Vectra Webinar
24. September & 3. Oktober 2019

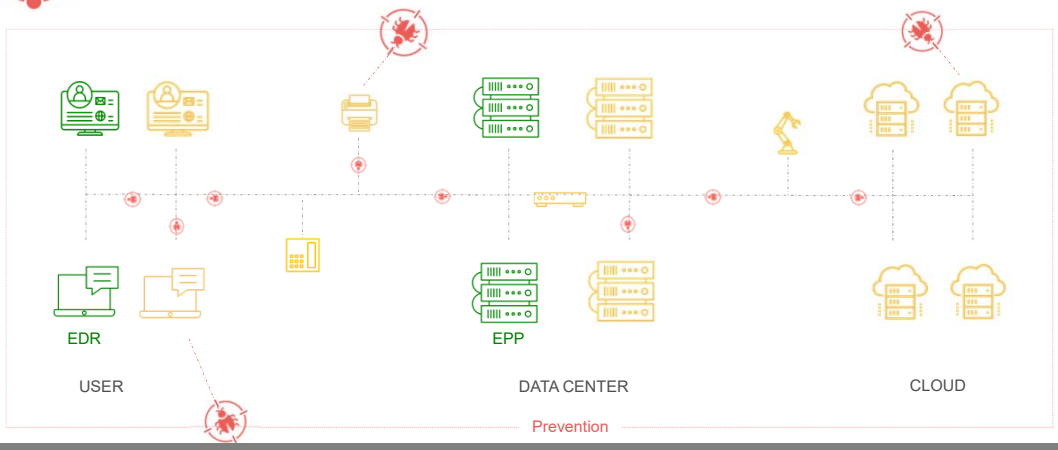
VECTRA AVANTEC Competence. Security. Trust.

Empowering cybersecurity heroes

Network Detection and Response

Fabian Gentinetta, Vectra AI Schweiz

There is a security gap

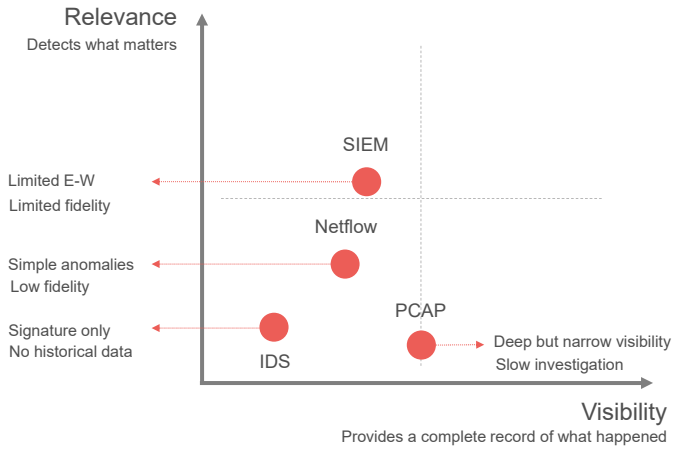


Only the Network provides full coverage

AVANTEC Competence. Security. Trust.

Vectra Webinar
24. September & 3. Oktober 2019

Legacy network security is the weak link

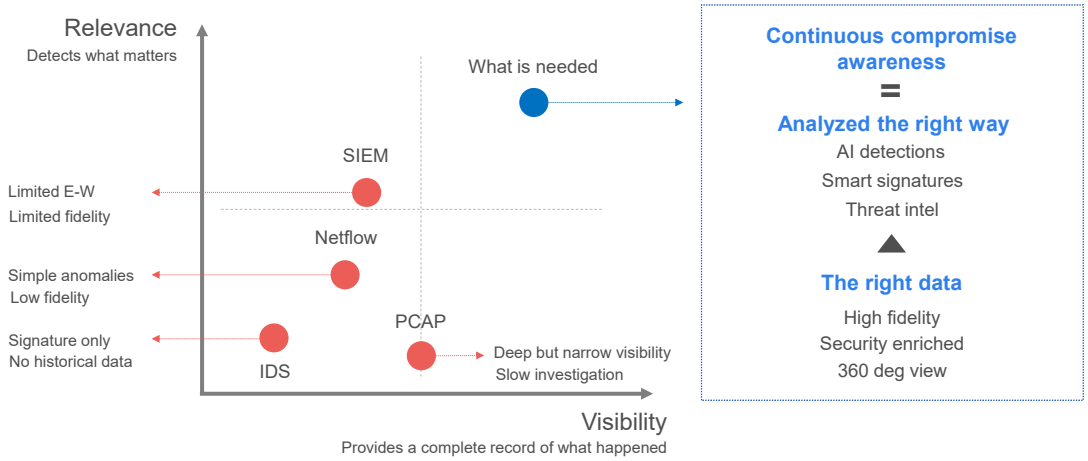


Resulting Challenges

- Too many blind spots – no visibility
- Attackers remain hidden for months
- Drowning in irrelevant alerts
- Time and resources

VECTRA

Legacy network security is the weak link

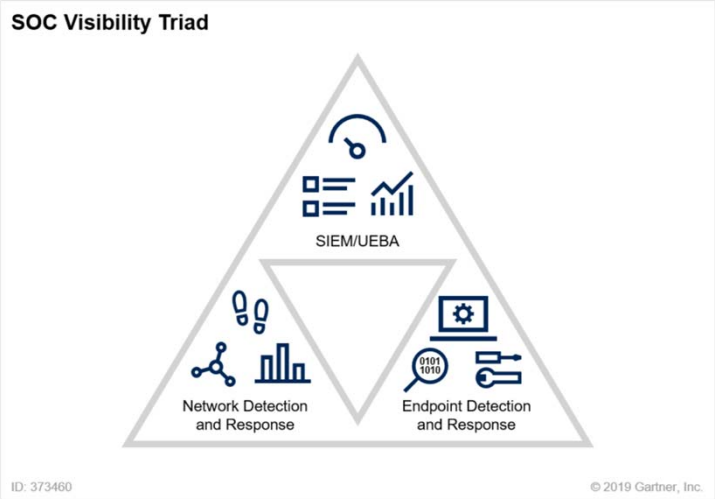


VECTRA

AVANTEC
Competence. Security. Trust.

Vectra Webinar
24. September & 3. Oktober 2019

Gartner: Network-centric approaches to threat detection and response

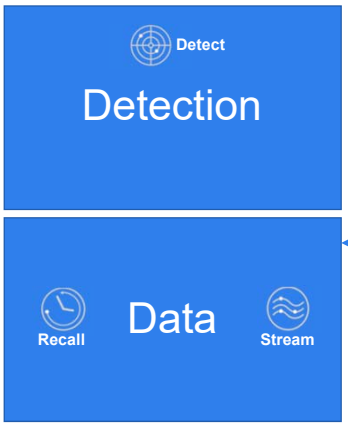


Source: Applying Network-Centric Approaches for Threat Detection and Response
March, 2019
ID Number: G00373460

All statements in this report attributable to Gartner represent Vectra's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation. The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

VECTRA

NDR Network Detection and Response



Find threats fast

High-quality starting points

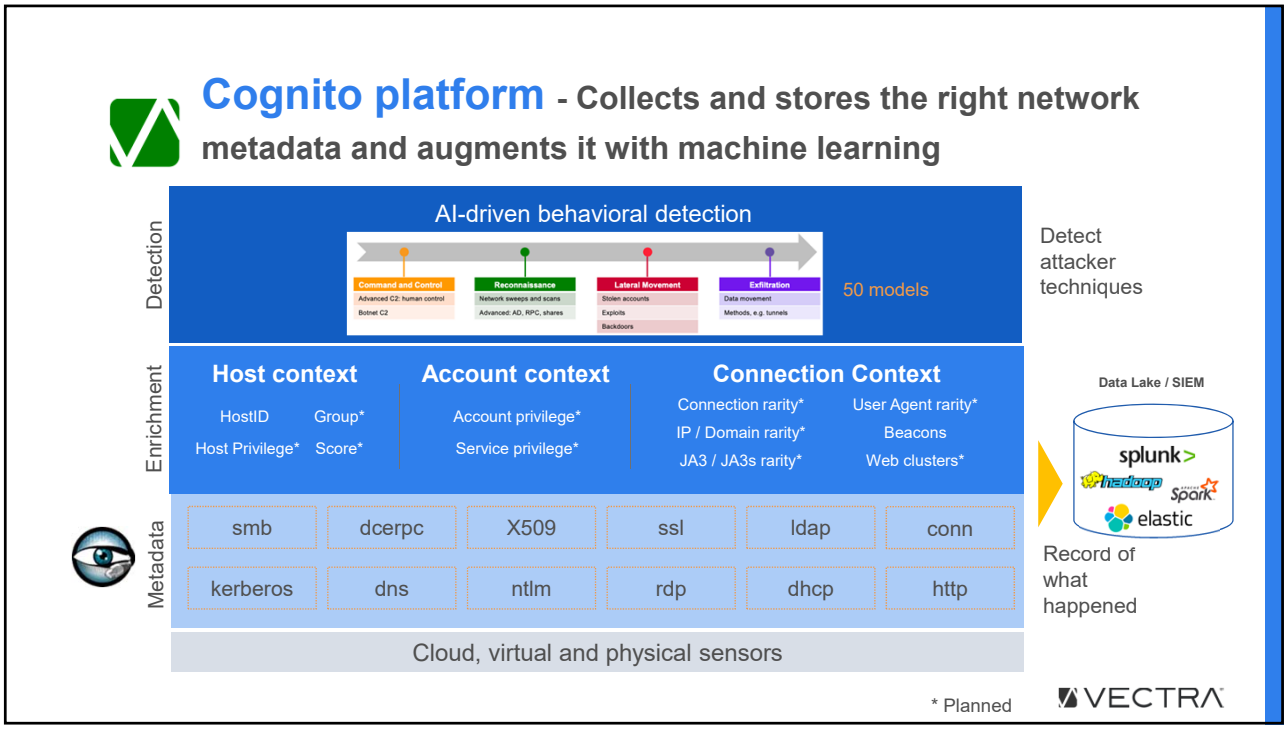
Investigate faster / Hunt

Build your own models

VECTRA

AVANTEC
Competence. Security. Trust.

Vectra Webinar
24. September & 3. Oktober 2019

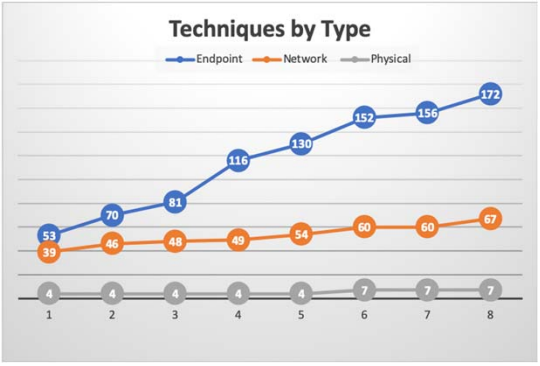


Demo

AVANTEC
Competence. Security. Trust.

Vectra Webinar
24. September & 3. Oktober 2019

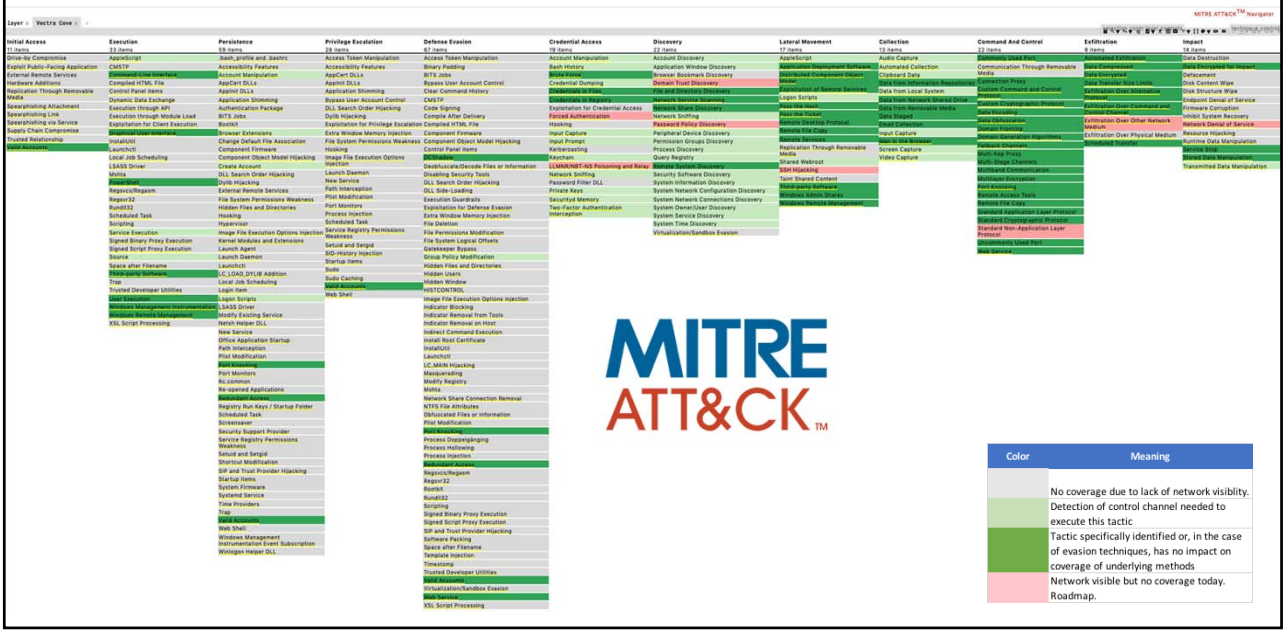
The evolution of MITRE ATT&CK



- Endpoint techniques change much faster than Network techniques
- Underscores the value of investing in network based attacker behavior detection

Endpoint techniques come and go…but the network remains

https://mitre-attack.github.io/attack-navigator/enterprise/



AVANTEC
Competence. Security. Trust.

Vectra Webinar
24. September & 3. Oktober 2019

AVANTEC
Competence. Security. Trust.