How do they do it: Enterprise Cybersecurity

BY BUSHIDO

CISO

- Police Chief

SOC

- 999 – What's Your Emergency?

CERT

- Firefighters

Threat Hunters

- Bobbies on the Beat

Detection Engineers

- K9 Unit

DFIR

- Crime Scene Forensics

NetSecOps

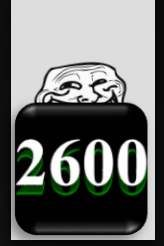
- Highway Patrol
- Air Patrol

Insider Threat

- Independent Office for Police Conduct

Threat Intelligence

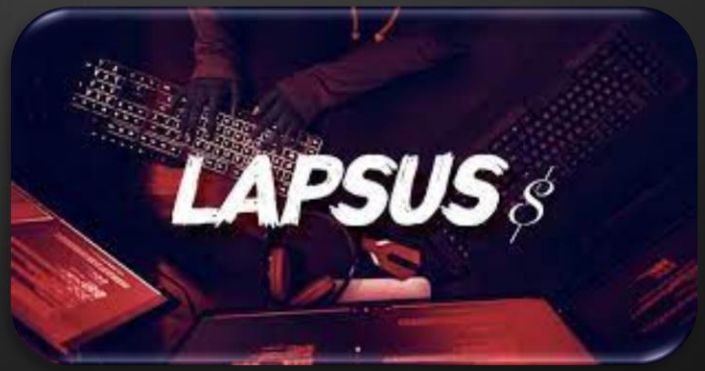
- Undercover Cops
- Wannabe Spooks
- Cyber Snitches



But Why?

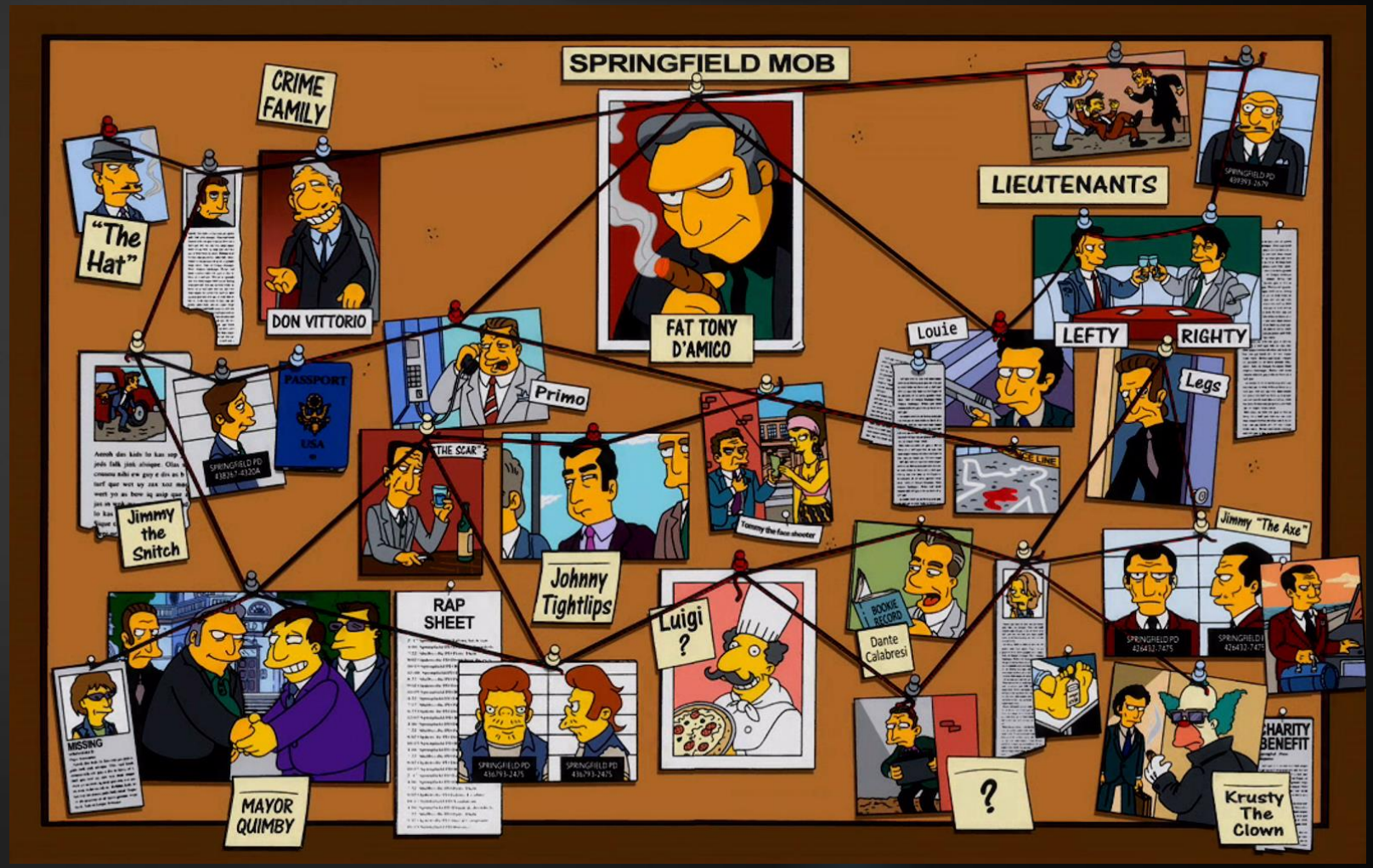
Threat Actors

- Criminals
- Thieves
- ASBOs
- Arsonists



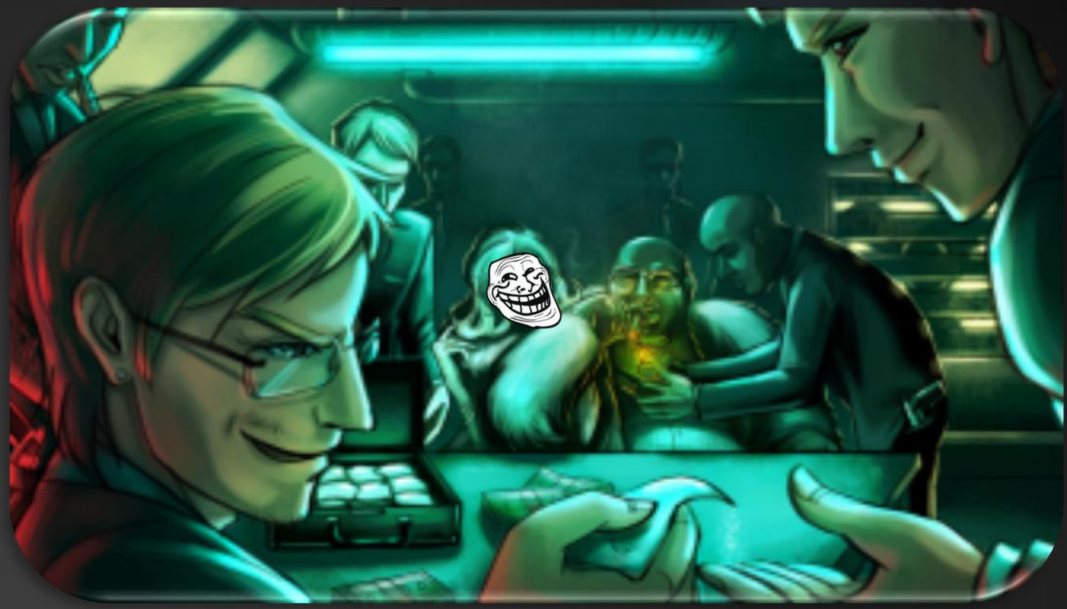
Organized Crime

- Ransomware
- Darknet Markets



Black Markets

- Credentials
- Data Brokers
- Access Brokers
- Malware-as-a-Service
- Ransomware-as-a-Service



Hopefully You Learned:

- CISO
- SOC
- CERT
- Threat Hunters
- Detection Engineers
- DFIR
- NetSecOps
- Insider Threat
- Threat Intelligence
- Threat Actors
- Organized Crime
- Black Markets