TANIUM

The future of risk management

GUEST SPEAKER
Renee Murphy
Principal analyst at Forrester

Running a successful business relies on effective risk management. However, in the IT engine room of many companies, there is a serious problem. IT teams are still struggling to run their vulnerability management programs in a risk-oriented way. The result is wasteful effort, dangerously exposed systems, and talented individuals tied up in complex and labor-intensive processes.

We recently caught up with our guest Renee Murphy, Principal Analyst at Forrester, in a webinar to discuss how to overcome these challenges. In this Q&A, she emphasizes that by adopting an automated approach to risk scoring and management, organizations can streamline auditing and compliance, enhance endpoint visibility, and minimize the chances of a serious cyber breach.

The market in risk and compliance management seems to be shifting away from prioritizing better remediation to being resigned to the fact that remediation will be challenging and thus focusing on the prioritization of the vulnerability and compliance gaps to be remediated. Why do you think that is?

Renee Murphy: I think there is a thought among compliance professionals that if they take a long, deliberative, and methodical approach to evidence collection and management, it somehow makes the assessments more reliable. I would argue that it does the opposite. When the business is making decisions at wire speed, finding problems with manual assessments is like looking for a needle in a haystack of needles. And treating everything in the environment like it is a critical problem is a fool's errand. Threats aren't all the same, some things are worse than others, and any data in the environment that can tell risk managers about situational awareness should be a welcome addition to the arsenal.

When you think about risk-based vulnerability management, what factors do you think leaders should take into account beyond threat intelligence, indicating the likelihood that an exploit is in the wild and being used?

Renee Murphy: For someone wanting to tell a risk story, vulnerability management data is like drinking from a fire hose. It isn't uncommon to hear security professionals talk about the vulnerability metrics they use to report security to executives and the board. It inevitably becomes a slide full of thousands of vulnerabilities and whether they ar=e worse or better than the month before. Put yourself in your CIO's position. How do I use that for anything? What risk is this mitigating? How good or bad is that? Without understanding the risk posed by the vulnerability and whether that vulnerability impacts the organization, we don't know what it will do, and we table it. Context is everything in risk management, and understanding the impacts and likelihoods of our biggest threats in the context of what matters to the business, makes a stronger, and more resilient and secure company.

Where do you see opportunities for IT operations and security teams to collaborate better on vulnerability management?

Renee Murphy: Risk management is the glue that can hold security, development and operations together. Risks are created by the business, and they need to be remediated by everyone in IT - together. If we talk about the threat, then we are talking in a silo with security people. If we are talking about RISK, we are a level above the silo, allowing everyone to collaborate on the mitigation strategy for the business. Ops and security used to be adversarial, but the effort to mitigate risk brings us together in a common goal.

Is it with new teams and workloads (e.g., SecDevOps)?

Renee Murphy: I am not an analyst covering SecDevOps, and I don't want to contradict the existing research. I will say that thanks to the nature of the threat and the implementation of strategies like Zero Trust, we are all security engineers now. Developers, operations teams, risk managers, and network managers are all responsible for security. Risk gives them the language and processes to collaborate.

KNOW YOUR IT RISK POSTURE

Request a five-day, no-cost risk assessment to get a comprehensive view of risk posture across your organization.

Request my assessment

In summary, what is the one key takeaway about risk and compliance management that you would recommend to organizations?

Renee Murphy: Automate. Automate. Automate. All the data you need to manage your business risk is already in your data center. It's in your monitoring tools, your logs, and your servers. And remember, if you treat everything like it's critical, then NOTHING is critical; and auditors don't take kindly to the attempt to justify a lack of risk management.