Requirements from user's point of view of AI empowered security services

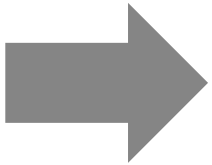
Paul Kwon (YoungMok Kwon)

CEO & Solutions Architect // PAGO Networks, Inc.

21.Jan.2019

Recent years …

Applying Machine Learning



Real World Environments of Endpoints Cyber Security

Types of Endpoints … to apply ML

Desktop

Laptop

Server

POS

ATM

KIOSK

Medical PC

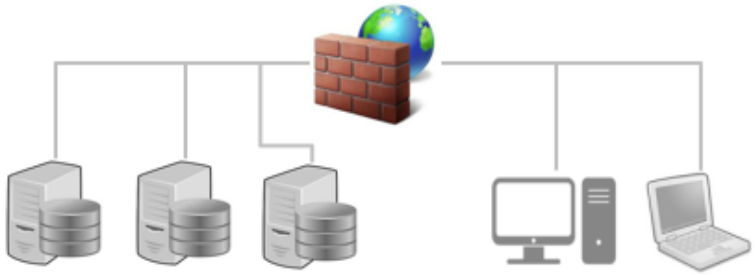
FA / Industrial PC

Types of OS ... to apply ML

Linux

Locations of endpoints ... to apply ML

Physical



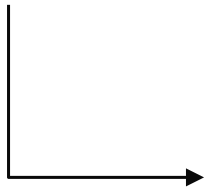
VDI

Cloud

Preventing the attacks from …

MALicious Files

MALicious Activities



with File-based Attack

File-less Attack

Found …

Already Lots of multi-layered technologies

- Signature
- Heuristics
- URL Blacklists

Usually preventing for Known MALxx

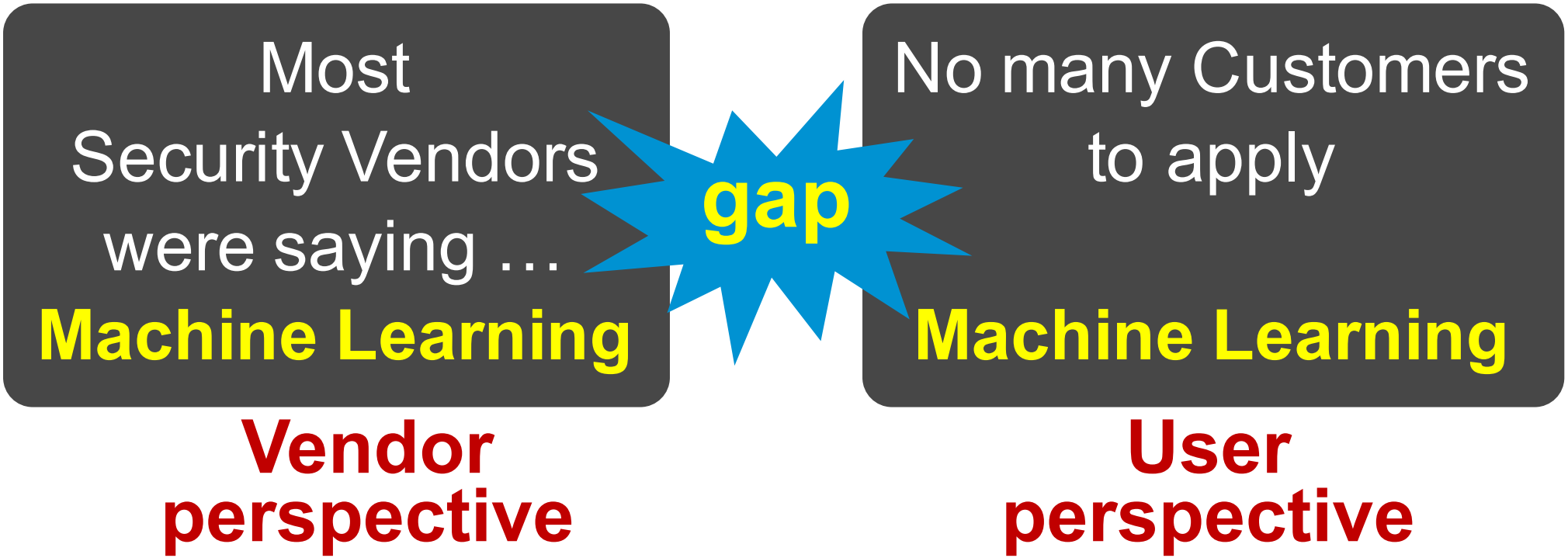
- Behavior Analysis
- Reputation Monitoring
- Anti-Exploit
- Cloud-Sandbox

Usually preventing for Un-known MALxx

- **Machine Learning**

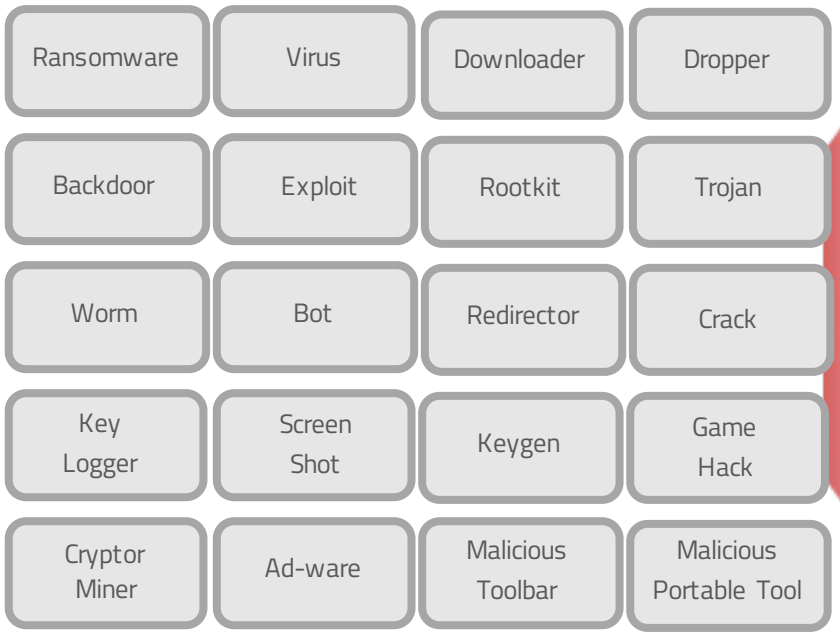
Let’s have a look at ML …

Gap and Not easy to apply ML for endpoints



Why … gap

Asked… what would you like to expect ?



Machine Learnging

regardless of
known & unknwon,

Make
prevention rate
Higher
than before.

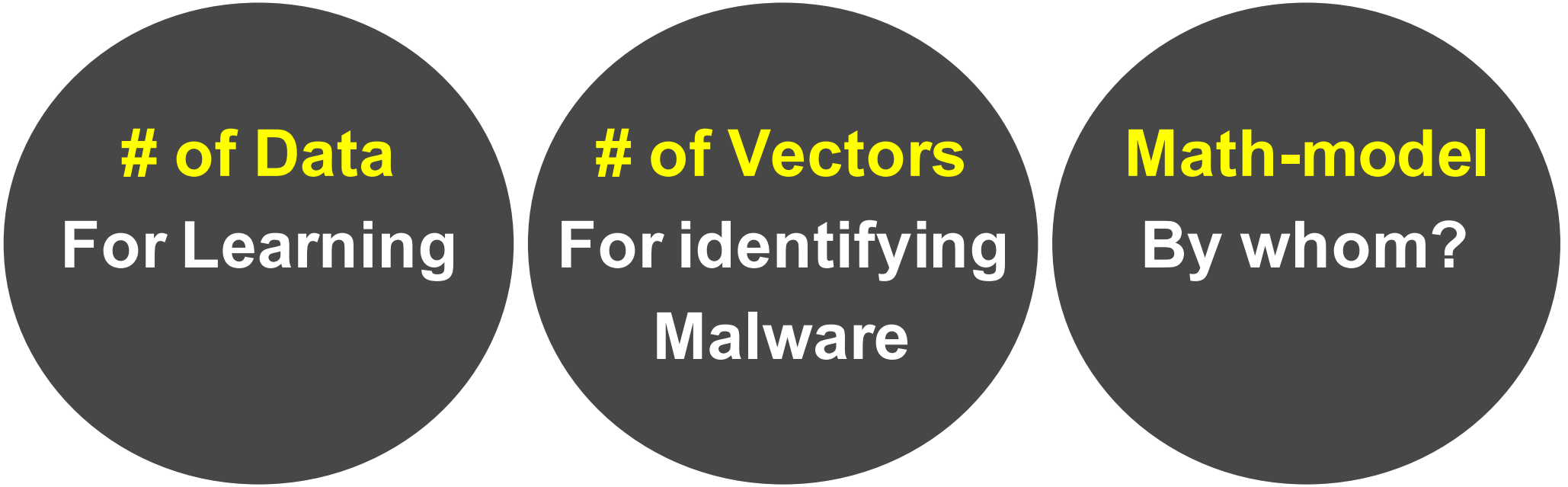
Asked … what is the obstacles ?

(A-1) Don’t know where ML will be applied

ML – **NTA**	ML – **Cloud**	ML – **Endpoint**
Network Traffic Analysis	Send data & get IOC	Math Model Is at endpoints

Asked … what is the obstacles ?

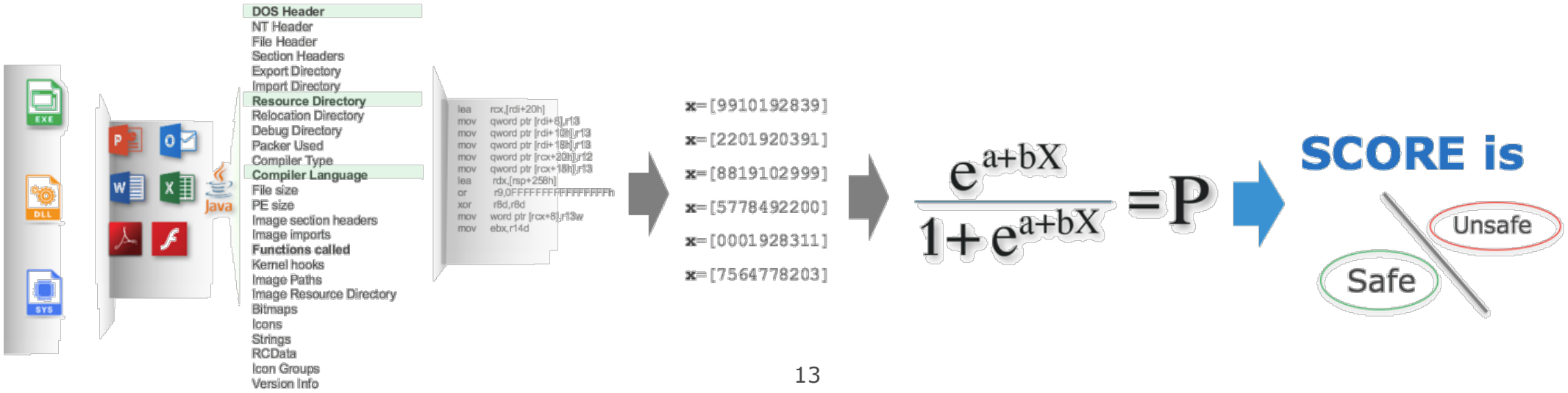
(A-2) Don’t know difference of each ML
Don’t know the mature level of ML



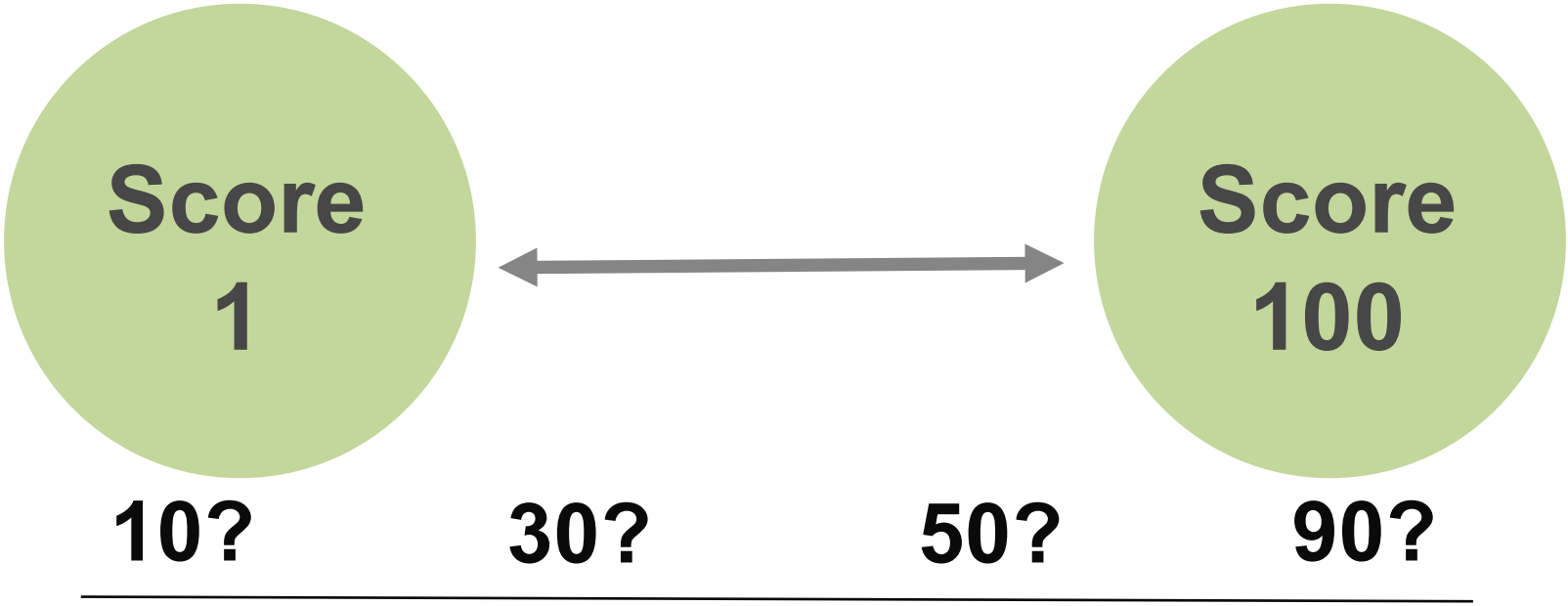
Asked … what is the obstacles ?

(A-3) Don’t know on how ML exactly works

Learning → Vectors → Math Model → “Scoring // Prediction”



Then … What "Score" should be prevented



Too Difficult.

Vendor says "It's the end-user's role"

End user should …

Prevent from

Score 1

Nobody knows what score?

Attacker applied

Lower Score

Then… What the result is.

“Scoring // Prediction” means …

User perspective

“It looks like malware”

- Real malware ?
- Exact information of malware ?

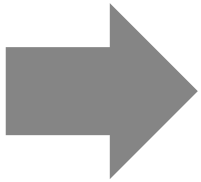
“It can be ...”

- False Positive ?
- False Negative ?

ML Technology is focusing on …

Increasing "Accuracy Rate"

- for lower false positive
- for lower false negative



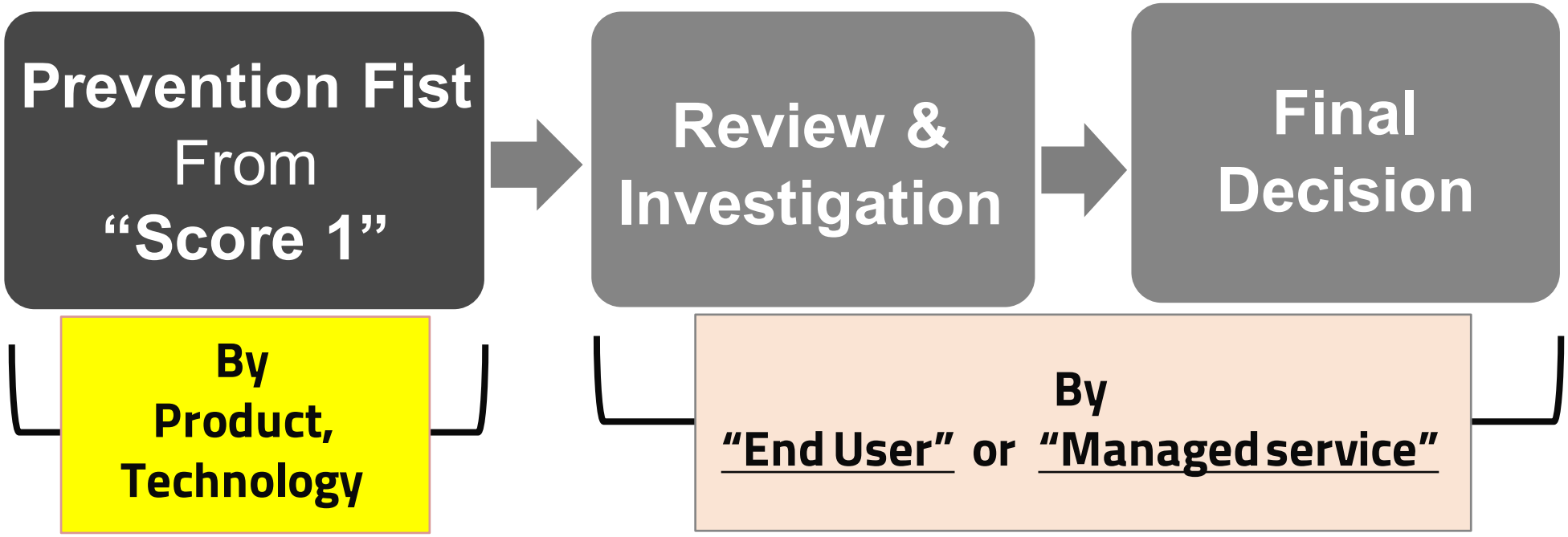
We know, Really Important

But, with the user perspective,

- still "It looks like malware"
- because of "Scoring / Prediction" technologies

To apply ML … to real world,

SHOULD apply NEW PROCESS



Requirement - Prevention First

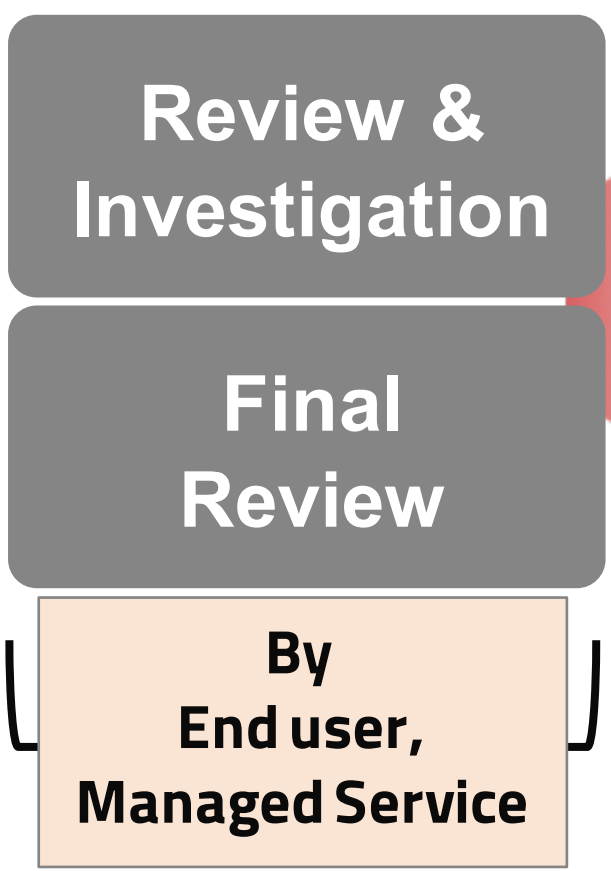
Accuracy

- Lower false positive
- Lower false negative

More evidence for scoring

- Static analysis
- Dynamic analysis
- IOC
- Threat intelligence
- Classification / Category

Requirement – Review, Final Decision



Need Experts or Services

- Dedicated IR (Incident Response)
- Review all “scored files”

Summary – user's perspective

Endpoint Cyber Security

With ML

- In a cyber security, ML is **NOT "AlphaGo / Alpha Zero"**
- ML needs a new process to apply
- ML assits Experts, need Experts & co-work with Experts
- Doesn't think ML is the normal policy-based product
- "Scoring" by ML should be treated as "Incident"
  so, Incident should be reviewed & investigated
- Need more IOC integration
- Need more threat intelligence integration
- More accurate math-model for responding new threat
- Next step for endpoint security is "Unsupervised" ML & DL

Thank You