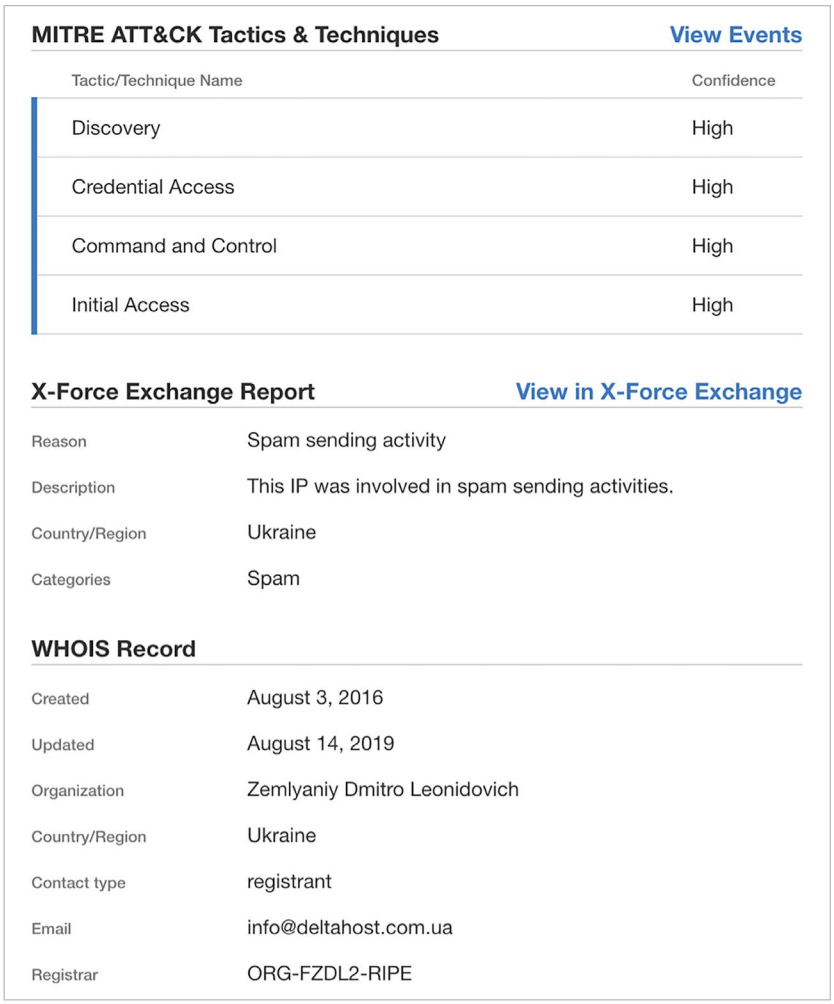


Figure 13. Selecting a Malicious IP Address

As investigators and incident responders, however, we cannot deny that one of QRAW's more important (and cool!) features is the aligning of observables and techniques to Mitre's ATT&CK Matrix. By utilizing a language and format that much of the industry has come to understand and rely on, QRAW provides context that is easy to consume by security analysts of any skill level.

> *With QRAW, we were able to make more confident decisions and perform more consistent investigations.*

When we started to assess this platform, we went in thinking that QRAW would help us correlate multiple data sources and provide useful insight into alerts. We soon learned that any of the problems we were used to having *had already been solved* for us in the background, which meant we didn't have to waste time bringing artifacts together. QRadar Advisor with Watson changed our perspective into the environment.

And when we changed our perspective, we were able to immediately focus on handling and neutralizing threats. Our time was spent solving problems, not connecting dots. Analysts can do what they're asked to do: help defend the network. We hope your analysts can easily say—and do—the same.

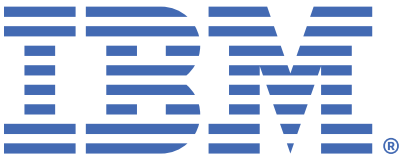
> QRadar Advisor with Watson changed our perspective into the environment so we could focus on handling and neutralizing threats.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response, and a GIAC Advisory Board member. He is also an incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:



Last Updated: February 13th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Cairo February 2020	Cairo, EG	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS Brussels February 2020	Brussels, BE	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS San Diego 2020	San Diego, CAUS	Feb 17, 2020 - Feb 22, 2020	Live Event
Open-Source Intelligence Summit & Training 2020	Alexandria, VAUS	Feb 18, 2020 - Feb 24, 2020	Live Event
SANS Training at RSA Conference 2020	San Francisco, CAUS	Feb 23, 2020 - Feb 24, 2020	Live Event
SANS Zurich February 2020	Zurich, CH	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Secure India 2020	Bangalore, IN	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Manchester February 2020	Manchester, GB	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Jacksonville 2020	Jacksonville, FLUS	Feb 24, 2020 - Feb 29, 2020	Live Event
ICS Security Summit & Training 2020	Orlando, FLUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Secure Japan 2020	Tokyo, JP	Mar 02, 2020 - Mar 14, 2020	Live Event
Blue Team Summit & Training 2020	Louisville, KYUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Northern VA - Reston Spring 2020	Reston, VAUS	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Munich March 2020	Munich, DE	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Jeddah March 2020	Jeddah, SA	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS St. Louis 2020	St. Louis, MOUS	Mar 08, 2020 - Mar 13, 2020	Live Event
SANS Paris March 2020	Paris, FR	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Prague March 2020	Prague, CZ	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Dallas 2020	Dallas, TXUS	Mar 09, 2020 - Mar 14, 2020	Live Event
Wild West Hackin Fest 2020	San Diego, CAUS	Mar 10, 2020 - Mar 11, 2020	Live Event
SANS Doha March 2020	Doha, QA	Mar 14, 2020 - Mar 19, 2020	Live Event
SANS San Francisco Spring 2020	San Francisco, CAUS	Mar 16, 2020 - Mar 27, 2020	Live Event
SANS Norfolk 2020	Norfolk, VAUS	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS SEC504 Nantes March 2020 (in French)	Nantes, FR	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS London March 2020	London, GB	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS Secure Singapore 2020	Singapore, SG	Mar 16, 2020 - Mar 28, 2020	Live Event
SANS Kuwait March 2020	Salmiya, KW	Mar 21, 2020 - Mar 26, 2020	Live Event
SANS Seattle Spring 2020	Seattle, WAUS	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS SEC560 Lyon March 2020 (In French)	Lyon, FR	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Oslo March 2020	Oslo, NO	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Madrid March 2020	Madrid, ES	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Dubai February 2020	OnlineAE	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced