MANAGING THE SECURITY SKILLS GAP: A FORCE MULTIPLIER FOR SECURITY ANALYSTS & INCIDENT RESPONDERS
Ask any CISO to name the top challenges of the job, and the first response is likely to be the security "skills gap" – the inability to find enough skilled people to handle an organization’s security needs. With over 200,000 security jobs unfilled in the US alone, security operations centers (SOCs) are continuously struggling to fill their teams to stay one step ahead of their attackers.

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.

What’s more, this scarcity increases the costs of hiring and retaining security talent. But even a company with unlimited budget, which is an unlikely scenario, will find it just about impossible to staff sufficiently to deal with the threats of today’s IT landscape.

And security trends only serve to amplify the problem. The scale and sophistication of threats continue to increase rapidly – for example, 70-90% of malware samples are unique or targeted to a specific organization – while the growth of legitimate data and traffic growth makes threat detection ever harder. False positives and blind spots make the identification and response of today’s most damaging threats next to impossible. Security alerts from SIEMs, IPSs, and firewalls overwhelm even the most highly skilled analysts. Incidents requiring investigation grow exponentially, while uncorrelated alerts fail to reveal the full scope of an attack.

The result is that even security-conscious organizations exist in a state of fear that an undetected exploit is living on their networks, quietly exfiltrating critical data like private emails, customer records, or intellectual property. That’s not just a security problem; it’s a critical business problem – a meta-risk affecting every part of an organization.

**TURBOCHARGE YOUR SECURITY TEAM**

So if the problem can’t be solved by hiring more people, what can you do to protect your organization from today’s advanced persistent threats?

Well, you need to dramatically increase the productivity of the people you do have. This involves strategies to turn your junior analysts into senior analysts, and turn your senior analysts into true “threat hunters.” Making any analyst – from novice to hunter – more impactful and efficient at their jobs to help close the human skills gap.

---


2 Verizon Data Breach Report, 2017
You can achieve those impacts through the intelligent application of “force multipliers” – strategies that make your analysts more effective and efficient.

1. Automate the threat detection process with advanced analytics, comprehensive threat intelligence, and optimized incident workflows. This ensures that security analysts focus on the real threats lurking in the sea of an organization’s data, and respond swiftly and efficiently.

2. Broaden the visibility across an organization’s IT infrastructure to include all meaningful sources, including logs, packets, netflow, and endpoints. This allows analysts to correlate multiple indicators of compromise (IOCs) to view the full scope of an attack, and to reconstitute full sessions to see what really took place.

In this way, security analysts can dramatically become more efficient and effective to keep bad actors out of your infrastructure. How dramatically? With the right tools, you can rapidly increase productivity.

**CLOSING THE SKILLS GAP WITH RSA NETWITNESS PLATFORM**

At RSA, we’ve developed an integrated tool set designed to make security analysts more efficient and effective, with much faster incident response. It’s like multiplying your security staff.

The RSA NetWitness Platform delivers end to end visibility across the organization – from logs, network, endpoints and threat intelligence - in a highly intuitive and blazing fast user interface. The user interface was designed from the ground up after 100s of hours of security analyst interviewing and testing. The Respond and Investigate workflows make it easy for security analysts to triage information rapidly because they have all the information they need in one screen - and will make threat hunters even more impactful by providing them insights and drills into all the data, business context and threat intelligence they need. From novice to hunter – these workflows will make any security analyst better at defending their networks.

In addition to its own modular logs, packets, netflow, and endpoint monitoring capabilities, it can consolidate alerts from your existing systems. Rather than simply “dumping” alerts on your overstuffed analyst work queues, RSA NetWitness Platform first enriches them with metadata about business context, identities and threat intelligence, correlating IOCs that would be impossible to match up solely with human skills. This provides prioritization of the threats that matter the most, casting them in clear relief for your analysts, no matter how hard they try to hide.
We continue to focus on improving the efficiency and effectiveness of security analysts of all levels, by providing out of the box machine learning and behavior analytics for alerting and detection and by prioritizing the most important incidents based on business risk – from identity and asset criticality data. The new RSA NetWitness Platform is a force multiplier for security analysts and incident responders.

Ultimately, the RSA NetWitness Platform enables analysts to detect and investigate the full scope of an attack and more rapidly respond to those threats that matter the most to an organization.

GET THERE FAST
Implementing this “force multiplier” is a straightforward process. RSA Professional Services or RSA Partners can quickly install and configure RSA NetWitness Platform, both to discover threats already lurking on your network, and to quickly detect and respond to future attacks.

For more information and to get started, discover RSA NetWitness Platform or visit the RSA Link Community.