AN INTERVIEW WITH TIM WAINWRIGHT, CEO, SRA

AMP UP YOUR SECURITY PROGRAM WITH YOUR SECURITY CONSULTING PARTNER

Over the years, cyber security services have played an important role in cyber security. First, as cyber security became a field adjacent to but distinct from IT, and now as the industry faces a talent supply shortage, independent experts have stepped up to offer an economy of scale that many organizations are unable to support.

The most successful security consulting firms attract experts who want the challenge of applying their specialization across diverse companies using the skills they've acquired while gaining a broad understanding of adversary tactics, techniques, and procedures (TTPs). Security Risk Advisors (SRA), an 11-year-old consulting firm based out of Philadelphia, has been the go-to for major enterprises and non-profits alike, helping them with security testing, simulation, and cloud security services, as well as a variety of other must-have capabilities for the modern organization. TAG Cyber spoke with Tim Wainwright, CEO at SRA about how their role as advisors and consultants has changed as the industry has evolved.

TAG Cyber: SRA was founded in 2010. What major changes have you observed across your customer base over the last decade?

SRA: We started SRA before almost all the major data breaches, a time when cyber security was nowhere near the priority it has become for the Board today. Ransomware, third party risk, the need for effective detection controls, NIST CSF and MITRE ATT&CK alignment have become priorities for all types of organizations – even Healthcare which was reluctant 10 years ago but which is now our third largest client vertical.

TAG Cyber: Anyone could, theoretically, use their experience in security to become a "consultant," but that doesn't necessarily mean they'll be successful. What does it take to be an effective security consultant in 2021?

SRA: Consultants need to do three things very well. 1) Continually develop knowledge that outpaces what clients can do for themselves, 2) Help clients translate, communicate, and operationalize that knowledge into effective, measurable controls, and 3) Challenge the status quo.

On this last point, there are some answers to security problems that have become very comfortable for boards and audit committees because of their simplicity and familiarity. Consultants today need to challenge and develop effective new approaches to old solutions like pen testing, third-party risk, password policy, and identity and access. There is a place for all these, but their assumed priority and legacy approach underperform and consume a lot of resources.

TAG Cyber: SRA focused for many years on traditional services like testing, strategy, and CyberSOC services but you now offer "Purple Teams." What is it?

SRA: My definition of Purple Teams (sometimes "attack simulations") is an open-book-exam process that prioritizes and demonstrates quantifiable improvements in defenses over time. All our clients have GRC teams, smart security engineers, and some of them have invested in their own red team capabilities. Purple Teams is the ultimate process to set the direction and coordinate their work together. The scope of testing techniques is more comprehensive than either pen testing or red teams and it gives credit for controls that work well as much as it identifies gaps. The specific gaps in detection give security engineers confirmed and agreed priorities. The Defense Success Metrics from Purple Teams lets GRC validate, report, and track simple, meaningful metrics. The most important aspect of Purple Teams is the teamwork and knowledge sharing. We love to facilitate this process and teach our clients how to do it. As we say at SRA, everyone "Levels Up."

TAG Cyber: Why was it important to develop this service now?

SRA: Our clients want to take a threat-driven approach to their security program. This means that they want to refocus on defending against threat actors instead of just pleasing auditors and compliance mandates. I wish there were a stronger intersection but unfortunately that is not the case. Purple Teams aims to simulate threat actor tactics and confirm controls will block or detect as expected. Purple Teams uses MITRE ATT&CK to form the scope and basis of Defense Success Metrics. The reason why this service is needed now is because security teams don't have a good way to document, repeat, and report on their work—it's another complicated effort that surpasses Microsoft Excel's usefulness.

> **Security teams don't have a good way to document, repeat, and report on their work—it's another complicated effort that surpasses Microsoft Excel's usefulness.**

So, for this reason SRA developed and maintains VECTR (vectr.io), a free tool for the industry that is being adopted quickly. We use it in our engagements but had the vision that it could be an excellent freeware platform—which to us means too good to be free. At least three SANS classes teach students how to use it, and we see more and more conference presentations all over the world reference VECTR. In a way, SRA wrote the book for modern purple teaming and it's done a world of good for organizations who want to measure their posture against threat actors and their techniques.

TAG Cyber: When a company is hiring a security consultant, what are some things they should ask themselves and the prospective firm to ensure a successful engagement?

SRA: Some of the key questions are: Is this company on the bleeding edge but able to adapt their approach and recommendations to our size, resources, and business needs? What contributions do they make to the industry, outside of paid engagements? Are they going to be independent when it comes to recommendations or do they also sell solutions (i.e., are they going to be constantly trying to upsell me)? Are they more focused on my organization's success or their own growth?