

Next Gen SOC Webinar

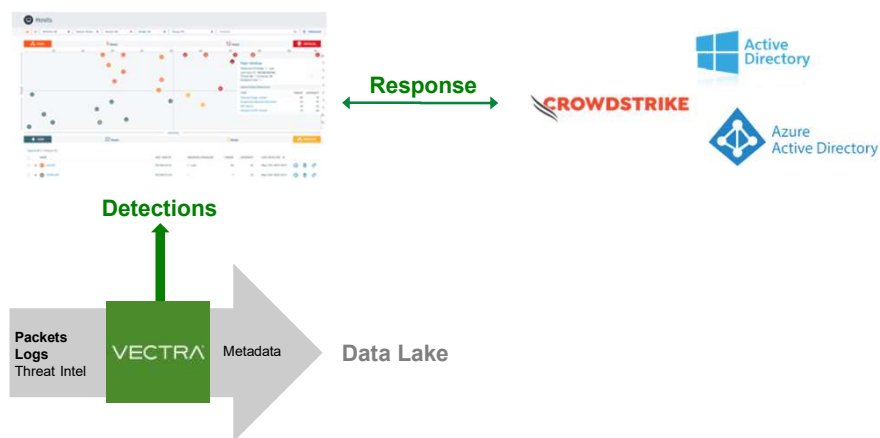
16. & 22. Juni 2021



Next Gen SOC Webinar

16./22. Juni 2021

Domain & Ecosystem of Vectra



Next Gen SOC Webinar

16. & 22. Juni 2021

Clear prioritization drives efficiency

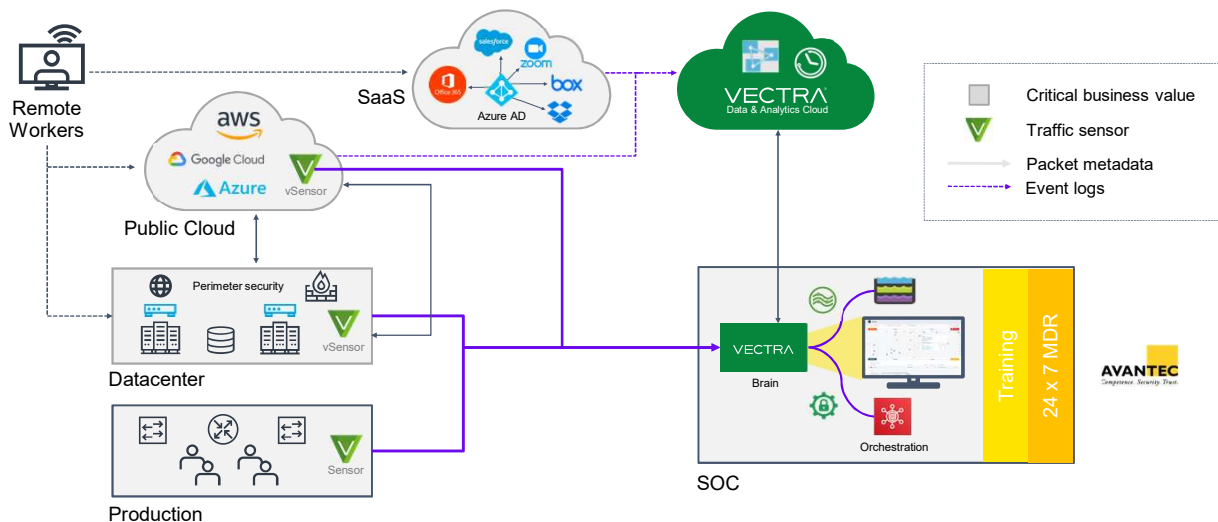


Drives workflow

ML-based

Detection profiles

NDR for Zero Trust Networks



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

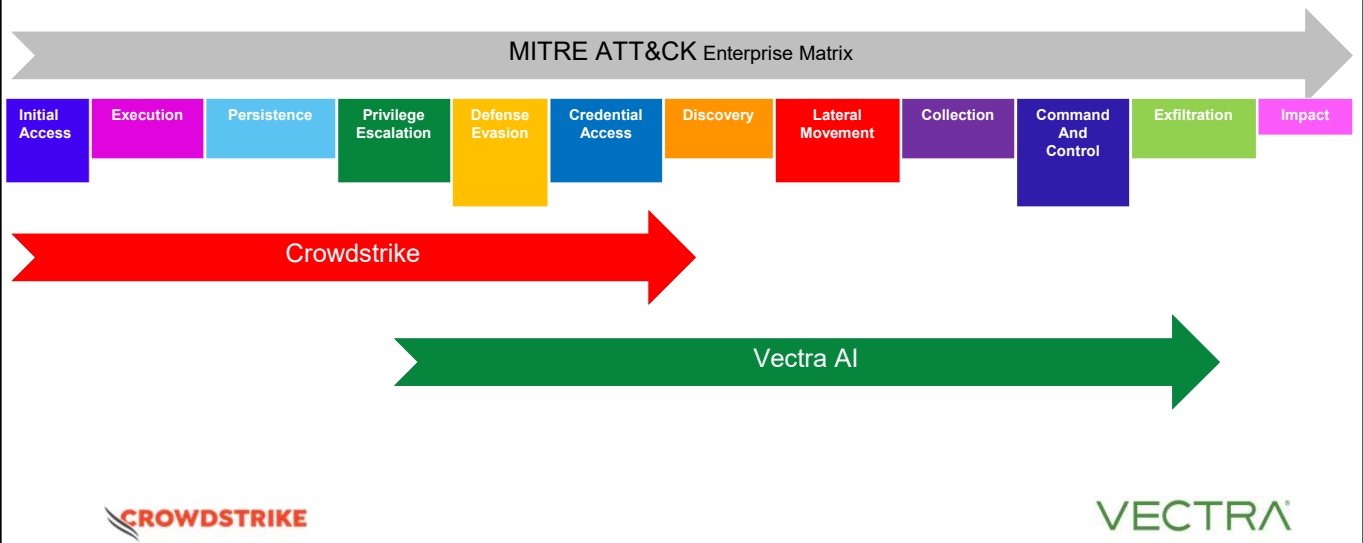
Hunt via NDR:

- 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



Next Gen SOC Webinar 16. & 22. Juni 2021

Vectra Coverage of Mitre 3.1

71 Direct Coverage
42 Indirect Coverage
59 Local to host or app
1 Roadmap
3 No coverage possible

MITRE ATT&CK

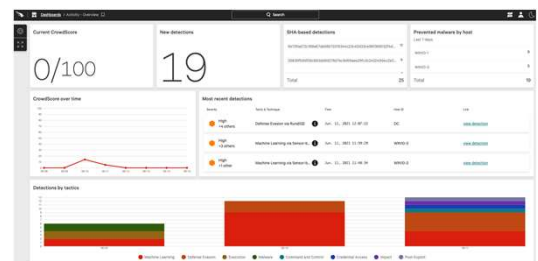
<https://mitre-attack.github.io/attack-navigator/enterprise/>

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

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

The screenshot shows the Vectra interface for a host named 'JacksonP' with IP 192.168.90.17. The main panel displays a 'Timeline' graph and 'Recent Activity' for a 'Service Control Manager' process. A pivot arrow points from the host's IP to the right.

The screenshot shows the CrowdStrike interface for host 'WIN10-3'. It displays a 'Host Info' section with various system details, a 'Cloud Instance Info' section, and a 'Detect History' table. The table lists several detections with their severity and threat types.

File Name	Summary	Description	Severity	Detect Count	Threat Position	Threat Position
api-ms-win-base-util-l1-1-0.dll	API-MS-WIN-BASE-UTIL-L1-1-0.dll	This file is a system component that is not a valid file.	High	1	1	1
api-ms-win-base-util-l1-1-0.dll	API-MS-WIN-BASE-UTIL-L1-1-0.dll	This file is a system component that is not a valid file.	High	1	1	1
api-ms-win-base-util-l1-1-0.dll	API-MS-WIN-BASE-UTIL-L1-1-0.dll	This file is a system component that is not a valid file.	High	1	1	1

VECTRA

CROWDSTRIKE

Remediation by Blocking the Host on Crowdstrike

Manual or automated blocking allows for quick remediation

The screenshot shows the Vectra interface for host 'JacksonP' with IP 192.168.90.17. The 'Host Information' section is on the left, and the 'Detections' table is on the right. A pivot arrow points from the host's IP to the right.

Category	Type	Threat	Certainty	Last Seen
C&C	Hidden	70	80	Feb 28th 2019 16:22
Lateral	Suspicious	20	95	Feb 28th 2019 12:05
Recon	Port Scanning	38	50	Feb 28th 2019 11:52

The screenshot shows a 'Change Containment Status' dialog box. It asks if the user is sure they want to 'Network Contain' the host. Below the question is an 'AUDIT LOG ENTRY' field containing the text 'looks like infected, further analysis required'. There are 'CANCEL' and 'CONFIRM' buttons at the bottom.

VECTRA

CROWDSTRIKE