Balancing artificial and human intelligence

To block increasingly stealthy adversaries, agencies need machine learning and human expertise

Bill Aubin
Vice President of Federal, Exabeam

WELL-FUNDED, HIGHLY MOTIVATED adversaries are using increasingly sophisticated methods of attack, and they're working in stealth mode. Unlike earlier denial-of-service attacks, for instance, today's adversaries don't publicize their successes. Once they gain access to a network, they want to stay there undetected as long as they possibly can — for months or even years. They move methodically across devices and users, being careful not to attract any attention to their movements while they're exploring and looking for the best way to exfiltrate data. A large percentage of the time, such lateral movement starts with a compromised credential.

Fortunately, machine learning is revolutionizing the analysis of the ever-expanding volumes of data being collected from disparate systems and security tools. The technology can detect the anomalous actions and behavior that could indicate a network breach in near-real time, which gives agencies a significant advantage.

Recognizing anomalous activity

Intrusions are often discovered because of a sudden change, such as a connection to a new IP address to offload data or a highly unusual time for a system login, which could indicate that an adversary has compromised a user's credentials.

A combination of behavior-based breach detection, machine learning and automation can help agencies recognize anomalies faster so that they can detect hackers much sooner and severely curtail the amount of damage they might cause.

Using artificial intelligence technologies can save significant time and allow analysts to focus instead on threat hunting and identifying activity that could be an early indication of a network intrusion.

Seeing the breadth and depth of an attack

Security orchestration, automation and response tools are invaluable for agencies, but those tools can trigger many false positives and increase pressure on security teams to close incident tickets as quickly as possible because that's how their effectiveness is being measured. Sometimes, though, they don't completely understand the nature of an incident and could end up addressing only part of the problem.

Agencies need to take the time to thoroughly understand what they're responding to. For example, let's say a phishing incident results in an agency employee clicking on a link and inadvertently downloading malware. An automated response could remotely wipe the affected computer, rebuild it, reload it and have it back up and running that day. But the user's credential has been compromised, and an adversary could still be inside the network getting access to data.

Machine learning and automation are game-changers, but they don't eliminate the need for security professionals to thoroughly understand what's happening on their agencies' networks. When human intelligence is combined with automated response, agencies can more decisively resolve security incidents. ■

Bill Aubin is vice president of federal at Exabeam.