Lecture 6

dinsdag 29 november 2022 10:37

IoT : less care about security, updates, ...

also: less incentive to provide updates, since sale has already been made

spam botnet
DDoS botnet

Dyn DNS DDoS attack used IoT devices
Mirai botnet brute-forces telnet of IoT devices
which often have weak passwords

Ricoh myPrint : hardcoded credential 2018

one-time programmable lock/alarm

lack of liability

IoT device software is often made using possibly vulnerable copy-pasted code snippets

software bill of material

software supply chain attacks
hundreds of backdoored GitHub libraries

un-patchable devices
publicly exposed devices
vendor out of business

long & unknown devices
unknown vulnerable devices
unknown vulnerable vendors

IP camera
industrial controller
HVAC

fixing bugs in original software forks is difficult

SBOM: software bill of materials
list of components, so that vulnerabilities in those components can be fixed

how to detect/stop cyber-threats?

advanced attack : generates anomalies
phishing
C2 server communication
watering hole

disgruntled employee...

solutions risk business continuity

blocking/detecting attacks perfectly is impossible
false positives
false negatives opposite of 'detection rate'

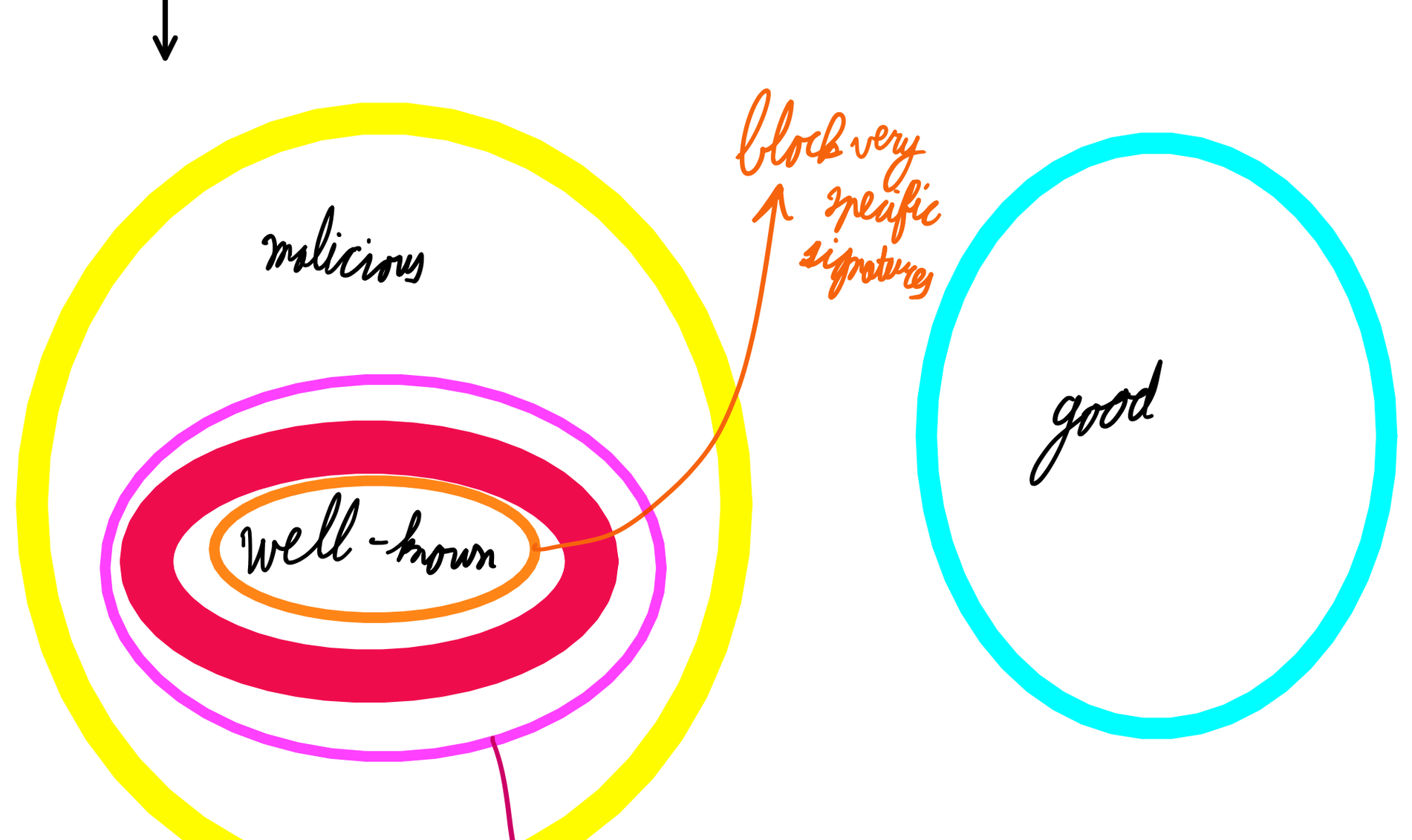
cost ≈ FP 1% ⇒ 1% of all events is raising a false alert (→ a lot!)
FN 1% ⇒ 1% of all attacks is not raising an alert

already finding 50% of attacks is very good especially since attacks consist of multiple stages, any one of which has to be detected

rejection-based : negative model / blacklisting / signature-based system / anti-virus
acceptance-based: positive model recognizes normal behavior

everything outside is considered anomalous

whitelist



blacklisting :

- signatures : when part of payload is known → problem when malware is changed slightly
  only works for known attacks (often: commonly occurring)
  requires frequent maintenance
  low-cost
  low false positives
  takes long time to update/generate signatures that give good coverage
  works in reconfigured system; systems change, but attacks do not
  → usable as blocking system
- heuristics : NOP sled in code
  UNION in web application form

alternatives to blacklisting
whitelisting manual
anomaly detection automatically

main difference: configuration
detection (boolean/threshold)

whitelisting can be done at different levels:
firewall
web-application firewall
ICS systems → gateways

different levels of accuracy

maintaining whitelisting is a pain in the neck

whitelisting can detect unknown attacks
but is
expensive
difficult to maintain
easy to circumvent unless there are many false positives
and gives little information about the attack

anomaly detection
flow based
? based

quantitative anomaly detection traffic amount
qualitative anomaly detection individual packets analysis

systems often have unpredictable behavior → anomaly detection is inaccurate