From Guards to Detectives: Evolving the Junior Security Analyst Role

By Mike Armistead, CEO and Co-Founder, Respond Software

Across all industries, we're coming to accept and, in some cases, look forward to augmenting human roles with the support of intelligent automation. There is a growing shift from fear of change, to welcoming it with open arms.

Garry Kasparov, one of the greatest chess players of all time who expressed skepticism when a computer beat him, is a perfect example of how perceptions of Artificially Intelligence (A.I.) are changing. In a recent interview, he admitted he changed his view after witnessing some of the world's greatest game players lose to machines, including when Google's AlphaGo defeated the world's best player of Go, a complex ancient strategy game.

An interesting takeaway for these so-called "defeated" human champions? By playing the computer, they all learned new methods and strategies that were unexplored before. Today, Kasparov says, "A.I. will help us to release human creativity. Humans won't be redundant or replaced, they'll be promoted."

That is exactly what the cyber security industry needs to achieve for Junior Security Analysts by arming them with intelligent automation. In doing so, we can help to accelerate the career progression of a security analyst starting from their first day through to the day they retire.

Attracting AND Retaining New Security Talent

The security industry is laser-focused on closing the skills gap; however, we continue to allow emerging professionals to experience disillusionment in the earliest (arguably, most critical) stages of their careers. Not only is the industry struggling to attract new talent, many promising junior employees are leaving the field of cybersecurity entirely. They're doing so out of frustration, stress, or boredom with the monotony of the tasks assigned to them.

In a recent study by the Cyentia Institute, 45 percent of surveyed security analysts said the reality in the Security Operations Center (SOC) does not meet expectations. One in four expressed dissatisfaction with their current job.

This is especially true of entry-level analysts, whose analysis duties typically consist primarily of monitoring raw alerts, looking for ways to enrich them with additional contextual information and—if they are lucky to be given additional responsibility—deciding which events to escalate. Despite knowing the vast majority of alerts are false positives, they worry they will miss that "needle in the haystack" event linked to a real attack and it will cost them their career.

Reducing attrition and recruiting the best and the brightest into the cybersecurity field will require collaboration across organizations and the industry as a whole.

Security Automation = Analyst Elevation

Humans alone simply don't have the capacity to keep pace with today's volume of data and threats. Trying to keep pace can both discourage and exhaust budding security analysts early on in their cybersecurity careers.

For any security analyst, detecting intrusions is rewarding and makes them feel like they're making a real difference. With the continued emergence of security automation, Junior Security Analysts experience more success on a day-to-day basis. Intelligent automation has the potential to shift the way Junior Security Analysts work significantly by:

- **Refocusing from the mundane to the imaginative**: Security analysts would rather act like detectives than mall cops, spending their time hunting threats and gathering intelligence than following routines or performing rote functions. Automated security workflow solutions, such as SOAR and SIEM) can take on many mundane aspects of the job, enabling human security

analysts to focus on its more interesting, complex, and “advanced” aspects—spending more time on higher value tasks that are more varied and exciting.

- **Sifting through fewer false positives**: Intelligent security automation tools such as the emerging Robotic Decision Automation (RDA) solutions can better categorize and decrease false positives. Not only does this reduce the level of frustration amongst security analysts but it provides them with more contextual information to determine what’s really going on in the environment.

- **Capturing the full security story**: Security analysis software can give frontline analysts a fuller view of what’s going on across the whole IT environment. It enables them to see each alert—not as a discrete event—or a piece of data streaming across a console—but instead as part of the story that’s taking place. Armed with greater context, analysts can make better decisions, faster that put them on the right path to resolving threats before they spread.

With the support of intelligent solutions, we can elevate frontline security analysts into more advanced roles—enabling them to focus on threat hunting and endeavors that need their invaluable and unparalleled human ingenuity.

A Promise to Budding Security Pros

We’ve attracted young professionals into the cybersecurity field by promising them the job of a seasoned detective, and yet, many of them end up serving as the equivalent of a security guard—relegated to watching hundreds of alerts scroll by to ensure they don’t miss something.

With Ponemon Institute estimating the average organization deals with over 200,000 security events each day, we’re putting early career analysts in front of nation-states and criminal syndicates and setting them up to fail.

Security analysts at all levels need more support to succeed and enjoy their work as this widespread job dissatisfaction has the potential to deepen the skills gap. Intelligent, automated security software can empower Junior Security Analysts to be more successful and enable the industry to deliver on the promise of a stimulating and rewarding career in cybersecurity.

About the Author

Mike Armistead is the co-founder and CEO at Respond Software. He is an industry veteran with three decades of leadership experience in the security, application development and consumer internet arenas. Mike co-founded Fortify Software in 2003 and acted as VP & general manager for both Fortify and ArcSight business groups after the companies were acquired by HP in 2011. Prior to Fortify, he held executive and key product positions at companies that include Pure Atria (IBM Rational) and Lycos. Over his career, Mike has led groups in all aspects of the organization, including marketing, development, operations and sales. His experience has spanned from managing large enterprises (+$350M revenues) to multiple start-ups in numerous industries.Mike Armistead can be reached online at mike@respond-software.com and at our company website http://www.respond-software.com