RED SIFT

How Can CIOs Stay Ahead of Bad Actors in 2023?

Security Leaders are bracing themselves for an onslaught of threats in 2023, not least of which include nation-state attacks, digital fraud, and cybercrime such as phishing, ransomware, BEC, and domain spoofing.

The socio-political macro landscape is changing, and this means the nature of threats facing organizations is constantly evolving. So, the attitude is fast shifting from security to building resilience, as businesses zero in on prevention, response, and recovery.

Today's Security teams must adapt to shrinking budgets, chronic understaffing, and ever-shifting priorities. What's a non issue from yesterday is a critical priority for today, requiring CIOs and CISOs to constantly reprioritize and mobilize their organizations to address new and emerging threats.

Prioritizing cybersecurity when everything is urgent

The CIO has always been pivotal to how an organization defines its technological infrastructure and IT operations. And now, its importance is further proven as we see it become a role more deeply integrated into company strategy, with 59% of CIOs expecting to hold a seat on their company's board of directors by 2025.

But with great influence comes great responsibility, and CIOs face a myriad of challenges all equally complex and demanding in both time and resource. Effectively utilizing Artificial Intelligence (AI), migrating to the cloud, increasing automation, facilitating interoperability between stacks, hiring talent, ensuring regulatory compliance with the likes of GDPR, and more all drain the CIO's time, energy, and budget.

Add to this the more recent demands on the CIO's plate, namely the push towards sustainability, using technology for the greater good, and effectively safeguarding data in light of high-profile privacy scandals such as the Solarwinds, Pegasus, and Optus breaches. Now the question becomes, how can CIOs prioritize cybersecurity when everything is urgent?

Implementing the foundational cybersecurity measures at scale

Security Leaders need tangible measures they can take to reinforce their most valuable and vulnerable assets, and this begins with getting the basics right. This may not sound revolutionary, but most businesses unknowingly aren't covering the foundational bases, meaning they leave themselves exposed in spite of best efforts. Getting the basics right looks like discovering your digital assets, monitoring your attack surface, securing your supply chain, blocking phishing attacks, securing your network perimeter, ensuring digital compliance, and building a cyber-first culture.

Forbes found that 84% of enterprise CIOs believe the internet needs an overhaul to control cyber risk. However, just a handful of organizations are using the measures, standards, and protocols proven to harden against threats, such as SSL, TLS, PKI, SPF, DKIM, DMARC, and MTA-STS. If more organizations were, perhaps an overhaul wouldn't be necessary?

Making your cybersecurity automated and interconnected

Threat actors are constantly attempting to infiltrate your business using a variety of tactics, techniques, and procedures, from business email compromise, and website domain impersonation to account takeovers. In this environment, it's no secret that having a single point of protection isn't enough. Attacks have increased in sophistication and scale-combining methods, and for these reasons they are very difficult to detect, particularly when they so well crafted and the target is under time pressure.

The general consensus is that the only way to fight the current level of sophistication is to fight back with AI and Integrated Machine Learning; re-enforcing what is discovered in one application across all applications and re-enforcing what is discovered by one user across all users. This isn't news to CIOs, with 60% believing AI and machine learning to be the top critical future technologies.

See, Solve, and Secure with the Red Sift Digital Resilience Platform

The Red Sift Platform gives organizations both visibility into, and direct control over, known and unknown vulnerabilities affecting their public-facing assets across email, domain names, and the web. Our integrated product suite works together to combat sophisticated, interconnected attacks across the evolving attack surface.

Learn more about the Red Sift Platform