# DeepSec 2017 Workshop: Hunting The Adversary – Developing And Using Threat Intelligence – John Bambenek

Posted on **October 12,2017** by **lynx**

The arsenal of components you can use for securing your organisation's digital assets is vast. The market offers a sheer endless supply of application level gateways (formerly know as „firewalls"), network intrusion detection/prevention systems, anti-virus filters for any kind of platform (almost down to the refrigerator in the office), security tokens, ~~biometrics~~, strong cryptography (just stay away from the fancy stuff), and all kinds of Big Data applications that can turn shoddy metrics into beautiful forecasts of Things to Come™ (possibly with a Magic Quadrant on top, think cherry). What could possibly go wrong? Well, it seems attackers still compromise systems, copy protected data, and get away with it. Why is that? Easy: You lack threat intelligence.

Image not found
https://blog.deepsec.at/wp-content/uploads/2017/10/320px-NP_CherenkovRadiation.jpg
Cherenkov radiation in a test reactor core.

Security often doesn't „add up", i.e. you cannot improve your „security performance" by buying fancy appliances/applications and piling them on top of each other. What you get is a heap of solutions solving very different problems. Your enemies of the day have patience, use superb reconnaissance, and employ sophisticated tools against you. Stealth is the key. Being not detected pays off. Before you panic and close shop, there may be a way to improve your defence – intelligence. John Bambenek (Bambenek Consulting / SANS Internet Storm Center) will conduct a training at DeepSec 2017 titled „Developing and Using Cybersecurity Threat Intelligence".

There is a lot of theoretical talk about how you can boost your „security intelligence". That's great, but you cannot boost your defences by just thinking about the implementation of, well, stuff. Getting to know what the capabilities of your adversaries are and using all your options to detect and disclose their activities is the most crucial step. During the course of the two-day training you will learn which tools you can use to gain insight into the attacker's mode(s) of operation, and – most important of all – how to integrate these capabilities into your existing infrastructure. Not everything you have done so far was in vain. The training will be a mixture of lecture and hands-on exercises. Mr Bambenek will show you that your chances of not getting hacked or to ward off an attack aren't as bad as you might think.

The workshop is intended for everyone having digital assets and needs to defend them. If you have read this blog article, then there's a high probability that you have sufficient digital assets to protect and a reason to attend the training.

Posted in:Conference,Security Intelligence,Training | Tagged:Adversary,DeepSec,SecInt,Security Intelligence,Workshop | With 0 comments