It’s amazing how many organizations I see that have a threat feed or two and assume that they’re safe, sound, and on the leading edge of vulnerability management as a result. And to be clear, some of them are, because they’re using world-class practices and processes to make use of the data. But others? They’re not making use of their threat intelligence in a way that will ultimately enable them to stay ahead.
THREAT INTELLIGENCE MISTAKES COMMONLY SEE:

The “One and Done” Problem

A lot of companies use exploit availability information from Metasploit, and therefore assume that they can stop worrying about having additional threat information. Metasploit is great, but it’s not comprehensive. There’s more bad guys, using different tactics, than Metasploit alone can represent. The existence of an exploit, even one that is as “point, click and shoot” as those in Metasploit, is not the same as a comprehensive data store of active threats based on volume and velocity. And is it possible that one of those “hidden” threats is the one that’s most likely to matter to your organization, based on your unique infrastructure and assets?

This can lead into a similar problem, which I call “The Threat of the Day” problem. This is where an organization spends too much time and energy on a single, high profile threat, without having the data or the processes to figure out which threat actually merits attention—the one that’s more likely to affect the organization itself.

A world-class security organization will have threat intelligence coming from multiple sources, enough that they complement each other and provide a fuller picture of potential attacks.

The “More is Better” Problem

This is the polar opposite of the “One and Done” problem—having so many sources of threat intelligence that the organization becomes overwhelmed. Imagine sitting in a conference where there’s ten speakers at the microphone, all at once, and your job is to listen to all ten of them, parse what they’re saying, and turn it into actionable information. Not so easy, right?

And this leads me directly into the next problem...
The “No team in Charge” Problem

Having all that threat information won’t help you if you don’t have the team in place to consume the threat intelligence and handle alerting and blocking. This problem particularly pertains to organizations that are just getting started with threat intelligence and don’t have their processes in place yet, and therefore don’t have a great way of making sense of the feeds they get.

As a result, they may see a lot of false positives from the feeds based on non-relevant data, or they just may get overwhelmed with the data. Before an organization sets up threat feeds, it’s important to have people in charge—and at least some semblance of a process for consuming the information, even if that process gets refined over time.

At the very least, make sure someone is responsible. There needs to be a “buck stops here” person in charge of threat information and taking action on the data.

The “No Context” Problem

Most organizations know that they have to aggregate threat data, but they often fail to truly analyze the data. Nothing can be done until the data is placed in context and an effective action plan can be developed. Data won’t help you unless it’s properly analyzed and understood.

Specifically, the team needs to contextualize the threat data with the specific vulnerabilities and weaknesses that the organization has. If a high-profile vulnerability such as “POODLE” is exposing a large portion of the Internet, it may not matter at all to your specific company, based on your own unique environment and assets. Rather, it may be far more important for you to take action on some other exploit that’s rarely discussed or seen.
The “No Communication” Problem

Once a process or consuming and analyzing threat data is in place, it’s essential to have an easy way to understand and share the output of the operation with the entire company. Non-technical business executives should be able to see at a glance which group of assets have which weaknesses, what threats are significant, and what remediation is taking place.

This is also important for letting the team itself get the recognition for the work it does in protecting the company—to say nothing of being able to get sufficient resources for the next fiscal year.

No one likes to build dashboards and reports all day, but there are vendors that can help. Communicating your company’s security posture at all times—and how your team has improved it—is a paramount responsibility of the security professional.

Kenna Can Help

Let me take a moment to discuss what my company does in regards to threat intelligence. Kenna is way to supercharge your vulnerability scanning by providing prioritization, visualizations, and—of course—integrated threat feeds. We actually provide eight threat feeds, and the data comes through in such a way so that you can:

- Prioritize what you need to fix in your own environment based on real-time threat information
- Clearly communicate your risk posture to the entire organization, everyone from IT developers who perform the remediation up to non-technical business people
- Understand vulnerabilities and weaknesses across all of your asset groups, without spending countless hours or days crunching through scanner data

Whether or not you use Kenna, of course, the point is to have not just threat feeds—but an actionable plan for making use of them, and ensuring that your company is sufficiently integrating and contextualizing what’s happening in the “real world” with what’s happening inside your own organization.

About Ed Bellis & Kenna Security

Ed Bellis is the Cofounder of Kenna Security, a SaaS platform that correlates external Internet breach data, exploit data and zero-day threat intelligence with internal vulnerability scan data so organizations can focus on fixing the most critical vulnerabilities. Kenna processes over a billion vulnerabilities a day against Internet breach data for its users.

Ed formerly served as the CISO of Orbitz, where he built and led the information security program and personnel for over six years. Ed has over 20 years of experience in information security and technology and is a frequent speaker and contributor to the information security community.

For more vulnerability management best practices: visit www.kennasecurity.com