In 2017, the autonomous hacking machines could seek out the vulnerabilities by big data. Human security team needs to know how to handle this new situation.

In 2019, more and more security mechanisms concern with the AI. For example, machine learning can detect outliers clearly and easily. These anomalous data help staff find out threats and attacks. However, ~~security AI still cannot be developed, because some curial points depend on human’s effort, such as the high quality training data and significant user feedback to fine-tune their monitoring. Moreover,~~ they thought 2019 is the year of AI winter. A slowdown of funding lags behind the expectation of AI research. But attackers will not be affected by investment. They keep going to improve their AI model to detect security gaps.

In 2017, as more and more data migrating to the Cloud, the possibility of being attacking is also growing. In 2018, the shift to the cloud has occurred at an astronomical rate. But the cloud vendors don’t have a comprehensive solution to address the data security for their customers. For example, the username and password verification should utilize the internet. If these data were intercepted, attackers could get bunch of data in the cloud. In 2019, edge computing can leverage the endpoint in harmony with the cloud. According to this way, the data processing could be done in the user’s device and then only metadata were sent to the cloud. ~~The main obstacle is trust mutually.~~

In 2017, no security process for new mobile devices. In 2018, IoT becomes a target for mass disruption. In 2019, industrial IoT disruption at scale. IoT will be the most challenging area of security. Not many security professionals have had time to focus on IoT and it is becoming the trend of our life. Cloud services offer the connection of exponential number of devices which can lead to shared technology vulnerabilities.

AI impacts on the two sides of cybersecurity. On positive side, the security team

For positive utilization of AI, the cybersecurity AI encounters some issues. Many high-quality training data are curial for AI model. They cannot find the profit of investment for cybersecurity AI at foreseeable stage. On the other hand, attackers can apply the AI tool for seeking the vulnerabilities.