SCHOELLER
NETWORK CONTROL

Security Operations 2023

Anhand des „HypeCyle“ von Gartner

Guarding your security

SCHOELLER

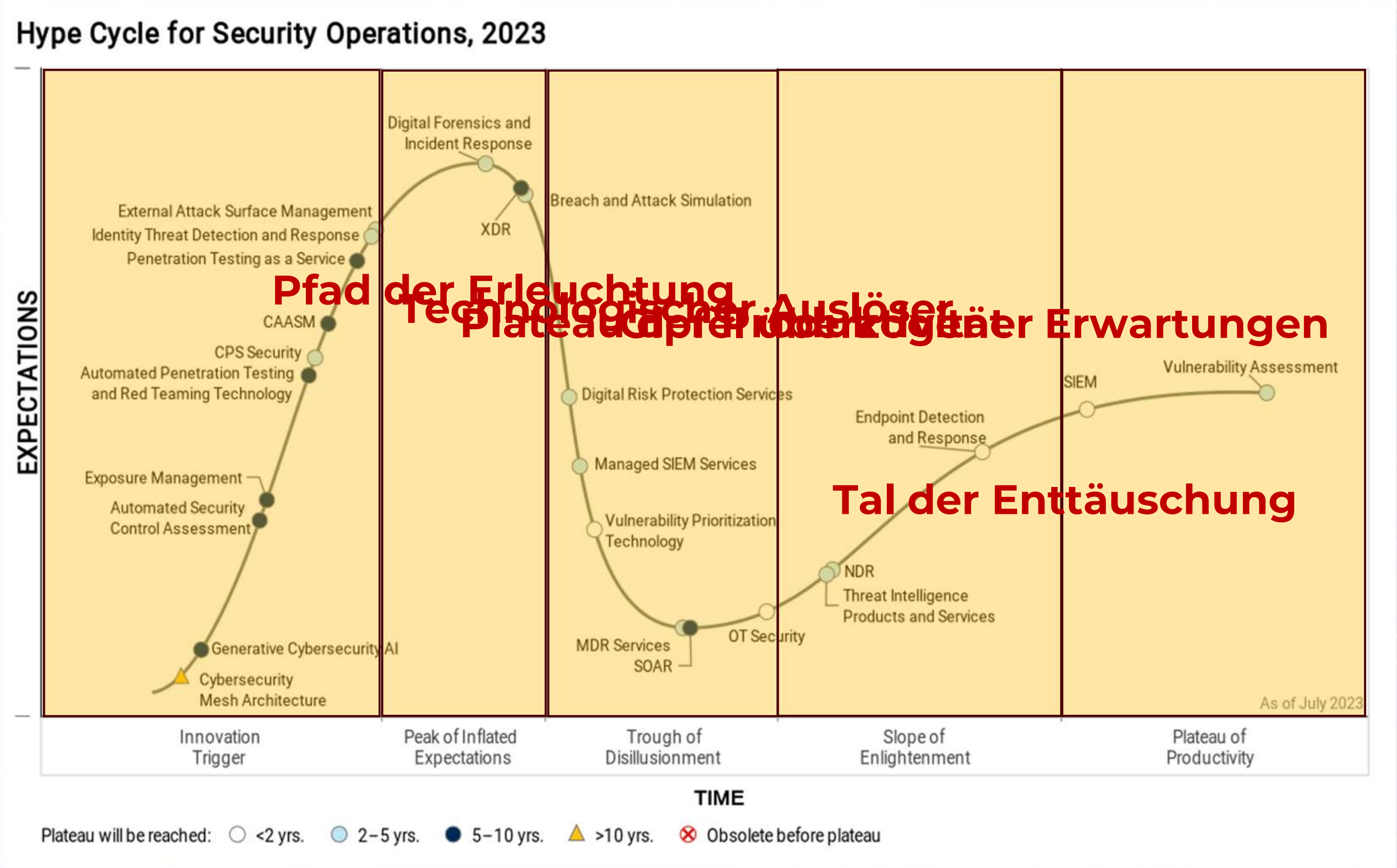
SCHOELLER
NETWORK CONTROL

Guarding your security

Franz Großmann

Geschäftsführer

Die „Hochschaubahn“ der Technologiebranche



Gartner.

SCHOELLER

Ständig neues „Zeugs“!?

XDR	Extended Detection & Response
CAASM	Cyber asset attack surface management
ITDR	Identity threat detection and response
EASM	External attack surface management

So manches stirbt auch einen leisen Tod!

CASB
2012- 2023

This year, the Hype Cycle for Security Operations saw the **retirement** of one innovation, cloud access security broker **(CASB)**. It has been ultimately consolidated into the security services edge (SSE) primarily due to its integration with secure web gateways (SWG) and zero trust network architectures (ZTNA), which are part of SSE.

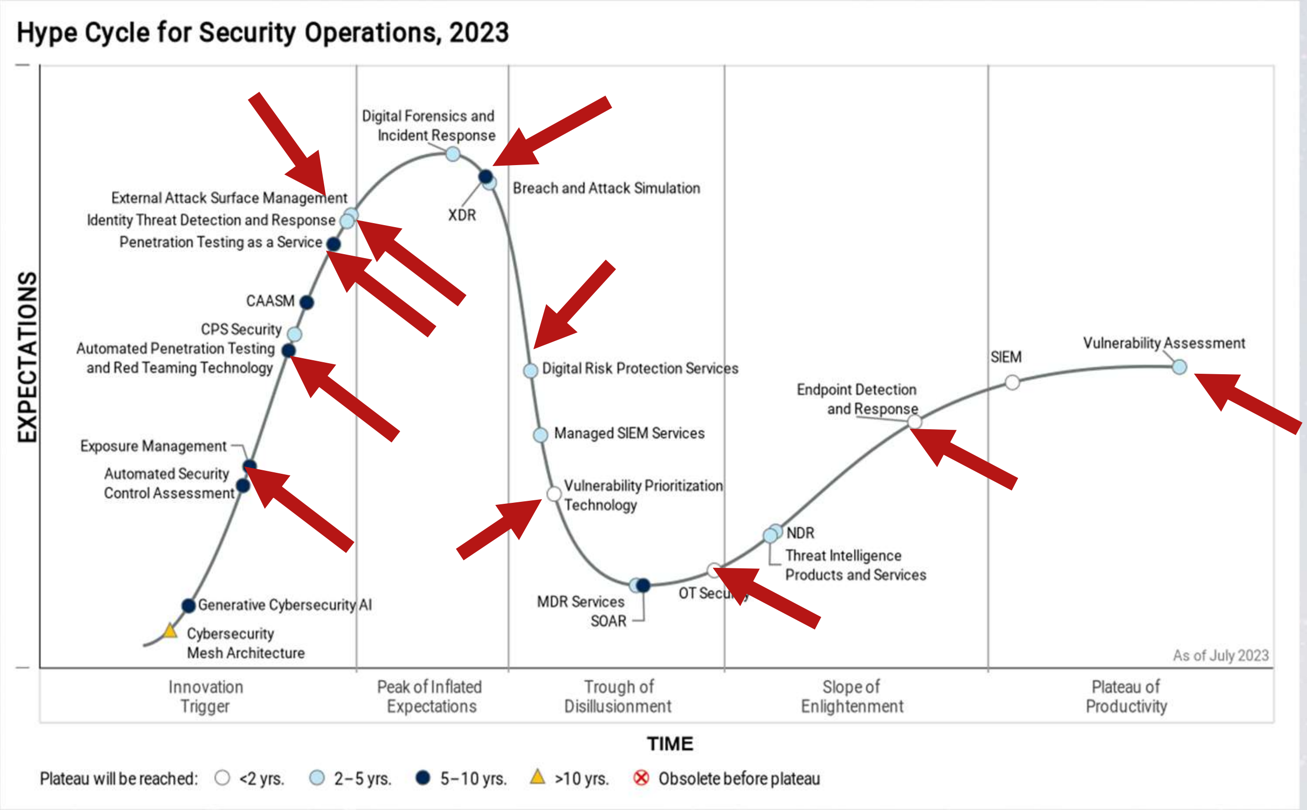
Worum geht es nun tatsächlich?

As we **know**, there are **known knowns**.
There are things we **know** we **know**.
We also **know** there are **known unknowns**.
That is to say we **know** there are some things we do **not know**.

But there are also unknown unknowns.
The ones we don't know we don't know!

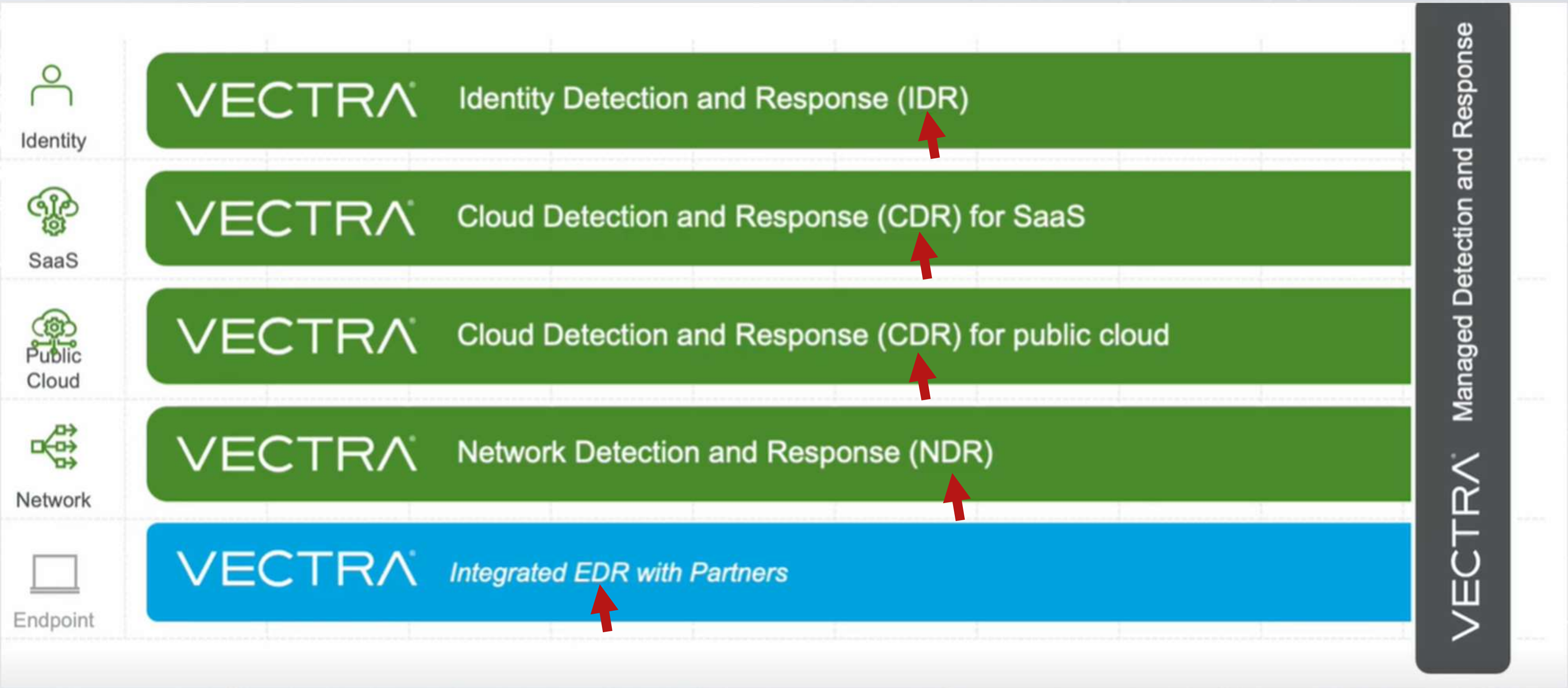
D. Rumsfeld during a Pentagon news briefing in February 2002

1.) Visibility → Assets, Angriffsflächen und Schwachstellen kennen!



Gartner

2. Detection → Erkennen von Vorfällen



Identity — VECTRA Identity Detection and Response (IDR)

SaaS — VECTRA Cloud Detection and Response (CDR) for SaaS

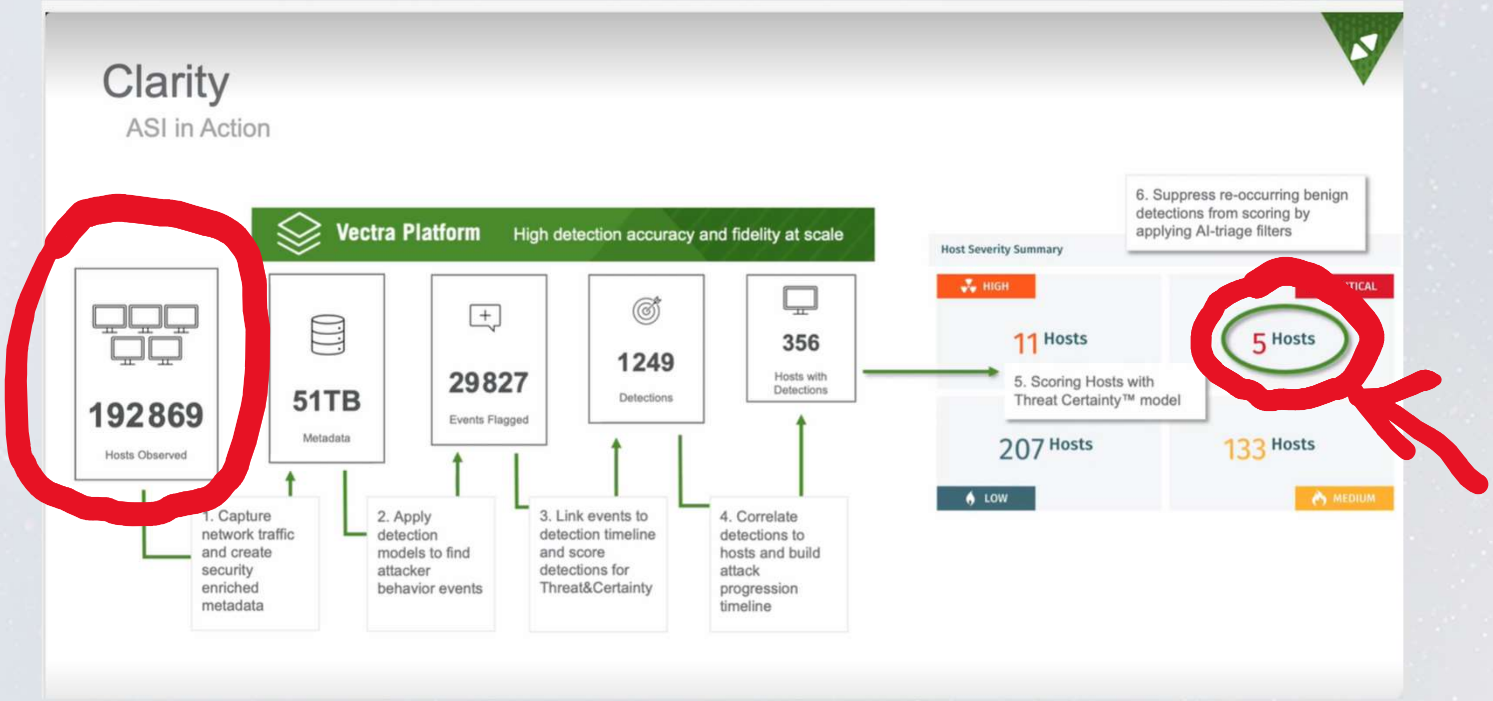
Public Cloud — VECTRA Cloud Detection and Response (CDR) for public cloud

Network — VECTRA Network Detection and Response (NDR)

Endpoint — VECTRA *Integrated EDR with Partners*

VECTRA Managed Detection and Response

2.1 Detection → Erkennen tatsächlicher Angriffe



Clarity

ASI in Action

Vectra Platform High detection accuracy and fidelity at scale

192869 Hosts Observed

51TB Metadata

29827 Events Flagged

1249 Detections

356 Hosts with Detections

1. Capture network traffic and create security enriched metadata

2. Apply detection models to find attacker behavior events

3. Link events to detection timeline and score detections for Threat&Certainty

4. Correlate detections to hosts and build attack progression timeline

5. Scoring Hosts with Threat Certainty™ model

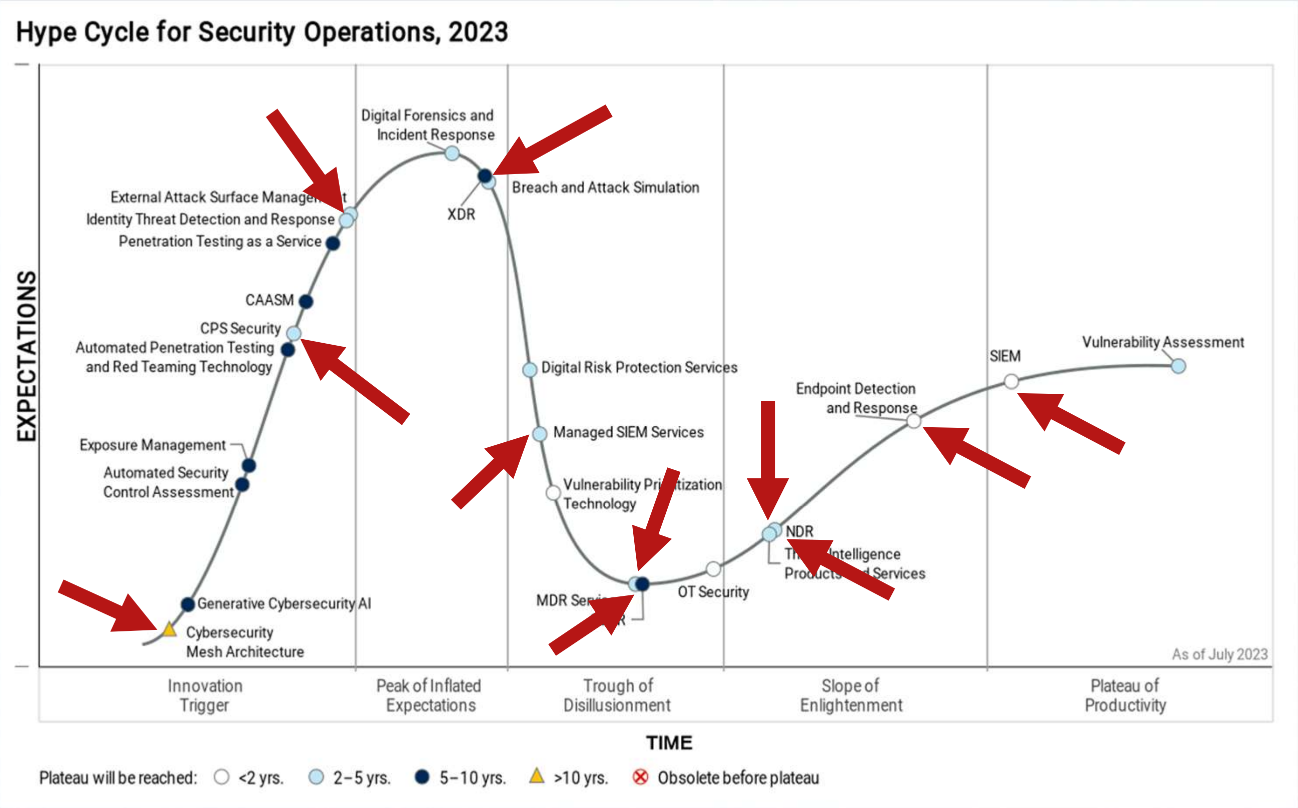
6. Suppress re-occurring benign detections from scoring by applying AI-triage filters

Host Severity Summary

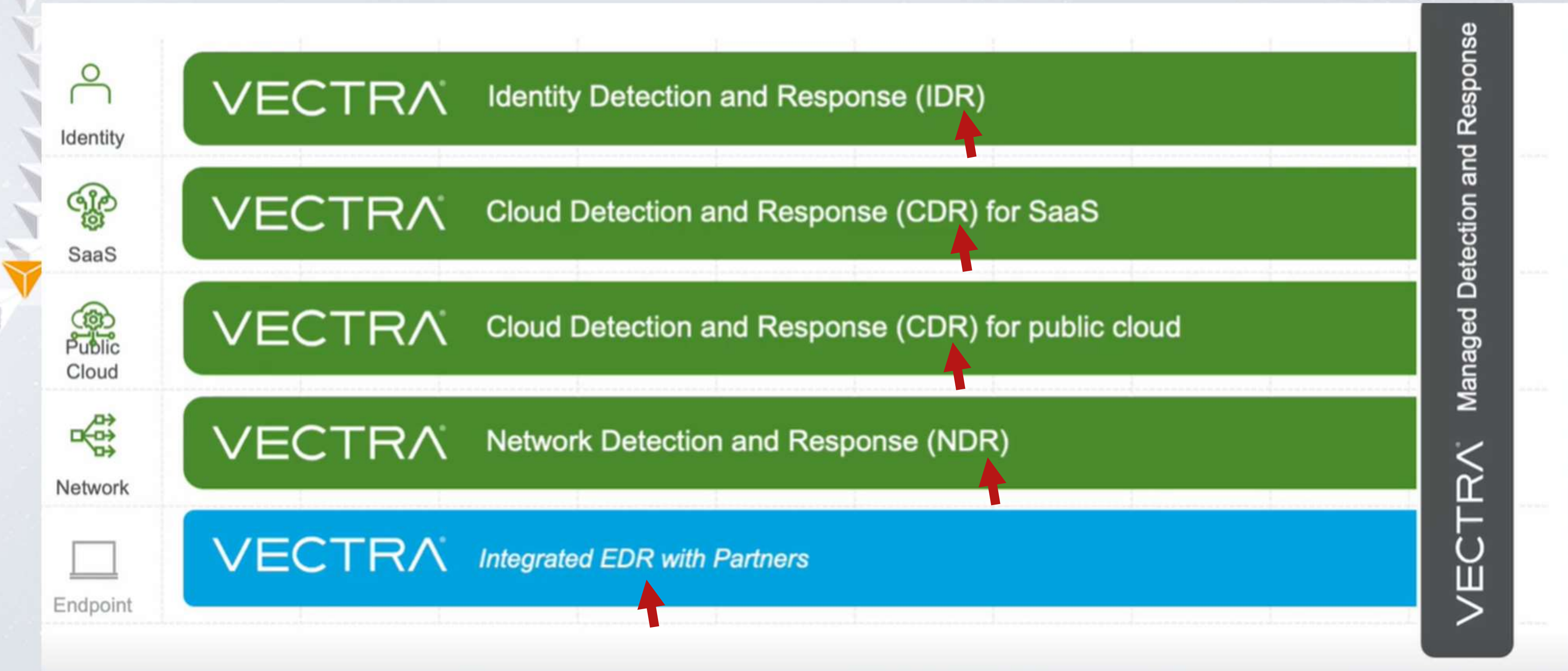
HIGH: 11 Hosts	TICAL: 5 Hosts
LOW: 207 Hosts	MEDIUM: 133 Hosts

SCHOELLER

2. Detection → Erkennen von Angriffen



3. Response → Reaktion und Wiederherstellung



Identity – VECTRA Identity Detection and Response (IDR)

SaaS – VECTRA Cloud Detection and Response (CDR) for SaaS

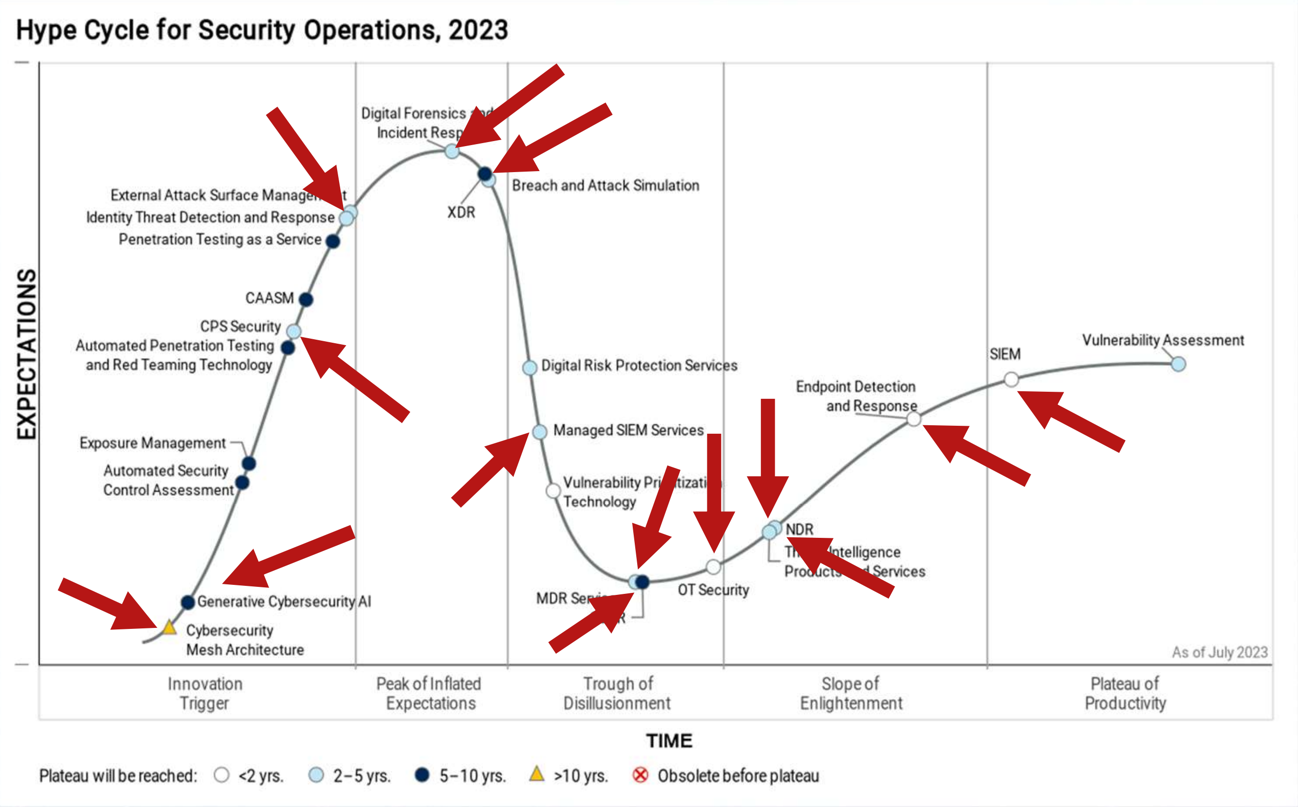
Public Cloud – VECTRA Cloud Detection and Response (CDR) for public cloud

Network – VECTRA Network Detection and Response (NDR)

Endpoint – VECTRA *Integrated EDR with Partners*

VECTRA Managed Detection and Response

3. Response → Abwehr und Wiederherstellung

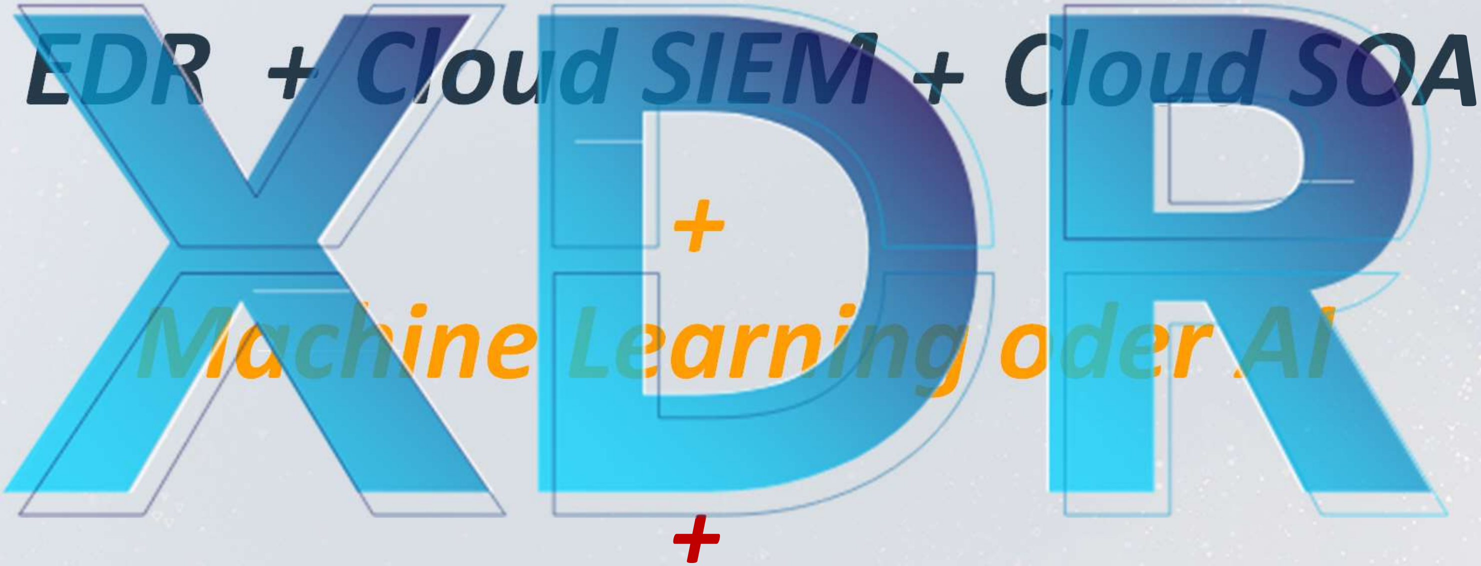


Hype Cycle for Security Operations, 2023

Gartner

Also, man nehme

Et voilà !



EDR + Cloud SIEM + Cloud SOAR

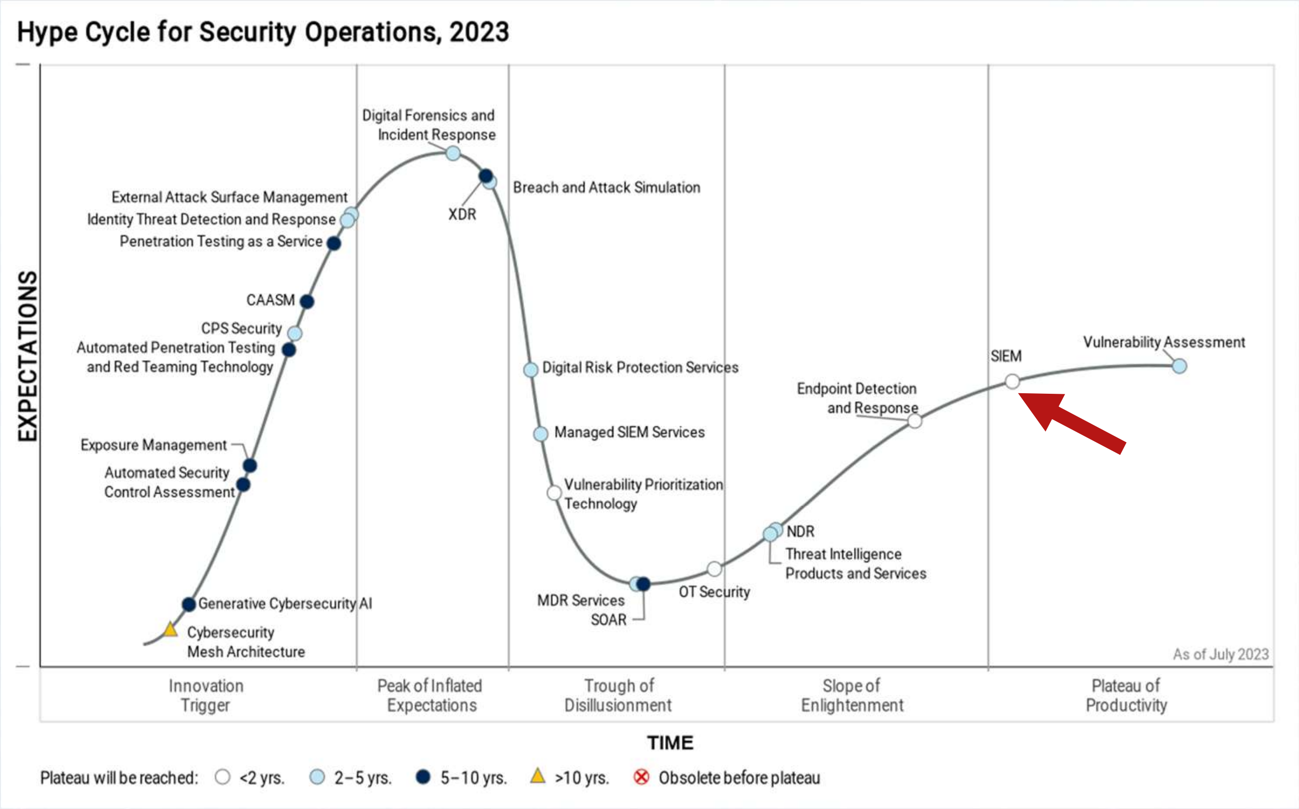
+

Machine Learning oder AI

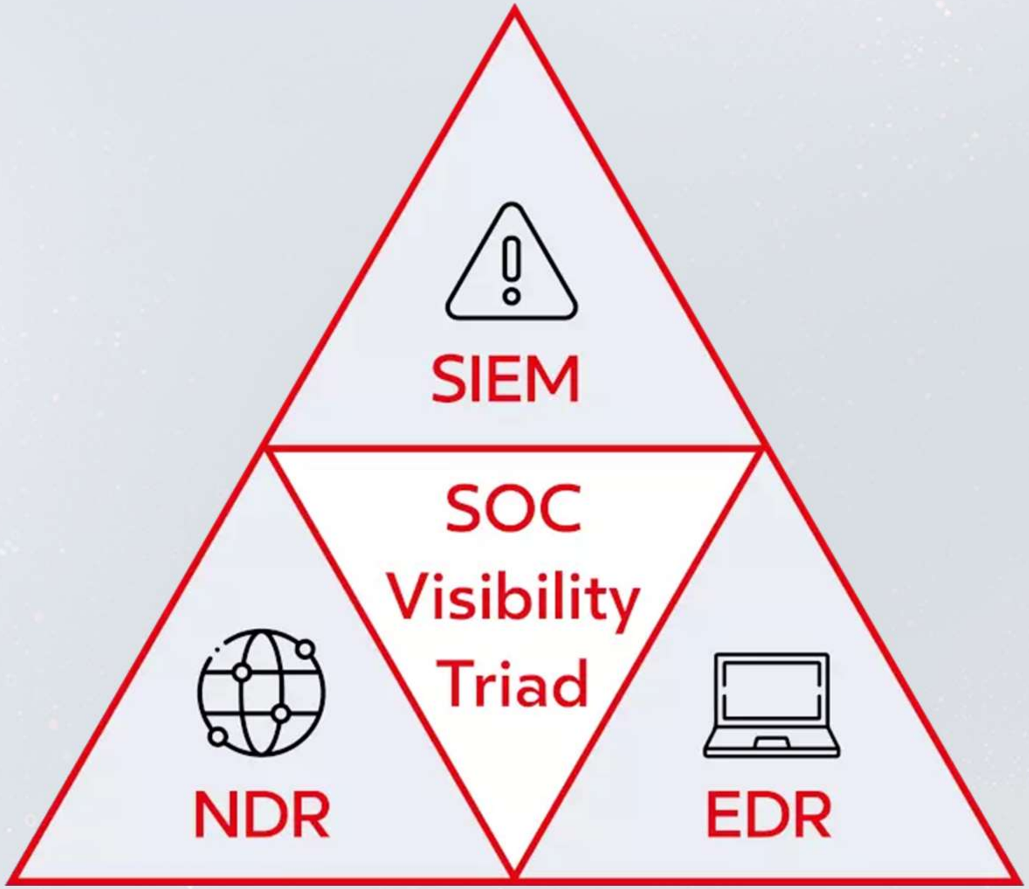
+

Feenstaub!

3. Response → Abwehr und Wiederherstellung



Gartner



1. ***Visibility***
2. ***Detection***
3. ***Response***

NETWORK CONTROL

Guarding your security