FORTINET

WHITE PAPER

Help Wanted: Next-generation AI for the Emerging Threat Landscape

AI-based Threat Detection and Response Can Relieve Overwhelmed Security Staff While Mitigating Risk

Executive Summary

Many cybersecurity teams—and even vendor research labs—are overwhelmed by the speed and sophistication of today's advanced threat landscape. And few see light at the end of the tunnel. Manual analysis, investigation, and security workflows demand overwhelming amounts of time, and the cybersecurity skills shortage means few additional team members are on their way to help. Artificial intelligence (AI) is heralded as a solution, but AI is often a buzzword and practical applications are often inadequate. They sometimes solve one problem—detection—but leave the team overwhelmed by the need to effectively respond. To bring relief to security operations teams, a new generation of AI is needed that can provide advanced analysis and research in addition to threat detection.

56% of senior executives say their cybersecurity analysts are overwhelmed.[1]

Not too long ago, cybersecurity threat detection and response were relatively straightforward and tactical at most organizations. Signature-based antivirus solutions did much of the work of threat detection, and threat response often occurred within regular business hours when staff members were present. For their part, threat actors also did a lot of manual work to propagate their malware and infiltrate systems. In short, organizations and their adversaries did battle at a human pace.

But as technology advanced, the task of cybersecurity became infinitely more complex—a daunting task even for seasoned professionals. Sprawling hybrid cloud infrastructures and proliferating Internet-of-Things (IoT) devices expanded the attack surface. Exacerbating the situation is the fact that cyber criminals are taking full advantage of technological advances[2] to attack their targets with precision, speed, and efficacy. As a result, unknown threats are increasing in frequency and scope,[3] and the speed of attacks is accelerating, with exfiltration of corporate data now happening in a matter of minutes.[4]

Increased Risk Brings Bigger Burdens

At the same time, cybersecurity—once viewed as a back-office function—is now a board-level concern.[5] This increase in emphasis is warranted, as the risks and costs associated with cybersecurity have intensified dramatically over the past decade. As an example, one study finds that cyber crime currently costs the typical organization $13 million—a 12% year-over-year increase and a 72% increase over five years.[6] Included in this total are indirect costs like brand degradation, regulatory penalties, and the business cost of lost data—which are often more painful for businesses than the direct costs.

Regardless of the specific source of risk, the advanced threat landscape just means added stress for the security operations team and its management. In a recent survey, 56% of senior executives reported that their security analysts are overwhelmed.[7] These beleaguered teams are the result of many factors that are converging, including:

An increasing velocity of attacks. Historically, cyberattacks moved at human speed, with real people manually executing each step of an attack.[8] This meant that manual processes at least had a decent chance of catching an exploit before it caused major damage. Now, bad cyber actors are automating many of their practices to enable them to carry out attacks at machine speed.

Early automation efforts by cyber criminals involved highly repeatable actions, exemplified by the distributed denial-of-service (DDoS) attack.[9] Adversaries are now raising the stakes by using emerging technologies to accelerate the execution of attacks of all kinds. For example, criminals are now developing traditional bots into AI-driven swarmbots that can act in individual groups to prepare malware, poke at various security gaps, and assemble together for a full onslaught on an organization.[10]

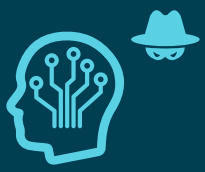
The Hide 'N Seek IoT botnet is something of a prototype of emerging approaches, "communicat[ing] in a decentralized manner using custom-built peer-to-peer communication to implement a variety of malicious routines."[11] Further, there are indicators that cyber criminals are beginning to use AI to enable accelerated fuzzing to discover new application vulnerabilities—turning a longtime tool of the good guys into another method of attack.[12]

As customized malware becomes the rule rather than the exception, unknown or zero-day threats are becoming more commonplace. Analysis by FortiGuard Labs shows that up to 40% of new malware detected on a given day is now zero day or previously unknown.[13] While some security vendors have robust detection engines and issue patches and signatures for new threats relatively quickly, the short period between detection and deployment of the signature is the riskiest time for organizations that are on the receiving end of attacks.

Increasing sophistication of cyber criminals. Efforts of adversaries to increase speed are just one element of their use of advanced technology to make their attacks more effective. Not too long ago, malware was mass-produced and reused repeatedly in identical form. That is no longer the case. In fact, 97% of viruses now change their characteristics on the fly using polymorphism,[15] meaning that a signature extracted minutes ago could be useless in thwarting a virus's spread.

Advances in technology enable cyber criminals to up their game with a variety of threat types. Phishing has evolved into spear phishing, which uses natural language processing (NLP) and data-scraping technology to target specific individuals with contextual, credible-looking malicious emails.[16] Ransomware is becoming more targeted to specific organizations, and U.S. local governments are a favored victim in recent months.[17] Cryptojacking is now available "as a service" to cyber criminals with less expertise.[18] And advanced anti-analysis techniques enable malware to detect when it is running in a sandbox or emulator, disable security tools on infected systems, and use junk data to make disassembly harder.[19]

"[A]dversarial automation is being used to create and launch new attacks at such a rate and volume that every strain of malware must now be considered a zero day, and every attack considered an advanced persistent threat."[14]



"In tomorrow's world, an offensive AI will be able to achieve the same level of [attack] sophistication in a fraction of the time, and at many times the scale."[20]

In short, the technological advances of the past few years are having similar impact for cyber criminals as they are for legitimate organizations—simplifying deployment, reducing cost, and eliminating many barriers to entry. This is because almost every kind of cyberattack is available as a hosted, full-service offering on the dark web, simplifying administration and taking advantage of extensive automation.

A rapidly increasing volume of alerts. As adversaries move to these more automated methods of disseminating malware and other threats, security teams can be overwhelmed by the sheer volume of threat alerts, eliciting a feeling that they are "constantly firefighting."[21] Over one-third of security professionals list keeping up with the volume of security alerts as one of their top challenges.[22] And 42% of them say their organization ignores a significant number of alerts because they cannot keep up with the volume.[23]

Generic threat feeds only exacerbate this avalanche of alerts. Organizations often attempt to "hedge their bets" by subscribing to multiple threat-intelligence feeds, but this only adds to the chaos.

One danger is the common problem of too much data—especially when added to an already overwhelming volume of alerts. For every feed that is added, organizations need to set up a way to analyze and triage vast amounts of data—some of which may not be relevant to a company's specific situation.[24] The potential result is false positives that impede operations, reduce the security team's productivity, and distract them from responding to legitimate threats. These outcomes can even cascade into areas that impact the bottom line, such as customer experience, brand reputation, and time to market.

Resource and skills allocation. When a specific team at a company is overwhelmed by the volume and complexity of their work, the normal remedy would be to add staff. The increasing velocity of threats makes this a less viable solution for security operations, as an infinite number of human analysis would be unable to catch many fast-moving threats.

But even if "throwing more people at the problem" were an effective solution, it would be impossible at most organizations. If anything, recent research has found that the long-discussed cybersecurity skills shortage is still with us—and is likely getting even worse. One study found that the worldwide skills shortage has increased to more than 4 million[25]—compared with just 2.6 million currently working in the field. Other recent surveys find that 53% of organizations report a problematic shortage of cybersecurity skills,[26] and that 41% are forced to recruit and train junior employees rather than hire the experienced cybersecurity professionals that they would prefer.[27]

The latter finding is concerning for all organizations—and especially those with less capacity to pay very high salaries for cybersecurity talent. For a security operations leader, finding an experienced analyst is well worth the extra cost, as professionals with five years of experience have seen more attacks and can complete threat investigations more quickly. But these professionals are quickly being priced out of the market for many organizations, forcing them to rely on less experienced employees.

In this environment of constrained human resources, optimizing the operational efficiency of the existing staff is critical. Yet this priority is beset with multiple roadblocks as well. The entire workflow for threat detection, response, remediation, and analysis is built around manual processes at some organizations. Even if the velocity of threats were not a factor, an automated approach would be necessary to move the cybersecurity staff from an overwhelmed, reactive stance to a strategic, proactive one.

CISOs find themselves "not only carrying out day-to-day operations, but also studying to learn of new risks."[28]

"The battleground of the future is digital, and AI is the undisputed weapon of choice."[29]

Conclusion

AI is reaching a tipping point where ever-increasing CPU power allows machines to perform a wider variety of tasks faster and more accurately than humans. This is evidenced by the rapid growth in investment in AI technology—almost a sixfold increase from 2016 to 2020, according to IDC research.[30]

On the security front, AI is now being deployed in the fight against cyber criminals. Some security vendors already use different elements of AI as a part of their offerings, but many of them are vague about just how comprehensive their AI efforts are. Most are focused on threat *detection*, which has the potential to make an organization more secure—but does nothing to relieve the stress of beleaguered security operations teams.

What is needed is a new generation of AI that helps organizations not only with detection of advanced threats but also research and deep analysis of threat intelligence and security incidents. Security analysts now largely gather that information manually. Automating that work would free them up to focus on proactive, strategic aspects of their jobs, rather than remaining in an endless cycle of "firefighting."

[1] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed January 27, 2020.

[2] For example, see Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018; Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[3] According to internal research, 75% of unknown malware detected by FortiGuard Labs was not found in the VirusTotal tool—which aggregates threat information from more than 100 security vendors.

[4] "2018 Data Breach Investigations Report," Verizon, 2018.

[5] "NACD Director's Handbook on Cyber-Risk Oversight," National Association of Corporate Directors, January 12, 2017.

[6] "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[7] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed January 27, 2020.

[8] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

[9] Ibid.

[10] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[11] Ibid.

[12] Derek Manky, "Using Fuzzing to Mine for Zero-Days," Threatpost, December 7, 2018.

[13] According to internal data from FortiGuard Labs.

[14] Saumitra Das, "When Every Attack Is a Zero Day," Dark Reading, April 23, 2019.

[15] Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[16] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

[17] "Threat Landscape Report Q2 2019," Fortinet, 2019.

[18] Jon Bove, "An Approach for Securing Advanced Threats for Your Customers," Fortinet, January 30, 2019.

[19] "Threat Landscape Report Q2 2019," Fortinet, 2019.

[20] William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.

[21] "Security Teams Overwhelmed by Rising Volume of Attacks," Dark Reading, May 31, 2017.

[22] Jon Oltsik, "Dealing with Overwhelming Volumes of Security Alerts," ESG, March 3, 2017.

[23] Ibid.

[24] Chris McDaniels, "Is Threat Intelligence Garbage?" Dark Reading, May 23, 2018.

[25] "(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide," (ISC)², November 6, 2019.

[26] Jon Oltsik, "The cybersecurity skills shortage is getting worse," CSO, January 10, 2019.

[27] Jon Oltsik, "Is the Cybersecurity Skills Shortage Getting Worse?" ESG, May 10, 2019.

[28] Quote from survey respondent, "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[29] William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.

[30] "2017 was just the tipping point for AI," Vision Critical, November 14, 2019.

FORTINET

www.fortinet.com

February 7, 2020 9:00 PM

593161-0-0-EN