

## Week 3 Workshop

# 程序代写代做 CS编程辅导

Key knowledge/skills: Cyber Kill Chain & Cyber threats

Case study (as brief and lecture) - "Company X and Company Y are competitors who both work on a secret Government project. Staff A (attacker) from Company X learned that Staff V (victim) is the lead architect in Company Y. A then crafted an email to Staff V using a recent Zero day vulnerability. Note that A developed the malware exploiting a recent Zero day vulnerability. V was lured to click on the malware in the email, which installed a backdoor, after successfully exploited the targeted vulnerability on Staff V's system. This gave A the remote control of Staff V's computer. After that, Staff A used a compromised server (C2 server) to issue commands to maintain the control of V's computer. One night, A started to upload key design documents from V's computer to a shared Cloud storage folder owned by Staff A."

WeChat: cstutorcs

Assignment Project Exam Help

Q1. Map the attack activities to Cyber Kill Chain (CKC)

Email: tutorcs@163.com

Q2. Map the following technical controls to Cyber Kill Chain (CKC), e.g., 'Email Security: CKC3 Delivery'; and what other controls you can think of?

QQ: 749389476

- Gateway controls such as Web Proxy, Email Security, DNS
- Network controls such as IPS (Intrusion Prevention System)
- Endpoint controls such as AV (AntiVirus), HIPS (Host-based IPS)

https://tutorcs.com

Q3. Assuming you have access to all the logs / security alerts of the above controls during the event, what are the key information/attributes can help detect/stop the attack?