NTT DATA Services

WHITE PAPER | SECURITY SERVICES

Outsmarting the Cybercriminals

How artificial intelligence and machine learning will transform digital security

JANUARY 2018

Point of View

Mike Barch, Vice President, Security Services, NTT DATA Services

NTT DATA

Table of Contents

Cybercrime is ...	3
Fighting fire with fire	4
Why AI and machine learning hold the key	4
Powering the security center	5
Toward a more automated future	5
The future is already here	6
About the author	7
What we do at NTT DATA Security Services	7
Sources	8

Follow Us:
@NTTDATAServices

Join the Conversation:
#NTTDSecurity

Connect With Our Expert:
Mike.Barch@nttdata.com

Cybercrime is ...

the scourge of modern society, with an epidemic of incidents and attacks affecting organizations in every corner of the world.

By 2021, the global cost of cybersecurity breaches will reach a staggering $6 trillion by some estimates, double the total for 2015.[1]

Cybercriminals are indiscriminate, launching crippling attacks on organizations large and small in both the public and private sector. In the U.K., a ransomware attack in April 2017 threatened to bring the country's National Health Service to a standstill;[2] in France, an attack on the presidential campaign of Emmanuel Macron threw the 2017 election into chaos;[3] in the U.S., Yahoo disclosed that a breach had seen 1 billion user accounts compromised in 2016;[4] and in the summer of 2017, an attack in India paralyzed the biggest container port in Mumbai.[5]

The stakes are high. Organizations unable to defend themselves from cyberattack risk extensive reputational loss in addition to the direct costs of a breach, estimated to average $3.62 million by the Ponemon Institute.[6] There's also the danger of confrontation with authorities and regulators that are increasingly concerned about data security and privacy. The European Union's General Data Protection Regulation, due to come into force in 2018, will include the power to fine organizations up to 2% of their global annual turnover for failures.[7]

Yet effective defense is tough — and getting tougher. Not only are criminals sophisticated and organized, with cybersecurity experts often forced to play catch-up, but also, new vulnerabilities offer opportunities that are all too easy to exploit. The rising trend of bring your own device (BYOD) in the workplace has provided one such opportunity, with criminals able to target corporate infrastructure through employees' personal devices. The Internet of Things (IoT) offers even richer pickings, with billions of poorly protected devices coming online.

How, then, do individuals and organizations protect themselves? The answer will increasingly lie in cyberdefense and security solutions powered by artificial intelligence (AI) and machine learning tools. Gartner states, "By 2020, investment in artificial intelligence/machine learning-based tools for IT resilience orchestration automation will more than triple, helping reduce business outages from cascading IT failures."[8]

Fighting fire with fire

Cybersecurity must evolve rapidly because cybercriminals move fast. The European Union Agency for Network and Information Security's latest research on cyberattack risk identifies no fewer than 15 categories of threats – and warns "cyber-threat agents are always a step ahead of the defenders."[9]

Organizations don't have the resources to mount effective defenses; conventionally managed cybersecurity tools, even when deployed by large teams of professionals in functions, such as IT or risk, can't cope with the volume, variety and velocity of attacks. They have performed admirably, but not well enough. While response times to attacks have fallen in recent years, a breach still takes an average of 146 days to detect, providing criminals with ample time to wreak havoc.[10]

The advent of BYOD has amplified the problem. In the U.S. alone, almost three-quarters (74%) of companies now allow their staff to access corporate IT infrastructure through their own devices, providing millions of new phones, tablets and laptops through which cybercriminals could potentially access their networks.[11]

The IoT phenomenon will be even more significant. By 2020, as many as 30 billion devices will be connected to the internet, three times as many as today.[12] Each device represents a potential access point to a cyberattacker, with manufacturers in many industries lacking the skills required to implement protective measures. Imagine a worker whose wearable fitness tracker syncs with his laptop, which is also connected to his company's network. The fitness device represents a new way in for an attacker.

Against this backdrop, organizations must find ways to automate cybersecurity defenses by outsourcing some of the work to tools that are capable of operating without human intervention, countering the scale of threats.

AI and machine learning represent an organization's best hope in this regard. AI is the science of getting computers to perform tasks that would normally require human intelligence; machine learning is a subset of AI — giving computers the capability to learn without being explicitly programmed.

Why AI and machine learning hold the key

Automated cyberdefenses already serve us well but have limitations. So-called signature-based tools such as anti-virus software can only cope with known issues. They're programmed to recognize and repel specific threats that have previously been identified. While such tools can be regularly updated, they are not an effective defense against unknown issues, where the form of attack is new or different in some way. This is, of course, how cybercriminals operate.

In contrast, systems powered by AI and machine learning have the ability to deter currently unknown threats too. They employ techniques, such as pattern-based recognition, to work out what might constitute a threat based on threats posed in the past, and to intervene accordingly.

These systems require data to operate effectively. Each new item of information from the network — how it operates in problem-free periods, the impact of incidents and breaches, the nature of legitimate and illegitimate communications, and many more potential inputs — adds to the learning process. Over time, as the system amasses greater volumes of data, it's able to recognize potential threats, both known and unknown, even more accurately and speedily — and on a scale no human could hope to match. The system learns to recognize a threat and is then able to respond accordingly.

Powering the security center

AI and machine learning tools have the potential to transform the way security operations centers operate, substantially improving the effectiveness and efficiency of their security information and event management (SIEM) platforms.

These platforms already manage the alerts constantly produced by an organization's IT network. They provide a human engineer with a long and growing list of issues to investigate — some of which will be threats that must be responded to, while others will turn out to be nothing to worry about.

As the volume of communications passing through SIEM platforms grows – and the sophistication of attacks increases – AI and machine learning tools will substantially shorten the length of the cycle from threat to response. They'll make a judgement, in real time, about the information and anomalies passing in front of them — and over time, as they build and learn from an ever-expanding dataset, their judgements will become increasingly accurate and comprehensive.

By 2020, Gartner predicts 10% of penetration tests will be conducted by machine-learning-based smart machines, up from zero in 2016.[8]

The aim is to enable the SIEM to be far more proactive and predictive before a human engineer becomes involved. The evolving algorithms of the system, powered by machine learning, will enable it to rapidly determine which threats require action — even if the threat has never been seen before — and to alert a human engineer accordingly.

Such solutions are already in deployment, building on the advances made in areas such as predictive analytics in recent times. They underpin machines and systems capable of making many of the decisions that formerly required human intervention, enabling a response to cyberthreat much closer to real time.

This is not to suggest that such systems will require no human intervention at all, even as the increasing size of their datasets enables more accurate decision making. Rather, they will reduce what would otherwise be an intolerable workload for human engineers, generating an action list consisting only of genuine threats and intelligence that drives prioritization of response.

Toward a more automated future

Over time, however, the need for human intervention will reduce. The first generation of AI and machine learning tools will dramatically improve detection, but as they develop further they will also begin to incorporate remediation.

That will require tools capable of making a broader set of judgements. For example, a platform detects a problem with a sales agent's laptop while he presents to clients at a remote location via a link to his organization's network. While the threat must be countered, simply cutting the network connection would leave the agent stranded; a human intervention would take this into account when considering the nature of the response, in a way that an automated system would currently struggle to match.

As these tools become more sophisticated, they will move into remediation, learning from datasets in order to understand what type of response to a problem is appropriate in any given situation. With defense points built into the system at every level, from individual device to network access points and within the corporate infrastructure, AI and machine learning tools will eventually be able to make practical decisions about where to employ a fix — and what type of fix — to mitigate the threat while minimizing disruption.

We will also see greater use of machine learning orchestration — the process of connecting security tools, integrating disparate security data, and providing security teams with the broad functionality to respond to all types of threats. When executed properly, this can be the connective tissue that streamlines security processes and powers effective security response.

With security orchestration, teams can utilize a single window for a coordinated response, both machine led and analyst driven. Still, there is a delicate balance between human intervention and automation that requires the right underlying architecture and intelligence. Automation must be earned, not given.

The future is already here

None of these solutions are theoretical; early adopters are already employing AI and machine learning technologies in their cybersecurity solutions and reporting good results. These tools now look set to shape the future of security in the years ahead, with extensive research and development and experimentation now delivering more sophisticated solutions at speed.

Adoption rates will increase rapidly. Right now, according to our estimates, it's probable that fewer than 10% of large organizations are using AI and machine learning technologies in cybersecurity — but that figure could rise as high as 50% within three to five years.

Organizations must be careful to select the right solutions. There is a danger of "AI washing," with vendors applying the term AI too indiscriminately, but we also have no choice but to move quickly. The threat posed by cybercriminals — and the scale of the opportunity presented by trends such as IoT — is too great to ignore. Harnessing AI represents our best chance of winning this battle.

About the author

Mike Barch, Vice President, Security Services, NTT DATA Services

Mike Barch was appointed vice president of NTT DATA Security Services in 2017 after moving over from NTT Com Security. Mike has distinguished himself in helping NTT Com Security transform into a services-driven security organization. With more than 30 years as a proven leader in the IT industry in both services and technology, Mike provides NTT DATA Security Services with a unique perspective and valuable strategic insight. He is a proven problem solver and brings a wealth of knowledge to the table, having served as the vice president and general manager of Managed Security Services and the Ethical Hacking business for British Telecom Americas. Prior to that, Mike augmented his leadership credentials by heading the sales effort in the Eastern United States for IBM/ISS, and spent 13 years working at 3Com Corporation, moving from territory sales representative to strategic account sales and, finally, to various sales management positions. His expertise ranges from driving sales to managing services, covering everything in between. Mike holds a bachelor's in Computer Science from Virginia Tech University.

What we do

As one of the leading providers of security services across the globe, NTT DATA Security Services can help your organization understand your existing risks and vulnerabilities and analyze your security posture. No matter where you are in your existing security journey, we plug any gaps and recommend steps for future-proofing your environment.

The three pillars of our services include:

- **Strategic Consulting Services:** Identifies the gaps within your environment and the risks associated with it.
- **Technical Consulting Services:** Mediates these gaps by leveraging your existing investments or by suggesting new investments aligned with business priorities.
- **Managed Security Services:** Takes a consultative approach and works for your business processes. We structure our solutions around your environment and needs.

Our Global Threat Intelligence Platform is the foundation for all of our services. Leveraging insights from monitoring data sources of our global client base, the platform offers advanced threat detection capabilities and incident response and containment services.

Sources

1. "Hackerpocalypse: A Cybercrime Revelation 2016 Cybercrime Report," by Steve Morgan, Cybersecurity Ventures.
2. "NHS cyber-attack: GPs and hospitals hit by ransomware," BBC News, May 13, 2017.
3. "Hackers hit Macron campaign with 'massive' attack," Financial Times, May 6, 2017.
4. "Yahoo Discloses New Breach of 1 Billion User Accounts" by Robert McMillan, Ryan Knutson and Deepa Seetharaman, The Wall Street Journal, December 15, 2016.
5. "Petya cyber attack: India is worst affected in Asia, Ukraine on top globally," The Indian Express, June 29, 2017.
6. "2017 Ponemon Institute Cost of a Data Breach Study," by Larry Ponemon, SecurityIntelligence, July 26, 2017.
7. "General Data Protection Regulation (GDPR) Portal," European Union.
8. Gartner, Smarter with Gartner, Gartner 7 Top Security Predictions for 2017, June 13, 2017.
9. "ENISA Threat Landscape Report 2016," European Union Agency for Network and Information Security, January 2017.
10. "Mandiant M-TRENDS EMEA report," FireEye, June 2016.
11. "BYOD Statistics Provide Snapshot of Future," by Michael Lazar, Insight, January 18, 2017.
12. "Roundup Of Internet Of Things Forecasts And Market Estimates, 2016," Forbes, November 26, 2016

Visit nttdataservices.com to learn more.

NTT DATA Services partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. As a division of NTT DATA Corporation, a top 10 global IT services and consulting provider, we wrap deep industry expertise around a comprehensive portfolio of infrastructure, applications and business process services.

NTT DATA