

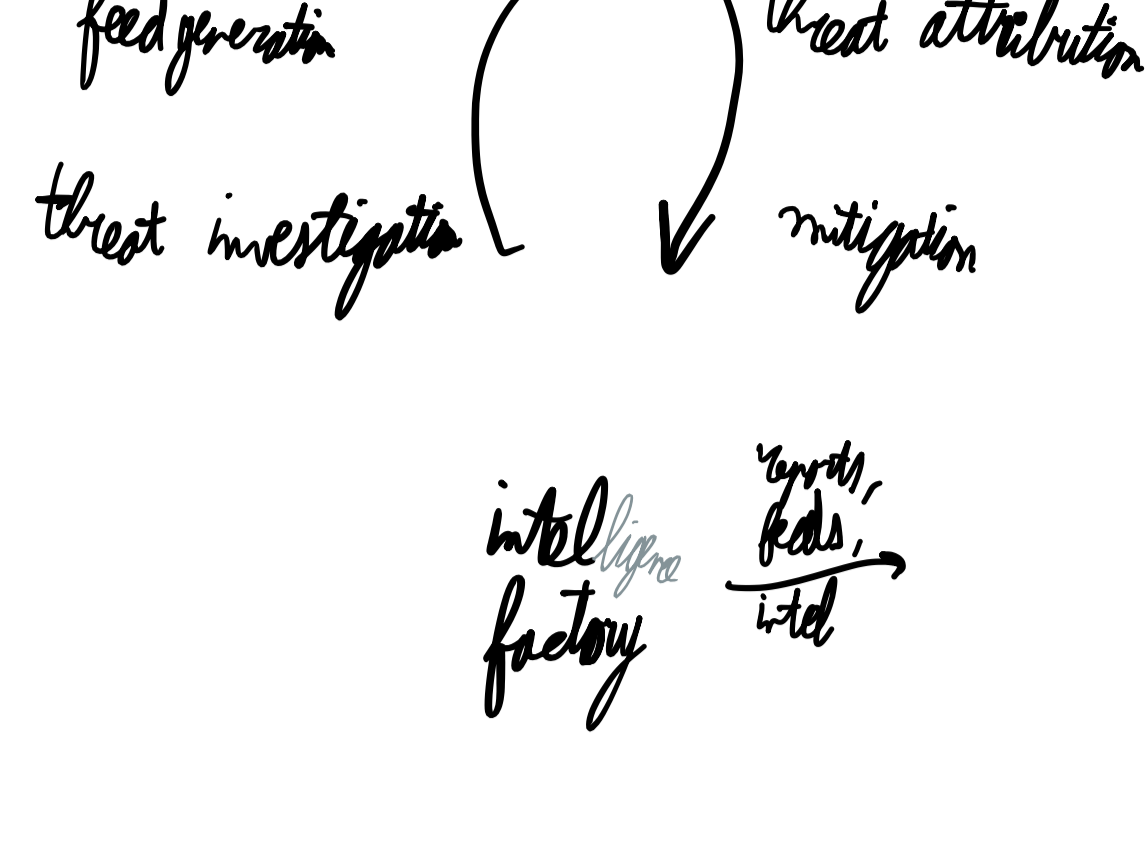
data comes from 'sensors'

UP = P 'kub' quite a bit of data => allows gathering information about devices

can use info to investigate what vulnerabilities might play a role

largest customer base: million devices

forensic: simulates behavior of devices to find out what attacks are being



knowledge is shared openly, initially because of open requirements from governments

getting access to actually used devices is sometimes difficult

e.g. actual PLC is probably not on Amazon

manufacturers make devices easy to install

everything called by default

many languages spoken -> threats come from many different backgrounds/countries

IT information technology *server, server computer, iPhone, ...*

first: focus on this

then: less so => OT security becomes important

OT operational technology

critical infrastructure
differs from IT

initial mindset: 'it has to work' -> security more like an accessibility threat

IOT internet of things

consumer IOT

enterprise/industrial IOT

IOMT internet of medical things

eventually: internet of everything

all things are connected

OTA: over the air update

IOT devices usually aren't

- agentable

and install software, manage software, update software

- manageable

difficult to retrieve information, apply changes, write their software

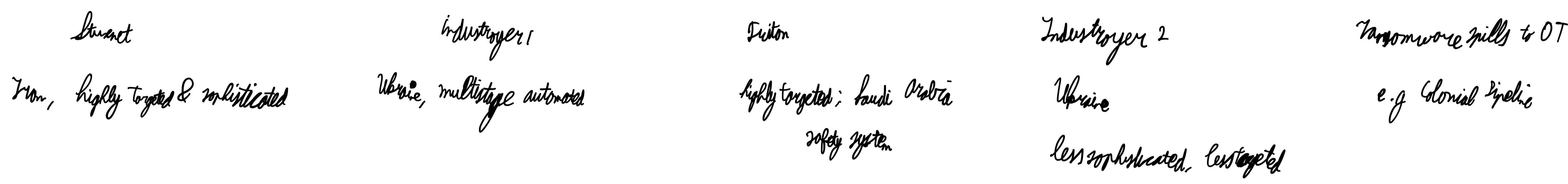
IP phones are common in companies

UPS = uninterruptible power supply

OT/IOT -> legacy, critical infrastructure, lack of authentication

are all more interconnected

kill chain -> roles such as technicians, initial entry, lateral movement



nation states -> criminals

key trends:

1. device landscape is changing
2. IOT devices used as entry points for attack
3. attackers want easy money

relevant threat actors depend on the target

attacker groups have very specific goals

most commonly targeted sectors

1. telecom
2. utilities
3. retail
4. manufacturing

most common targeted devices

1. SCADA
2. PLC / controllers
3. VoIP
4. routers
5. UPS

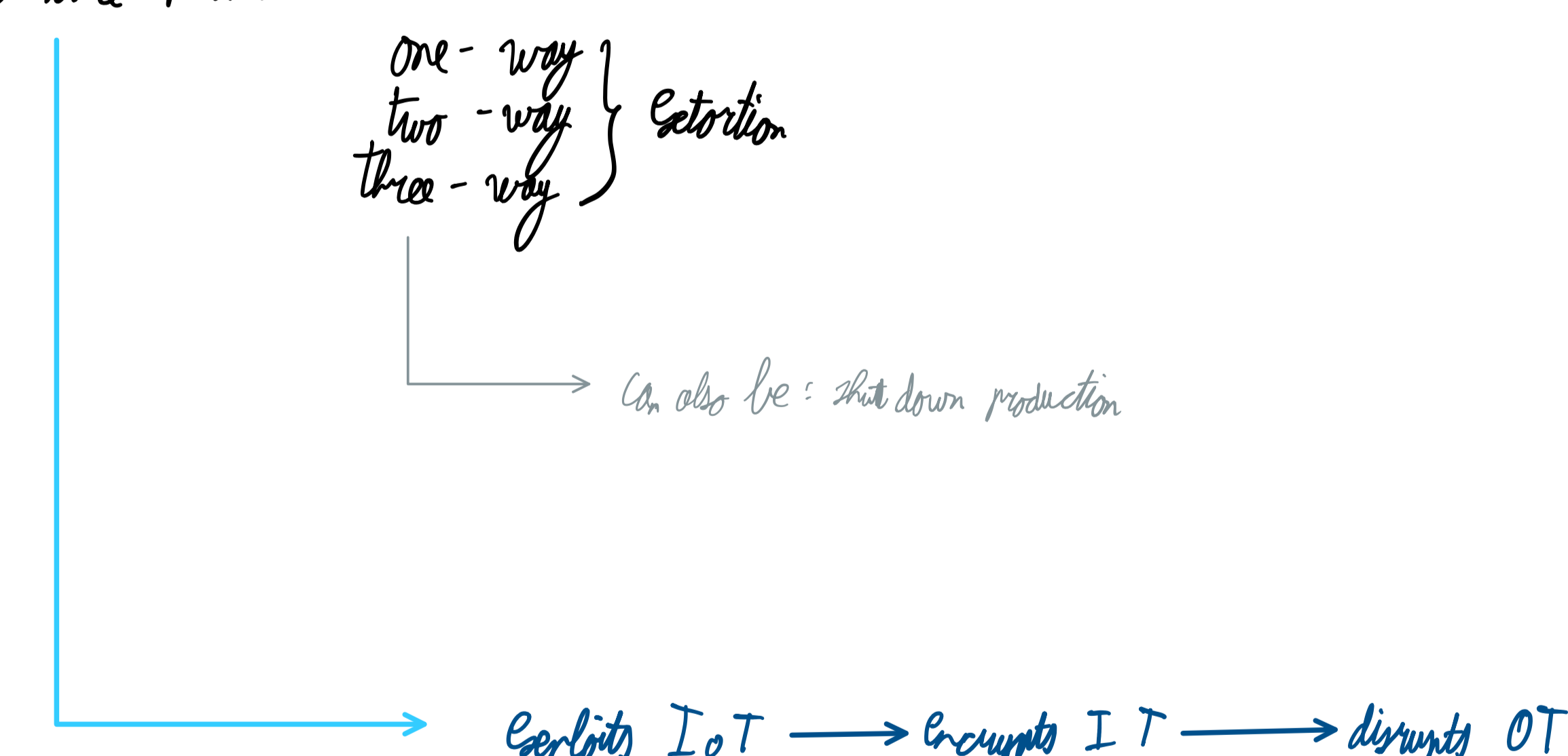
Criminal software as a service

ransomware as a service

default/weak credentials are still often used to get in

infsec is often not involved when IOT/OT devices are purchased

Transparency 4 IOT



1. exploit for initial access & persistence
2. WinRM or port forwarding, RDP credentials
3. SSH tunneling
4. drop & execute, discover exploit dump
6. exfiltrate & encrypt
8. network scan & DoS

published report -> later: similar attacks received in practice

2023 predictions:

- hacking groups
- state-sponsored
- critical infrastructure

observations:

1. attacks are not immediate and fully automated
2. cyberware-as-a-service means that hundreds of very similar attacks are happening
3. methods & techniques are well-known

NIST cybersecurity framework functions

identify

protect

detect

respond

recover