ATTACKIQ

SIX

SUCCESS TIPS FOR NEW CISOS

2022

1. In the current business environment, it's critical to allocate cybersecurity investments to tools that deliver maximum efficacy and ROI. By evaluating the performance of your existing tools before you add new solutions, you can make smarter budget decisions. Automated security control validation helps you see where you have control gaps or need improvements, so you know where to consolidate or invest.

2. Use a risk-based approach in order to plan your cybersecurity budget. Look at the threats most relevant to your industry, company size, and operating environment, then consider the cost to the company and the probability of risk occurrence, so you understand what to prioritize and address first. One way to take control of risk is by adopting a threat-informed defense.

3. Focus on continuously improving the skills of your internal talent, so they can defend against increasingly sophisticated attacks. Provide your security team with opportunities for additional education, including participation in basic and advanced cybersecurity classes. Specialists appreciate companies that care about professional development. One excellent free resource for cybersecurity certifications and education is AttackIQ Academy.

4. Encourage red and blue teams to share practical experiences. Breach and attack simulation platforms provide a powerful way for your team to share real-time performance data and threat intelligence. This collaborative approach is called purple teaming and allows you to strengthen your security posture by quickly tackling and fixing gaps together, rather than in a siloed and adversarial approach.

5. If the lack of resources or expertise has to be solved in the short term, or the existing team is struggling to deal with the increased software security levels and constantly evolving protection technologies, gain help from third-party IT security providers. Co-managed services such as AttackIQ Vanguard combine the most advanced automated tools with professional expert support to ensure timely detection, threat hunting and remediation.

6. Take advantage of community resources. Your cybersecurity team can augment their expertise by reaching out to industry leaders and peers for knowledge on how to solve advanced challenges. Such resources include the Center for Threat-Informed Defense, industry events like Purple Hats, Black Hat, Gartner Security & Risk Management Summit, and RSA; and videos / podcasts like Cyber Ranch, Cyber Insecurity, and Risky Biz. The Information Systems Audit and Control Association (ISACA) is also a great source of training and professional interaction.

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com