

## Al has been part of the toolbox for 15+ years

2009: Detection - NBA/NBAD

2015: Detection & Threat Intelligence - Security Analytics

2020: Detection & Response - SOAR/Automation

2023: Extended Detection & Response - XDR, Analyst Augmentation

SecOps is all about removing UNCERTAINTY (who, what, where, why)

Traditional AI started with hardest detections first: UNKNOWN-UNKNOWN

Later shifting towards more of KNOWN-UNKNOWN

Challenges: lack of training data, rare events, zero-shot learning

Breakthrough in detections around 2019 with MITRE ATT&CK framework

Generative AI entering in 2023, boosting the analyst, but watch out for adversaries!



## AI/ML is deeply embedded in the Security Stack

**Detection: LLM+NLU in Email Security** 

Malware Detection / Threat Intelligence: ML generating rules and IOCs

Classification: MITRE ATT&CK TTP attribution

Prioritization: Kenna Vulnerability Risk, XDR Incident Risk

Response Recommendations: User actions prediction

Analyst Augmentation: Incident summarization, LLM dialog



## Shift the focus to outcomes

XDR-driven outcomes

**Detect** sooner

Where are we most exposed to risk?

How good are we at detecting attacks early?

Prioritize by impact

Are we prioritizing the attacks that represent the largest material impacts to our business?

Speed up investigations

How quickly are we able to understand the full scope and entry vectors of attacks?

Accelerate response

How fast can we confidently respond?

How much can SecOps automate?

Are we quantifiably getting better?





## The alert prioritization in Cisco XDR saves us a ton of time and helps us investigate the most important issues first!

Lead Developer and Division Lead for Programming, Large Enterprise

