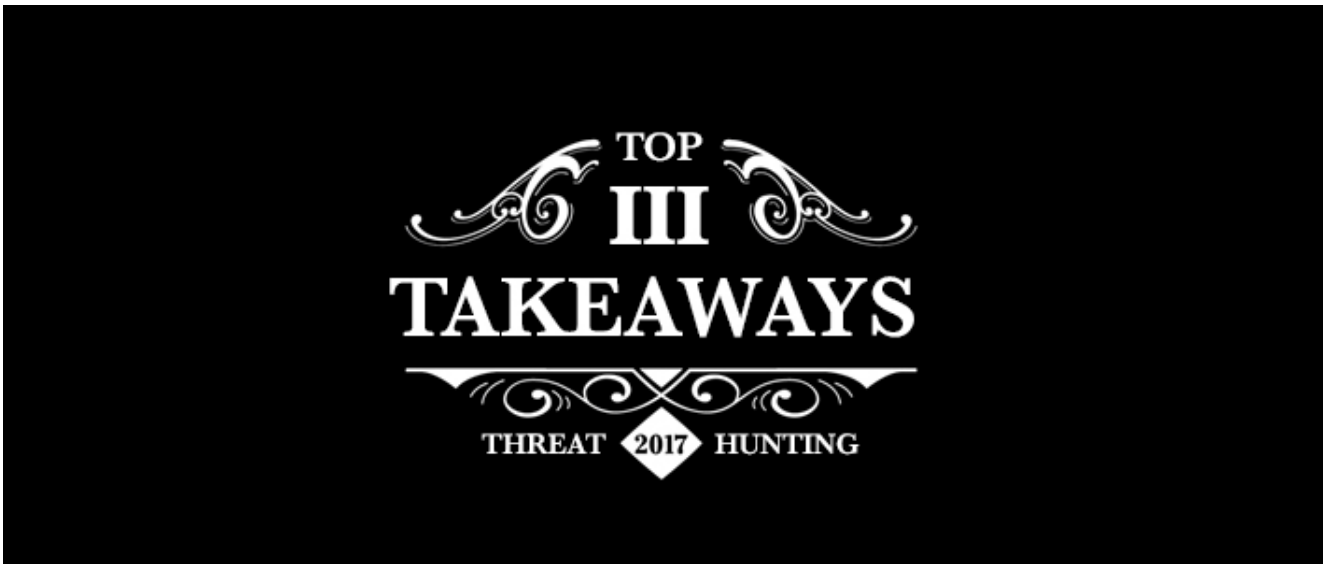
TOP 3 TAKEAWAYS FROM DERBYCON

(/blog/)



(/top-3-takeaways-derbycon/)

September 26, 2017 by Ryan Nolette (https://sqrrl.com/author/ryan/)

TOP 3 TAKEAWAYS FROM DERBYCON

This past week I had the pleasure of going down to DerbyCon 7.0. Along the way, I got to see some fantastic presentations, an excellent Capture the Flag competition, and the tragic death of at least one insect (https://www.csoonline.com/article/3227910/security/hackers-create-memorial-for-a-cockroach-named-trevor.html). Here are a few of my takeaways from the conference.

1) Derbycon is one of the last remaining community first focused security conferences in the nation.

On the DerbyCon website, they state that “the idea of DerbyCon is to promote learning and strengthen the community. We are a community of peers learning from one another.” This definitely encapsulated my experience at the conference. The majority of the attendees I encountered were friendly and approachable which helped to foster and mentor the attendees newer to the field. I saw examples of teaching throughout the conference and not limited to just the talks. Witnessing someone find their first vulnerability and exploiting it is a magical experience. Additionally, the hosts of DerbyCon streamed all of their tracks live, to the entire Internet, completely free. I loved this for two main reasons- first, it demonstrated how much the DerbyCon hosts care about the community. Second, it puts pressure on other conferences to do the same, which will contribute to the community as a whole.

2) Threat Hunting as a concept with practical application is growing.

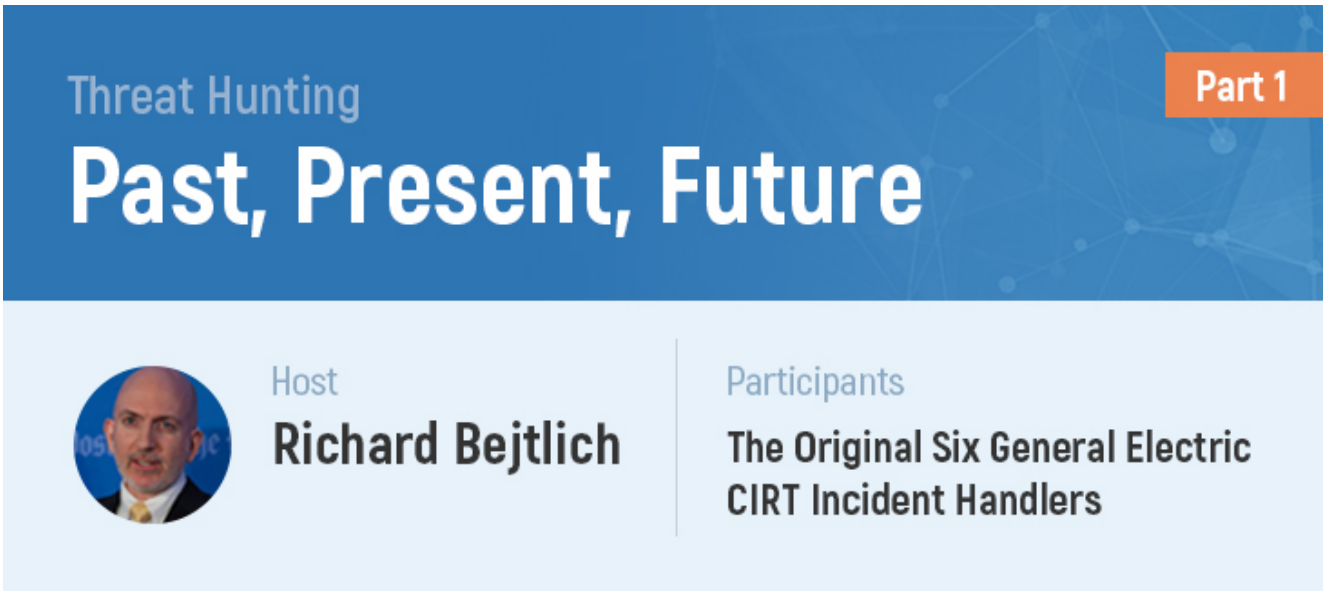
There were 7 different hunting talks this year, highlighting the increased prominence of threat hunting, as it is adopted by more and more SOCs. They can be viewed here:

- Jared Atkinson and Robby Winchester (https://www.youtube.com/watch?v=VCF8EpQbRTs) – Purpose Driven Hunt: What do I do with all this data?
- Mauricio Velazco (https://www.youtube.com/watch?v=hVTkkkM9XDg) – Hunting Lateral Movement for Fun and Profit
- Ryan Nolette (https://www.youtube.com/watch?v=YFBHkRrARMI)– How to Hunt for Lateral Movement on Your Network
- Joe Desimone (https://www.youtube.com/watch?v=GkH83bhu6gU)– Hunting for Memory-Resident Malware
- Robert Simmons (http://www.irongeek.com/i.php?page=videos%2Fderbycon7%2Fmainlist&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IrongeeksSecu – Advanced Threat Hunting
- Todd Sanders (https://www.youtube.com/watch?v=Y2Vif--ixsM)– We're going on a Threat Hunt, Gonna find a bad-guy.
- Zach Grace (https://www.youtube.com/watch?v=2pVbsaEWkII)– changeme: A better tool for hunting default creds

3) The Derbycon CTF is one of the best I've attended with flags for every skill level.

I sat with many different groups of people this year during the conference and all of them were welcoming. Each group had a mix of seasoned vets and first timers attempting the CTF. The vets mentored and taught the first timers without annoyance and with a joy and excitement that reminded me of teachers I had back in school. I have never met a group so willing to pause their own work to help walk someone through their questions and issues. The best part was that they did not just give the answers to the requester but instead asked them a series of leading questions helping the requester learn to think through the problem in a different way and get to the answer on their own.

While I was there, I also got the chance to give a presentation on detecting and identifying lateral movement activity on your network. You can pick up the presentation notes (https://github.com/sonofagl1tch/PresentationsAndBlogs/blob/master/presentations/LateralMovement_1hr_derbycon.pdf), or you can watch the entire presentation here (https://www.youtube.com/watch?v=YFBHkRrARMI).



(https://sqrrl.com/origins-threat-hunting/)

September 19, 2017 by Sqrrl Team (https://sqrrl.com/author/george/)

EXPLORING THE ORIGINS OF THREAT HUNTING (HTTPS://SQRRL.COM/ORIGINS-THREAT-HUNTING/)

Threat hunting is one of the fastest-growing information security practices today. But what really defines threat hunting and how did the practice start?

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

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

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/)

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)

Watch Overview

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