Twitter Thread by Chris Sanders ■



Chris Sanders ■
@chrissanders88

For threat hunting, a non-trivial amount of the work is referencing, creating, and updating system and network inventory. This doesn't get talked about enough as a skill set that someone develops. 1/

Threat hunting is all about finding anomalies that automated detection mechanisms don't find. That means manual anomaly detection, which sometimes means weeding out things that are normal. 2/

For example, let's say you discover a binary that runs in the middle of the night on a host and that's weird! So, you eventually search for the prevalence of that behavior and see it running on other hosts in that department. 3/

At the same time, you find this host talking to a weird internal system on an odd low port you haven't seen before. In this case, that behavior is nowhere else on the network. 4/

Eventually, you talk to an IT person or user in that department and find out the process is some special software they use and the weird system is a dedicated server for it, and it's all legit. Job's not done, though. 5/

Now, you gotta write that stuff down. It needs to be in a place where other analysts can quickly reference it, and even better, where you can reference it a year from now when you've long forgotten about it. 6/

In my hunting class, I teach folks how to take effective hunting notes and translate those into some sort of security wiki as necessary. Beyond that, hunters gotta know how to access and interact with whatever inventory software the org is running. 7/

I say this bc I have a lot of followers here and people who take my hunting class who are caught off guard by the need to do these things. Knowing a network is a critical part of the job, and the ability to do that effectively is a skill set you must develop as part of it. 8/

Not all threat hunting is chasing attackers through servers. Much of it is finding things that are normal and documenting them so you (or your peers) don't spend as much time on them later. 9/

As far as referencing knowledge sources. Consider that for every behavior you might identify, ask yourself, how would I determine if this was normal? You should be able to answer this for the most common types of behaviors you'll see. 10/

Behaviors might include processes launching, per-protocol network communication, authentication, file deletion, and many other observable things. Sometimes answerable with evidence, but sometimes other sources of knowledge like an asset DB. 11/

For example, how would you know if an auth behavior was normal? Well, you can look at past auth behaviors, look at those behaviors within a department, look at future auth behaviors, ask the user, or look at a security wiki, or past tickets. 12/

More broadly, to determine if a behavior is normal, it means crafting SIEM/data search queries (looking in the past), setting up new data capture (looking in the future), or examining other sources of facts (asset DB, AD, etc). The last two are the most overlooked. 13/

You can think of this like a doctor who is trying to determine if some test result is normal for a patient. If possible they look historically, if not they look in the future. Sometimes they examine related sources of facts. 14/

Bottom line: If you are a threat hunter, you are also a custodian of network knowledge. Take time to develop that skill. Ignore that responsibility at your own peril. 15/

There are two great ways to start today.

First, do you have some sort of wiki or repo where you can store network knowledge? No? Set one up.

Second, figure out what asset DB software you use, get access, and learn how to query it effectively and quickly. 16/

This morning's thread brought to you by the screams of hundreds of analysts who thought they wanted to be threat hunters but didn't realize what the job fully entailed.

Alas, it's a beautiful day to catch bad guys. 17/17