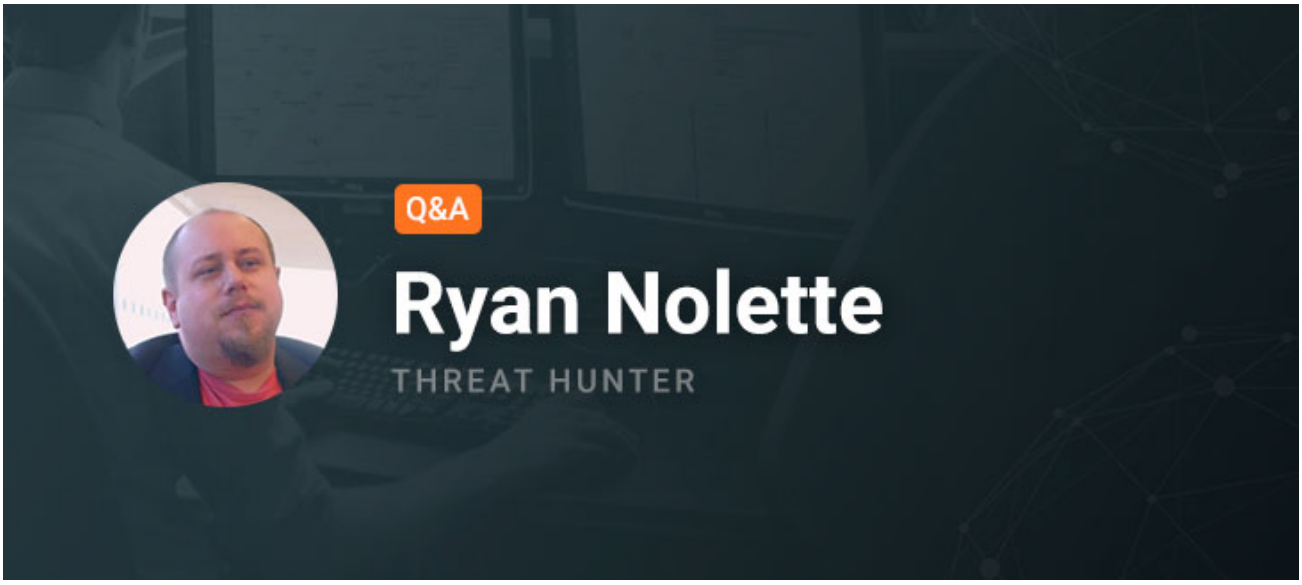
ENDPOINT AND NETWORK HUNTING: A Q&A WITH RYAN NOLETTE

(/blog/)



(/endpoint-network-hunting-qa-ryan-nolette/)

September 5, 2017 by Sqrrl Team (https://sqrrl.com/author/george/)

ENDPOINT AND NETWORK HUNTING: A Q&A WITH RYAN NOLETTE

Ryan Nolette is a security technologist at Sqrrl. Throughout his career he has attained experience in IT/Security planning at a large scale and is proficient in multiple platforms and security techniques. He has experience with troubleshooting, auditing and installations, network intrusion detection, security, incident response, threat intelligence, threat research, computer forensics, and network/systems auditing.

Key Takeaways:

- Network and endpoint hunting aren't that different. Instead of trying to differentiate between them, shoot for full-stack analysis.
- When looking for buy-in from the C-Suite, make sure you have quantifiable metrics for how hunting procedures can save money for a firm

How do you prioritize hunting for network and endpoint data? What is the best way to obtain IOCs to orient your hunts? In this interview, we talk to Sqrrl's resident security subject matter expert, Ryan Nollette, about his takes on tips for gathering, analyzing, and applying data when threat hunting.

This interview was originally posted in conjunction with the Threat Hunter Spotlight (https://www.brighttalk.com/summit/threat-hunting-series) series which features conversations with top-level threat hunters to discuss a range of topics, from spotting adversary tactics, techniques, and procedures to leading hunt teams. Ryan's original "Threat Hunter Profile" can be found on the Sqrrl blog (https://sqrrl.com/threat-hunter-profile-ryan-nolette/). The original interview is available here (https://www.youtube.com/watch?v=N7JvE9nBCJs).

Question (Q): What value do you see in making the distinction between network and endpoint hunting, and how do you move from one to another?

Ryan Nolette (RN): The main difference between network and endpoint hunting is that they're not very different or at least that you shouldn't distinguish between them. What you're really looking for is "full-stack analysis." Basically, you want to be able to take an event that occurs from however you've been alerted to it, whether it be a network event or an endpoint event, and trace that throughout your stack.

So if I have a firewall alert go off for a known C&C beaconing, then I want to be able to take that, bring that network traffic all the way through my stack (my web proxy, my firewall, my IDS, et cetera). Grab all the data that's associated with that network event, and resolve it to find what the hostname is. That way, I know the originating host that generated it.

From there, I want to find out what process on that host actually initiated that connection and what other processes have been running that process. I want to be able to do that, from top to bottom. That way, I have a full picture of everything that

happened. Not only is that valuable for me to make sure I correctly scoped the event, it's also a valuable training mechanism for junior members of the team trying to discuss with either coworkers or senior members and share, "This is what I learned today. I hope it will help you later on." And it really helped me justify cost to management down the line of showing them, "Look, here's the full picture of what happened. Here's the scope of impact. Here's all the systems affected, and cost per system if they remained infected."

Q: What are some of the limitations that are preventing analysts approaching hunting with full-stack analysis?

RN: One of the main things for preventing people is always cost. Having all those products in your stack is extremely expensive if you go with all primetime vendors. But, you can actually use a lot of open-source technologies in that security stack to help you save money and put it towards either some kind of correlation mechanism or hunting tool which are actually going to provide more return on your investment in the end.

I know that sounds like a very business-y thing to say, but part of being a security professional is understanding the impact to the business. What that means, is everything comes down to dollars. If you can't justify whatever's happening in dollar amounts, small words, and pretty pictures, a lot of people aren't going to pay attention to it and either never read your report, no matter how good it is, or they're just not going to care after the first couple of minutes.

As for people in the industry that are doing threat hunting, full-stack analysis is something that everybody tries to go for. I'm a member of a couple of different threat hunting groups and security groups. A lot of the stuff we talk about is, "What do we have in our home labs and what do we have in our security stack at work?" Almost every single person has some kind of endpoint tool, whether it be an EDR tool or something free, like Sysmon, that will grab endpoint events. They'll also have an IDS for the network, like Security Onion or Bro. Some kind of firewall, usually pfSense (another free thing that works really well with all those tools).

Q: For those out there who want to start hunting on their own, what would you say are the important data sets to look at?

RN: That actually has a ton of answers to it. But to try and simplify it, the data that I'm looking for is all dependent on your operating system. For my answer, I'm going to stick just to Windows, as it's probably most prevalent in most enterprises. There's a ton of great system information in your basic event viewer that you can grab. Who logged in and when, what applications installed, etc. But also, if you use something like Process Explorer or Sysmon, you're able to generate data around what events are happening. When a binary's executed, what child processes does it have, what registry keys are created/deleted/modified, and what files were touched and modified. That's extremely valuable information to figure out how the malware is interacting with your operating system. Sysmon, we can find out the network connection information that the processes generate, which then, we can sync up with our network data and continue from the endpoint analysis to the network analysis.

Therefore, we're taking both endpoint data and network data now, and being able to correlate them together. While it sounds really easy to dom in practice, it's extremely difficult to do, and as anybody that makes any kind of correlation software for a living can tell you, it's time-intensive, complicated, and manual. Trying to roll your own is quite difficult. But that's a lot of the data sets that I look at.

What I'm doing with that information is attempting to normalize it so I can throw it into a database for correlation. Rinse and repeat, and rinse and repeat, rinse and repeat for the same sample or multiple samples. Eventually, I go back and I start doing big data analytics against the database.

Q: How do you actually take what you create from those kind of analyses and output it as threat intelligence, that you can then use later?

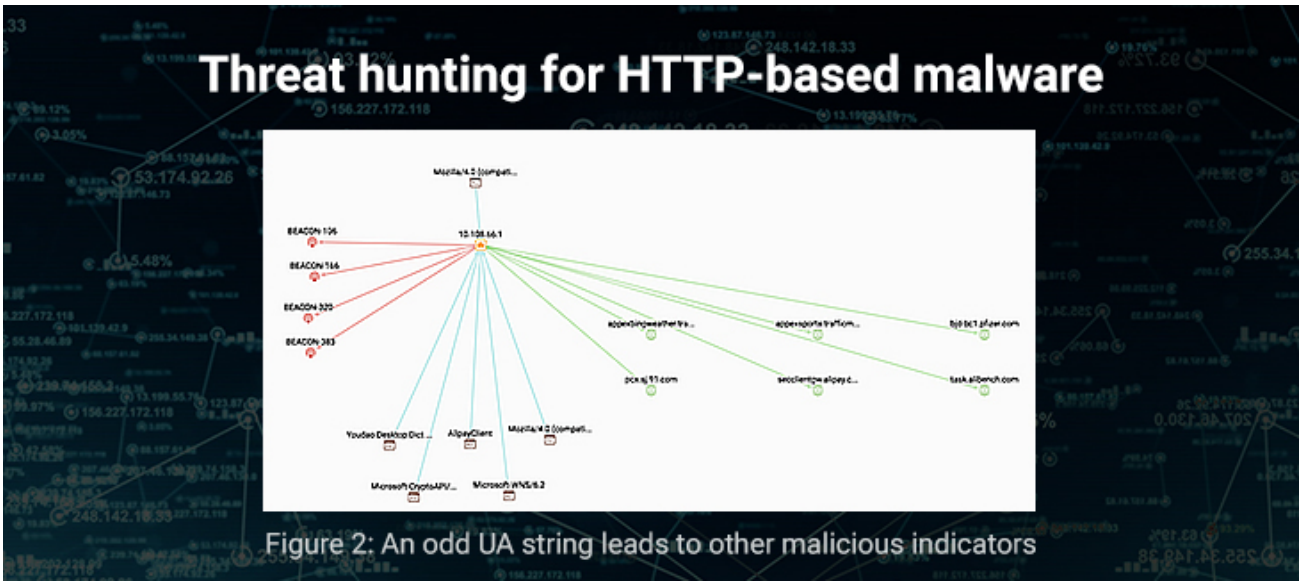
RN: Probably the biggest difference between what I'm doing and what would be considered threat research is that you get paid to be a threat researcher. This is my home lab. But the concepts, theories, and tactics, are very, very similar. Some things in threat research you'll do is actually grab binaries and break them down and disassemble them to read their core components and actually analyze their code. This is commonly referred to as reverse engineering. I'm not going to that level, mostly because I don't feel the need to for a lot of what I'm doing. If I need to, I'll break out a couple of my favorite tools with REMnux, SIFT, or IDA pro and actually

start to reverse-engineer a binary. But most of the time, executing it and watching it tells me all the stuff I care about to be able to identify it, detect it, and stop it, or flag it, tag it, and bag it, as i like to say.

For threat intel, this is kind of nice because it goes into a lot of the free tools. I mentioned Security Onion and pfSense earlier. They both accept a lot of threat intelligence feeds. If I'm detonating a bunch of Trojan binaries and I want to get alerts on it, i can use a feed from ZeuS Tracker, to leverage a large list of known bad IOCs to match against. I do the same for other binaries by using services like virustotal and other malware repositories. That's all free. Cost is not a barrier of entry here.

Q: How do you go about connecting the dots between all these disparate data sets that you're talking about?

RN: I use IOCs primarily for correlation. Using the term IOCs is difficult here, because there's OpenIOC and IOC that are formats, but what I want to specify is the hardest part about using threat intelligence is trying to normalize the threat intelligence into a format that's usable across all of your existing data sources. There's a plethora of formats and standards out there. TAXII, YARA, OpenIOC, etc, the list goes on and on. A lot of the code that I've written over the years is just trying to normalize a bunch of that and dump it from different source types into one main database that I can then use.



(https://sqrrl.com/threat-hunting-http-user-agents/)

August 31, 2017 by Chris Sanders (https://sqrrl.com/author/chrissanders/)

THREAT HUNTING FOR HTTP USER AGENTS (HTTPS://SQRRL.COM/THREAT-HUNTING-HTTP-USER-AGENTS/)

An attacker will use the minimal amount of effort required to compromise your network. That means when it's possible to reuse applications, tools, and protocols…. they'll do it! This is one reason why attackers often use HTTP to facilitate communication to and from infected hosts. In this post, I'll discuss the HTTP user agent field and demonstrate how you can use Sqrrl to hunt for HTTP-based malware.

READ MORE
(https://sqrrl.com/threat-hunting-http-user-agents/)

Next Post

Browse by Topic

Featured Defenders

Subscribe to Blog

Email Address

SUBSCRIBE

Featured Posts

Top #InfoSec Twitter Accounts (From A Threat Hunter's Perspective)

By Danny Akacki
(/top-infosec-twitter-accounts/)

Is Threat Hunting-As-A-Service (THaaS) for you?

By Luis Maldonado
(/threat-hunting-service-thaas/)

Threat Hunting for Uncategorized Proxy Events

By Chris Sanders
(/cyber-threat-hunting-sqrrl-uncategorized-proxy-events/)

Threat Hunting for Lateral Movement

Resources

Webinar

Threat Hunting for Misbehaving PowerShells
(http://info.sqrrl.com/threat-hunting-for-misbehaving-powershells)

eBook

Hunt Evil: Your Practical Guide to Threat Hunting
(http://info.sqrrl.com/practical-guide-to-threat-hunting-ebook)

Whitepaper

The Who, What, Where, When, Why and How of Effective Threat Hunting

By Brandon Baxter
(/threat-hunting-lateral-movement-identifying-pivot-points/)

Threat Hunting for Evidence of Eavesdropping

By Matthew Hosburgh
(/hunting-evidence-eavesdropping/)

Threat Hunting Starting Points: Web Shells

By James Bower
(/3-threat-hunting-starting-points-web-shells-edition/)

Effective Threat Hunting
(http://info.sqrrl.com/sqrrl-sans-hunting-white-paper)

Whitepaper

Technical Guide: Nuts and Bolts of Sqrrl's Threat Hunting Platform
(http://info.sqrrl.com/sqrrl-product-paper-0)

Watch Overview

(https://www.youtube.com/watch?v=Vl_zLBc4KQM&t&width=640&height=480)

(https://twitter.com/SqrrlData)

(https://www.facebook.com/SqrrlData)

(https://plus.google.com/116795302724746825954/posts)

(https://www.linkedin.com/company/sqrrl)

(http://www.youtube.com/user/sqrrldata)

SQRRL NEWSLETTER

Subscribe to our mailing list

PRODUCT (/PRODUCT/SQRRL-ENTERPRISE)

Sqrrl Enterprise (Https://Sqrrl.Com/Product/Sqrrl-Enterprise/)

Technology (Https://Sqrrl.Com/Product/Architecture/)

Architecture (Https://Sqrrl.Com/Product/Architecture/)

Security Behavior Graph (Https://Sqrrl.Com/Product/Behavior-Graph/)

User And Entity Behavior Analytics (Https://Sqrrl.Com/Product/User-And-Entity-Behavior-Analytics-Ueba/)

Test Drive VM (Http://Info.Sqrrl.Com/Trial-Software-Vm-1)

SOLUTIONS (/SOLUTIONS/USE-CASES/)

Use Cases (Https://Sqrrl.Com/Solutions/Use-Cases/)

Cyber Threat Hunting (Https://Sqrrl.Com/Solutions/Cyber-Threat-Hunting/)

Cyber Incident Investigation (Https://Sqrrl.Com/Solutions/Cyber-Incident-Response-And-Investigation/)

PARTNERS (HTTPS://SQRRL.COM/SQRRL-PARTNER-PROGRAM/)

Threat Hunting Ecosystem (Https://Sqrrl.Com/The-Sqrrl-Partner-Program/)

Technology (/Partners/Technology)

Sales (/Partners/Sales)

SERVICES (/SERVICES/SQRRL-ENTERPRISE-SUPPORT/)

Sqrrl Enterprise Support (Https://Sqrrl.Com/Services/Sqrrl-Enterprise-Support/)

RESOURCES (/RESOURCES/)

Datasheets (/Resources/#Datasheet)

EBooks (/Resources/#Ebook)

Quick Reads (/Resources/#Quick-Read)

Reports (/Resources/#Report)

Videos (/Resources/#Video)

Webinars (/Resources/#Webinar)

Whitepapers (/Resources/#Whitepaper)

COMPANY (/COMPANY/OVERVIEW/)

Overview (Https://Sqrrl.Com/Company/Overview/)

Team (/Company/Team/Management)

Advisors (Https://Sqrrl.Com/Company/Team/Advisors/)

Blog (Http://Blog.Sqrrl.Com)

News Room (Https://Sqrrl.Com/Company/News/)

Careers (Https://Sqrrl.Com/Company/Careers/)

Contact Us (Https://Sqrrl.Com/Company/Contact-Us/)

GET A DEMO (HTTP://INFO.SQRRL.COM/SQRRL-ENTERPRISE-DEMO-REQUEST)

BLOG (/BLOG/)

CONTACT US (HTTPS://SQRRL.COM/COMPANY/CONTACT-US/)