New Jersey Institute of Technology

ENGL 102 Introduction to Research Writing

Analyzing Data Breaches: Impact on Financial Performance and the Role of AI-Driven Prevention

Dennis Perdomo

Analyzing Data Breaches

Impact on Financial Performance and the Role of AI-Driven Prevention

Table of Contents

Abstract

The number of cyber breaches keeps consistently increasing year over year. Standard cybersecurity policies must be reviewed and reworked with new technologies and innovative methods to adapt to the modern era. Artificial intelligence and machine learning have become a cybersecurity standard among industry leaders, yet untapped potential exists. By further evolving AI and ML through experimental methods such as deep learning, cybersecurity can develop from primarily reactive to predictive, tracking down threats before they happen. Two exciting applications of AI and ML in cybersecurity are Deep Reinforcement Learning and honeypots. Both have great potential in defending sensitive data in real-world situations, surpassing the current cybersecurity models widely used by companies and organizations. If properly optimized, AI and ML can be the tools needed to spearhead a new era of data security.

Introduction

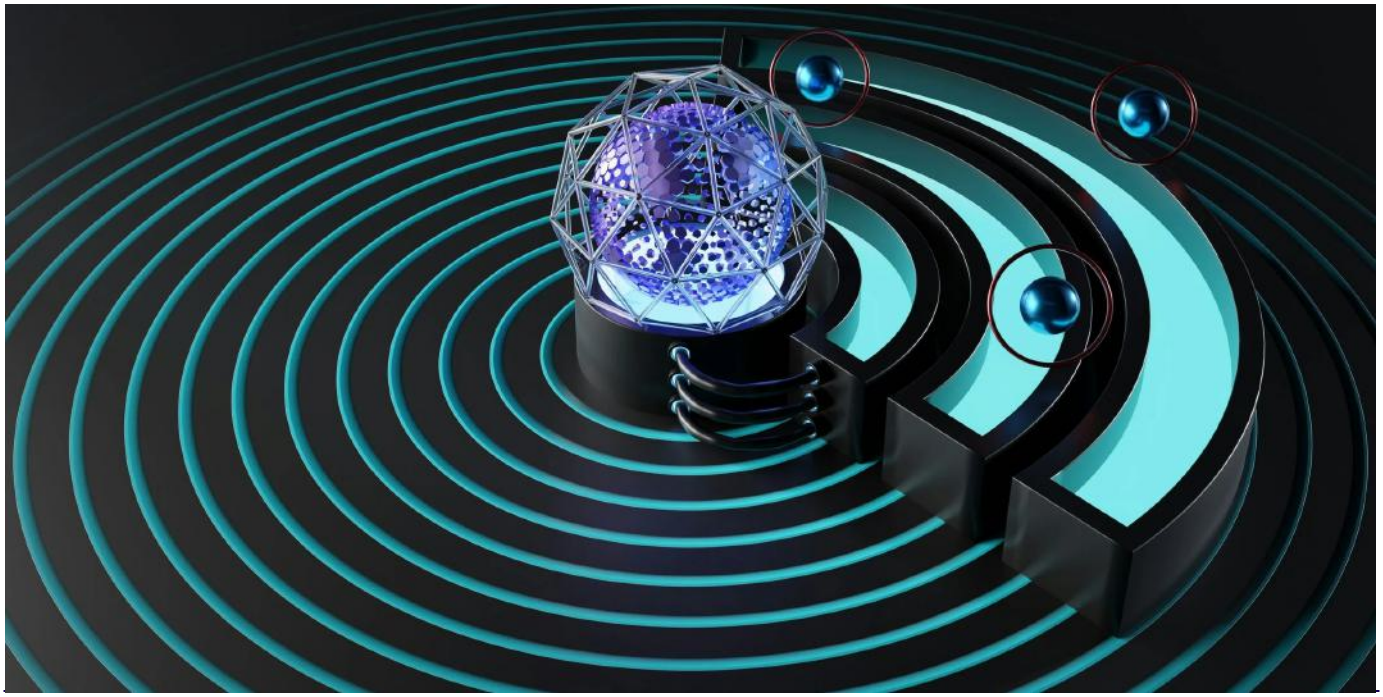
Privacy and data have become increasingly important in the ever-evolving technological modern era. As consumers realize the importance of their data, they become more cautious of their information and how companies, governments, and other entities protect it. Therefore, prominent institutions have shifted their attention to cybersecurity, pouring billions of dollars into protecting their data.

However, despite the increased protection, devastating data breaches have plagued the past decade. Cyberattackers are constantly innovating new techniques to break through even the most fortified cyber defenses, using technological advancements to their advantage.

These data breaches can lead to financial losses, reputational damage, legal implications, and potential harm to victims, and they have only increased in recent years. Over the last decade, the number, frequency, and severity of these breaches have increased.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as new technologies for combating data breaches. By using AI and ML defence strategies, cybersecurity policies can turn from reactive to proactive, seeking out dangers before they happen. This revolutionary technology is the step forward needed to combat the rise in cyber breaches.

Organizations can keep their data secure by using new and experimental AI- and ML-powered cybersecurity methods, saving billions and keeping their reputation intact.



Cyber Breaches: An Ever-growing Threat

Cyber breaches become more common, advanced, and potent every year. Criminals have taken advantage of digitization, using new methods to gain an advantage over vulnerable companies, organizations, and individuals for personal benefit.

According to IT Governance, 2023 saw a staggering 8,214,886,660 records breached, endangering the privacy of people's data, leading to significant loss of privacy for organizations and civilians alike (IT Governance, 2024). Large-scale cyber breaches, like the recent Russian cyberattacks on Ukrainian state registers in 2024, can lead to fearmongering and panic, making cybersecurity necessary to prevent psychological warfare (Kramarenk & Dmytriieva, 2024).

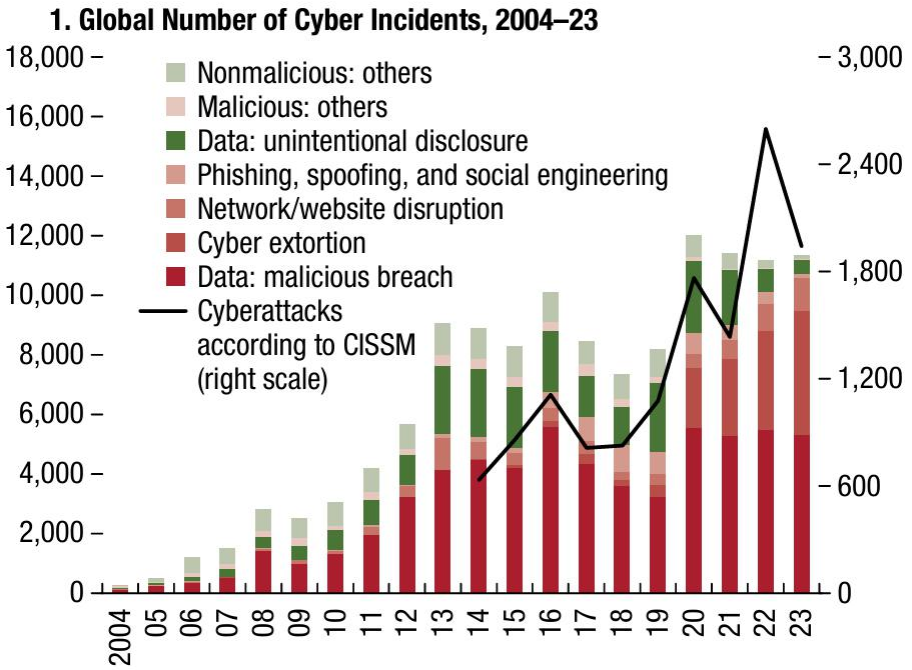
The rise in cyber breaches is due to the exploitation of vendor systems, cloud misconfiguration, and the development of advanced ransomware attacks (Madnick, 2024). Additionally, the rise of AI-powered cyber schemes, such as advanced AI-phishing scams, has significantly impacted cybersecurity. To warn unsuspecting individuals of new hacking techniques, FBI Special Agent in Charge Robert Tripp spoke at a conference, warning the public:

> " As technology continues to evolve, so do cybercriminals' tactics. Attackers are leveraging AI to craft highly convincing voice or video messages and emails to enable fraud schemes against individuals and businesses alike." (FBI, 2024).

Despite companies' best efforts and the increased implementation of AI and ML in cybersecurity, cyber breaches remain a consistently growing hazard.

Since 2004, cyber incidents have only increased year over year. The International Monetary Fund (IMF) reports that "the number of cyberattacks has almost doubled since before the COVID-19 pandemic" (IMF, pg.97, 2024). The statistic demonstrates a worrying trend of malicious cyber breaches becoming more potent and frequent at an alarming rate, as shown by Figure 1.

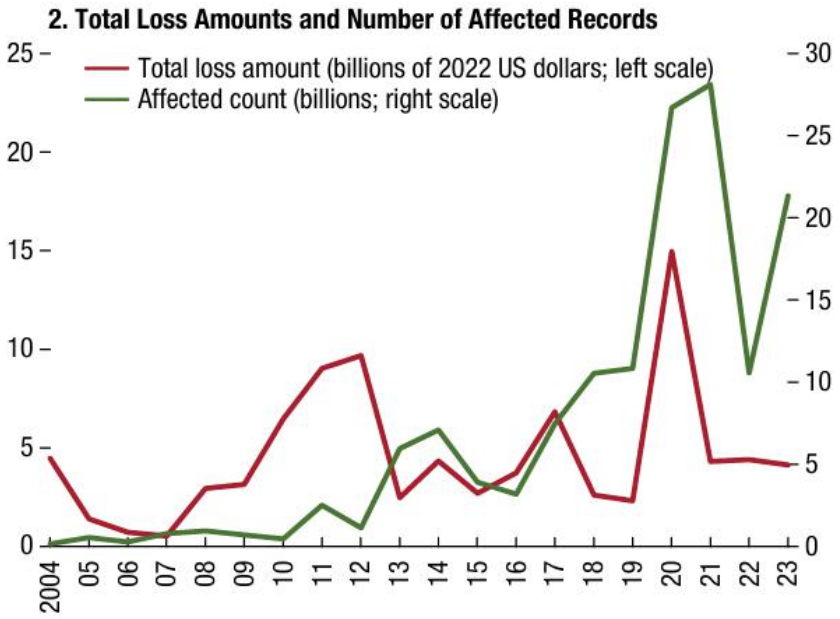
Figure 1



(IMF, pg. 98, 2024)

Financial Impact

Figure 2



(IMF, pg. 98, 2024)

As the sheer volume of reported cyber attacks has risen, so have the reported losses due to cybersecurity-related issues. Companies report widespread losses as significant figures succumb to the rise in cyber attacks. As the numbers continue to grow, it is essential to look at both cyberattacks' short-term and long-term effects.

Billions of dollars lost in market cap

Figure 2 highlights the financial destruction of cyber breaches. Each year, companies lose billions of dollars due to cyber attacks, numbers likely to rise without formulating a proper cybersecurity policy that implements modern technology.

Cyber incidents are especially harmful in the short term, where they can lead to a troubling ripple effect in the company. The Harvard Business Review reported that "publicly traded companies suffered an average decline of 7.5% in their stock values after a data breach, coupled with a mean market cap loss of $5.4 billion"(Huang et al., 2023).

In addition to the losses (which can take up to 46 days to recover, if at all), a single breach can amount to 26 times the financial damage of the breach in ripple effects (Help Net Security 2021). One such incident was the SolarWinds incident, where hackers breached U.S. government agencies via compromised SolarWinds Orion software (Zorz, 2020).

Long-term effects are emerging

According to IBM, the global average data breach cost in 2022 reached $4.35 million. Within the United States, the number doubled, as the U.S. averaged $9.44 million (Huang et al., 2023). These costs include ransomware payments, lost revenues, and audit fees. The healthcare sector, for example, lost $1.9 million daily due to ransomware attacks, totaling $7.8 billion in 2021 (Bischoff, 2024).

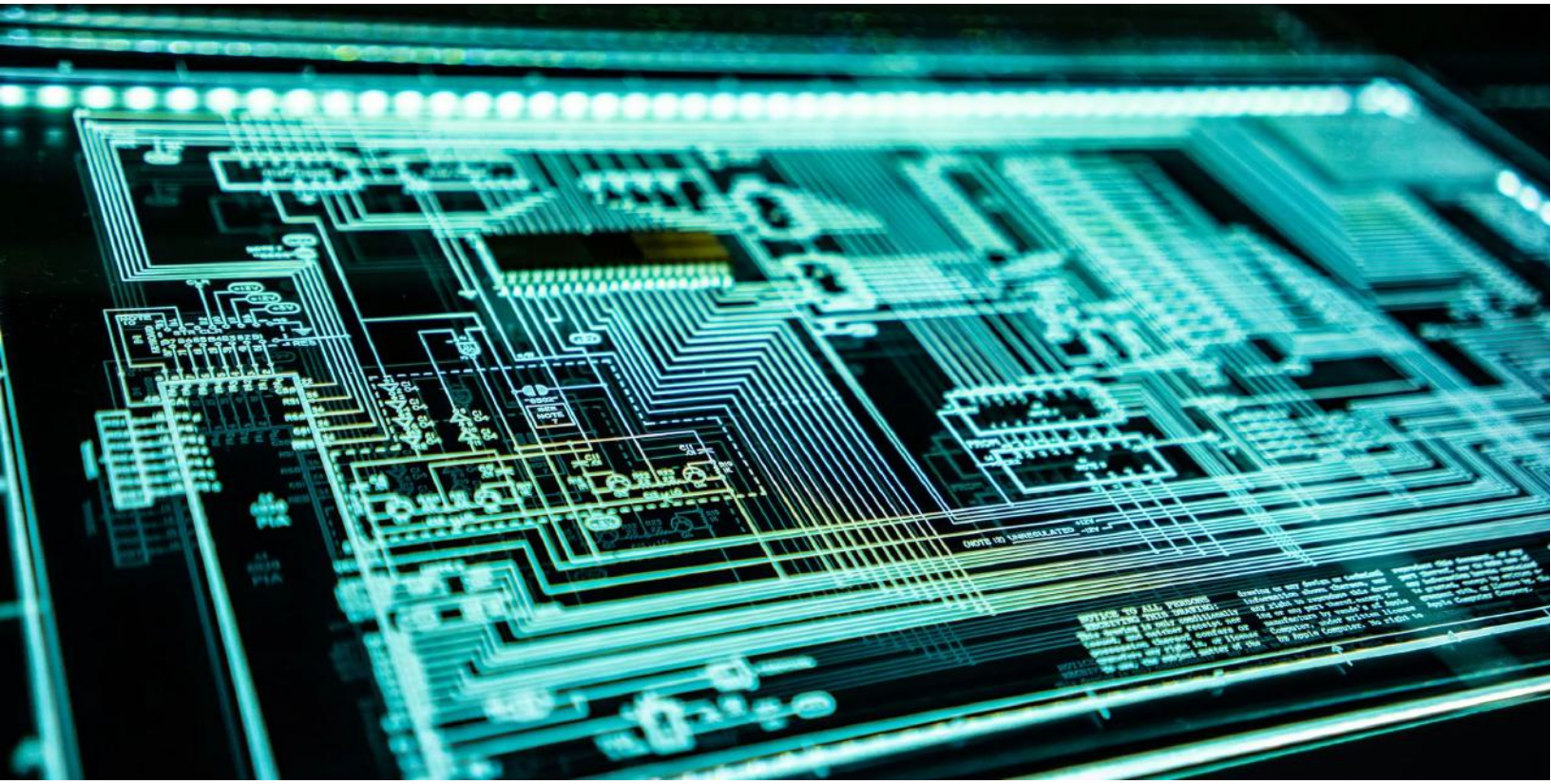
These costs impact not only companies but also consumers. 60% of organizations raised their prices after experiencing a cyber breach, damaging a company's market position (Kaplan, 2025).

The bleak reality is that companies and organizations are losing the cybersecurity battle, and more importantly, the AI and ML battle.

Hackers have elevated their skills and are using experimental techniques with grave consequences, whether the consequences are loss of privacy, billions of dollars down the drain, or foreign forces spreading panic.

Corporations need to implement AI and ML further in cybersecurity, transforming their approach to cyberattacks from reactive to proactive.

Winning the Digital Arms Race



Cybersecurity in the modern age

Artificial intelligence and machine learning have already had a revolutionary impact on cybersecurity in a short period. Industry leaders rely on innovations such as deep learning, a machine learning section miming the human brain's complex decision-making power using multilayered neural networks.

One key application of deep learning models is high-performing intrusion detection and protection systems (IDS/IPS), which allow these systems to detect malicious threats through pattern recognition of other similar cyber attacks. The immediate detection is incredibly resourceful in preventing attacks.

However, despite technological advancements, the number of attacks and damage caused consistently rises. Cybersecurity professionals and hackers are in a "digital arms race," where both sides are battling to use artificial intelligence and machine learning to best each other. The logical step is to continue with the progress.

Deep Reinforcement Learning

One promising advanced method of AI in cybersecurity is deep reinforcement learning (DRL). In DRL, deep learning allows the DRL model to process raw data at a high capacity. DRL is quickly emerging at the forefront of AI-driven cybersecurity.

Deep-Q-Network (DQN) is a model-free DRL approach that uses the Bellman Equation. When tested against other DRL models, such as Proximal Policy Optimization (PPO), Advantage Actor-Critic Approach (A2C), and Asynchronous Advantage Actor-Critic Approach (A3C), DQN was the most successful in preventing an attack in an OpenAI Gym simulation.

When faced against three attack profiles (Av1, Av2, Av3, with Av1 being the least skillful and least persistent and Av3 being the most skillful and most persistent), DQN was successful in preventing attacks in 79.6%, 82%, and 57.3% of the cases, respectively, while achieving corresponding defense success rates of 93.3%, 95%, and 84.1% (Dutta et al., 2023). None of the other DRL models came close to matching DQN's efficiency.

The experiments suggest that model-free DRL algorithms can yield positive defence outcomes and combat cyber threats. While still a very experimental method, DRLs can predict threats before they occur and prevent them by training against threats. The advanced threat detection is possible because the DRL can process complex functions (like Q-values) and adapt to up-and-coming threats.

“Deep learning outshines any deny list, heuristic-based, or standard machine learning approach.
The time it takes for a deep learning-based approach to detect a specific threat is much quicker than any of those elements combined.”

- Mirel Sehic, vice president general manager for Honeywell Building Technologies (MIT, 2023)

Honeypots

In cybersecurity, honeypots are decoy systems that simulate weaknesses to bait attackers and lure them away from sensitive data. By observing threats, cyber professionals can analyze and learn from attacks while the information is heavily protected.

One fascinating development in the honeypot field is AI-driven honeycombs powered by large language models (LLMs). These AI models can process large datasets, recognize patterns, and generate human-like responses. Recent developments have only strengthened these models, making them more effective.

Meta has developed its LLM-powered honeycomb, the LLaMA-3 model. The LLaMA-3 model has proven capable of demonstrating high realism and deceiving sophisticated attackers. Compared to its competition, such as GPT-4, LLaMA-3 proved more resource efficient, cost-effective, and modern while still producing highly accurate and relevant responses when creating realistic interactions in honeypot systems (Chrisli, 2024).

While still an emerging field, honeycombs that use LLMs have the potential to be incredibly resourceful, providing more human-like responses than traditional static honeypots, and using AI and ML to interpret and respond to threats more efficiently.

Limitations

While higher-powered AI and ML approaches to cybersecurity remain exciting and dynamic prospects, more time is needed to perfect and properly use these techniques. Moving forward with caution and nuance is crucial, as failure to do so could result in more problems when protecting data.

DRLs need more time to optimize efficient and secure defense against cyber threats. While DRLs provide a step forward in autonomous cybersecurity, researchers worry about the vulnerability of DRL systems, as research acknowledges that "adversarial attacks can manipulate the learning process, leading to compromised decision-making by the agents" (Tolba et al., 2024).

Researchers have also voiced their concern about scalability issues. The DRL's ability to coordinate many agents in real time, especially in dynamic and complex networks, is a primary challenge that must be overcome to ensure efficient security (Tolba et al., 2024). Effective communication protocols are needed to overcome such challenges.

Likewise, honeypots must be examined and carefully developed to ensure they can handle real-world threats. The LLaMA-3 model, for instance, is a forerunner amongst other honeypot systems yet faces its challenges. Key challenges are the lack of persistent memory, issues with emulating accurate commands, and limited dynamic response generation (Chrisli, 2024). These limitations could lead to a lack of realism when creating the honeycomb trap, defeating its intent.

While these limitations worry developers, they will use recent technological developments to become more efficient and secure. The upside potential of these systems far surpasses modern techniques. If given the proper development and research, AI—and ML-powered cybersecurity systems can be the key to a safer, secure future.

Conclusion

As technology progresses, digital threats intensify, becoming too much for current security policies to manage. Too much is at stake to leave in the hands of cybercriminals. Hackers are using new methods as network usage is at an all-time high. New attack patterns are proving to be too much for standard security regulations. Companies are losing billions daily, individuals are losing their privacy, and citizens are losing their peace. AI- and ML-driven procedures, such as Deep Reinforcement Learning and honeypots, provide a secure, cost-effective method more suited to face off against cyber attacks, turning the focus from reactive to proactive, shutting down threats before they happen. Cyber professionals and hackers are in an AI arms race, as the increased usage of AI and ML offers new possibilities, with intricate benefits and consequences that demand nuance and development. More than ever, cybersecurity needs to implement AI and ML to protect invaluable information against increasingly dangerous and unpredictable threats.

References

Bischoff, P. (2024, December 18). Ransomware attacks on US healthcare organizations cost $20.8Bn. Comparitech. https://www.comparitech.com/studies/ransomware-studies/ransomware-attacks-hospitals-data/

J. A. Christli, C. Lim and Y. Andrew, "AI-Enhanced Honeypots: Leveraging LLM for Adaptive Cybersecurity Responses," 2024 16th International Conference on Information Technology and Electrical Engineering (ICITEE), Bali, Indonesia, 2024, doi: 10.1109/ICITEE62483.2024.10808265.

Dutta, A., Chatterjee, S., Bhattacharya, A., & Halappanavar, M. (2023, February 3). Deep reinforcement learning for cyber system defense under dynamic adversarial uncertainties. arXiv.org. https://arxiv.org/abs/2302.01595

FBI. (2024, May 8). FBI warns of increasing threat of cyber criminals utilizing Artificial Intelligence. FBI. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

Holdsworth, J., & Scappichio, M. (2024, December 19). What is deep learning?. IBM. https://www.ibm.com/think/topics/deep-learning

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023, May 4). The devastating business impacts of a cyber breach. Harvard Business Review. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

IMF. (2024). Global financial stability report. International Monetary Fund.

Kaplan, C. (2025, February 11). Summarizing the PONEMON cost of a data breach report 2022. HALOCK. https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/

Kramarenko, D., & Dmytriieva, D. (2024, December 20). Ukraine suffers largest cyberattack since 2022: Russian Hackers Disrupt Key Services. RBC. https://newsukraine.rbc.ua/news/ukraine-suffers-largest-cyberattack-since-1734704699.html

List of data breaches and cyber attacks in 2023 – 8,214,886,660 records breached. IT Governance Blog. (2024, July 12). https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

Madnick, S. (2024, February 19). Why data breaches spiked in 2023. Harvard Business Review. https://hbr.org/2024/02/why-data-breaches-spiked-in-2023

MIT Technology Review. (2023, September 15). Deep Learning delivers proactive cyber defense. MIT Technology Review. https://www.technologyreview.com/2022/07/20/1056140/deep-learning-delivers-proactive-cyber-defense/

A multi-party data breach creates 26x the financial damage of single-party breach. Help Net Security. (2021, September 23). https://www.helpnetsecurity.com/2021/09/27/multi-party-data-breach/

Tolba, Z., Dehimi, N. E. H., Galland, S., Boukelloul, S., & Guassmi, D. (2024). Multi-Agent Deep Reinforcement Learning Applications in Cybersecurity: challenges and perspectives. https://ieeexplore.ieee.org/Xplore/home.jsp

Zorz, Z. (2023, November 14). Hackers breached U.S. government agencies via compromised SolarWinds Orion software. Help Net Security. https://www.helpnetsecurity.com/2020/12/14/compromised-solarwinds-orion/