How to build **stronger security teams**

Frontline security practitioners can thrive with the help of machine learning and executive sponsors

Steve Moore
Chief Security Strategist, Exabeam

BASED ON THE LESSONS WE'VE LEARNED during the coronavirus pandemic, government networks may permanently become virtual, remote environments. The old approaches often don't scale well for remote users, so the focus must shift to credentials and how to protect them.

As computing resources move to the cloud, the credential is what glues everything together. Network defenders need to be able to record each action associated with a credential and know whether that behavior is normal or abnormal.

With agencies operating in a complex mix of cloud and on-premises environments, it can be difficult to understand what's going on and, more important, what's normal and what's abnormal.

Machine learning through modeling allows agencies to answer those questions more quickly, more efficiently and with a higher degree of confidence than humans can.

For example, Exabeam builds timelines of users' network activity. Throughout the day, we can chart what an individual did and know whether that activity was typical or shows signs that credentials might have been compromised. We can automatically pull in data from multiple sources — such as antivirus software and intrusion-prevention systems — and model it, backed with machine learning. The end result is a human-readable storyboard that facilitates decision-making.

Avoiding the trap of overconfidence

Exabeam recently surveyed leaders and frontline workers at security operations centers about a wide range of issues for our 2020 State of the SOC Report. Among the risks we identified is a particularly challenging one to tackle: overconfidence.

In our survey, 82% of both government and nongovernment SOC professionals rated their ability to detect threats very highly. However, only 48% of them also said they could see what they needed to see in order to do their jobs. Perhaps not surprisingly, we found that executives tend to have a rosier picture of an agency's security than frontline workers do.

Nevertheless, a team that is overconfident in its ability to find and respond to threats represents an internal risk. The situation warrants an independent evaluation and a candid discussion among leaders and frontline staff.

Addressing employee turnover

In the biggest discrepancy, 64% of frontline workers cited the lack of a well-defined career path as the No. 1 reason for employee turnover, but only 15% of executives saw it as an issue. Leaders need to talk to employees about their concerns and establish clear goals and opportunities for advancement. They should begin today so they can build strong teams that will help agencies tackle the complex challenges of a rapidly evolving security landscape. ■

Steve Moore is chief security strategist at Exabeam and host of "The New CISO" podcast.