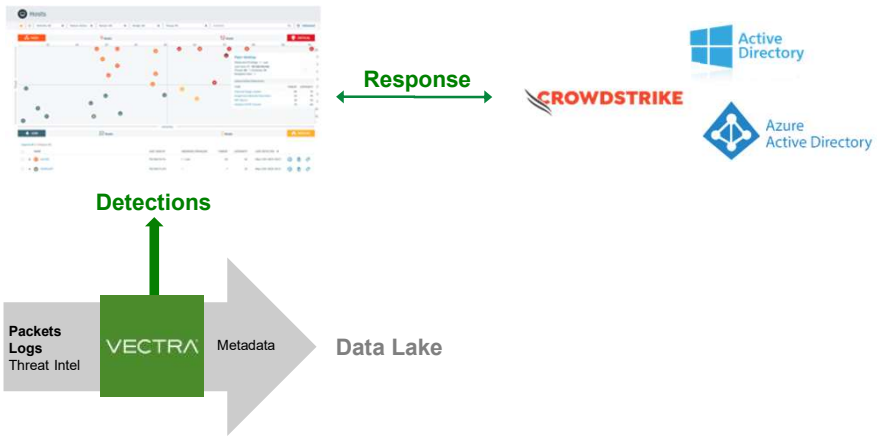
Next Gen SOC Webinar
16. & 22. Juni 2021

AVANTEC
Competence. Security. Trust.

Next Gen SOC Webinar

16./22. Juni 2021

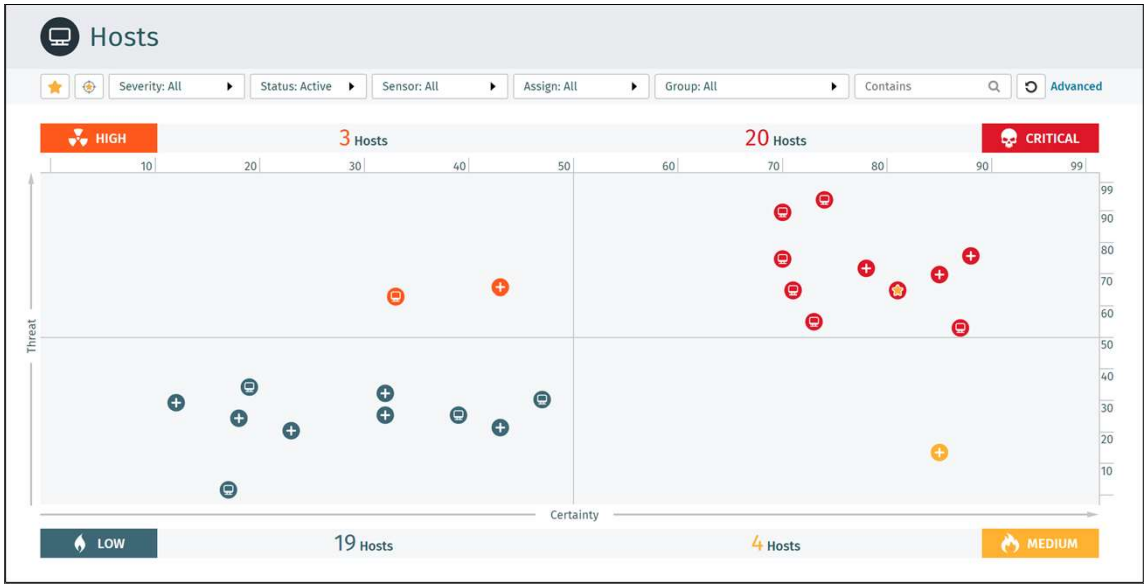
Domain & Ecosystem of Vectra



AVANTEC
Competence. Security. Trust.

Next Gen SOC Webinar
16. & 22. Juni 2021

Clear prioritization drives efficiency

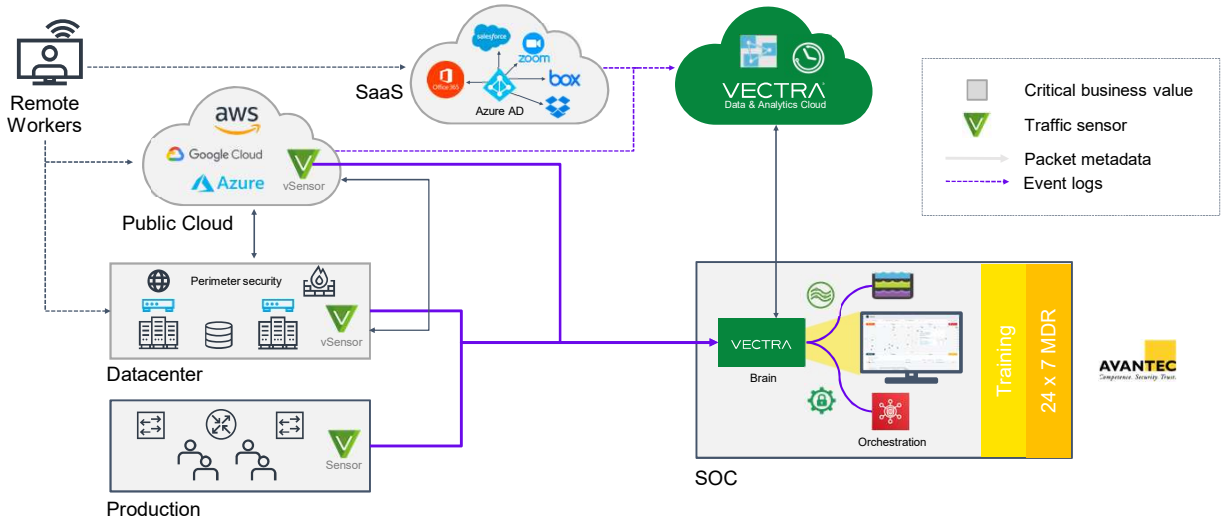


Drives workflow

ML-based

Detection profiles

NDR for Zero Trust Networks



AVANTEC
Competence. Security. Trust.

Next Gen SOC Webinar
16. & 22. Juni 2021

Hunt via EDR:

- Look at rare and threatening sequences of patterns in process starts and actions on the endpoint

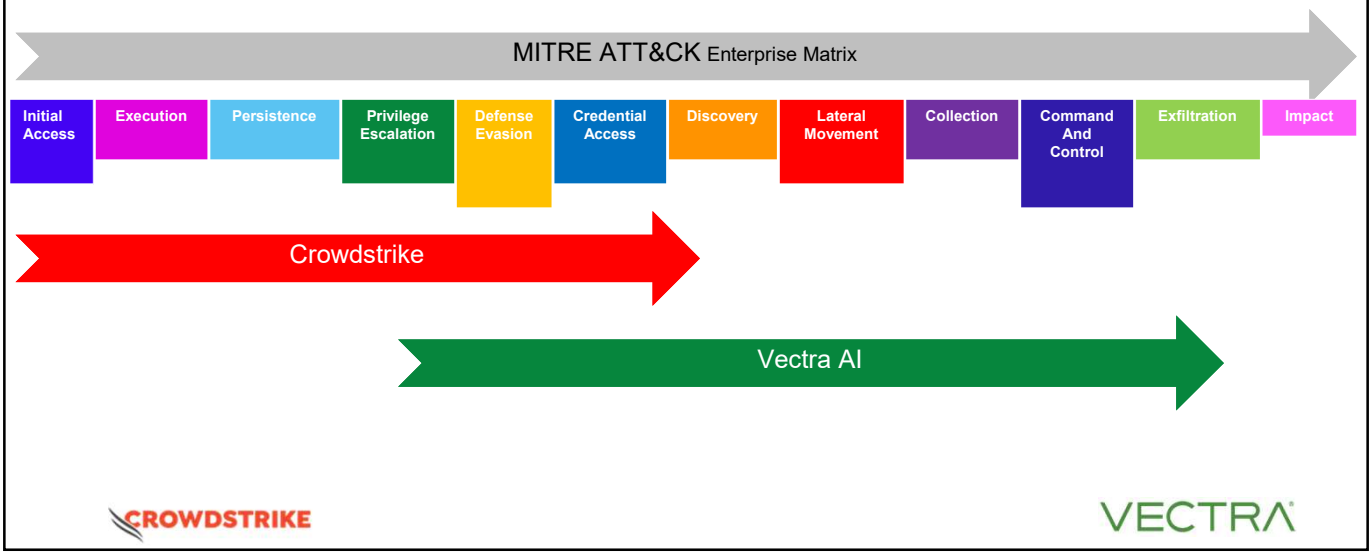
Hunt via NDR:

- Look for rare and threatening sequences of patterns of communications and actions on the network

Hunt via EDR + NDR— follow the bouncing ball

- Look for threatening sequence of patterns on the endpoint
- View that endpoint's behavior through the network lens to uncover additional threats
- Expand view to additional endpoints that show that network behavior
- Find commonalities in the endpoints' behaviors to decide whether to continue hunt or try a new tack

Vectra and Crowdstrike Provides Complete Coverage of the MITRE ATT&CK Matrix

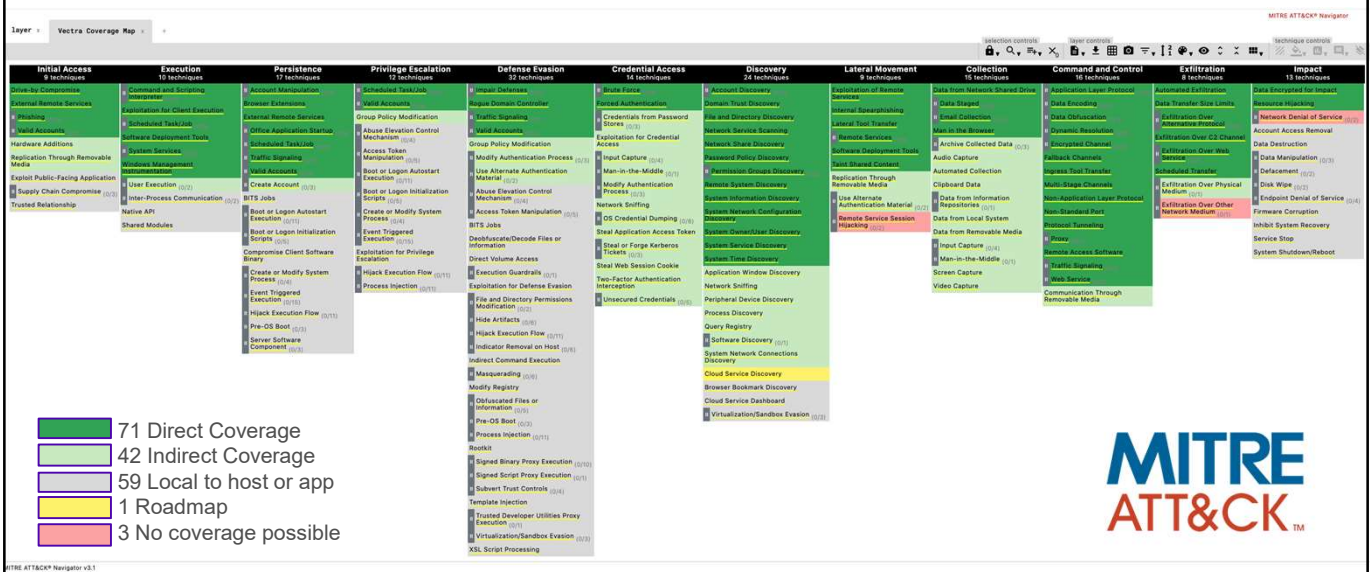


CROWDSTRIKE VECTRA

AVANTEC
Competence. Security. Trust.

Next Gen SOC Webinar
16. & 22. Juni 2021

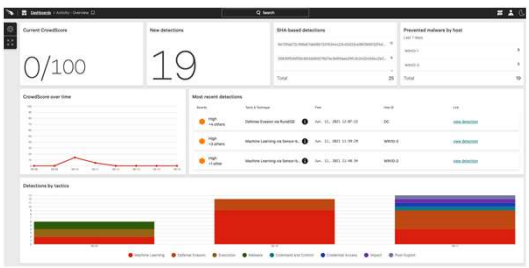
Vectra Coverage of Mitre 3.1



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

NDR + EDR: Combined Visibility for Early Threat Detection and Response

- Combine network and endpoint context for faster triage
- Quick remediation driven by integration between Crowdstrike and Vectra



VECTRA

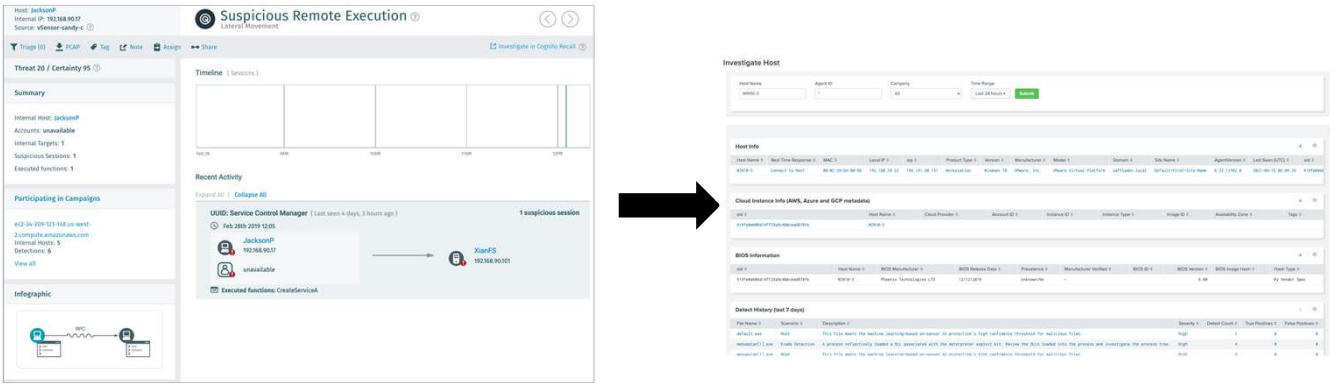
CROWDSTRIKE

AVANTEC
Competence. Security. Trust.

Next Gen SOC Webinar
16. & 22. Juni 2021

One Click Pivot from Vectra to Crowdstrike

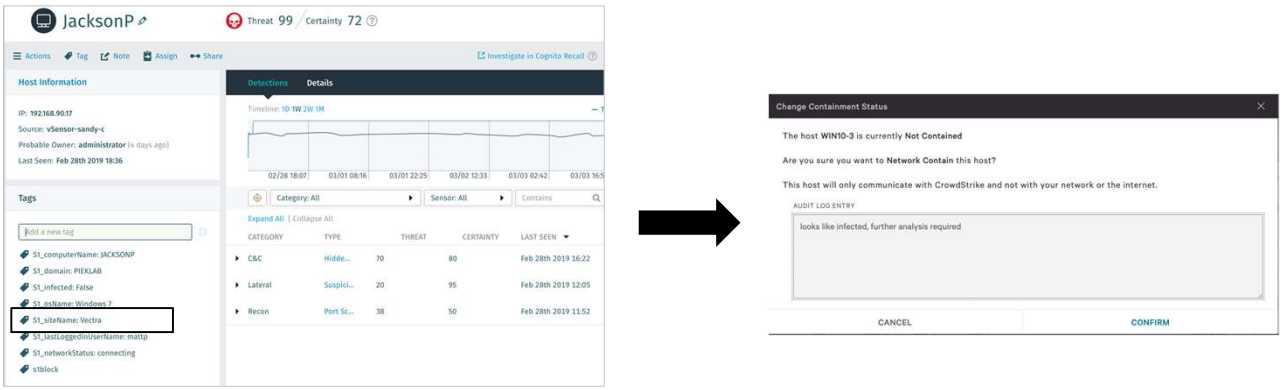
Pivot allows seamless transition from network to endpoint for faster triage



VECTRA CROWDSTRIKE

Remediation by Blocking the Host on Crowdstrike

Manual or automated blocking allows for quick remediation



VECTRA CROWDSTRIKE

AVANTEC
Competence. Security. Trust.