TAG Cyber

Security Annual

2023

SPECIAL REPRINT EDITION

CONTINUOUS THREAT EXPOSURE MANAGEMENT WITH CYMULATE

AN INTERVIEW WITH CAROLYN CRANDALL, CHIEF SECURITY ADVOCATE AND CMO, CYMULATE

AI WILL BE THE END OF CYBERSECURITY (AS WE KNOW IT)

THE INTERSECTION OF AI, TRANSPORTATION AND SMART CITIES: CHARTING A SECURE AND ETHICAL FUTURE

TAG CYBER DISTINGUISHED VENDOR

Cymulate

The need to reduce cyber risk has never been greater, and Cymulate has demonstrated excellence in this regard. The TAG Cyber analysts have selected Cymulate as a 2023 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Cymulate's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Cyber Security Annual
www.tag-cyber.com

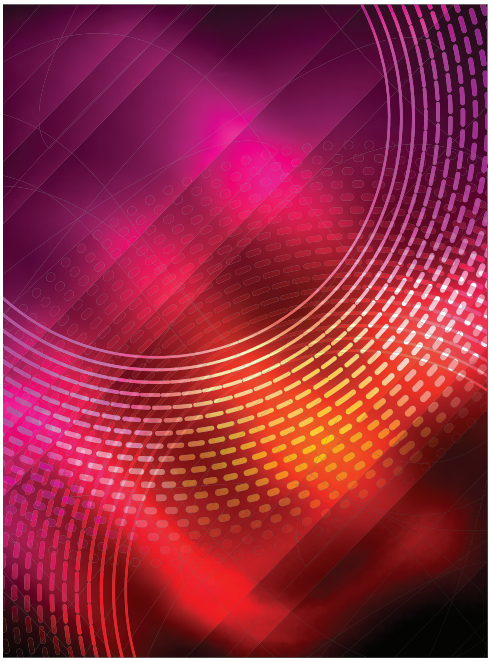
REPRINTED FROM THE TAG CYBER SECURITY ANNUAL

TAG CYBER Cymulate

AN INTERVIEW WITH CAROLYN CRANDALL, CHIEF SECURITY ADVOCATE AND CMO, CYMULATE

CONTINUOUS THREAT EXPOSURE MANAGEMENT WITH CYMULATE

In the world of cybersecurity, automation can help companies deal with the latest cyberthreats and regulatory pressures. Cymulate's platform allows companies reduce exposure by continuously monitoring, testing and validating the functionality and efficacy of their security systems. Last year, we had the pleasure of talking with Cymulate about their security posture management program, and we recently met with the company again to learn more about their wide range of unique solutions, as well as hear their insights regarding future cybersecurity trends.



TAG Cyber: What is a continuous threat exposure management (CTEM) program?

CYMULATE: We are the first vendor to meet the full spirit of a continuous threat and exposure management program. CTEM is a multiyear initiative that helps organizations move beyond only tactical and technical remediation to reduce their long-term exposure. It also helps with communications between technical and business leadership in an effort to simplify complex technical information and issues. We deliver a unique, full exposure management program with a modular platform that automates and consolidates assessments from attack surface management (ASM), breach and attack simulation (BAS), and continuous automated Red Teaming (CART). Additionally, the platform can ingest exposure data from other sources to prioritize vulnerabilities and accelerate remediation. This innovation evolves traditional human-driven pen-testing, bringing forward self-service and automated breach feasibility and security control validation. Collectively, this reduces cyber risk by providing businesses of all sizes a cost-effective solution to frequently test and validate that security systems are operating and alerting correctly.

TAG Cyber: Tell us about the benefits of your solution for security leaders who want to strengthen their organization's cyber resilience.

CYMULATE: Using our technology, organizations can continuously assess, optimize, rationalize, and prove security efficacy and improvement. Our automated solution improves visibility to exposure, while reducing the risk of a breach by continuously validating security controls and testing breach feasibility. Businesses need to discover and prioritize exposures quickly, and this goes beyond simply understanding exposure by adequately prioritizing where you patch and where you focus. Due to the volume of vulnerabilities and often the inability to patch, security teams need to understand whether their security controls effectively detect, alert, and respond to threat activity, including whether compensating controls activate when other controls have been bypassed. We are also helping improve communications between security and business leaders with reporting that is tailored to each role and provides documentation that business leaders can understand, monitor, and act on.

Attackers are more aggressive and destructive than ever before, so many customers have set their 2023 focus on data-loss prevention (DLP).

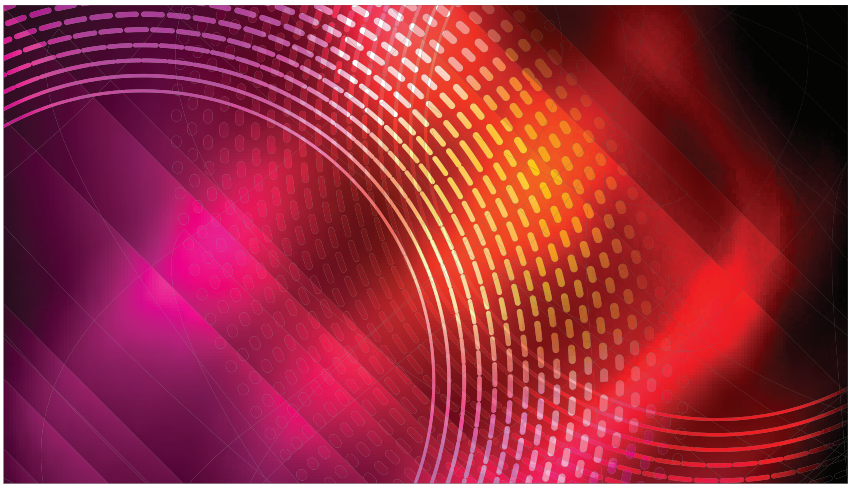
TAG Cyber: Tell us more about how enterprise teams can prioritize security decisions using your platform.

CYMULATE: Exposure assessment and security validation are baseline security activities for businesses of all sizes. As companies mature in their programs, they need to optimize their environments and automate repeatable processes. Enterprises are experiencing increased pressures related to attack frequency and severity, regulatory issues, and staff shortages. Therefore, they need to turn to automation to keep up and respond to today's threat activity. Businesses of all sizes can easily achieve this using the Cymulate platform, which allows them to quickly assess their internal and external attack surface for exposures and prioritization. They can also leverage over 120,000 out-of-the-box attack simulations to test the efficacy of their security controls. Attack-based vulnerability testing and customized scenarios easily automate testing for emergent and advanced threats, which is appealing to sophisticated security teams. More mature organizations can leverage automated discovery operations and other aspects of Red Teaming that don't require direct supervision, allowing staff to perform more frequent testing in more areas of the organization. Large enterprises also appreciate that Cymulate limits the use of agents to one per environment, thereby simplifying deployment and maximizing scalability. In a time when vendor consolidation is a crucial focus, we provide modular licensing within a single platform, making it easy for customers to expand as their needs change. Attackers are more aggressive and destructive than ever before, so many customers have set their 2023 focus on data-loss prevention (DLP). Our platform validates that DLP and cloud access security broker (CASB) tools are detecting and alerting as needed, even when upstream security controls have failed.

TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.

CYMULATE: Due to unrelenting cyberthreat activity, organizations will shift from threat management to exposure management to be more proactive versus reactive in addressing cyberthreats. This is underpinned by regulatory and insurance pressures that are pushing companies to develop, maintain, and validate reasonable cybersecurity practices, as well as describe those practices in public filings by explaining how senior leadership oversees these programs effectively and promptly reports breaches. Another trend we see is around cybersecurity market consolidation. Economic anxiety, staffing challenges, and growing supply chain threats are impacting cybersecurity spending

and the number of vendors that a business is willing to support. The global economic downturn has led to across-the-board consolidation among cybersecurity teams, specifically regarding the number of cybersecurity solutions and planned projects, along with staffing and training policies. This consolidation points to hard times for niche players and point solutions, while established companies with broad offerings are more likely to prevail, which might create merger and acquisition (M&A) opportunities for these bigger fish. Staff reductions could lead to a dangerous tipping point, creating a significant loss in cyber readiness and business production, thereby increasing breach feasibility. The automation of vulnerability assessment and security control validation can immediately enhance productivity for security teams dealing with limited skill sets that need help with repeatable tasks. Enterprise security is clearly consolidating, which will result in both customers and vendors needing to understand each security solution's role—where there are overlaps and where there are gaps. For Cymulate, this creates an opportunity for our customers to understand exposures, prioritize vulnerabilities, and test the efficacy of security controls. In the process of doing this, businesses will start to understand what test scenarios their business requires. During this process, they'll progress into new capabilities, such as automated Red Team testing, which will help offset the volume of testing they need to complete, while addressing the staffing challenges that businesses face today.



AI WILL BE THE END OF CYBERSECURITY (AS WE KNOW IT)

DR. EDWARD AMOROSO

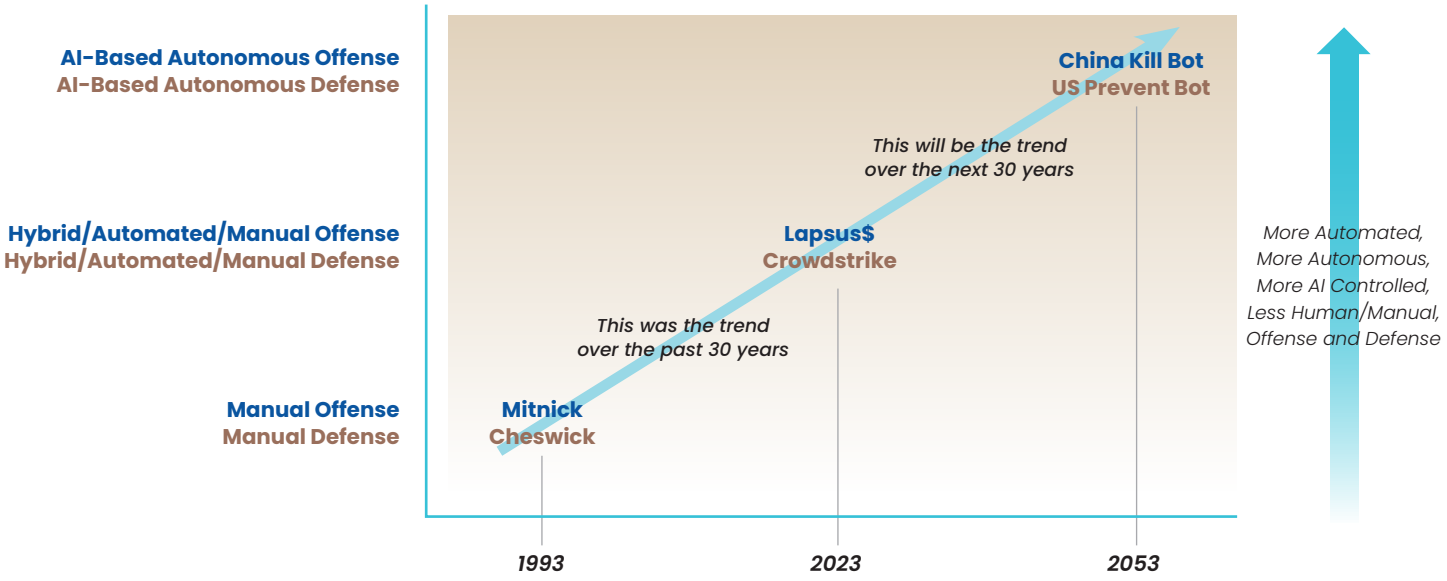


Figure 1. Author's Prediction of AI's Influence on the Future of Cybersecurity

I believe we can now glimpse the *end* of cybersecurity, as we know it—and it will be driven by artificial intelligence. Now, before you go and cancel your Series A term sheet or reduce your CISO's quarterly budget, let me explain what I mean.

Almost exactly 40 years ago, David Letterman set up a wonderful competition between a humidifier and a dehumidifier, fighting it out in the same room, while the humans watched to see which would win the vapor contest.

This display of machine versus machine offers a crude glimpse into where cybersecurity is headed long-term. That is, in the future cyber offensive and defensive platforms will be AI-controlled and autonomous. It will be AI versus AI.

Humidifier Vs. Dehumidifier. The Late Night Show with David Letterman, July 5, 1983

This is a logical extrapolation of where cybersecurity has always been headed. The earliest hacks and protections in the Awesome Nineties were controlled manually. **Kevin Mitnick**, the hacker, and **Bill Cheswick**, the hackee, typed into keyboards.

Now—roughly 30 years later—every cyberattack and every cyber defensive platform combines human operation with strong automated controls. For example, TAG Cyber seesthat botnets now run via combined human/automated control, as do protection platforms.

And so, perhaps 30 years from now, we should expect to see 100% automated offensive tools targeting 100% automated defensive platforms. And, as with the humidifier and dehumidifier conflict, the humans will watch to see who wins.

This has nice implications. First, it will be a great leveler. The asymmetry between nation-states and corporate targets could be a thing of the past when both organizations have the same tech. Both big and small teams use the same Windows 365 today, for example.

In addition, AI will drive cybersecurity risk into the same category as, say, physical bank robberies. There will be some incidents, certainly, but the intensity and frequency will drop to a level that no longer requires the same level of attention.

However, because AI will enable creativity, we should expect to see both *malicious* creativity as well as *defensive* creativity. And this, my friends, will be the future of cybersecurity. I think that perhaps we should call this *Cybersecurity 2.0.*

Yes, perhaps in the future humans will use external AI to threaten the normal AI-to-AI combat. Or maybe fake news or outcomes from biased AI will become a new industry. Who knows? But with ongoing advances in AI, this will look nothing like what we have now.

THE INTERSECTION OF AI, TRANSPORTATION AND SMART CITIES: CHARTING A SECURE AND ETHICAL FUTURE

CHRISTOPHER R. WILDER

In 2017, I found myself at the epicenter of an emerging technological revolution in autonomous vehicles and smart cities. As an industry analyst, I was collaborating with industry titans like AMD, Hewlett-Packard, Intel, NVIDIA, Kontron AG, Microsoft and other organizations–including government agencies. We were working to create a roadmap for ethical AI principles. Our territory included AI-based automation and generative AI in the transportation and smart city domains. Simultaneously, we were exploring the potential of advanced storage and computing power, which could eventually enable machine and deep learning algorithms to achieve self-awareness. (I continue to advise governments and organizations on deploying next-generation solutions that advance critical infrastructure and communications to improve the lives of the people they serve.)

At this pivotal moment in AI's evolution, examining the ethical and technical challenges and opportunities that AI presents, including the often-overlooked aspect of cybersecurity, seems essential. In this article, I'll delve into these aspects, address key considerations for vendors in this industry, uncover specific ethical use cases and leave you with a few predictions.

NAVIGATING THE ETHICAL LANDSCAPE: CHALLENGES AND OPPORTUNITIES

Let's look at some of AI's ethical challenges and opportunities in transportation and smart cities, including key concerns like data privacy, bias, job displacement and environmental sustainability.

THE PROBLEM:

Transportation and smart cities teeter on the edge of an ethical challenge as they rely heavily on vast data from various sources. This data often includes **personal information that can identify individuals,** creating a potential minefield of privacy issues. (For more information click here.)

OPPORTUNITIES:

- Organizations must strengthen data protection measures and implement anonymization techniques to safeguard personal information.
- They must develop transparent data collection and usage policies to build trust among users.
- They should collaborate with regulators and policymakers to establish industrywide data privacy standards.

THE PROBLEM:

AI algorithms trained on **partial or inaccurate data** can amplify these flaws, leading to skewed decision-making.

OPPORTUNITIES:

- Identify and address biases in training data to ensure fairness and equal representation.
- Implement explainable AI (XAI) techniques to enhance transparency and accountability in AI decision-making.
- Foster access and inclusion throughout the AI development process to incorporate various perspectives.

THE PROBLEM:

The rise of AI-based automation in transportation and smart cities will **displace numerous jobs**, particularly in public transit, trucking and traffic management sectors. (For more information click here.)

OPPORTUNITIES:

- Develop strategies for reskilling and upskilling workers to prepare them for new roles in an AI-driven economy.
- Collaborate with governments and educational institutions to create job opportunities in emerging fields related to AI and smart city technologies.
- Encourage entrepreneurship and innovation in AI and transportation to generate new employment opportunities.

THE PROBLEM:

AI applications must be able to **scale and perform efficiently** to meet the demands of growing urban populations and increasingly complex systems. (For more information click here.)

Building and deploying ethical AI-based solutions requires a comprehensive approach that prioritizes ethics throughout.

OPPORTUNITIES:

- Leverage advancements in hardware, such as graphical processing units (GPUs) and custom AI accelerators, to improve the performance and efficiency of AI algorithms.
- Adopt cloud and edge computing technologies to optimize resource utilization and reduce latency.
- Develop modular AI solutions that can be easily scaled and adapted to accommodate evolving requirements and technological advancements.

THE PROBLEM:

As AI-based transportation and smart city solutions become increasingly interconnected, they become more **vulnerable to cyberthreats**. Ensuring the security of these systems is paramount to maintaining public trust and safeguarding the continued growth of AI in these sectors.

OPPORTUNITIES:

- Implement multilayered cybersecurity strategies, including encryption, intrusion detection and threat intelligence to protect AI systems and the underlying infrastructure.
- Foster a security-focused culture within organizations, emphasizing the importance of cybersecurity at every stage of the AI development and deployment process.
- Collaborate with government agencies, industry partners and cybersecurity experts to develop and adopt standards, regulations and best practices for AI in transportation and smart cities.

KEY CONSIDERATIONS FOR VENDORS, ENTREPRENEURS AND INNOVATORS

Building and deploying ethical AI-based solutions requires a comprehensive approach that prioritizes ethics throughout. Let's explore some of the key concerns for enterprises, vendors, entrepreneurs and innovators seeking to ensure the responsible use of AI and the promotion of social and environmental sustainability.

THE PROBLEM:

Innovators, entrepreneurs and vendors must **navigate the rapidly evolving landscape of AI** in transportation and smart cities with their eyes wide open. Further, they must consider several factors to remain competitive, build better products and ensure ethical, unbiased and secure AI solutions.

OPPORTUNITIES:

- Develop, join and maintain partnerships with various stakeholders, including policymakers, regulators, academics and other industry players.
- Prioritize research and development activities focused on innovative AI solutions that address real-world challenges and enhance the quality of life in urban environments.

- Ensure AI solutions adhere to ethical guidelines built with transparency, accountability and fairness.
- Invest in the education and upskilling of employees to keep pace with the fast-changing AI landscape and maintain a competitive edge in the market.
- Address critical cybersecurity issues by implementing robust security measures and fostering a culture of security awareness within the organization.

ETHICAL USE CASES AND PREDICTIONS FOR THE FUTURE

As we reflect on the ethical considerations of AI-based solutions, it's important to consider the potential impact on the future. By examining trends and predictions we have seen in the field, we can better prepare our clients for the challenges and opportunities ahead while also focusing on responsible innovation and ethical best practices.

THE PROBLEM:

The pace of technological innovation continues to accelerate, so it is **critical to consider the ethical implications** of its use. From AI and machine learning to virtual reality and autonomous vehicles, there are numerous areas where organizations must weigh many factors. (For more information click **here**.)

OPPORTUNITIES:

- AI-powered traffic management systems can optimize traffic flow and reduce congestion while prioritizing pedestrian safety and accessibility.
- Autonomous public transportation systems can provide equitable access to transport services and enhance mobility for all residents, including the elderly and people with disabilities.
- AI-driven environmental monitoring and management systems can enable more efficient use of resources, can reduce pollution and can promote sustainable urban living.
- Predictive maintenance systems that leverage AI to identify potential infrastructure issues before they escalate can minimize disruption and optimize resource allocation.

As AI technology advances, the transportation and smart city sectors will benefit from this transformative shift. By addressing ethical and technical challenges and embracing AI's opportunities, we can pave the way for our urban environments to have a more secure, efficient and sustainable future.

EMBRACING THE HUMAN-AI SYMBIOSIS

We must recognize that AI is neither a panacea nor a replacement for human intervention and intuition. While working in the cybersecurity and cognitive computing group at HP Labs, we embarked on teaching drones how to learn and identify bad actors. The science was sound, but we could not decouple the science from the engineering because cognitive computing, much like AI, has no feedback loop. Computers can look at a puppy and a kitten side by side and not determine the difference. They both have immutable traits, such as ears, a nose and a tail, and both are super cute. However, a 2-year-old human child knows the difference immediately because they have a feedback (input/output) loop, while the AI or cognitive computing algorithm does not. We must not discount the disparity between human-AI symbiosis for augmenting common human tasks and capabilities. No amount of algorithm training can replace the human factor, nor should it.

AI will continue to play a pivotal role in shaping the transportation and smart city sectors in the coming years. This evolving landscape calls for a human-AI symbiosis, where technology augments human capabilities, creating a more efficient and harmonious human experience. Below are several areas where AI will both enhance and assist organizations to be better prepared and to respond to threats:

1. **AI-assisted urban planning** can integrate predictive analytics, citizen input and environmental factors to design sustainable, livable and resilient cities.
2. **AI-enhanced emergency response systems** can optimize resource allocation, streamline communication and improve overall preparedness during natural disasters or other crises.
3. **AI-driven public health initiatives** will leverage data analytics, predictive modeling and real-time monitoring to enhance community health, track disease outbreaks and inform public health policies.
4. **Smart energy grids** powered by AI enable dynamic energy distribution, demand forecasting and optimized utilization of renewable energy sources.
5. **AI algorithms** automate the tedious and time-consuming tasks involved in SOC operations, such as threat detection, analysis and response. AI can quickly identify potential threats and alert security analysts for further investigation.

THE ROAD AHEAD

The AI revolution in transportation and smart cities presents immense potential for transforming urban landscapes. It also poses significant challenges that require a proactive and collaborative approach. Stakeholders must foster a culture of continuous learning, innovation and collaboration while actively engaging with regulators, policymakers and the public to create a shared vision. Moreover, interdisciplinary collaboration and ethical AI development are crucial in addressing multifaceted urban challenges and ensuring AI-powered solutions that are secure, transparent and unbiased.

Balancing innovation with moral responsibility is essential, and addressing concerns such as data privacy, bias, job displacement and environmental sustainability is also paramount. As we move forward, embracing a human-AI symbiosis that supports inclusive innovation, prioritizes collaboration and helps build a global AI ecosystem will pave the way for a more secure, efficient and sustainable future.

Cymulate's Extended Security Posture Management allows organizations to measure and maximize operational efficiency while minimizing risk exposure. Based on real-time data, Cymulate protects IT environments, cloud initiatives and critical data against threat evolutions. Using simulation, evaluation and remediation, Cymulate empowers and defends organizations worldwide, including leading healthcare and financial services.

TAG CYBER
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL