Stephanie Fissel

Aug 7, 2020 • 5 min read

4 Ways Data Science Weaponizes Cybersecurity to Fight the Biggest Threats

In recent years, the world of cybersecurity received an upgrade with the help of data science, integrating cyber knowledge over the last few decades with big data and artificial intelligence to more effectively identify threats, stop attacks and intrusions, properly identify malware and spam, and prevent dangerous cyber-attacks.

. . .

Data science has already proven its power alone, and as many sectors implement and determine its wide range of capabilities, there lies the ability to fundamentally transform many fields and find better solution to the world's problems, when leveraged correctly. One field that has shown increased benefits with the added usage of data science is cybersecurity. Data science changes how threats are identified, approached, and resolved and also plays a significant role in the prevention of future cyber-attacks.

While there are various ways in which cybersecurity has been impacted by data science, there are four main improvements that stand out. These include the transition to fact-based cybersecurity, advanced detection of threats from intruders, enhanced ability to predict attacks, and better insights into behavior analytics of hackers.

1. Fact-Based Cybersecurity

Since the inception of cybersecurity, the sector was mostly driven by fear, uncertainty, and doubt, which resulted in subjectively-made decisions. This way of operating would not last very far into the future and there was a need for data-driven solutions to cybercrime. The recent use of data science has enabled the cybersecurity sector to move from being heavily based on assumptions to actually being factual. This has led to the improvement of many techniques to more efficiently combat cyber threats and revolutionize the field.

2. Advanced Intrusion Detection

The implementation of data science has allowed for the use of machine learning in cybersecurity to more readily react and respond to emerging threats. With machine learning, organizations are able to identify and classify risks sooner, enabling response teams to take combative measures before security threats manifest. This is done by automatically flagging new threats of spam and malware based on similarity to known exploits and displayed behavior patterns, therefore reducing false positives, saving time and money.

Log analysis technologies also play a part in taking data to correlate logs and integrate threat intelligence services to heighten their detection capabilities and extract actionable information. As data sets become larger and algorithms sharper, there will be a seen improvement in detection systems. The downside to this increase in data science technology is that, inevitably, machine learning will be employed by attackers to improve their own tactics and skills.

3. Enhanced Predicting Ability

Data science is evolving the threat landscape to help businesses become more predictive in their risk mitigation strategy instead of reactive. Machine learning also plays a prevalent role in predicting the risk of future cyber-attacks as organizations can feed machine learning algorithms with past and present data about intrusions. This can then be used to easily identify outliers in data which allows for data scientists to analyze past exploits and behavior patterns to predict future attacks before they happen, resulting in better management of the system and a more effective way of spotting intrusions. It can observe patterns from minor outlier attacks that could become major threats.

4. Insights into Behavioral Analytics

Organizations can also better understand the behavior of attackers through reliable data analysis. Analyzing attackers' behaviors through vast resources of information can help to predict future behavior, making it easier to deal with bad actors.

With the use of data science, anomalies and abnormalities in user behavior caused by intruders can easily be identified and prevented in the future to decrease the severity of intrusion. Frequently, there is a correlation of unusual events when an intrusion is being carried out. Data science is that link between identifying those abnormalities and being able to see bigger picture.

• • •

A common thread through all of the improvements above is the extensive amount of rich data that data science provides for cybersecurity purposes. Big data analysis allows the opportunity to view large data sets and uncover hidden patterns, unknown correlations, and other important information. Assessing all of the real data one has from real users is crucial to insights and threat prevention.

There is already so much value that data science has contributed to cybersecurity, but there is no doubt that many more opportunities and assets will be discovered in the future, vastly opening up the greater potential for cybersecurity in the years to come.

Citations:

"Artificial Intelligence and Machine Learning: How They Both Intersect with Cybersecurity." Webinar., www.cybered.io/webinars/artificial-intelligence-machine-learning-how-they-both-intersect-w-1223.

Images of stacked clipboard papers, brain, and hexagon weave design. Mindfire Technologies — Innovations That Work, 5 Mar. 2019, www.mindfireit.com/cyber-security/cognitive-security-ai-driven-cyber-security/.

Miller, Jen A. Image of computer screen with code. CIO, 16 Dec. 2015, www.cio.com/article/3015952/the-year-in-fraud-2015-in-13-numbers.html.
Morgan, Peggy, et al. "How Data Science Can Answer Cybersecurity Challenges." JAXenter, 22 Nov. 2018, www.jaxenter.com/data-science-answer-cybersecurity-152210.html.

Parker, Douglas. "How Data Science and Cybersecurity Will Work Together." Colocation America, Colocation American Staff, 26 May 2020, www.colocationamerica.com/blog/data-science-cybersecurity.

Sachdeva, Karan. Image of artificial intelligence plugging into cybersecurity. IBM Big Data & Analytics Hub, 20 July 2017, www.ibmbigdatahub.com/blog/cyber-security-powered-ai-and-machine-learning.

Tannam, Ellen. "Data Science Is Changing How Cybersecurity Teams Hunt Threats." Silicon Republic, 19 Oct. 2018, www.siliconrepublic.com/enterprise/data-science-cybersecurity.

"The Big Connect: How Data Science Is Helping Cybersecurity." Infosecurity Magazine, 12 June 2019, www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/.