Explore – Impact of Computing Innovations
Written Response Submission Template

Please see Assessment Overview and Performance Task Directions for Student for the task directions and recommended word counts.

Computational Artifact

2a)

A new innovation in cyber security is to use machine learning to assist existing systems [1]. The innovation works by using algorithms that study how a user interacts with a web page every time he or she logs in [1]. Whenever unusual activity is seen by the algorithm, the user is notified [1]. My artifact describes how the innovation works by explaining how machine learning works for cyber security in a similar way to this paragraph. The first image also demonstrates what a deep learning algorithm may look like on a chart.

2b)

I created the artifact with google slides, google search, and google images. First, I searched for multiple articles that would help me to understand the topic of machine learning being used for cyber security. Next, I created a new slideshow in google slides, which I then put a brief summary of how the innovation works. Then, I searched for images that related to what I was trying to the innovation. My searches were machine learning, cyber attack, and cyber security. I found some images that looked good and then placed them on the slide. Finally, I saved the slide as a pdf.

Computing Innovation

2c)

One beneficial effect of this innovation is that people will be able to keep their data more safe from cyber attackers. The automated systems that this innovation will create, as well as the previous solutions used alongside automation, will be able to create secure systems that work very fast [6]. This increase in detection speed will help companies to observe different methods of attacks, which will allow for the companies to train their machine learning algorithms to detect more threats before they reach a wide amount of users.

One Harmful effect of this innovation is that the increased security will also encourage the people behind cyber attacks to create stronger attacks, which will be able to pass through the more secure systems [6]. This could make it difficult for companies to implement cyber security systems because they will have to keep making better and better machine learning algorithms to protect users against the increasingly strong cyber attacks. Eventually, there may even be a point where the companies can not do much more to make their systems more secure.

Another beneficial effect of this innovation is that companies will save a lot of time when finding cyber security threats. Researchers say that up to 21,000 hours are wasted each year by cybersecurity companies trying to analyze false positives in attack detection [4]. The speed of machine learning algorithms will help to detect actual threats much faster than systems made up of only humans and software [4]. This saved time can allow for companies to develop better security for their users, as well as developing themselves as a company.

2d)

Machine learning algorithms are designed to analyze data of users on a website or in a program. Currently, there are four main ways that algorithms are trained: supervised learning, ensemble learning, unsupervised learning, and semi-supervised learning [1]. Supervised learning is when the people creating the

algorithm feed labelled data to the algorithm, so that it will learn how to categorize different types of data [1]. Ensemble learning is like supervised learning, but it uses multiple types of sorting algorithms [1]. Unsupervised learning is when the developers of the algorithm feed data that is not labelled to the algorithm, so that it can sort through the data in its own way [1]. Semi-supervised learning combines both supervised and unsupervised learning by feeding the algorithm both labelled and unlabelled data [1].

An example of data is the user's patterns, such as when he or she usually logs in [1]. The algorithm can detect that the account has been active at an unusual time, so it notifies the user of the security concern. Machine learning algorithms can also study the types of files being uploaded and downloaded. By studying both safe and unsafe files, the algorithms can recognize unsafe patterns in the file's data and warn the users [1]. The algorithms can also study the patterns of other security systems' data to find vulnerabilities [1]. This allows for developers to improve the cyber security of users.

A security concern is that cyber attackers may start using machine learning algorithms to study what the security algorithms say is acceptable in files. This will allow for cyber attackers to find weaknesses in algorithms and become more dangerous, which will make it more difficult to develop better security algorithms.

References

2e)

[1] 1681725802152208. (2018, October 04). Machine Learning for Cybersecurity 101 – Towards Data Science. Retrieved January 24, 2019, from https://towardsdatascience.com/machine-learning-for-cybersecurity-101-7822b802790b

[2] A. H., & G. A. (2018, December 19). New Guidelines for Responding to Cyber Attacks Don't Go Far Enough [Digital image]. Retrieved January 24, 2019, from https://newsroom.unsw.edu.au/sites/default/files/styles/full_width__2x/public/thumbnails/image/shutterstock_1050436496_1.jpg?itok=jNlK4gt7

[3] Feedforward Deep Learning Models [Digital image]. (n.d.). Retrieved January 24, 2019, from http://uc-r.github.io/public/images/analytics/deep_learning/deep_nn.png

[4] Johnson, K. (2019, January 17). Machine Learning Algorithms in Cybersecurity Solutions. Retrieved January 24, 2019, from https://spinbackup.com/blog/machine-learning-algorithms-cybersecurity/

[5] N. I. (2018, July 20). CTO vs. CISO: Who should have ultimate responsibility for cyber security? [Digital image]. Retrieved January 24, 2019, from https://s26913.pcdn.co/wp-content/uploads/2018/07/AdobeStock_157468959-1013x440.jpeg

[6] Why Big Data and Machine Learning are Essential for Cyber Security. (2018, October 23). Retrieved January 24, 2019, from https://insidebigdata.com/2018/10/25/big-data-machine-learning-essential-cyber-security/