Group 3 presents

DATA ANALYSIS NEWS

Tuesday February 20, 2024 Issue #1

IN THE NEWS
Generative AI & CyberSecurity.

Dylan Young

Generative AI is everywhere these days, most specifically in social media. AI in today's society has the ability to be a leading potential software to help organizations efficacy and efficiency when it comes to their threat intelligence programs. In recent years, organizations have realized that they need to focus on having threat intelligence programs. According to ESG Research "72% of enterprise organizations (with 1000 or more employees) find it hard to sort through CTI noise to find relevant information, while 63% of firms admit they don't have the right staff size or skills to develop an appropriate CTI program." Will **Generative AI** be able to help with these problems that organizations are having with their threat intelligence programs? The answer is yes. Here are some examples on how **Generative AI** could help according to ESG

- "Thirty-three percent of cybersecurity professionals say that threat intelligence reports feature too much technical detail, making them difficult for business managers to consume. This isn't surprising since threat intelligence analysts are buried in technical details about indicators of compromise (IoCs), malware, adversary tactics, techniques, and processes (TTPs), the MITRE ATT&CK framework, etc. Generative AI could help the threat intelligence teams create summary reports tailored to different technical and business consumers. This combined with CTI consumer feedback can help organizations continuously improve the quality, relevancy, and timeliness of these reports over time."
-"Twenty-five percent of cybersecurity professionals say that they have few if any personnel with threat intelligence skills. Generative AI can't alleviate the need for advanced intelligence skills, but it can help train junior personnel while helping them bolster contributions by creating detection rules, assessing whether files/scripts are malicious or not, and comparing vulnerabilities with known exploits in the will

Generative AI won't replace threat analysts or make automation decisions on its own, but it could act as a helping device and for organizations that are understaffed and can't properly train their personnel.

Some Pros and Cons of **Generative AI** in Cyber Security.

Pros -

Enhanced Threat Detection
Automated Security Measures
Innovative Problem-Solving.

Cons-

Sophisticated phishing attacks
Data privacy concerns
Unpredictable behavior

The main use for **Generative AI** is playing a key role in training purposes. **Generative AI** can be used to create realistic cyberattack simulations for training purposes. An example of those could be phishing emails to create complex malware attacks.

Vulnerabilities -

Generative AI models are trained on data that is collected from all kinds of sources - and not always in a transparent fashion, it is unknown exactly what data gets exposed to this additional attack surface. When data is stored for a long time for the most part they don't always have good security measures / safeguards in place. The best way to protect your sensitive data is to keep out your sensitive data when adding it to generative models. According to Collins Ayuya "Instead of blindly trusting whatever security protocols these vendors may or may not have in place, it's a better idea to create synthetic data copies or avoid using these tools entirely when working with classified data. Instead, use generative AI to supplement your projects when working with less sensitive information."

Overall Generative AI can be very useful if used correctly and safely.

13 TOP GENERATIVE AI and CYBERSECURITY SOLUTIONS

1	Google Cloud Security Workbench
2	Microsoft Security Copilot
3	CrowdStrike Charlotte AI
4	Cisco Security Cloud
5	Airgap Networks ThreatGPT
6	SentinelOne
7	Synthesis Humans
8	SecurityScoreCard
9	MOSTLY AI
10	Sophos
11	Cybereason
12	Cylance by BlackBerry
13	Trellix

Source: "Generative AI and Cybersecurity: Ultimate Guide"

The Future of Cybersecurity:Data Analytics and Automation

Dalton Grimes

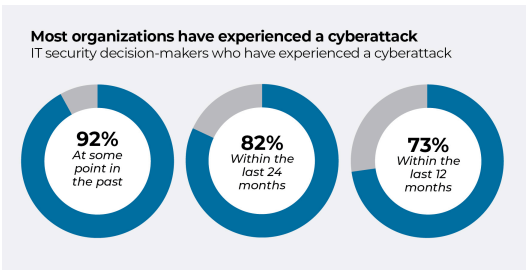
In recent years, cybersecurity threats have evolved in a way unseen before. Notably, the tactics used to breach security measures are becoming more subtle and leave less of a trail behind. With threats becoming less obvious and more dangerous, there comes a need for improvements in cybersecurity. When discussing ways to combat these threats, **data analytics** and **automation** can play a vital role in detecting privilege escalation, exfiltration, and lateral movement.

Through the use of **data analysis**, cybersecurity can be greatly improved by using the tools to detect, prevent, address and help stop cyber threats and breaches of privacy. This would be an example of cybersecurity data science, which refers to the application of data science techniques to cybersecurity data. Through many different methodologies (ex: statistical analysis or machine learning), patterns and relationships within cybersecurity data can be addressed. Predictive models can be built in order to aid in threat detection and can help improve an organization's processes for cybersecurity. But, where can cybersecurity analysts and professionals source the data from? Given that these people work in cybersecurity, they would be able to access the large amounts of data through network traffic, logs, and threat intelligence feeds. By understanding and processing this data, security measures can be upgraded and cybersecurity practices can be improved for the future.

Automation in cybersecurity is a concept that can be described as using advanced systems backed by AI and machine learning that help improve cybersecurity processes and cause them to run more efficiently and quicker. Cybersecurity Automation can detect and deal with cyber threats before anything is compromised and accessed by the hacker(s).

So, how can cybersecurity be automated? First, cybersecurity automation takes tasks that are repeatable without assistance from a human and automates those tasks. By giving the software the ability to do tasks on its own, it frees up the cybersecurity professional to complete other necessary tasks. By streamlining the processes normally done by humans, it reduces the chance of manual error while also increasing efficiency, making faster decisions, and also can save money that can be used for other projects. The automation tool can do something such as scanning a network for vulnerabilities or threats. If the tool finds an issue or vulnerability, then a report can be generated and a security team can analyze it to see the threat level and ways to mitigate it in the future.

Another use case of automation is compliance monitoring. This is the process of monitoring systems and networks so that it is easier for an organization to identify and find a solution to a problem. There are also industry standards that need to be followed, and by having an automated monitoring system, there is less of a chance of an organization being fined or penalized for not complying with the standards.



Pictured above are some visuals relating to the commonality of cyberattacks on organizations. With the extremely high amount of organizations experiencing attacks in the last 12 months, it is imperative that cybersecurity processes need to improve. The use of data analytics and automation can help in this area from the ways described in previous paragraphs. Image is courtesy of tanium.com (https://www.tanium.com/blog/5-charts-that-show-why-it-pays-to-prevent-a-cyberattack-rather-than-fight-one/).

Both **data analytics** and **automation** are great methods to deploy to help combat cybersecurity threats. These methods can be used separately or together, and can provide solutions to many organizations out there. As technology continues to grow and become more accessible to people, there will always be a constant need to fend off cyber threats, especially as technology improves. Hackers and people looking to infiltrate systems will always try and find ways to breach security measures, so it is imperative that there are ways to fight this so people and information can stay safe.

The Highest Reviewed Data Analytics Software.

Sonya Crockett

The right software is essential for using data analytics to the advantage of you or your business. It might be easy to find a software that, on paper, might seem like the best for you and your needs, it may be a dud when in actual practice. Here is the highest reviewed data analytics software, reviewed by the people who actually use it.

1. Microsoft BI- By far the highest reviewed software out there. Microsoft BI is best for visualizations, and utilizes commonly known tricks and tools from excel making it very user friendly. Although too much data may slow it down. The overall consensus is that Microsoft BI is a software that is easy to use.
2. Tableau- This software is best for businesses who are looking to use their data to grow. While some may think it gets a bit pricey, particularly for the Enterprise version the knowledge gained could outweigh the cost.
3. Google Analytics- Google has introduced the most cost effective, yet still powerful tool for data analytics. Plans start out at no cost, feature great visualizations, and have predictive capabilities that can offer insights to help any business.
4. Qlik Sense- The most collaborative of all the softwares reviewed. Qlik beautifully uses third party data to create insights for its user. Qlik can lean on the more expensive side, and it may take the average user some extra time to fully grasp.
5. Looker- Looker is the most lingual. It can understand multiple dialects of SQL. Looker also works great with all the big cloud platforms. Unfortunately if you only need read access you will be charged full price.

A Career Path In Data

Sonya Crockett

Here you are, you know SQL, the foundations of Python, and the CRISP-DM process forward and backwards, but what can you do with this wealth of knowledge? Time to start your path to a career in data analytics. There are many different paths to choose from in this field. While yes there is the straight forward path of becoming a data analyst in data analytics but there are many careers to choose from: data scientist, data engineer, or Chief Data Officer. According to the U.S Bureau of Labor Statistics demand for data analysts is predicted to rise 35% from 20220 to 2032, making it one of the more in demand fields. The starting pay is higher than most entry level tech jobs. So how do you begin? First things first get your resume in order. Next create an appealing portfolio full of great examples of your work. There are many free dataset sites such as Kaggle, and Google Datasets, where you can create projects to put into your portfolio. In addition to showing off your skills in SQL, machine learning, and data cleaning be sure to include projects that show off your communication skills such as presentations and reports.

Next it's time to find a job. An internship is a great foot in the door, especially while still in school, but what if your internship has ended and school is over? Start Networking with data professionals. Meet Up is a great source for events geared towards people in tech and particularly data. Then begin applying for junior data analyst positions or just data analyst positions. Handshake, Hired, and Data Camp Jobs are all great places to begin. Finally, you are hired, you're working and you're having a great time but where can you go from here? There are many paths you can take your experience with data. Want to be your own boss? Become a consultant. Are you fluent in Python and Machine Learning? Become a data scientist. Or perhaps you specialize in a particular industry where there are healthcare analysts, social analysts, and insurance underwriting analysts. The data career path may seem like a straightforward path down the tech tube but it could pivot you down the medical field, or finance district.

Careers In Data and average salaries according Indeed.com

Data Analyst	$75,307
Senior Data Analyst	$97,348
Data Scientist	$122,511
Data Analytics Consultant	$77,365
Data Analytics Manager	$89,287
Marketing Analyst	$65,848
Health Care Analyst	$63,411
Chief Data Officer	$178,606

Data in Careers

What can data provide?

15 Careers in Data Analytics: Exploring Your Future in Data (springboard.com)

Jettie Burkhead

Reasons to work in an analytics job include the flexibility modern organizations offer, the continuous learning on offer, and the opportunity to work with like-minded professionals.

- **Variety of Roles**- There are many different types of roles within the field of analytics including data scientists, and data engineers which means that there is likely a role that aligns with your interests and skills.
- **Use of Technology**- Analytics professionals use cutting edge technology and tools to extract insights from data which can be exciting and challenging.
- **Impactful Work**- Professionals in this industry can paly a crucial role in helping organizations make data driven decisions , which can have a significant impact on the success of the organization.
- **Career Advancement**- As you progress in this industry, you're likely to find opportunities for career advancement , with many professionals starting in entry - level roles and working their way up to management positions.
- **Job Security**- As data becomes an increasingly important asset for organizations, the demand for analytics professionals is likely to continue to grow, providing job security in the field.