AI Lesson Plan: How is AI involved in CyberSecurity

Develop a lesson plan to demonstrate how you would use AI in your classroom to fit your grade/age level. Lesson plans will be shared at the final live session on December 17th.

Name: Meghan Jacquot

Subject(s) Taught: Engineering, AP CSP, Chemistry, AP Literature, AP Rhetoric

Grade Level: 10, 11, and 12 Grades

Intro & Purpose

Describe how you would introduce your topic to spark student interest.

This would be for my 5 student, 12th grade, Advanced Engineering Class. I would start with semi-current events. It would depend on when I am teaching it, but if I was teaching it soon, (December 2020) this is current. I would ask some general questions. Has anyone ever been hacked? Had their identity stolen?

What do you know about the Baltimore Public School hack that just happened? The FireEye hack that just happened?

How is AI involved in CyberSecurity?

Use these slides for the lesson - it is view only, so you'll need to make a copy. Then you can either have students make a copy or give them editing permissions. [Click here for your classes you'll probably want to delete the test slide.

https://docs.google.com/presentation/d/1zwZmffgJfpQPkEnyxB00IOIvt6hn-7kamuCOSuJ91ls/edit?usp=sharing]

Key Terms

List the key terms relevant to your topic.

AI, CyberSecurity, SOC (pronounced like sock) Monitor, IoC, EC2, DNS, AWS (note that some terms only apply if you watch all videos on the QRadar website)
Activity

Describe a learning activity that would aid student understanding of your topic. List the resources needed.

After the brief discussion about hacking/identity theft discuss that nowadays AI is being paired with CyberSecurity firms on both sides (offensive and defensive). Depending on how this is structured and the length of your classes this will be more than one class period.

Have students navigate to this website to take a tour of IBM’s AI + CyberSecurity QRadar Demo
Watch the AI + CyberSecurity Video and the Investigate Threats with Watson video
https://mediacenter.ibm.com/media/0_8rac5g3o

https://qradar-demo.mybluemix.net/?cm_mc_uid=81508977910016020906173&cm_mc_sid_50200000=85947211603377138363&ga=2.37280232.977420025.1603109317-211869374.1602181127&_gac=1.14820866.1602508583.EAIaIQobChMIv9GrrcGM7AIbdbACh2NPAdnEAYASABEgLg_D_BwE
Then have students use Mentimeter to share their thoughts and then discuss

https://www.menti.com/vwc2hr4k3b
Mentimeter question:
How is the AI helping the CyberSecurity specialist?

All the videos on QRadar are interesting, so I have included definitions of terms below for all of them in case the lesson is expanded.
Assessment

Describe how you would assess student learning and understanding

For homework have students research one of these aspects from IBM or choose their own AI + CyberSecurity area to research
https://www.ibm.com/security/artificial-intelligence?p1=Search&p4=43700050370544833&p5=b&cm_mmc=Search_Google-_-1S_1S-_-WW_NA-_-%2Bai%2Bcyber%2Bsecurity_b&cm_mmc=Search_Google-_-1S_1S-_-WW_NA-_-%2Bai%2Bcyber%2Bsecurity_b&cm_mmca7=7170000060890276&cm_mmca8=kwd-338456356546&cm_mmca9=Cj0KCQiA8dH-BRD_ARIsAC24umZu3hZv0Xg15fLcKz9cvIUVTg9VaYuCCFy9ckA1TEw07BSx3afHEaAk1UEALw_wcB&cm_mmca10=404375117716&cm_mmca11=b&gclid=Cj0KCQiA8dH-BRD_ARIsAC24umZu3hZv0Xg15fLcKz9cvIUVTg9VaYuCCFy9ckA1TEw07BSx3afHEaAk1UEALw_wcB&gclsrc=aw.ds
This is another option
https://builtin.com/artificial-intelligence/machine-learning-cybersecurity

Outcome: Students write a Tech OpEd about a source of their choice that combines AI and CyberSecurity. In the next class they will share out what they learned in small groups.

HW Assignment:
https://docs.google.com/document/d/1mIeqXE_kgSVEusiYNtI8FZUiVZi-3FVXWghBzGlwac/edit?usp=sharing

References/Resources:

- Article for Hacking of the Baltimore Public Schools

- Article for Hacking of FireEye

- Article for Hacking of US Goverment agencies
  https://www.reuters.com/article/us-usa-cyber-amazon-com-exclusive-idUSKBN28N0PG and
  https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html and

- 2017 data

- What is AI?
  [https://www.technologyreview.com/2018/11/10/139137/is-this-ai-we-drew-you-a-flowchart-to-work-it-out/](https://www.technologyreview.com/2018/11/10/139137/is-this-ai-we-drew-you-a-flowchart-to-work-it-out/)

- What is CyberSecurity?

- AI + CyberSecurity

- IoCs - Indicator of Compromise - demonstration that a cyber threat has occurred
  [https://www.forcepoint.com/cyber-edu/indicators-compromise-ioc](https://www.forcepoint.com/cyber-edu/indicators-compromise-ioc)

- SOC - Security Operation Center
  [https://digitalguardian.com/blog/what-security-operations-center-soc](https://digitalguardian.com/blog/what-security-operations-center-soc)

- DNS
  [https://www.cloudflare.com/learning/dns/what-is-dns/](https://www.cloudflare.com/learning/dns/what-is-dns/)

- EC2