e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712154

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The Evaluation and Role of AI in Combining Cybersecurity Threats

Himanshu Sisodiya, Dr.Bajrang Yadav

BBA Student, NIMS Institute of Business Studies, NIMS University, Jaipur, Rajasthan, India

NIMS Institute of Business Studies, NIMS University, Jaipur, Rajasthan, India

ABSTRACT: In today's digital-first world, cybersecurity has become a critical priority across all sectors. This paper examines the evolving nature of cyber threats, with a focus on recent high-profile attacks to identify vulnerabilities in current security systems. It also explores the future trajectory of cybersecurity, highlighting emerging threats and the technological innovations needed to address them.

The study further investigates the growing role of Artificial Intelligence (AI) in enhancing cybersecurity efforts. AI's ability to detect complex patterns, automate responses, and offer valuable insights has strengthened the ability of security professionals to counter sophisticated cyber threats. However, the increasing use of AI also presents risks, as cybercriminals leverage these technologies for malicious activities.

The paper concludes that the combination of AI-driven solutions, advanced security technologies, and proactive organizational strategies is crucial to safeguarding digital assets. A collaborative, forward- thinking approach will be essential in ensuring robust protection against future cyber risks.

I. INTRODUCTION

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

Cyber threats also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

II. KEY CHALLENGES

The future of cybersecurity is notoriously hard×to predict. After all, every aspect of the ψindustry changes continuously. Cyber threats evolve and the tools that defend against them mirror those changes, evolving in their own right to better defend increasingly complex networks.

The future of cybersecurity is notoriously hard to predict. After all, every aspect of the industry changes continuously. Cyber threats evolve and the tools ~~that de~~fend against them mirror those changes, evolving in their own right to better defend increasingly complex networks.

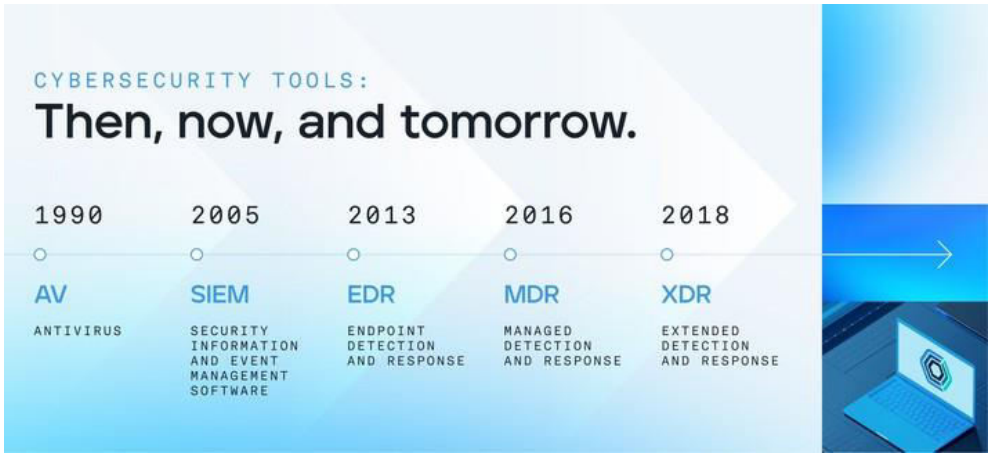
The evolution, at least as far as tools go, looks a bit like this:

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712154

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Cyber threats that'll remain an issue

Certain cyberattack tactics are bound to stick around—and that's because they've proven to work. As such, these are the threats that our experts believe still pose a serious cybersecurity risk.

Ransomware

III. ADDRESS INNOVATION (ROLE OF AI)

The Role of AI in Cybersecurity

Artificial Intelligence (AI) has proven to be a crucial asset in tackling cybersecurity concerns, offering the development of Intelligent Agents to address specific security challenges effectively.

How Does AI in cyber security assist security professionals?

AI in cybersecurity assists security professionals by recognizing complex data patterns, providing actionable recommendations, and enabling autonomous mitigation. It enhances threat detection, supports decision-making, and speeds up incident response

How cybersecurity benefits from ai

A self-learning AI-based cybersecurity posture management system proves indispensable in overcoming these challenges. By continuously and autonomously collecting data from an organization's information systems, this system can analyze and correlate patterns across millions or billions of signals relevant to the enterprise's attack surface

This innovative approach provides enhanced intelligence to human teams across various cybersecurity domains, including:

IT Asset Inventory: Achieving a comprehensive and accurate inventory of all devices, users, and applications with access to information systems while categorizing and assessing business criticality.

Threat Exposure: Staying up to date with global and industry-specific threats, empowering organizations to prioritize security measures based on likelihood and potential impact.

Controls Effectiveness: Assessing the impact and efficacy of existing security tools and processes to strengthen security posture.

Breach Risk Prediction: Predicting vulnerability and potential breaches by considering IT asset inventory, threat exposure, and control effectiveness, enabling proactive resource allocation for mitigation.

Incident Response: Providing contextual insights to prioritize and respond swiftly to security alerts, identify root

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

causes, and improve incident management processes.

Transparent solutions: Ensuring that AI recommendations and analyses are transparent and understandable, fostering collaboration and support from stakeholders at all levels of the organization, including end users, security operations, management, and auditors. By harnessing the power

IV. WRAP-UP (LESSIONS FROM RECENT ATTACKS)

Recent high profile attack
June 2023: A Pakistani-based hacker group infiltrated the Indian army and education sector in the group's latest wave of attacks against Indian government institutions.The hack is the latest in a series of targeted attacks from this group that have intensified over the past year.

December 2023: Russian hackers hit Ukraine's largest mobile phone provider, Kyivstar, disabling access to its 24 million customers in Ukraine. Hackers claim to have destroyed more than 10,000 computers and 4,000 servers, including cloud storage and backup systems. The attack began hours before President Zelenskyy met with President Biden in Washington D.C.

December 2023: Ukraine's military intelligence service (the GRU) claims to have disabled Russia's tax service in a cyberattack. According to the GRU, the attack destroyed the system's configuration files, databases, and their backups, paralyzing Russia's tax service.

November 2023: Suspected Chinese hackers launched an espionage campaign against Uzbekistan and the Republic of Korea. Hackers use phishing campaigns to gain access to their target's systems and decrypt their information.

November 2023: Chinese hackers compromised Philippine government networks.
Beginning in August 2023, hackers used phishing emails to imbed malicious code into their target's systems to establish command-and-control and spy on their target's activities.

November 2023: Trinidad and Tobago's Prime Minister Dr. Keith Rowley declared the latest ransomware attack against the country's telecommunications service to be a "national security threat." Hackers stole an estimated six gigabytes of data, including email addresses, national ID numbers, and phone numbers.

November 2023: Denmark suffered its largest cyberattack on record when Russian hackers hit twenty-two Danish power companies. The attack began in May 2023 and appeared to be aimed at gaining comprehensive access to Denmark's decentralized power grid. Hackers exploited a critical command injection flaw and continued to exploit unpatched systems to maintain access

V. CONCLUSION

Cybersecurity is no longer an optional investment; it is a fundamental necessity for organizations, governments, and individuals. As cyber threats continue to evolve in sophistication, the future of cybersecurity remains unpredictable, requiring constant adaptation and vigilance. Recent high-profile attacks, such as the June 2023 infiltration of Indian institutions by a Pakistani-based hacker group, serve as a stark reminder of the critical need for robust defense mechanisms.

Artificial Intelligence (AI) has emerged as a powerful ally in this battle, enabling faster threat detection, autonomous mitigation, and better decision-making capabilities for security professionals. However, AI itself can also be weaponized, necessitating balanced and ethical implementation.

The path forward requires a blend of innovative technologies, skilled professionals, and strong international

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

cooperation. By prioritizing proactive defense strategies and fostering a culture of awareness, we can build a safer and more secure digital ecosystem for the future.

REFERENCES

1. Upguard. (n.d.). How to Perform a Cybersecurity Risk Assessment. Upguard. Retrieved from https://www.upguard.com/blog/how-to- perform-a-cybersecurity-risk-assessment
2. Field Effect. (n.d.). What Is the Future of Cyber Security? Field Effect. Retrieved from https://fieldeffect.com/blog/what-is-the-future-of- cyber-security
3. ECCU. (n.d.). The Role of AI in Cyber Security. ECCU. Retrieved from https://www.eccu.edu/blog/technology/the-role-of-ai-in-cyber- security/
4. CSIS. (2023, December). Significant Cyber Incidents. Center for Strategic and International Studies. Retrieved from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents#:~:text=December%202023%3A%20Russian%20hackers%20hit,cloud%20storage%20and%20backup%20systems

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com