PROGRAMS THAT IDENTIFY BASIC ATTACKS ON ARTIFICIAL INTELLIGENCE

Ismoilov Sirojiddin Rasuljon o'g'li

Student of Tashkent University of Information Technologies Fergana branch

Murodullayeva Rayhona Abdurahmon qizi

Student of Tashkent University of Information Technologies Fergana branch

Shamamatova Sayyora Jo'raboy qizi

Student of Tashkent University of Information Technologies Fergana branch

Abduraximov Ozodbek Azimjon o'g'li

Student of Tashkent University of Information Technologies Fergana branch

Abstract: The article mainly discusses the systems and programs that detect network attacks based on artificial intelligence, their advantages over each other, and several software tools. At the same time, more attention was paid to the Darktrace program. The origin and importance of this program in organizations, as well as three main advantages, were highlighted.

Keywords: NIDS, Darktrace, McAfee Advanced Threat Defense (ATD), Palo Alto Networks Cortex XDR, Cisco Security and Automation (CSA), CrowdStrike Falcon XDR, cyber security, network traffic, anomalies.

AI-based network intrusion detection systems (NIDS) are a powerful tool to protect your network from cyber attacks. AI-based network intrusion detection systems are security systems that use artificial intelligence (AI), specifically machine learning (ML) and deep learning (DL), to analyze network traffic and detect malicious activity. Unlike traditional NIDS that rely on predefined attack signatures, AI-based NIDS can detect previously unseen anomalies and new threats.

Main part

Below we look at some examples of AI-based network intrusion detection software.

Darktrace: This AI cybersecurity company uses a form of unsupervised machine learning called anomaly detection to identify threats. Their system studies typical patterns of network traffic and then flags anything that deviates from those patterns as suspicious.

McAfee Advanced Threat Defense (ATD): This suite of security products includes Network Intrusion Detection and Prevention System (NIDPS), which uses machine learning to detect and block known and unknown threats.

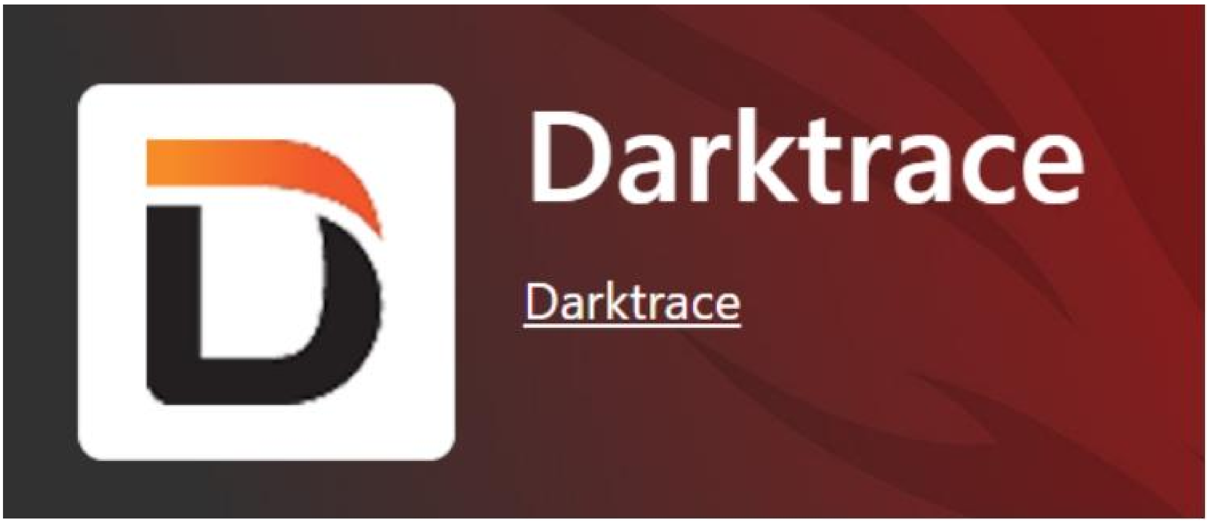
Palo Alto Networks Cortex XDR: This advanced detection and response (XDR) platform uses machine learning to analyze data from a variety of sources, including network traffic, endpoints, and cloud workloads. This allows it to detect and investigate threats more effectively.

Cisco Security and Automation (CSA): This platform includes a machine learning-based NIDS that can detect a wide range of threats, including zero-day attacks and malware.

CrowdStrike Falcon XDR: This XDR platform uses machine learning to correlate data from various sources to identify and investigate threats. It also includes endpoint protection and detection and response (EDR) capabilities.

It is no exaggeration to say that Darktace, which is one of the programs that are widely used today, especially in the field of business and finance, is noteworthy.

Darktrace is a cybersecurity solution that helps businesses prevent real-time cyber attacks, including ransomware and email phishing. This enables IT professionals to ensure security against threats to cloud environments and critical infrastructure, and to detect new or insider threats arising from malicious behavior. The application provides organizations with enterprise network security through machine learning technology and network traffic analysis (NTA) system. Professionals can use the app to prevent cyber disruptions without affecting regular business operations. Darktrace offers many features such as behavioral analysis, endpoint management, threat response, vulnerability scanning, whitelisting or blacklisting, and more. Darktrace Cyber AI Loop helps users reduce risk and enhance security. The Darktrace Cyber AI Loop is built on continuous feedback and an interconnected understanding of the enterprise. Darktrace tracks and protects people and digital assets in the IT ecosystem. Self-Learning AI learns simple life patterns to detect inappropriate and malicious behavior. This includes insider threats, industrial espionage, IoT compromises, zero-day malware, data loss, supply chain risks, and long-term infrastructure vulnerabilities.



The rise of the digital age has given way to the development of smarter, faster and more innovative technologies that have changed the way companies do business. But as technology advances, so do the threats businesses face. In 2013, Darktrace, an AI-powered cybersecurity software, emerged as a solution for businesses managing a rapidly evolving, complex threat landscape as they seek to digitize. Darktrace has a powerful software stack powered by self-learning artificial intelligence, enabling organizations to detect, investigate and respond to cyber threats in real-time, wherever they are will give.

The technology behind Darktrace was envisioned by a group of mathematicians and intelligence experts at the University of Cambridge as a new way to combat the rise of rapidly evolving cyber security threats. Among them were former CIA director of information Alan Wade and former head of MI5, Lord Evans of Weardale KCB. On April 30, 2021, just 8 years after its founding, the company launched its IPO on the London Stock Exchange at a valuation of $2.37 billion. In the years since its inception, Darktrace has quickly become a leading global player in AI cybersecurity, trusted by over 7,400 organizations in over 100 countries. The company was also named "Security Company of the Year" at the 2016 Info Security Global Excellence Awards. received a number of awards in the nomination and was recognized by Fast Company as one of the most innovative companies in the field of artificial intelligence in 2022.

3 key differentiators that set Darktrace apart:

Autonomous and automatic. Unlike most traditional security solutions that require people to manually identify signatures and constantly update them, Darktrace requires no human intervention. Instead, software learns from existing patterns to detect and respond to anomalies before disruptions occur.

A proactive approach. Most current cybersecurity defenses, such as patch management, log monitoring, and SIEM, are reactive, meaning they focus primarily on responding to incidents and preventing future attacks. provides an "always on" approach to cyber security that prioritizes prevention in order to improve human skills to protect organizations from potential threats before they arrive.

Speed and scalability. With Darktrace, threat testing is automated at speed and scale, reducing testing time by 92%. In addition, Darktrace software is designed to seamlessly integrate with existing security infrastructure, is compatible with all major cloud providers (including AWS, Google Cloud Platform, and Microsoft Azure), and spans up to 1 million devices.

REFERENCES:

1. Umaraliyev, J., Abdurakhimov, O., & Isokjonova, S. (2023, June). USE AND EFFECTIVENESS OF INFORMATION TECHNOLOGIES IN MEDICINE. In Academic International Conference on Multi-Disciplinary Studies and Education (Vol. 1, No. 11, pp. 148-151).
2. Umaraliyev, J., Turdaliyev, K., Isoqjonova, S., & Abdurakhimov, O. (2023). ITS APPLICATIONS AND PROSPECTS IN EDUCATION. Interpretation and Researches, 1(11). search the horse
3. O Abduraximov, A Tojidinov, U Nazirjonov. IDENTIFICATION AND AUTHENTICATION IN INFORMATION SECURITY. NETWORK DISPLAY TECHNOLOGY. Академические исследования в современной науке, 2023. (Vol. 2, No. 21, pp. 26-32).
4. AO Azimjon o'g'li, TA Ilhomjon o'g'li . NETWORK OPERATING SYSTEMS. XALQARO ANIQ FANLAR TAHLILI, 2023. (Vol. 1, No. 2, pp. 51-54).
5. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li.

AVTOTRANSPORT VOSITALARINI KIBERHUJUMLARDAN HIMOYA QILISH BO ‘YICHA YO ‘L XARITASI . Новости образования: исследование в XXI веке, 2023. (Vol. 2, No. 13, pp. 70-74).

6. Ilhomjon, T. K., Azimjon, A. O., & Nazimjon, N. U. (2023). CLOUD TECHNOLOGIES AND CLOUD COMPUTING. JOURNAL OF SCIENCE, RESEARCH AND TEACHING, 2(8), 79-81.
7. Ilhomjon o'g'li, T. A., & Azimjon o'g'li, A. O. (2023). ANDROID XAVFSIZLIGI, XAVSLIK TIZIMLARINI YAXSHILASH. PEDAGOG, 6(6), 753-757.

8. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Information and Communication Technologies in Education LMS Systems. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 28-31).

9. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li . Lms Systems and Their Description. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 22-24).

10. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Education to Give in Processes Information and Communication Technologies. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 18-21).

11. TA Ilhomjon o'g'li, NU Nozimjon o'g'li, AO Azimjon o'g'li. Grid Analysis and Design. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 25-27).

12. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li . Информационные И Коммуникационные Технологии В Образовании LMS Системы. American Journal of Science on Integration and Human Development (2993-2750). (Vol. 1, No. 6, pp. 17-20).

13. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. The Evolution of Graphical Interfaces for Programming TRACE MODE 6 Algorithms. American Journal of Pediatric Medicine and Health Sciences (2993-2149). (Vol. 1, No. 6, pp. 72-74).

14. TA Ilhomjon o'g'li, NU Nozimjon o'g'li, AO Azimjon o'g'li. Grid Tahlil Va Loyihalash. American Journal of Public Diplomacy and International Studies (2993-2157. (Vol. 1, No. 5, pp. 132-134).

15. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Ta’lim Berish Jarayonlarida Axborot-Kommunikatsiya Texnologiyalari. American Journal of Language, Literacy and Learning in STEM Education (2993-2769). (Vol. 1, No. 6, pp. 26-29).

16. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. Lms Tizimlari Va Ularning Tavsifi. American Journal of Engineering, Mechanics and Architecture (2993-2637). (Vol. 1, No. 6, pp. 36-38).

17. 17.Jamshidbek To‘xtasin o‘g, U., & Azimjon o‘g‘li, A. O. (2023, June). THE TRANSFORMATIVE ROLE AND IMPORTANCE OF TELECOMMUNICATION TECHNOLOGIES IN OUR DAILY LIVES. In " ONLINE-CONFERENCES" PLATFORM (pp. 138-139).

18. Turdaliyev, K., Abduraximov, O., & Isoqjonova, S. (2023). OPPORTUNITIES OF DIGITAL TECHNOLOGIES. Наука и инновация, 1(15), 8-11.

19. Isoqjonova, S., Abduraximov, O., & Turdaliyev, K. (2023). ZAMONAVIY DUNYODA ROBOTLARNING O’RNI HAMDA AHAMIYATI. Talqin Va Tadqiqotlar, 1(10).

20. Nafisaxon, T. U., Jamshidbek To’xtasin o’g, U., Arsenevna, D. E., & Azimjon o’g’li, A. O. (2022). AVTOMATLASHTIRILGAN AVTOTURARGOH IMKONIYATLARI VA QULAYLIKLARI. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(25), 45-48.

21. Tashlanova , N., & Abduraximov , O. (2023). TURIZM SOHASIDAGI ELEKTRON TIJORAT. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/809

22. K Turdaliyev, O Abduraximov, J Umaraliyev. (2023). FOCL AFZALLIKLARI HAMDA KAMCHILIKLARI. MOBIL SU’NIY YO’LDOSH VA OPTIK TOLALI TARMOQLAR. Development of pedagogical technologies in modern sciences. 2(4), 123-128.

23. TK Ilhomjon o'g'li, AO Azimjon o'g'li, NH Maxmudjon o‘g‘li, (2022). MASOFAVIY TA'LIM MODELLARI VA MASOFADAN OQITISH TIZIMLARI. SUSTAINABILITY OF EDUCATION, SOCIO-ECONOMIC SCIENCE THEORY, 1(4), 113-116.

24. U Jamshidbek To'xtasin o'g, TA Ilhomjon o'g'li, AO Azimjon o'g'li, (2022). AXBOROTLARNI AVTOMATLASHTIRILGAN BOSHQARUV TIZIMI. PEDAGOGICAL SCIENCES AND TEACHING METHODS, 2(17), 22-25

25. Абдурахимов , О. А., & Махмудов , У. Р. (2023). ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ВОЛОС, МОБИЛЬНЫХ СПУТНИКОВЫХ И ОПТИЧЕС- КИХ СЕТЕЙ. *Educational Research in Universal Sciences*, *2*(6), 147–150. Retrieved from http://erus.uz/index.php/er/article/

26. Azimjon o‘g‘li, A. O. (2023). REVOLUTIONIZING INDUSTRIES AND SHAPING THE FUTURE. ISSN 2181-4120 VOLUME 1, ISSUE 17 JUNE 2023, 347.

27. Jamshidbek To‘xtasin o‘g, U., Elyorbek o‘g‘li, I. A., & Azimjon o‘g‘li, A. O. (2022). IIS VOSITALARI YORDAMIDA VEB-SAYT BOSHQARUVI. Journal of new century innovations, 18(1), 64-69.

28. Ilhomjon o‘g‘li, T. K., Jamshidbek To‘xtasin o‘g, U., & Azimjon o‘g‘li, A. O. (2023, July). ZAMONAVIY TEXNOLOGIYALAR JAMIYATDAGI TARAQQIYOTIDAGI O ‘RNI VA AHAMIYATI. In International Conference on Architecture and Civil Engineering (pp. 1-3).