Farah Alhamzawi

Independent Study & Mentorship

Mr. Green

14 September 2023

Annotated Bibliography: The Future of Cyber Protection

Townsend, ByKevin. "A Deeper Dive into Zero-Trust and Biden's Cybersecurity Executive Order." *SecurityWeek*, 18 Aug. 2023, www.securityweek.com/deeper-dive-zero-trust-and-bidens-cybersecurity-executive-order/.

In recent months, President Biden has extended an Executive Order to provide more protection to civilians because Federal agencies still have not met the basic cybersecurity standards necessary to protect America's Sensitive data." Throughout this article, the author, a Senior Contributor at SecurityWeek, discusses the advantages of this order and what is to come through this executive order.

The purpose of the new order is to create awareness of daily active threats; through this awareness, action can be taken to protect critical information and individuals' information from cyberattacks. With this executive order, this topic would be addressed and seen as relevant; however, through the recent increase in cyberattacks through malware in the past year, The U.S. has noticed the danger of the cyber web. This order enacts a Zero-trust Plan. This plan implements a zero-trust architecture as the most practical method of improving the nation's cybersecurity posture. Zero trust is a cybersecurity paradigm that assumes no implicit trust for any entity, regardless of location or ownership. Through this article, they explain this concept as so:

"We are still trying to define zero-trust. It means different things to different people." That is part of the purpose of having a plan for a plan:

"In the coming 12 to 18 months, we will see the evolution of a real definition of zero-trust and the parts and the pieces that make up a zero-trust architecture... "But we found it was not effective ... The zero-trust concept applied to the house means every door and window – including those inside the house – needs a separate key and authorization. Every room in the house, cupboard, and drawer needs to have a different focus of authorization and authentication."

This way of defining zero trust allows assets to be identified and micro-segmented while allowing authorized users to identify, authenticate, and issue keys only when needed. The key would be created and stored securely and be controlled by multi-factor authentication.

Through this new Executive order, the government plans to develop and integrate federal departments and agencies by adopting the zero-trust approach to cybersecurity. This is significant because if this plan is successful, they may start implementing it nationally to citizens in case of threat.

Barrus, Richard. "Attack Surface Management: Dark Web Deep-Dives and More." *Pivot Point Security*, 16 Mar. 2023, www.pivotpointsecurity.com/attack-surface-management-dark-web-deep-dives-and-more/.

Every individual has a digital footprint. Whether they signed up for a shopping website or were commenting on a post, it is all considered for a digital footprint. A digital footprint is a web of everything an individual has ever done online. Through this footprint, cyberattacks can be hidden in plain sight and cause damage to that footprint as well as the device that has been attacking. Throughout the article, the author discusses a digital footprint and how that is associated with an attack surface manager.

An attack surface manager is an up-and-coming service that proactively identifies and alerts on cyber threats and risks across a company's ever-expanding internet-connected digital footprint. Through this profession, a service called "white-glove service"

provides a deep dive into dark web forums and monitoring. Through this platform, the user can monitor for keywords and profiles and view dark web forums trying to attack them.

Throughout the article, the author discusses the approach to the Saas platform; this is when there is a "big account team and support team that helps you onboard and configure and all those things as a part of getting the platform into your organization. As it moves into operationalizing that data daily, a user has an account management team that can help. Nevertheless, if the user is looking for a much more tailored approach, we have those services to accompany it." Through these types of advancements in cybersecurity, users can protect themselves through multiple platforms that companies provide them.

Aubrey, Curt, et al. "Cyber AI: Real Defense." *Deloitte Insights*, www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html. Accessed 14 Sep. 2023.

Through the innovations of cyber AI, organizations can detect and enable cyber threats faster and anticipate cyber attacks in advance. Through this article, the authors explore the topic of cyber AI and its advantages in the cybersecurity field. At the beginning, the topic of cybercrime comes into effect; the articles explain the rise in cybercrimes and how much individuals and businesses have lost since the uproar of cybercrimes in 2018. They introduce the topic of AI and how AI can enable organizations not only to respond faster than attackers but also to anticipate the attacker's next moves and react in advance, which causes less threat. Through these advancements, they predict that the global market assumed growth of 19 billion U.S. dollars in the past couple of years.

Through the effect of companies, new businesses started to emerge, targeting the cyber protection field. They caused many to be able to work remotely, allowing them to not endanger their digital footprint by connecting to different vulnerable services that would be

easily hacked. However, that is not the only case; there has been a new adoption of 5G networks over the years. 5G networks, which are stronger and more protective than before.

While reading through the article, the authors take excellent account of the contribution of AI to defend against present cyber threats. The employment rate has grown by approximately 89% through the new jobs created because of AI. However, when talking about AI's contributions, through its advances, there has been an increase in threat detection, which causes a reduction in cyber attacks daily. Advanced analytics and machine learning platforms cause many advantages to our society, for instance, by analyzing and storing a high volume of data generated by security tools and being trained to distinguish between legitimate and malicious files, connections, devices, and users. AI networks can provide real-time understanding to assist and understand the expanding enterprise of the attack surface. AI and machine learning provide supply chain risk management automatic progress when monitoring the physical and digital supply chain environments and tracking how essays are composed and linked.

AI can be trained to enable a more proactive security poster and promote cyber resilience, allowing organizations to operate even when faced with attacks. Through the help of AI and machine learning, areas such as policy configuration, compliance monitoring, and threat and vulnerability detection could happen automatically without the assistance of the cybersecurity team. The article states that in a service that consists of security analysts, around 50% concluded that the most frustrating thing is how many cyber attacks they are consistently notified of and how difficult it is to prioritize the attacks because they are all important. However, with AI's help, they can control those attacks by allowing the AI to conduct a lassi and a counterattack when it comes to minor attacks and leaving the major cyber attacks to the cyber team. Although AI is efficient, it cannot replace human security professionals. Analysts are trained to function in more strategic roles that would be difficult for an AI to replace because it is not as "human."

Although AI has advantages in cybersecurity, it will grow to be dependent on cybersecurity. In the article, the author includes the evolution of table-stakes weapons against AI-driven cybercrimes. However, there is a way to move forward through AI. Isolated, manufactured knowledge will not settle the present or the impending complex security challenges. Manufactured knowledge's ability to perceive plans and adaptively advance dynamically as events warrant can accelerate acknowledgment, guideline, and response, help facilitate the strain put on SOC experts, and enable them to be more proactive. These workers will remain well-known, but PC-based knowledge will change their positions. Affiliations should reskill and retrain specialists to help change their fixation from triaging alerts and other lower-level capacities to extra fundamental, proactive activities. Finally, as the parts of manufactured consciousness and simulated intelligence-driven security risks begin to emerge, manufactured reasoning can help security bunches prepare for the conceivable improvement of PC-based knowledge-driven cybercrimes.

"Cybersecurity Trends: Looking over the Horizon." *McKinsey & Company*, McKinsey & Company, 10 Mar. 2022, www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon.

In this article, the author, McKinsey, examines three of the latest cybersecurity trends and their implications for organizations facing new and emerging cyber risks and threats. Cybersecurity has always been a never-ending race; however, through this perception of cybersecurity, many advancements in the field have emerged in the past couple of years. Through these advancements, vulnerabilities come to light, which causes us to prepare ourselves earlier. In the article, McKinsey states three cybersecurity trends with large-scale implications. The first would be on-demand access to ubiquitous data and information platforms, which is growing. By implying the ongoing growth of applications and extensive data sets that cause the marketplace to generate an increasing profit percentage for years to come. Through this increase in profit, organizations collect more customer data, causing a new understanding of purchasing behavior and allowing organizations to create a more effective forecast demand. Through these

forecasts and the creation of new products, new technology platforms, including data lakes that can aggregate information, have allowed companies to create a better business model and the gathering and centralization of data.

Recent high-profile hacks frequently took use of this increased data availability. During routine software upgrades, harmful malware was disseminated to clients in the 2020 Sunburst hack. Similarly, attackers in early 2020 gained access to more than five million visitor data using hacked staff credentials from a third-party program used by a prestigious hotel chain.

The second implication would be hacked using AI, machine learning, and other technologies to launch increasingly sophisticated attacks. Unlike in the past, stereotypical hackers who work alone are no longer the main threat; however, hackers hack multibillion-dollar enterprises using advanced tools, such as AI, machine learning, and automation. Over the next several years, the hackers can expedite the attack life cycle, from reconnaissance through exploitation. In the past couple of years, multiple countries have been the target of malware cyberattacks. Since 2019, ransomware attacks have been more frequent every year. Cryptocurrencies and ransomware as a service have significantly reduced the cost of starting an assault. Other types of disruptions usually increase these assaults. For instance, during the initial wave of COVID-19, which occurred between February 2020 and March 2020, the number of ransomware attacks climbed globally by 148%. Phishing attacks increased by 510 percent in February 2020 compared to January.

Lastly, McKinsey discussed the implication of an ever-growing regulatory landscape and continued gaps in resources, knowledge, and talent that will space cybersecurity. In many businesses, there needs to be cybersecurity skills, knowledge, and competence. Most firms need to know how to identify and mitigate digital risks since digital and analytics revolutions have generally lagged behind improvements in cyber risk management. The issue is complicated by regulators' more significant control over company cybersecurity capabilities, which is frequently done with the same level of scrutiny and focus as operational and physical security

issues in critical infrastructure and credit and liquidity problems in the financial services sector. At the end of the article, Mckensey explains how we can move forward with the information she has provided and the necessary things to think about soon.

Engstler, Michael. "Council Post: The Cyber Digital Twin Revolution." *Forbes*, Forbes Magazine, 24 Feb. 2021, www.forbes.com/sites/forbestechcouncil/2021/02/25/the-cyber-digital-twin-revolution/?sh=58dd827e24f2.

In the article, Michel Enfstler, a former Forbes council member, discusses the new information they have concluded through research and an interview with Cybellum CTO and Co-founder over the digital twin revolution in cybersecurity. In the last couple of years, different machines around us have wrapped up more adroitly than we are. Advancement and improvement hold up for no one, and the broad allocation of IoT has saturated brilliantly, free capabilities into everything from passing on machines and robots to ice chests and cars.A see underneath the hood reveals that this IoT advancement is fueled by CPUs, computer programs, and web organizers that drive the decision-making and execution of our quick machines. In reality, the preeminent progressed sharp machines, or like the first afterward related cars, can send over 100 specific program components and, as frequently as conceivable, have more lines of code than an F-35 warrior fly.

Shockingly, this bit of information comes with its dangers. Malevolent computer program engineers are calmly and unfalteringly analyzing and dismembering our intelligent machines' specific computer program components. Their reason? To discover vulnerabilities through which they can enter the inside framework and capture delicate information for cash-related select-up, or more appalling.Cybersecurity experts are leveraging the most recent troublesome mechanical patterns and inventive advanced concepts to remain one step ahead of programmers and ensure that we stay secure and secure. Named one of Gartner's "Top 10 Vital Innovation Patterns for 2019," computerized twins are one such case. These virtual bridges interface the physical and computerized

universes by advertising point-by-point representations of complex, real-world frameworks. The benefits of their utilization enable modern, speedier capabilities within the examination, efficiency, generation, conveyance, and more.

Within cybersecurity, digital twins energize unused conceivable outcomes over the whole esteem chain. Suitably named cyber computerized twins, their utilization is expanding unused scales of efficiencies in everything from inquiry about, advancement, testing, and investigation to IP assurance and seller administration.

Cyber digital twins can create a digital version of any natural object online. This computerized copy is used to pretend fake cyberattacks, find vulnerabilities, and study potential risks before creating the device. We must first utilize digital twins to address cybersecurity threats and protect against weaknesses adequately. These digital copies help us understand how software works and give power to our physical products. These mirrors display critical information that cybersecurity experts need to keep our intelligent machines safe.

Cyber digital twins are created by studying the software. Firmware is software inside a device that controls how the device operates. The analysis details the device's physical properties, like its hardware and operating system. It also tells us how the device uses memory and how the software was introduced. This new method speeds up cybersecurity and research while safeguarding the supplier's valuable intellectual property.

Even the most basic intelligent machines are manufactured using several different software components, each provided by a different company. Every seller makes their own software using different computers, instructions, tools, and other parts. Learning and acquiring the necessary tools to analyze and safeguard every system component can be difficult and costly. Cyber digital twins make it easier for security experts to examine firmware by giving them clear and detailed copies. These versions can be used with different tools to find weaknesses, study new dangers, and find privacy problems. Software developers must ensure that the code

inside their software components is secure. However, companies still have to be able to use the firmware code for security, testing, following rules, and other reasons.

With cyber digital twins, vendors do not have to give out the actual firmware with their essential intellectual property. Instead, they can use the cyber digital twin, which contains all the essential information cybersecurity experts need for their analysis. This means that vendors can share important information about their products without worrying that someone will steal their ideas. This new way of doing things allows for more openness and clarity in making and delivering things. The safety and compliance of all software components in our intelligent machines are thoroughly evaluated and scrutinized. As stated earlier, it is not easy because each supplier uses many different types of technology. Doing the necessary research and assessment requires experts who understand all the different technologies, configurations, and versions being used. This means that if more components are being used, more researchers will need to conduct the necessary research and assessments.

Cyber Digital twins help researchers with challenging tasks. Instead of wasting valuable and costly time examining the binary code to find the necessary information, researchers can concentrate on conducting their tests and evaluations. This way, cyber digital twins make it easier to do research and assessments and save time because users do not need to be cybersecurity experts.

This article explains how important it is to have proper protection for user's intellectual property (IP), to standardize and harmonize your cybersecurity measures, and to have efficient research and assessment processes. These benefits ensure that the user's entire operation is safeguarded against cybersecurity threats. They deal with many essential security problems throughout manufacturing while making products faster and cheaper.

When users assess a cyber digital twin solution, ensure users know how it works with their current systems and procedures and how it can meet compliance standards and regulations. The centralized approach and visibility it provides make vulnerability management more efficient and optimized, making integrating with users' systems and tools more accessible.