

VECTRA[®]

VECTRA AI

Warum moderne Security ohne AI nicht möglich ist!

27.03.2025



PRESENTING



TOBIAS GROND

Regional Sales Manager, Vectra AI

DAS UNTERNEHMEN VECTRA AI



Customer First, Partner Centric

- + Founded 2011, Privately held
- + Headquartered in San Jose, CA
- + 580+ employees
- + 113 countries
- + 3 Global SOCs
- + >1100 customers
- + >\$100M ARR



AI Driven

- + Research + Data Science + Engineering
- + 150+ AI-driven attacker behavior models
- + 35 patents in AI-driven threat detection
- + Most referenced vendor in MITRE D3FEND (11)
- + Cover >90% of MITRE ATT&CK techniques



WAS KUNDEN MÖCHTEN

See and stop cyber-attacks
before they become breaches

HERAUSFORDERUNGEN AUS SICHT DER KUNDEN

- > **More attack surface**
63% are forced to cover a larger attack surface
- > **More visibility gaps**
75% lack the visibility they need to confidently cover
- > **More hidden threats**
97% worry about missing a real attack hidden in alerts
- > **More alert workload**
90% can't keep pace with 4484 alerts per day
- > **More talent shortage**
67% considering or actively leaving their job

The
Defenders'
Dilemma





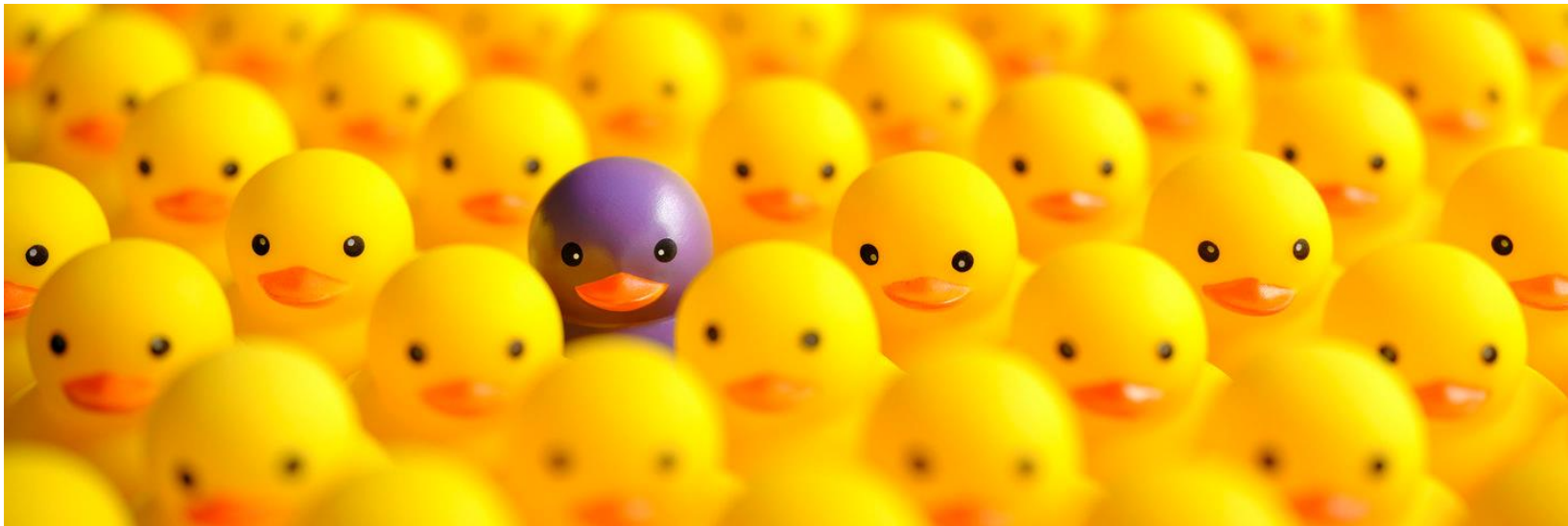
VECTRA[®]

WIE FINDET MAN ANGREIFER?

WENN ES NUR SO EINFACH WÄRE...



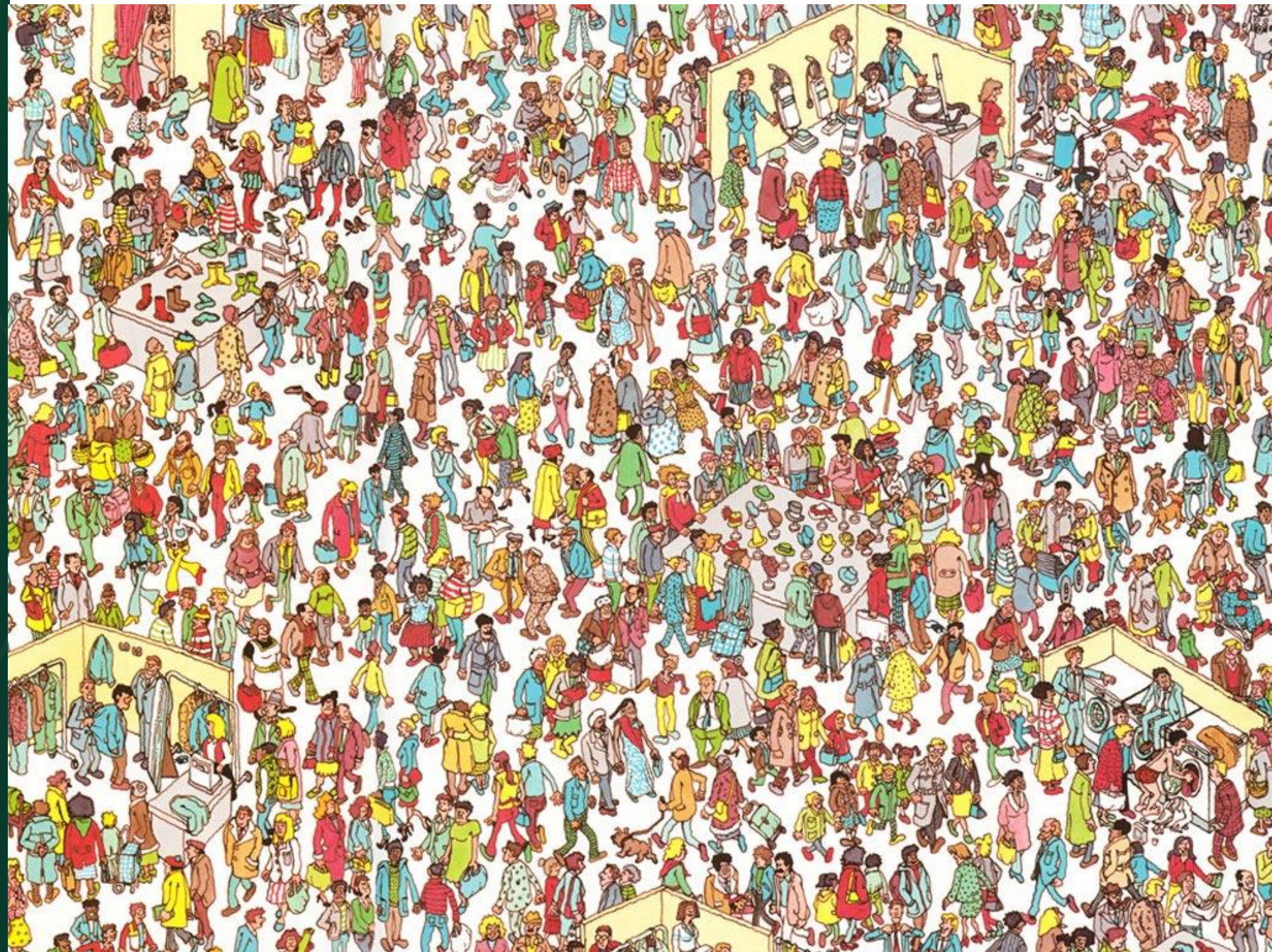
UNTERSCHIEDLICH ≠ SCHLECHT



SCHLECHT ≠ UNTERSCHIEDLICH



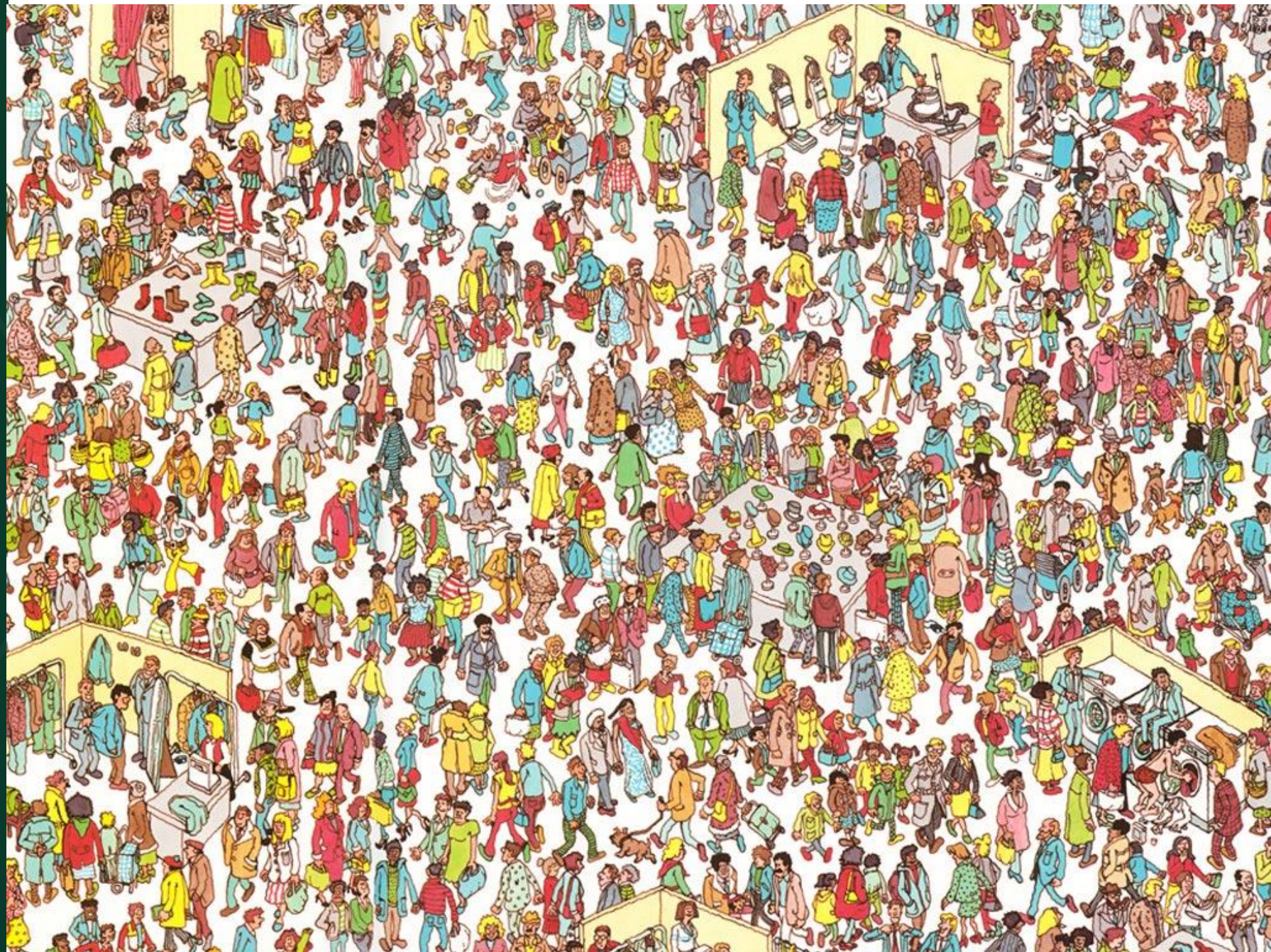
BIG DATA



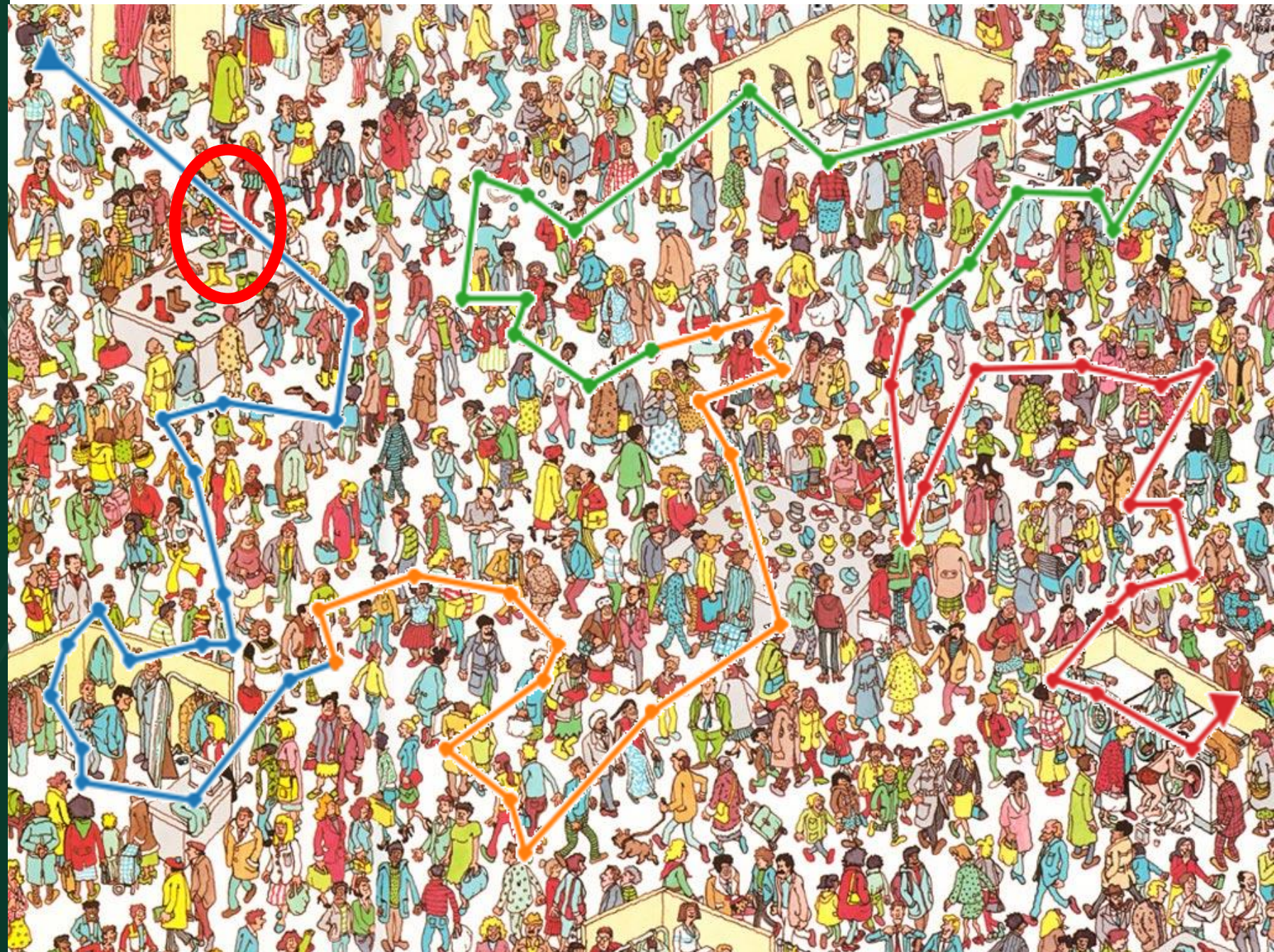
Was suche ich?



Welche Daten brauche ich?



Anwendung des Algorithmus



THE ONLY AI OPTIMIZED TO DETECT ATTACKER METHODS

1

Analyze **attacker methods**

MITRE | ATT&CK®

Per-domain analysis enables deep coverage

2

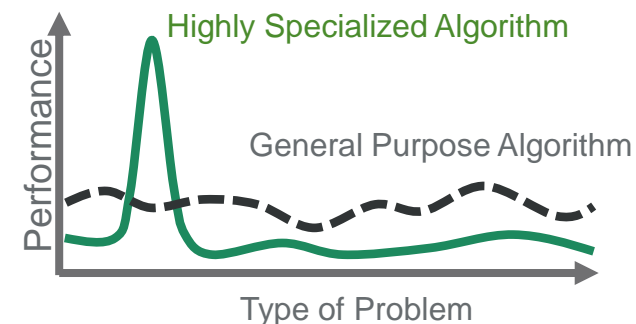
Define **countermeasures**

MITRE | DEFEND™

Define techniques to detect attack methods

3

Use the **optimal ML** approach for each

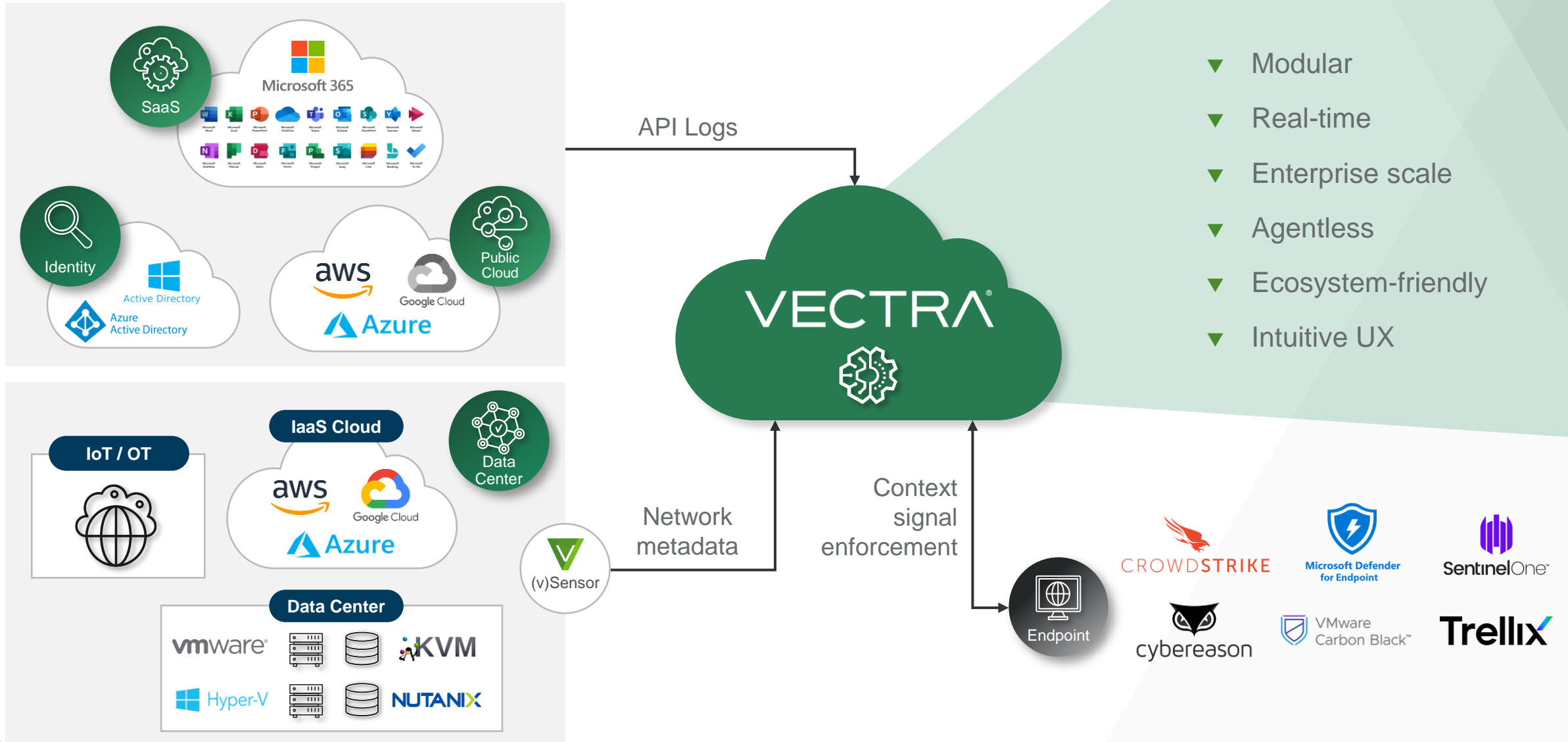


Security-led approach to AI

Powered by cutting-edge ML

Outcome: higher coverage, lower noise vs simple anomaly-based detection

VECTRA AI PLATTFORM ARCHITEKTUR



- ▼ Modular
- ▼ Real-time
- ▼ Enterprise scale
- ▼ Agentless
- ▼ Ecosystem-friendly
- ▼ Intuitive UX

DAS BESTÄTIGEN AUCH UNSERE KUNDEN

"Mit Vectra dauert das, was früher Monate dauerte, jetzt nur noch Minuten."

"Vectra gibt uns einen Hinweis auf die Dinge, die wir wollen."

"Bei den kritischen Warnungen ist ein enormer Rückgang zu verzeichnen, 80 % weniger."

"Vectra sagt uns, welche Dinge wir priorisieren müssen - wir reduzieren unsere Arbeit von 1000 Warnmeldungen pro Tag auf 10."

"Wir haben die Zeiten für die Erkennung von Bedrohungen von mehreren Tagen auf wenige Minuten verkürzt."

"Vectra hat unsere Effizienz erhöht und die Zeit, die wir brauchen, um auf Angriffe zu reagieren, um etwa 50 Prozent reduziert."

"Vectra hat die Workload unserer Mitarbeiter um 200 Prozent reduziert."

"Vectra filtert 99 Prozent der Alerts heraus, die wir sonst bearbeiten müssten."

"Anstatt Tausende von Warnmeldungen zu erhalten, bekommen wir nur noch 2 bis 3 pro Tag. Wir verschwenden keine Zeit mehr mit 'false/positive's'."

VECTRA®