The Future of Cybersecurity:
- Artificial Intelligence, Machine Learning & Automation

Danny Li, Co-Owner & CTO
HKBN Group
10th September 2021

Common Misunderstanding

- IT ≠ Network:
  - Network connects IT systems, it supports IT
  - Network provides connectivity
- IT ≠ Information Security
  - Operation ≠ Governance
- Firewall ≠ Secured:
  - You need a lock for your front door but you still need a safe for your Rolex
- Hacker won't sleep, actually they prefer to work when you are off

What are the Biggest Challenges in Cybersecurity Incident Response?

- Visibility
    - What is going on in your network?
    - What staff are doing when WFH?
- Lack of Expertise
- You don’t know what you don’t know!

Challenges in Cybersecurity - Visibility

- In traditional network infrastructure, at least you have everything “contained” inside
- Under “New Normal” WFH arrangement, you have no visibility on client side
- If you don’t have visibility, how can you “response” to incident?

Challenges in Cybersecurity - Lack of Expertise

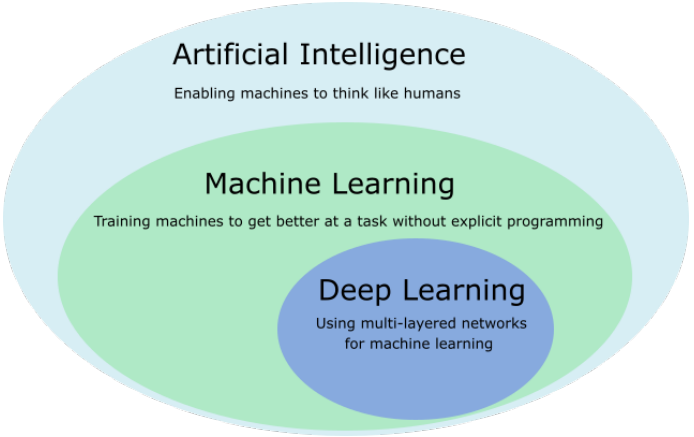
- It is a global shortage of cybersecurity expertise
- Heavy workload & tedious work results in high turnover rate
- What % of time we spent on “interesting” task like threat hunting?

Challenges in Cybersecurity
- You don’t know what you don’t know

- Spending millions of dollar on something you know but it’s hard to justify investment on something you don’t know
- How to discover what you don’t know?
- How to qualify & quantify them?

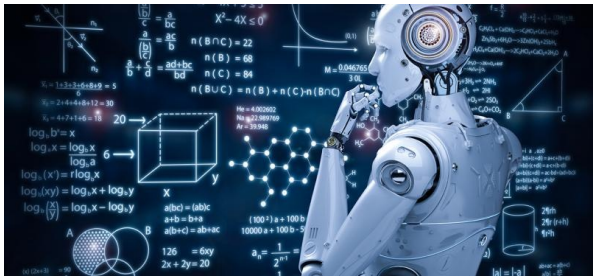
Solutions

- Machine Learning (ML)
- Artificial Intelligence (AI)
- Security Orchestration, Automation and Response (SOAR)



Solutions - Machine Learning

- Use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy
- Learn the pattern, take out the tedious work from human
- Reduce human error
- Solve the “learning curve” problem during staff turnover



Solutions - Artificial Intelligence

- Simulation of human intelligence in machines that are programmed to think like humans and mimic their actions
- AI learns to solve simple problem and free the human mind for more complicated issues
- Human can focus on more interesting threat hunting task

Solutions - SOAR
Security Orchestration, Automation and Response

- SOC / SIEM generating hundreds of alert everyday

- If most of the alerts will be handled similarly -> automate them
- Critical alerts that need immediate action -> response ASAP to minimize impact

The Future of Cybersecurity will rely on

- ML - frees you from tedious work, focus on interesting task and improve talents retention rate
- AI - helps you discover what you don’t know, with improved visibility you can invest wisely
- Orchestration and Automation - allow you to response quicker, every second counts in Cybersecurity

香港寬頻
HONG KONG BROADBAND NETWORK

The End

Make our Home a Better Place to Live