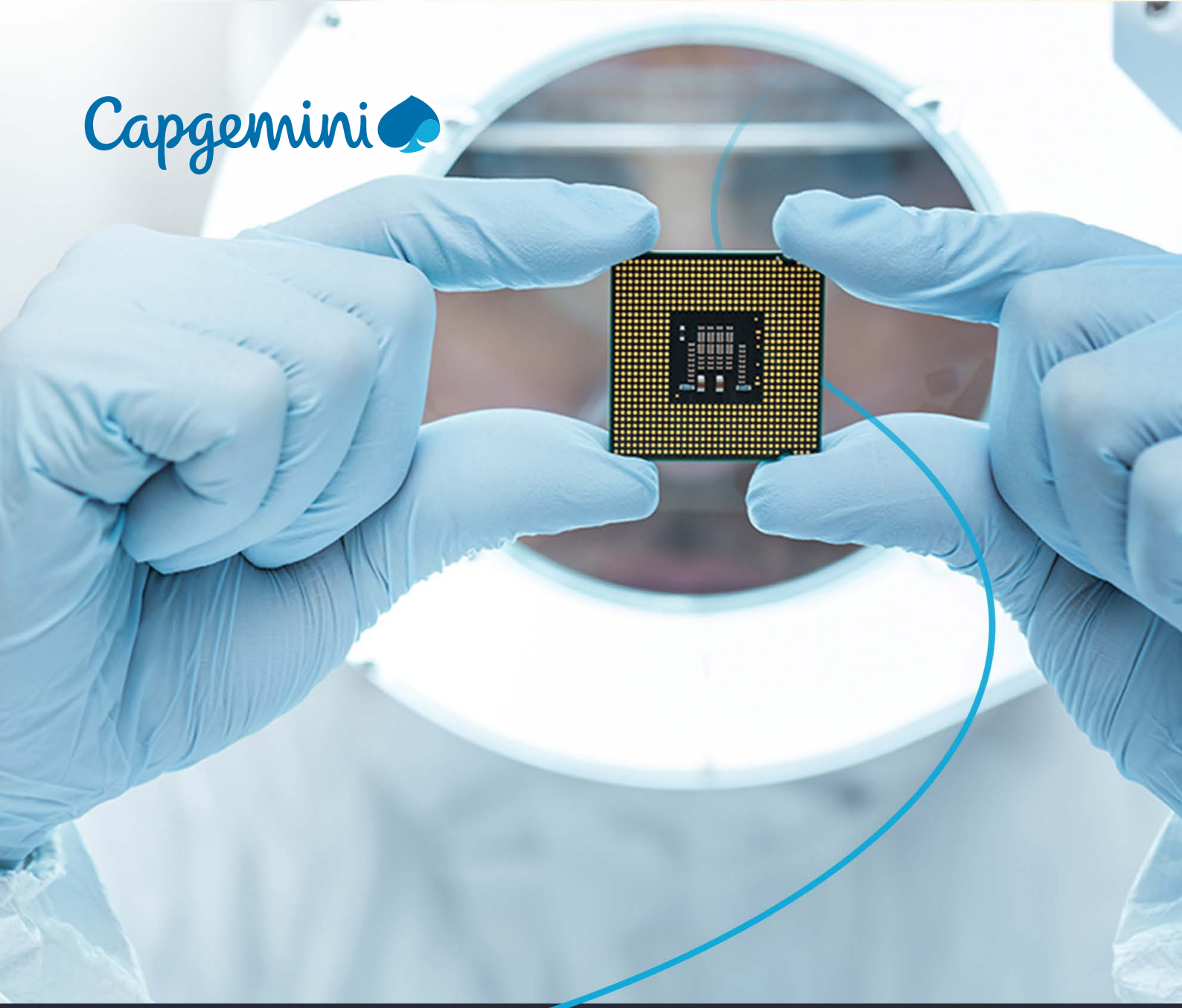

AI IN CYBERSECURITY: NOT AN ETHICAL DILEMMA

Building trust in the digital era requires the speed and intelligence of AI.

CYBERCRIMINALS HAVE NO ETHICS.

The debate about the ethical implications of applying AI to business processes is legitimate and important. We have all experienced both the benefits and the unintended consequences of AI in our day-to-day lives. The thought of applying this powerful technology to the protection of our personal information and our corporate data should give us pause.

And yet cybersecurity is one area where there is a clear case not only for using AI, but for broadening and accelerating its adoption throughout the enterprise and its Security Operations Centers (SOCs), among others. The obvious reason: malicious actors have no ethics. They are using AI to create and launch new attacks, and without AI-based defenses their exploits are far more likely to be successful. This paper takes a closer look at why companies must harness AI as a first line of defense, and why the use of AI is not only ethical but morally imperative.

HOW AI IS USED BY HACKERS AND MALICIOUS ACTORS

Time doesn't stand still for cybercriminals and hackers—not even during the pandemic. They are engaging in their own form of digital transformation and are harnessing ever-more-sophisticated technologies to carry out their attacks and exploits. To cite just a few recent trends in cyberthreats:

- Botnets with adaptable variants that actually mutate to infect devices and launch denial-of-service attacks
- Cryptojacking or cryptocurrency mining attacks that hijack compute power and bombard network infrastructure with traffic, slowing communication to a crawl
- "Dumpster diving" attacks that use AI to search for personal information in discarded emails, texts, and other forms of online communication
- Credential stuffing or "password spraying" attacks where hackers attempt to remotely access large numbers of accounts at once using account credentials that were stolen with the help of AI models.

These are only the tip of the iceberg, and the list doesn't include traditional and ongoing threats such as ransomware attacks, phishing, SQL injection, spyware, zero-day exploits, man-in-the-middle attacks, host redirection, and many more. In all, more than a billion malware samples were detected in 2020, and the number keeps rising.

When it comes to direct enterprise attacks, adversaries are leveraging advanced capabilities, building automation into their attack processes and toolsets, and likely taking advantage of other capabilities such as machine learning and potentially AI to increase their speed and capacity. For example, it is entirely possible for AI models to optimize effectiveness by determining when applications or users are most vulnerable, collect knowledge of what prevented the attacks in the past, and use that data to overcome defenses in the future.

HOW AI CAN HELP THWART CYBERSECURITY RISKS

The key capability AI gives cybercriminals is speed. They can do more harm in less time and adapt to new security responses faster by applying machine intelligence to their operations.

By the same token, AI gives security teams the speed they need to counterbalance and outperform attackers. By harnessing AI and automation, SOCs can scale to meet the growing volume, size, and diversity of AI-based cyberattacks.

AI empowers computers to collect, analyze, and disseminate information much faster than a team of human security analysts can. In turn, AI can make SOCs more effective by reducing manual analysis, evidence gathering, and threat intelligence correlation — driving faster, more consistent, and accurate responses.

For example, security operations teams can use AI to do the same job a security analyst would do—faster. That higher level of speed enables organizations to stay a step ahead of cybercriminals who are also using AI technologies and use the power of AI effectively to identify and thwart attacks.

More specifically, SOCs can tightly couple AI with emerging data integration capabilities to increase cybersecurity effectiveness. One example: create a security data lake—a holding tank for threat data—and use advanced algorithms to analyze all incoming data from every source for cybersecurity risks and threats.

When security analysts can spend their time investigating real threats, rather than sifting through countless alerts, they can focus their time on remediation and prevention of attacks. The net result is better protection for the enterprise and its employees, customers, and partners.

WHY TRADITIONAL ETHICAL CONCERNS DO NOT APPLY

Capgemini recognizes that there are many valid ethical concerns about using AI for any purpose, let alone cybersecurity. However, when it comes to cybersecurity, there is far greater risk in NOT employing AI, and there are offsetting benefits that do not pertain to other applications of AI. To illustrate, below are a few examples of ethical concerns and why they do not apply to using AI in cybersecurity.

Concern:

The use of AI in cybersecurity will cost jobs.

Response:

The use of AI in cybersecurity will help alleviate a critical skill shortage. Today enterprises around the globe are struggling to find qualified cybersecurity professionals. In fact, 70% of respondents in ISACA's State of Cybersecurity 2020 Report say fewer than half of their cybersecurity applicants are well qualified; while 32% of them say it takes six months or more to find a qualified candidate for an open position. According to another recent study, the world needs a 145% increase in its cybersecurity workforce.

Moreover, the use of AI will actually lead to new hiring. There is a growing role for data scientists in security operations, and most SOCs are actively looking for professionals with expertise in analyzing and interpreting data and its impact on cybersecurity. In short, AI will not outright replace analysts but can augment existing teams that are stretched thin, enabling them to do more in less time.

Concern:

The implementation of AI will overwhelm security teams.

Response:

The use of AI can help prevent cybersecurity teams from being overwhelmed. The sheer volume of data that is pouring into the enterprise is already very difficult to manage, and analysts are spending considerable time manually identifying common malware infections. AI enables them to deal with the data, automate and accelerate processes, and spend more time identifying and remediating the highest priority threats and attacks.

As is the case with any new technology adoption, this will not be an overnight success. It will take time to develop the right training sets, to align on the right AI models, and to find the right applications of the technology. The real key will be moving from the academic design to actual operations – proving and improving AI in the field.

Concern:

The use of AI in cybersecurity will only accelerate the arms race with cybercriminals.

Response:

The use of AI will reduce the success rate of cybercriminals. The speed at which cyberattacks are conceived, prepared, and launched is already accelerating dramatically. The ethical choice is whether to allow cybercriminals to seize the upper hand, or to harness the tools we have and protect our data and our organizations. AI and automation are the only tools that deliver the speed and scale needed to keep pace and mitigate risk.

Concern:

The use of AI in cybersecurity will outpace current data privacy regulations and governance capabilities.

Response:

The use of AI will underscore the need for universal guidelines for ethical AI use and serve as a catalyst for expanding important guidelines have already been published, including the European Commission's ethics guidelines for trustworthy AI, the German Data Ethics Commission's opinion on general ethical and legal principles concerning AI and algorithms, the Alan Turing Institute's report on understanding AI ethics and safety, the OECD's recommendations for 36 countries, and more.

In addition, expanding the use of AI in cybersecurity can lead to setting up a governance body to implement measures of accountability to give customers and employees the means to raise any concerns with AI systems through ombudsmen, grievance redressal authorities, and regulators.

Concern:

It is ethically wrong to trust the interpretations and analysis of AI without human involvement.

Response:

We agree. The power of AI—drawing intelligent insights from massive amounts of data—is also its weakness. The insights drawn from AI are based in logic, not emotion or experience, and this can lead to critical errors in judgment. Our collective experience from the COVID-19 pandemic is just one example: If you asked an AI engine who should be vaccinated first, it would crunch the data and respond that those with the largest and most lasting economic impact should be first in line. However, human decency would favor the elderly and those with pre-existing conditions, and in fact our societies prioritized those groups.

Equally important, speed is of the essence when it comes to remediation. In the world of IoT, we can't want for humans in all cases. If a plane is under attack while in the air, we need to harness the speed of AI to prevent critical failures.

Simply put, a human must be involved in the interpretation of AI analysis. Whether it's data drawn from intelligent IoT devices, self-driving cars, medical devices connected to the body, or Secure Access Service Edge network architectures, humans must ultimately maintain control over decisions made by AI models and actions taken as a result.

That is why Capgemini has consistently advocated for AI models that depend on human involvement while also reducing the manual tasks required of humans. Only through this model can we combine the speed, scale, and trust required to protect our enterprises—without compromising on our ethics.

THAT'S THE "WHY." NOW LEARN "HOW."

AI is the quintessential element for the fast and accurate responses needed in today's volatile threat landscape. To take the next steps toward effective and ethical use of AI in cybersecurity, and to learn how to implement AI in your SOCs, contact **cybersecurity.in@capgemini.com.**

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 290,000 team members in nearly 50 countries. With its strong 50 year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion.

Get the Future You Want | www.capgemini.com

For further information please contact:

cybersecurity.in@capgemini.com