* **A general description of the threat and where you learned more about it**
* **How it occurs and example(s) of this threat attacking an organization.**
* **How the topics covered in this class (or previous classes) might mitigate the threat**
* **ARTIFICIAL INTELLIGANCE IN CYBER SECURITY:**
  + Today’s systems generate so much security data that human experts are rapidly surpassed. People cannot find the attack elements fast enough or reliably enough. By comparison, computers excel at these operations. AI then helps them to make sense of what they find. It can even help by offering suggestions to security teams of processes to handle them.
  + Opportunistic malware lacks the understanding and contextualization of a human attacker. While certain characteristics might be deemed clever, e.g. how it moves laterally or how it exfiltrates data, this kind of malware is mostly static according to its source code once it has been unleashed.
  + AI Algorithms are Very Good at identifying outliners from certain pattern which Baselines what is normal and then dives deep into abnormal events from which one can detect the Attacks. This is called unsupervised learning algorithm.
  + Supervised algorithms are also used to detect the threats which are being trained on the specific set of training sets. If the specific Sets are not trained well or the Training sets are not good enough then the Algorithm won’t be efficient
* **ARTIFICIAL INTELLIGANCE FOR DEFFENCING:**
  + **USING BIO METRIC AS LOGIN**
    - deploying AI for cybersecurity has introduced biometric login techniques for secure logins. AI systems can scan fingerprints, retina and palm prints accurately. Such biometric logins can be used in combination with passwords that are already in use with devices like smartphones
  + **DETECTING THREATS AND MALICIOUS ACTIVITIES** 
    - Cybersecurity firms are training AI systems to detect malware and viruses with the help of several datasets that include algorithms and codes. Using such data, AI can perform pattern recognition that helps identify malicious behavior in software. Moreover, [AI and machine learning can play a crucial role](https://www.allerin.com/blog/machine-learning-and-ai-play-a-crucial-role-in-cyber-security) in online security.
    - Machine learning can analyze path traversals of websites to detect whether a website navigates to malicious domains. Likewise, AI-based systems can recognize malicious files, like web shell, and preemptively isolate them from the system.
    - AI systems can be trained to analyze micro-behavior of ransomware attacks to recognize ransomware before it encrypts a system.
    - Furthermore, AI systems can use predictive analytics to AI-based alternatives that will always be quicker and more effective than a manual approach.
  + **LEARNING WITH NATURAL LANGUAGE PROCESSING**
    - AI-powered systems can automatically collect data for reference by scanning articles, studies and news on cyber threats. AI systems use Natural Language Processing for selecting useful information from the scanned data. Such information will provide insight into cyber attacks, anomalies, mitigation and prevention strategies. Using the analyzed information, cybersecurity firms can identify timescales, calculate risks, harvest data and make predictions. Therefore, cybersecurity firms can stay updated on current cyber threats and prepare effective strategies to secure organizations from numerous cyber attacks.
  + SECURING CONDITIONAL ACCESS
    - AI systems can use Multi-Factor Authentication for this purpose. With this approach, the system will collect user information to analyze the behavior of the user, application, device, network, data and location. Using such information, the AI-powered system can automatically change any user’s access privileges to ensure data security on remote networks.
  + LIMITATIONS:
    - the data used for training needs to be accurate, as inaccurate data will lead to inefficient outcomes. Therefore, finding and collecting precise datasets can be a tedious and time-consuming task.
    - If black hat hackers get to know what data sets are AI of your system is trained on they can create another AI system which could potentially can pose threat to the existing AI cyber security system
* **ARTIFICIAL INTELLIGANCE FOR ATTACKING:**
  + **Autonomous malware**
  + **Intelligent evasion techniques**
  + **Low-and-slow data exfiltration**
* **AI TOOLS WHICH ARE USED FOR CYBER SECURITY:**
  + **Symantec’s Targeted attack analytics (TAA) tool**
  + This tool was developed by Symantec and is used to uncover stealth and targeted attacks. It applies AI and machine learning on the processes, knowledge, and capabilities of the Symantec’s security experts and researchers.
  + TAA unveils suspicious activity in individual endpoints and collates that information to determine whether each action indicate hidden malicious activity. The TAA tools are now available for **Symantec Advanced Threat Protection (ATP)** customers.
  + **Sophos’ Intercept X tool**
    - Sophos is a British security software and hardware company. Its tool, Intercept X, uses a deep learning neural network that works similar to a human brain.
    - In 2010, the US **Defense Advanced Research Projects Agency (DARPA)** created their first Cyber Genome Program to uncover the ‘DNA’ of malware and other cyber threats, which led to the creation of algorithm present in the Intercept X.
    - Intercept X utilizes behavioral analysis to restrict new ransomware and boot-record attacks.  The Intercept X has been tested on several third parties such as NSS labs and received high-scores. It is also proven on VirusTotal since August of 2016. Maik Morgenstern, CTO, AV-TEST said, “One of the best performance scores we have ever seen in our tests.”
  + **Darktrace Antigena**
    - Darktrace Antigena is Darktrace’s active self-defense product. Antigena expands Darktrace’s core capabilities to detect and replicate the function of digital antibodies that identify and neutralize threats and viruses.
    - With the help of underlying machine learning technology, Darktrace Antigena identifies and protects against unknown threats as they develop. It does this without the need for human intervention, prior knowledge of attacks, rules or signatures. With such automated response capability, organizations can respond to threats quickly, without disrupting the normal pattern of business activity.
* **Top 10 companies Merged AI with Cyber Security** 
  + **Versive: VSE Security Engine uses AI to sort and detect the critical risks from routine network Activity**
  + **Logrhythm**
  + **Anomali**
  + **CrowdStrike: Healthcare**
  + **Cybereason: Aero Sapce**
  + **Draktrace: Direct TV**
  + **Jask**
  + **Fortinet:(Majority of fortune 500 companies use)**
  + **High-Tech Bridge:Web and mobile:**
  + **Palo Alto Networks: Used by 150 countries**
* **TOP 2018 AI CYBER ATTACKS:**