CLOSING THE SKILLS GAP

Cybersecurity experts always say "the human element" is the weakest link in the security chain, and that's correct. We don't have enough humans.

Any number of statistics paint a troubling picture of the talent shortage in cybersecurity, so here are several: in the annual Frost & Sullivan Global Information Security Workforce Study for 2015 (which polled 13,930 professionals), 62 percent of respondents said they had too few people on staff, up from 56 percent the prior year. That same survey projected a 6 percent increase in cybersecurity jobs during 2015—and a 1.5 million person shortage of qualified IT security professionals by 2020.

In other words, even if your company has an unlimited budget for cybersecurity—which isn't likely even in this field—you will still not find the staff you need. The problem isn't money. The problem is lack of skilled labor, period. "35% of the open positions in cybersecurity can't be filled today because there are not enough skilled candidates. A lot of those skills are very technology oriented linked to processes such as risk identification, risk prevention, and control implementation."*

At the same time, the evolution of cyber-attacks and of modern IT usage are both shaping how the cybersecurity profession should confront the "skills gap." "The ability to translate very nuanced technology-related risks into business implications are crucial skillsets that can help organizations align cybersecurity to their business needs."* On the threat side, phishing attacks are more and more common; they were the top threat cited in the Frost & Sullivan survey, by far. On the IT systems side, more and more companies now accept a world of cloud-based data storage; users working remotely on open Wi-Fi networks and mobile devices; and an extended enterprise with many outside parties working temporarily on parts of your network. That makes the very idea of perimeter-based security obsolete.

Now string all those factors together: a personnel shortage no single company can overcome; cyber threats based on disguising themselves as legitimate users; and a modern IT world where smart identity management is more important than a tough firewall. Combined, those forces are pushing us to a security world that uses better, automated analytics to help security professionals—a system that can empower any security analyst to do more, and do it more effectively, as he or she sorts through vast troves of IT activity to find the real threats.

So how did we get there?

The Plight of the Overworked Analyst

As mentioned earlier, phishing is the threat most commonly cited by IT security professionals. And really, why wouldn't it be? If the primary goal of most hackers is to extract data, the simplest way to do that is to trick another into sending valuable information that should be kept "in the family." What's more, as so much corporate activity happens online today, hackers who use phishing as the method of attack can also hide amid all the legitimate activity on the corporate network. The same environment that makes their attacks easier also makes the security analyst's job harder.

That point bears repeating, because it drives back to the fundamental challenge facing the security community: there are too many threats, hiding amid too much data, for security analysts to manage. Entry-level security analysts know the threat of phishing (and web application attacks, and SQL injection, and all the other common attack techniques) as well as senior security analysts; they simply don't have the same skill to identify those threats rapidly. Senior security analysts, meanwhile, have so many threats coming through the door, demanding immediate attention, that they cannot devote their sharper expertise to other important tasks like threat actor identification.

What those junior, Level 1 analysts lack is an understanding of how to put potential threats into context—how to separate what looks like a threat from what genuinely is a threat. Senior security analysts do know the difference, because they have been working at the problem (and, usually, at your specific organization) for longer periods. But if we don't have enough people with the senior security analyst's expertise, then we need to bring analytics to bear for more junior staff. They gain more ability to identify threats and act against them more quickly; while more senior analysts gain the most valuable resource of all—time—to confront more challenging security threats. And for better or worse, the corporate community will have no shortage of those threats any time soon. "When you think about the concept of technology risk and cybersecurity risk, it involves collecting and analyzing a tremendous amount of data. Our ability to collect the data accurately and completely can be just as important as the ability to monitor data and understand trends and nuances. Traditionally, this has been done at a very expensive human capital investment, meaning we would apply more and more human resources to these tasks."*

How to Bring Automated Analytics to Bear

Consider how good analytics (set aside the automated part for a moment) unfolds when it works well. First, the analyst needs full visibility into the IT environment: all the activity, from all the users, all the time. The analyst needs to combine packet capture (that is, data about the activity) and logs (data about the users). That information must be comprehensive, and correctly normalized—which may not be easy to do, depending on the technology you have to blend the various types of data into one coherent landscape of security risk.

Assuming your organization can accomplish all that, the security analyst has what he or she needs most: context. That lets the analyst investigate the potential threat properly, and if necessary, eradicate it from the system.

As mentioned above, however, the modern corporate world has too many threats to review, and not enough skilled analysts to review them properly. A junior analyst might try to investigate a threat with incomplete context and reach the wrong conclusion: perhaps they prohibits a legitimate activity by mistake, or misunderstand the full nature of a threat and fail to eradicate it completely. Or more senior analysts devote time to helping the junior analysts understand context for that endless series of threats, rather than spend time trying to monitor more strategic security risks.

Take the example of suspicious internet domains. The organization needs to understand which domains are new but harmless (say, many thousands of users across the enterprise suddenly flocking to a music star's new website); which ones are suspicious but permissible (a select few senior executives visiting a domain that might be an acquisition target); and which ones are high-risk (the North America sales VP suddenly visiting an obscure domain in China 50 times a day).

A large business with 50,000 employees can easily visit 150,000 new IP addresses every day. At that volume, manual review isn't feasible. A security analyst might use a tool for packet capture to find suspicious domains, but with no time for proper analysis, he stands a greater chance of delivering a false positive: blocking access to a legitimate website, or denying email to a legitimate recipient. That, in turn, drives up the chance of the worst outcome of all: unhappy employees who start trying to evade pesky IT security.

So how would automated analytics work in such situations? The ideal is to do both packet capture and log analysis at once—or to phrase it another way, to integrate user behavior patterns into incident detection. That brings the analyst much closer to automated analysis, earlier in the attack cycle. Now your junior analyst can make more informed decisions without relying on help from senior analysts, and senior analysts can invest their time on more strategic security goals. "In some cases, when you apply machine learning, artificial intelligence, or cognitive capabilities, you can find correlations that humans may not be able to identify. However, we still need the human touch to make those risks real and relate this information back to the business priorities."* Rather than spend their time on threat analysis, security professionals can focus on response planning and threat eradication.

That benefit of automated analytics also informs how the CISO might justify this idea to the CFO and the board concerns about return on investment. This isn't an approach that lends itself to the argument, "if we invest in automated analytics we can cut the IT security budget by 10 percent." It does, however, bring more ability to your junior-

level analysts, that they can behave and work more like senior-level analysts. A more realistic way to explain the ROI here is along the lines of, "Automated analytics will let our staff handle more work more quickly, and more accurately. Then we can invest future dollars in other security projects instead of throwing more bodies at the problem."

The alternative is to continue doing packet capture, and plenty of solutions can do that job well enough. Without automated analysis to put potential threat in context, however, organizations are still stuck with huge amounts of manual work, or must hire costly professional services to create analytical tools (that will still require a fair bit of manual review). True automation will learn from user behavior what "normal" behavior at your organization is, and then put your analysts on the path to more productive work. That closes the skills gap and the talent shortage in a world where we don't have enough workers, and won't for a long while yet.

Takeaway points:

The security community does not have enough skilled labor to meet the soaring threat of attacks, and will not close that gap any time soon.

Automated analytics, to help sort and classify suspicious behavior early, can empower your existing security analysts to work more effectively on more complex tasks—essentially, closing the skills gap and letting one analyst do more work.

Automated analytics also confronts the cybersecurity landscape of the future, where perimeter-based security no longer works very well and analysts will need to make more judgments about suspicious activity; those analysts need new tools to make better judgments, more quickly.

*All KPMG quotes in this paper are attributed to Greg Bell, Principal, KPMG Cyber Security Services Strategy Lead

About RSA

RSA helps leading organizations around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA's award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, go to www.rsa.com.