WWW.CXOINSIGHTME.COM

CXO INSIGHT Middle East

ISSUE 49 \ JANUARY 2023

OUTLOOK 2023

Industry experts weigh in on trends set to shape the tech landscape this year.

PUBLICATION LICENSED BY SHARJAH MEDIA CITY

THE WAY FORWARD FOR MODERN BUSINESS

LEE ROSSEY, CTO AND CO-FOUNDER OF SIMSPACE, EXPLAINS THAT SIMULATIONS OF THREAT ATTACKS AND DEFENSIVE ROLE PLAY BY TEAMS AND INDIVIDUAL MEMBERS IS THE BEST WAY TO BUILD ORGANIZATIONAL ROBUSTNESS.

In 2021, ransomware attacks cost the world over $20 billion. Cybersecurity should be a top priority for top executives looking to avoid crippling fines and reputational damage. However, 90% of CIOs acknowledge their companies spend millions on inefficient security solutions. CEOs are losing sleep as they struggle to find worthwhile investments that will keep operations secure.

Most organisations do not have a methodology to validate cybersecurity. Those that have cybersecurity best practices at the heart of their culture, are better placed to make investments that protect their network.

When strategising how to operationalise security infrastructure, security decision makers should concentrate on:

Right team

Providing expert training has proven to be the best tool to retain best talent. Staff feels valued and invested in by their employers, driving them to perform operationally effective security.

Security exercises

Every professional team trains first for individual skills, then they train as a team. Cybersecurity teams should follow the same process to validate whether they are ready to protect.

Trust, but verify

Verifying how businesses behave under attack, being able to separate the significant signals from the noise is often the difference between being secure or being compromised.

Everyone's problem

No matter how state-of-the-art your technology is, 85% of breaches are in fact due to human errors. Being able to emulate traffic, mistakes and behaviours is key to building confidence.

Executive commitment

It takes commitment to be a secure organisation and operation. Leaders have to talk about how security impacts brand, customers, social responsibility.

Simulation exercises

Before and after every update to a stack, CISOs must test their security stacks. Red team exercises allow organisations to do this. In these exercises, red teamers will act as hackers and throw everything they can think of at the company's network. Old and new attack tactics, techniques and procedures will be deployed to see what cracks and what stands strong.

CISOs and their teams should keep detailed logs of the effects of these simulated attacks on their network before and after adjustments to the security stack.

Businesses have to ensure that both organisational consolidation and expansion do not lead to vulnerabilities, and that potential threats inherent within the stack itself are minimal.

Validate team and processes

Cyber training experts swear by tabletop exercises, but they are only as good as the table they are on if you do not actually practice a response. CISOs need to evaluate their team's incident response skills and make sure they have hired people who have the capabilities to identify threats and respond to them quickly and effectively.

One way to do this is through purple teaming – when red teams acting as offense and blue teams acting as defence work together to share knowledge. Purple teaming enables team members to collaborate with one another, and identify personal strengths and weaknesses.

Following the exercise, teams should hold a post-mortem to identify if any training programs need to be developed to boost employees' abilities. A problem addressed should always be coupled with a solution.

CISOs are responsible for providing team members the tools they need to be better at their jobs.

Confidence building

After testing both the stack and personnel, CISOs should ensure every member of the team is acquainted with each tool in their stack and involve their team in decision-making process. They should let their teams conduct trials with different tools before making a decision about which ones to invest in.

CISOs are not just responsible for making sure their company is not hacked. They are responsible for making sure their tools and people are working as a united front to keep bad guys out.

CISOs may already have the tools they need to succeed in their backyard. They may also have holes in their staff or stack that are zero ROI. Identifying gaps does not mean just finding holes in technology or the team, but figuring out how they can be effective together.