WHAT I'M THANKFUL FOR AS A SECURITY PRACTITIONER

(/blog/)

(/im-thankful-security-practitioner/)

November 22, 2017 by Ryan Nolette (https://sqrrl.com/author/ryan/)

WHAT I'M THANKFUL FOR AS A SECURITY PRACTITIONER

In the spirit of the season I thought I would share a few things I am thankful this year as a security practitioner:

Family:

While often not mentioned in many security blogs, family plays a large role in the success of a practitioner. Working in SecOps means long work hours, high stress, and constant tinkering while trying to stay up to date on new technologies and threats. This means

home life often takes one for the team in order to support the practitioner. I want to say thank you to my family for helping me be successful this year and all the years prior. Thank you.

My team:

My team is often an extension of my own family. The long hours and trial by fire tend to forge the strongest of bonds between teammates. It comes from being in the trenches together and knowing that you can count on them and that they can count on you when in need. From the veterans that mentor junior analysts and handle the big projects, to the junior analysts with a thirst for knowledge and the desire to be the best they can be. Thank you. Also, a good manager and/or mentor is worth their weight in gold plated memes. I won't name anyone by name here but I wouldn't even be in the security field if it wasn't for my first mentor, and I wouldn't still be successful if it weren't for my last two. Thank you.

The Open Source Community:

I don't know of many security practitioners without a home lab or a test lab at work to try new things out. Thanks to the open source community and the software they pour their time, sweat, and tears into, we practitioners are able to try new things without breaking the bank. Some of the most popular tools in the industry are open source and get used in enterprise production environments all the time. Things like Bro IDS, SecurityOnion, cuckoo, pfsense, OpenVPN, sysmon, SIFT, and REMnux. These are just a few of the security specific tools and applications I use everyday. I could go into all the others I use daily on my laptop but the list would be too long. Thank you to all who contribute to the development of these. And to the users of these wonderful technologies, please remember to donate to the projects.

If you've read this far, then you've probably started thinking about some people you know who helped you along the way that you've lost contact with. I suggest taking a few minutes over this long holiday weekend to reach out to them and reconnect. And don't forget say thank you for all they've done.

And as always, remember my motto: Flag it, Tag it, and Bag it.

For more threat hunting insight:

- Read Ryan's blog post (https://sqrrl.com/finding-evil-when-hunting-for-lateral-movement/) on threat hunting for lateral movement

- Watch our podcast (https://www.youtube.com/watch?v=N7JvE9nBCJs)on endpoint and network threat hunting
- Check out our training session (http://info.sqrrl.com/building-a-threat-hunting-team-david-bianco) on building a threat hunting team
- View our webinar (http://info.sqrrl.com/threat-hunting-lateral-movement)with Carbon Black featuring Ryan on how to threat hunt for lateral movement

(https://sqrrl.com/media/demo-1.png)

(http://info.sqrrl.com/demo)

(https://sqrrl.com/5-types-threat-hunting/)

November 21, 2017 by Danny Akacki ()

5 TYPES OF THREAT HUNTING (HTTPS://SQRRL.COM/5-TYPES-THREAT-HUNTING/)

“How do I hunt?”. The instinctual first question uttered by anyone with a mind to build a threat hunting program. Any answer should, as all good philosophies, change over time. You get new information, gain new experiences, etc. The only sure answer is never a singular one. Any threat hunting initiative is a daunting task. This stuff is hard. It’s not even the actual technical competencies that are hard, it’s the logistics of it all. This post endeavors to define a starting point by offering varied plans of attack, how they influence the success of a hunt team, and how Sqrrl can help with those plans.

READ MORE
(https://sqrrl.com/5-types-threat-hunting/)

Next Post

Scoping Attacks By Following Attacker Breadcrumbs

By Chris Sanders
(/scoping-attacks-by-following-attacker-breadcrumbs/)

The Hunter's Den: Command and Control

By Josh Liburdi
(/the-hunters-den-command-and-control/)

A Framework for Cyber Threat Hunting Part 1: The Pyramid of Pain

By Sqrrl Team
(/a-framework-for-cyber-threat-hunting-part-1-the-pyramid-of-pain/)

A Framework for Cyber Threat Hunting Part 2: Advanced Persistent Defense

By Sqrrl Team
(/a-framework-for-cyber-threat-hunting-part-2-advanced-persistent-defense/)

Threat Hunting for Command Line Process Execution

By Chris Sanders
(/threat-hunting-for-

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
(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)