Cybersecurity Investigator 2

Briefing Cards

Briefing Card #6:

Good afternoon! As you may recall, our city is experiencing a ransomware attack. The malware on our computer has encrypted data in many of our city's departments; as a result, various city services have been unable to proceed as usual.

As a result of your investigative efforts, we have determined the usernames of a known hacker network that was conspiring to carry out this attack. Law enforcement officials have further identified the IP addresses associated with these usernames:

- RottenJGL: 63.146.24.122
- NtA_GR8Daisy: 71.166.168.13
- ineedbitcoin: 96.234.175.22
- CookieMonstr: 149.2.123.33

I am releasing two documents to the public to aid in the investigation: An Internal Memo from the police chief that was sent just days before the attack and a Server Security Log from the date it was hacked. We don't know exactly what time the attack took place, so we have included extensive records from the entire day's log of activity from CITYSRV1 (City Server Number 1).

- We need to know three things:
- Which department was attacked
- Who the attacker was
- What they did to the network

Briefing Card #7:

I am pleased to announce that, as a result of your investigative efforts, law enforcement has been able to apprehend the suspect whose username was NtA_GR8Daisy (Not a Great Daisy), who initiated the attack on our city.

We are also working closely with a cybersecurity firm to try and restore as much of our city's data as possible. The recovery process will likely take several months, and I appreciate your help and patience in restoring normal operations as soon as possible.

In the meantime, we must take measures to protect our city from future attacks. I have compiled a list of best practices in cybersecurity.

Unfortunately, due to budget constraints, we can only adopt five of the strategies on this sheet, and I need your help to determine which strategies will be most effective. Please divide into small groups and look at this list to determine which five strategies your group would recommend for our city.