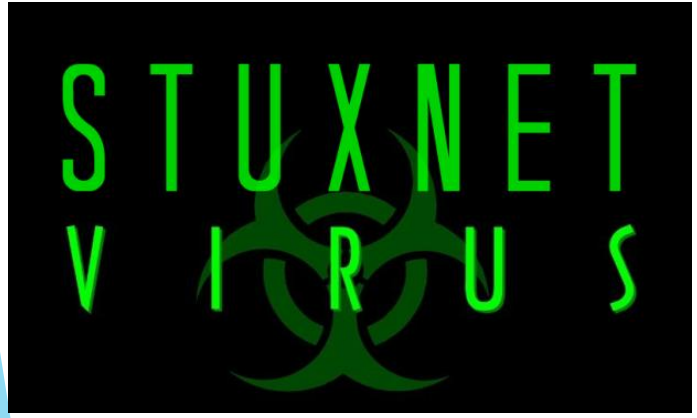
What is Cyber Security?

SUMMARY
AMERICA
ACTIVE STOCKS
LONDON
ACTIVE STOCKS


STUXNET
VIRUS

What are we defending?

- IP
- ID
- Financial transactions
- Sensitive data: commercial, academic, military, political
- Processes: critical infrastructure
- People and processes are a point of entry
- Clients, partners and suppliers are a risk (TPRM)

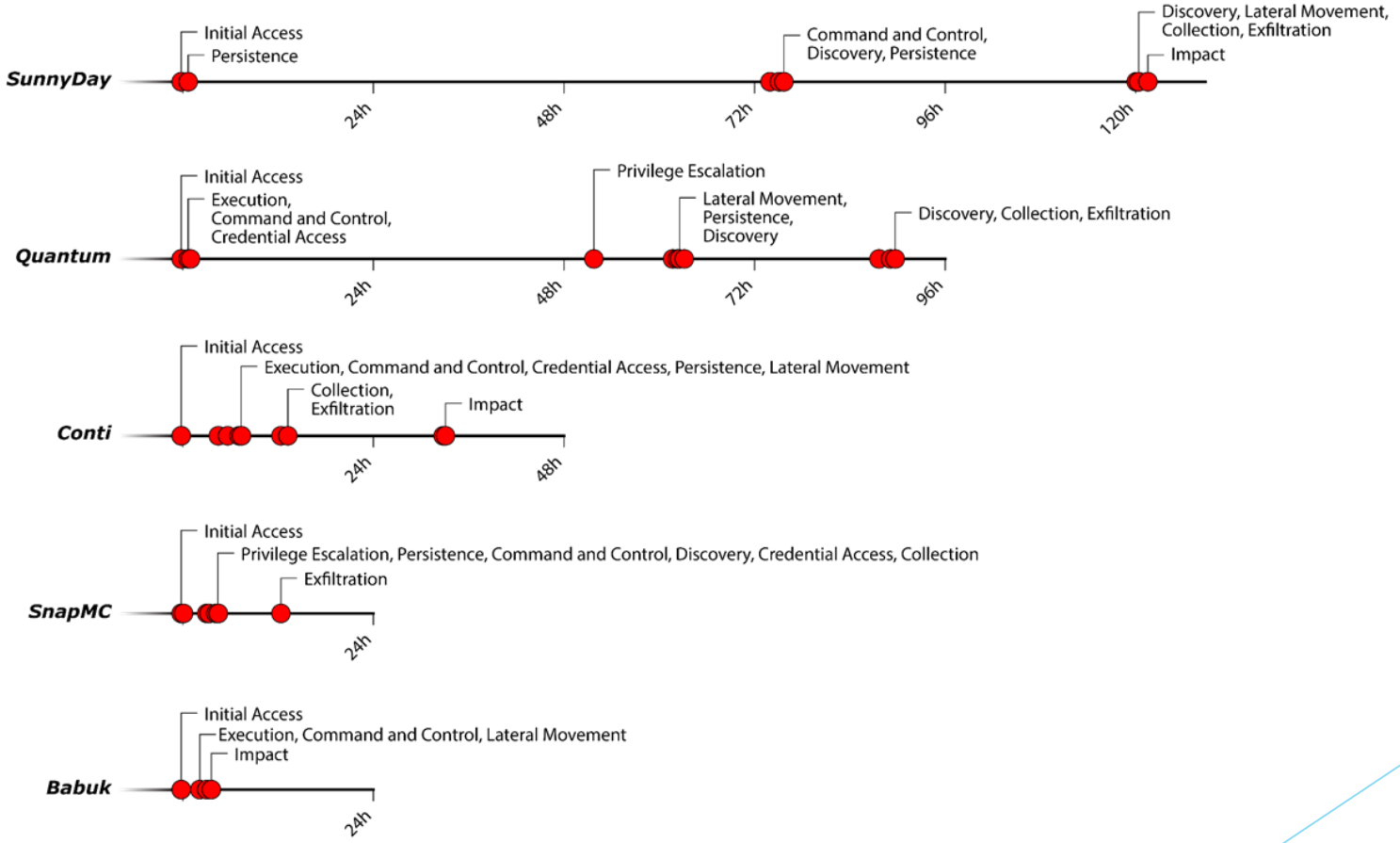
Dynamics of cybercrime

Perpetrator:

- No skills
- Simultaneous execution
- High degree of division of labor

Victim:

- Determined by technology and degree of security care
- No link to perp in time and location
- No need to be a target…


SunnyDay
Initial Access
Persistence
Command and Control,
Discovery, Persistence
Discovery, Lateral Movement,
Collection, Exfiltration
Impact
24h
48h
72h
96h
120h
Quantum
Initial Access
Execution,
Command and Control,
Credential Access
Privilege Escalation
Lateral Movement,
Persistence,
Discovery
Discovery, Collection, Exfiltration
24h
48h
72h
96h
Conti
Initial Access
Execution, Command and Control, Credential Access, Persistence, Lateral Movement
Collection,
Exfiltration
Impact
24h
48h
SnapMC
Initial Access
Privilege Escalation, Persistence, Command and Control, Discovery, Credential Access, Collection
Exfiltration
24h
Babuk
Initial Access
Execution, Command and Control, Lateral Movement
Impact
24h

Ransomware business model

24 Bn turnover	50% in US	Average ransom 2019 $400k → 2020 $800k → 2023 $1.500k
Recovery costs have doubled in one years	32% pays, recovery 65%	Top 10 does not operate in RF

It is not a war…

- TECH - Computing power: Moore’s law
- ECONOMIC - Protectionism is on the rise
- LEGAL – CISOs are facing charges
- GEOPOLITICS – data souvereignty (Mario Draghi)
- AI – is a catalyst

AI Impact on cyber security

Offense

- LLM: chatbots, phishing emails
- Perimeter scanning, elastic search
- Firewall settings/system reaction

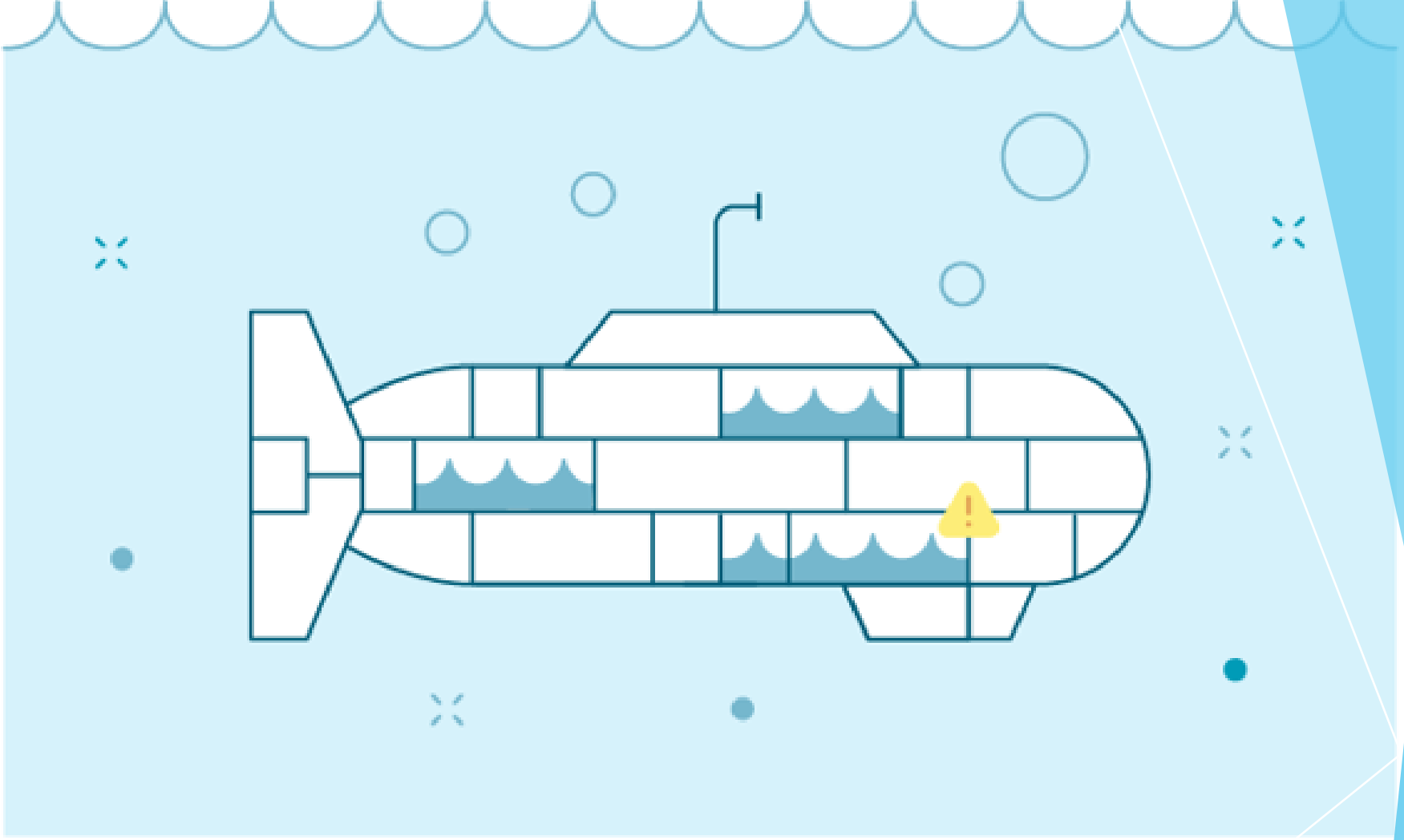
- Malware engineering
- Disinformation

Defense

- Spam filters
- Perimeter scanning, elastic search
- Anomaly detection, Rule writing for SOCs (XDR), Threat intel: APT signatures
- Reverse malware engineering
- …can we model sane decision making?

Challenge to society: sober up

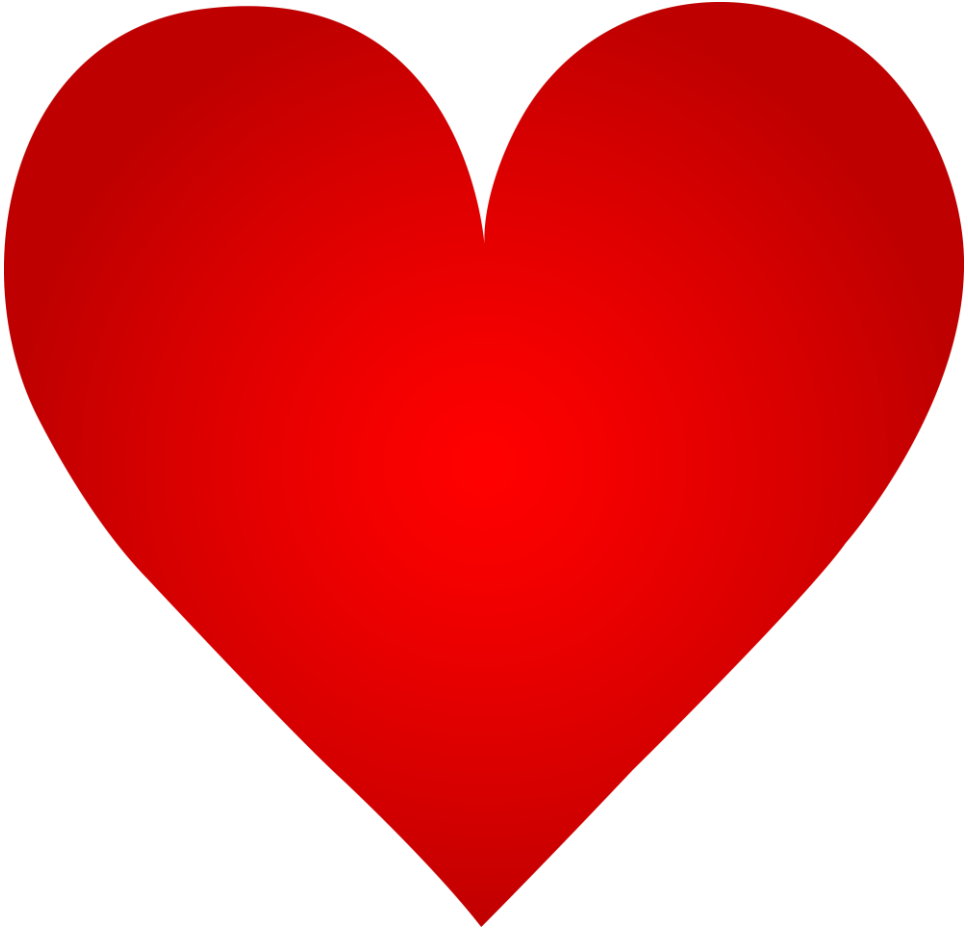
- Sobriety in applications/systems (CMDB, kill your legacy systems)
- Segmentation
- Data classification
- IAM: zero trust
- Compliance (NIS2, GDPR, DORA, AI act)



Human leadership is key

- Small span of control
- Mandate close to execution
- High degree of transparency & cooperation
- All talents welcome
- Fear, control **SPEED**
- Fuck ups are encouraged: assume breach….

- Assume humility

- Politics will not change
- Huge rise in inflation
- Human rights for the happy few
- Budget cuts in academia
- Rapid sequence of major, unsettling events

- Focus on your talent
- Be the best you can be
- Do not take responsibility for someone else's misbehaviour
- The fruit of your labor will save the world