AI
The future of cybersecurity
In the first half of 2016 alone, an attack against a Ukrainian power grid caused a blackout in the Western part of the country, a string of US hospitals was hit with ransomware, hackers targeted the IRS with fraud schemes, and $81 million was stolen from Bangladesh’s Central Bank in a heist. Organizations across industries and sectors are seeing their cybersecurity vulnerabilities exploited, and their constituents are suffering as a result.

Cybersecurity threats are growing in both volume and sophistication. According to PwC’s The Global State of Information Security Survey 2016, security incidents saw a 38 percent increase in 2015 compared to threats detected in 2014. The 2015 Cyberthreat Defense Report from CyberEdge Group found that more than half of survey respondents felt that a successful cyber attack against their network would take place within the year, while an ISACA study revealed that only 38 percent of global organizations claim they’re prepared to handle a sophisticated cyber attack.

This is partly due to a cybersecurity talent shortage crisis. The ISACA survey found that 45 percent of organizations surveyed worldwide reported they are hiring more cybersecurity professionals, but 94 percent say it’ll prove difficult to find skilled candidates. Meanwhile, cyber attacks cost an estimated $400 billion a year—expected to cost a whopping $2.1 trillion in 2019.

Amid this rising tide of malware, breaches, and hacks, organizations must evolve their security practices faster than hackers. Their survival depends on staying ahead of the curve, as well as on shutting down attacks before it’s too late. But this isn’t a human task—or isn’t just a human task. Maintaining vigilance in this perilous cybersecurity landscape will require enterprises to start leveraging artificial intelligence (AI).
A brief overview of white hat AI

Artificial Intelligence has become a Silicon Valley buzzword that gets thrown around more often than it’s understood. AI hasn't (yet) taken the form of robots—such as those in HBO's *Westworld* or movies like *Her* and *Ex Machina*—that interact with humans as if they, too, are human. In real life, it's an academic field that studies how to train computers to mimic human intelligence, meaning they can analyze a given state or situation and act on that state to achieve a specific result. AI is math, statistics, logic, and optimization—not magic or science fiction—and it’s becoming a pillar of the modern cybersecurity arsenal.

Traditional cybersecurity focused on known threats. Protective software was built with an index of known threats that it detected and blocked. But when hackers aren’t deploying known threats or using threat signatures, this approach becomes futile. It puts organizations in a reactive, defensive position, where cybersecurity is always a few steps behind and the most pernicious threats can easily sneak through defenses.

AI holds great promise for cybersecurity, because it enables organizations to be proactive in a larger, more complicated landscape, where the threats may come from organized crime or nation state actors with hefty resources and talent backing them up. As former Symantec CTO Amit Mital put it, AI is one of the “few beacons of hope in this mess”—the mess being cybersecurity, which is “basically broken.”

AI can monitor, analyze, and detect threats with greater speed, accuracy, and scale than even the most talented and experienced IT experts. Algorithms do the heavy lifting of identifying potential security issues by analyzing millions of data points and recognizing abnormal behavior in real time. They can grow, evolve, and adapt along with the threats, ensuring nothing falls through the cracks. Given that the average financial or commercial business faces multiple attacks per month—and it takes more than six months for most businesses to detect data breaches—AI-based monitoring is the only way to be truly vigilant.

AI prioritizes the most malicious, high-impact alerts, which enables IT departments to allocate their time and energy more effectively and avoid “alert fatigue.” AI is a critical tool in sifting out genuine threats from standard organizational noise and identifying threats never seen before. Another advantage of AI is its predictive possibilities. The technology can anticipate how and when an attack is most likely to hit. The opportunities are endless.

---

Amit Mital, former CTO, Symantec
The DARPA Cyber Grand Challenge

To capitalize on and encourage innovation in the cybersecurity field, the legendary Defense Advanced Research Projects Agency (DARPA) hosted the Cyber Grand Challenge at the DEF CON hacker conference in 2016, which pitted AI systems against each other in a “Capture the Flag” tournament. Seven teams of academics, researchers, and companies (whittled down from more than 100 teams) created AI bots to evaluate software, test for vulnerabilities, generate security patches, and apply them to protected computers on a network. Teams also defended against their opponents and waged counterattacks.

The challenges were rooted in real-world problems. For example, one of the bots was the SQL Slammer denial-of-service bug that infected 75,000 victims within 10 minutes in 2003 and slowed down internet traffic. Using their AI systems, teams identified vulnerabilities and patched them within minutes. The competition lasted for nearly 12 hours.

The winner of the DARPA Cyber Grand Challenge was ForAllSecure, a company founded in 2012 by David Brumley, Thanassis Avgerinos, and Alexandre Rebert. The team worked in software security and binary analysis for more than a decade.

“Our goal is to make the world’s software safe,” Avgerinos and Rebert said. “To achieve this goal, ForAllSecure has two main thrusts. The first one is developing automated tools to check software security. For instance, we ran our tools on all the Linux software we could find and identified around 12,000 bugs within a few minutes of analysis per program. The second aspect is cybersecurity training. Educating people in cybersecurity and hacking will enable them to write safer code.”

During the Cyber Grand Challenge, ForAllSecure built an automated reasoning system that used a probabilistic model to predict which software was currently under attack and which software should be patched. The AI in its bug-finding system directed the search through a program to maximize the likelihood of finding bugs quickly.

The founders said AI is an important tool, because the threat landscape is continuously changing, with new vulnerabilities found every day. “Automation and rapid reaction are key for mitigating attacks,” they said. “AI is about speed and scale. Reasoning about the security of hundreds or thousands of programs that a modern computer is running is a monumental task. Through program analysis and automation, you could potentially uncover and fix vulnerabilities in minutes, whereas a human analyst would need orders of magnitude more time just to skim through those programs.”
Thanks to advancements in AI, the cybersecurity landscape is at a tipping point. Amir Husain, the founder and CEO of SparkCognition, said that AI experienced a number of false starts throughout the past few decades—due to insufficiently sophisticated algorithms, a lack of data, or customer readiness—but that is shifting.

“The availability of data and sensors, the Internet of Things, really significant improvements in algorithms, work on deep learning—all of these things were happening while data was becoming more available with the cloud and the cost of computing resources went down,” he said. “All of that happened at the same time, and now, it’s a great time to launch an AI company.”

Husain, a serial entrepreneur, was inspired to found SparkCognition after realizing the extent to which digital threats were transforming into physical threats. Perhaps the most iconic example of this type of digital weaponry is Stuxnet. Stuxnet was a virus that, as WIRED writer Kim Zetter wrote in her book Countdown to Zero Day, “escaped the digital realm to wreak physical destruction on equipment the computers controlled.” Stuxnet caused centrifuges that enriched uranium in Iran to fail at an unprecedented rate.

Through this example, among others, Husain realized that businesses based on a physical footprint, like energy and manufacturing, were grossly unprepared for these types of attacks. Factories and plants were filled with sensors collecting massive amounts of data, and they were largely unprotected.
“At a large utility, a single generator or turbine can cost upward of $50 million, and the largest utility in the US has more than 700 of these turbines,” Husain said. “The risk posed by any one of these assets being taken over via malware is tremendous. You have huge systems spinning at thousands of RPMs—kinetic energy that can be discharged if such a system goes out of control, resulting in disastrous failure. It would be the equivalent of a pretty substantial bomb going off in the facility.”

SparkCognition works with businesses across industries to protect them from cybersecurity threats, as well as equipment failure. The company’s AI-based platform harnesses and analyzes infrastructure data from connected devices in real time and alerts the customer if there are any changes that may indicate a problem with the device. Its technology models physical and virtual assets, learns from data, and gleans insights to keep the assets protected and mitigate risk.

“We have a new approach we call cognitive fingerprinting that uses a combination of techniques from genetic algorithms,” Husain said. “We take vast amounts of sensor data and organize a genetic competition for a deep array of deep learning neural networks. The genetic algorithm causes these deep networks to be trained up on different aspects of data and makes them compete with regards to accuracy and recall to gauge the efficacy of a model. Then, we have a proprietary way of selecting a subset of these that are good performers.”

SparkCognition’s approach is taking off. Now, the company has more than 50 customers, including prominent companies from energy, manufacturing, and retail, who are eager to protect their industrial internet and IoT assets.

“We have to accept the reality of living in a world where cybersecurity has been weaponized,” Husain said. “The best we can do is it turn up the level of monitoring, and doing that with human beings is nigh impossible. The only way we can do that is with AI. I think it would be impossible any other way.”

- Amir Husain, founder and CEO of SparkCognition
**Better than a human**
The tipping point Husain mentioned is evident in the number of AI cybersecurity products that have emerged during the past few years. ForAllSecure and SparkCognition are two in an exciting and growing sector addressing a diverse set of security challenges with a diverse set of approaches.

**Invincia**, for instance, offers an Advanced Threat detection system that combines machine learning and behavioral monitoring to eliminate endpoint security blind spots. Its goal is to kill enterprise IT threats without impacting business performance, and it’s amassed more than 35,000 customers. **Interset’s** AI-based platform correlates multiple data classes—linking security events to users, machines, applications, and files. Its analytics platform surfaces threats across enterprise networks and removes false positives to prioritize risks, which allows security teams to stop the theft of sensitive data.

**Vectra** provides continuous, automated threat surveillance throughout an organization to proactively expose hidden and unknown cyber attackers in a network. It uses AI, machine learning, and behavioral traffic analysis to expose the fundamental behaviors of attackers as they spy, spread, and steal in the network. **Hexadite** connects to existing security detection systems to investigate every threat, leveraging artificial intelligence to apply targeted mitigation to stop security breaches in their tracks.

“Hexadite solves the cybersecurity capacity problem,” said Nathan Burke, Hexadite’s VP of Marketing. “If companies could automatically investigate every alert from every detection system without wasting the time of scarce security staff, they would. But with an overwhelming number of alerts and a shortage of cybersecurity staff, there’s just no way for companies to investigate more than a tiny percentage of the alerts they see.”

Burke said AI is at the center of Hexadite’s approach, because it solves problems and executes tasks mimicking the human cognitive process, including: understanding the scope of the problem at hand; knowing where to find sources of information to solve the problem; ingesting data from the outside; analyzing data to determine what is known good, known bad, or unknown; deciding what actions to take based on data analysis; determining whether those actions solved the problem; and running an analysis to see whether what was uncovered in the course of the process can apply elsewhere.

“The single largest risk has nothing to do with APTs, zero days, or things like file-less malware,” he said. “The biggest threat is the lack of capacity to follow up on the increasing threat volume and subsequent alert volume drowning security teams today. Put simply, AI is the only possible way to keep up.”

**Man + machine, together**
As the world becomes increasingly digital and connected, no sector or business will be immune from the need for sophisticated security protocols. By 2020, there will be more than 200 billion connected devices in the world, according to predictions from Intel. Banks, hospitals, retailers, media organizations, manufacturers—all will need to stay ahead of cybersecurity threats if they hope to survive, and staying ahead can’t be done by humans alone.

That said, humans can provide benefits and expertise that AI can’t. We’re still a long way away from a world where machines can understand nuance to the same degree as a human. Erasing humans from the cybersecurity equation is just as risky as foregoing the help of AI altogether. The most powerful cybersecurity arsenal is one that combines the benefits of human intelligence with the benefits of artificial intelligence. Only together can they keep hackers at bay.