The future of cybersecurity is **autonomous**

AI can counter an attack faster than humans — and tip the scales back to the side of network defenders

Nick Warner
Chief Operating Officer, SentinelOne

TODAY'S CYBERATTACKERS ARE relentless. They move with such sophistication and speed that humans alone can no longer effectively solve the cybersecurity challenge. As the defenders of our nation's most critical assets and citizens' most sensitive information, federal cybersecurity professionals should not be left to play Russian roulette against such formidable adversaries.

For years, our defenders have been forced to scour mounds of disparate data seeking the proverbial needle in a haystack for telltale signs of intrusion. There is hope, though, in the form of rapidly evolving machine-speed security technologies. New innovations are leveling the playing field for defenders and, in the right hands, can tip the scales back in our favor.

Keeping pace with innovative adversaries

Analysts have too much atomic data and not enough context about that data. When they don't have the full picture, they can't take appropriate action. Re-creating each attack by hand takes painstaking care. And though analysts often relish this challenge, there's simply not the time to do so for every presented case.

Forward-thinking organizations are using artificial intelligence/machine learning (AI/ML) capabilities to fortify user endpoints and server workloads across an array of operating systems. These automations are designed to monitor the growing number of attack vectors in real time and present the full context of an attack in a view that's easy to understand and modeled after a kill chain.

Adversaries have their own playbooks consisting of tactical objectives such as reconnaissance, privilege escalation, lateral movement, and data collection and exfiltration. The steps to accomplish each tactic include myriad techniques strung together to form a campaign.

To keep pace with modern attacks, we must understand adversaries' techniques. Unfortunately, many agencies are not equipped to do so, resulting in a lopsided guns-versus-knives battle. What if we could have automatic visibility into adversary techniques? Better yet, what if we could recognize five techniques that individually are benign but together form a strong indicator of a data exfiltration tactic if executed in succession and in a certain way?

What if AI/ML automation could interpret complex technique relationships and take action on our behalf — or at least point us in the right direction so that we, the security operators, see it in the endless ocean of available data?

Shutterstock/FCW Staff

> **Modern solutions provide more signal and less noise.** Modern solutions assist overburdened security administrators rather than becoming work in and of themselves.

A new approach

At SentinelOne, our approach to defeating the adversaries of today and tomorrow is rooted in AI/ML that's purposefully designed to identify whether something is innocuous or truly bad. SentinelOne Singularity™, a FedRAMP Moderate-compliant security platform, connects AI/ML models, telemetry and context with automation and response so that it can make a decision in milliseconds and take action in real time.

Our strategy is proven in practice, as evidenced by the results of recent years of MITRE ATT&CK testing.

What is becoming increasingly evident through third-party testing and real-world breach scenarios is that legacy approaches, such as antivirus, do not solve the most critical cybersecurity problems faced by federal agencies today.

Modern solutions provide more signal and less noise. Modern solutions assist overburdened security administrators rather than becoming work in and of themselves.

The best solutions can recognize what adversaries are doing independent of human intervention, reducing mean time to respond and enabling faster recovery — all in the hopes of creating continuity for our people, our government and our nation. ■

Nick Warner is chief operating officer at SentinelOne.