Hybrid Attack Journey:

How a global manufacturing company stopped a slew of ransomware attacks

Table of Contents

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai

How a global manufacturing organization with an expanding hybrid attack surface continues to stay ahead of highly evasive cyber attackers.

In the modern hybrid enterprise, hybrid attacks are rendering traditional approaches to threat detection and response inefficient and ineffective. Even when an organization has taken all the right steps to secure their environment, attackers will still try to gain access. And too often, they are able to find exposure and move beyond prevention controls where the only way to stop them is by prioritizing post compromise attacker activity.

hybrid attack: One that can start with anyone or anything, move anywhere at any time, and ***disrupt business operations*** at scale, despite having every preventative measure in place.

In this eBook, we'll take a close look at how a global organization successfully defended their environment from relentless hybrid attackers who utilized a variety of tactics and techniques to launch multiple ransomware attacks. You'll understand:

- How hybrid attackers continue to work to uncover exposure with existing security in place.
- Which specific defense strategies worked to stop post compromise attacker activity before damage was done.
- Three core areas the organization relies on to stay ahead of future attacks.

A note about the report details: The identity of the customer used in this report has been kept anonymous to protect their privacy, however, we received their permission to use actual communications details during each incident which you'll find throughout this document.

Organization, SOC environment and hybrid attack journey

Organization details:

- Manufacturing industry
- 14 production facilities in 8 countries
- Presence in 5 world regions
- Between 5-6K employees

Key SOC deployments:

- EDR (Microsoft Endpoint Detection and Response)
- Vectra NDR (Network Detection and Response)
- SIEM (Splunk Security Information and Event Management)
- Vectra MDR (Managed Detection and Response)

Attack journey

⚠ **2021** **Ransomware attack in the U.S.**

⚠ **2023** **OT Ransomware attack in Brazil**

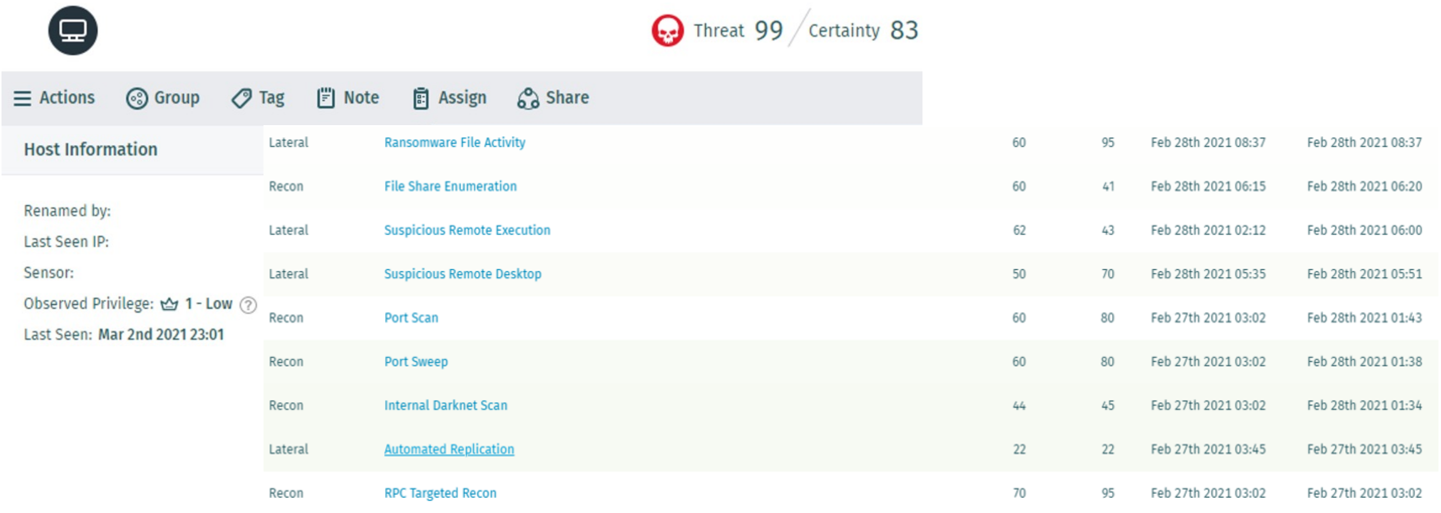
⚠ **2023** **Email Malware in India**

2021 Ransomware Attack in the U.S.

Incident details:

SOC team received detections alerting about malicious activity. Without Vectra's MDR service deployed at the time, the internal team would handle investigation and response in-house.

28th of February	Comment
5PM	Strange detections on USA saw via e-mail notification from VECTRA (Port Scan, Lateral Movement, Ransomware).
6:30PM	At least 2 Server files encrypted (12 devices were compromised)
7PM	Network isolation
7:30PM	A deep analysis on VECTRA events were made (no data exfiltration were found on the log)
9PM	Internal alignment Meeting on how to move on
1st of March	
4AM	SAP and O365 connection allowed on clean clients
10AM	Validation of database (Active Directory, SQL) à no issue
11AM	Virus Scan started on clients (still running at 5:30PM)
2nd of March	
9AM	System recovery
3rd of March	
12AM	All up and running again, no business impact



Host Information

Renamed by:

Last Seen IP:

Sensor:

Observed Privilege: 1 - Low

Last Seen: Mar 2nd 2021 23:01

Lateral	Ransomware File Activity	60	95	Feb 28th 2021 08:37	Feb 28th 2021 08:37
Recon	File Share Enumeration	60	41	Feb 28th 2021 06:15	Feb 28th 2021 06:20
Lateral	Suspicious Remote Execution	62	43	Feb 28th 2021 02:12	Feb 28th 2021 06:00
Lateral	Suspicious Remote Desktop	50	70	Feb 28th 2021 05:35	Feb 28th 2021 05:51
Recon	Port Scan	60	80	Feb 27th 2021 03:02	Feb 28th 2021 01:43
Recon	Port Sweep	60	80	Feb 27th 2021 03:02	Feb 28th 2021 01:38
Recon	Internal Darknet Scan	44	45	Feb 27th 2021 03:02	Feb 28th 2021 01:34
Lateral	Automated Replication	22	22	Feb 27th 2021 03:45	Feb 27th 2021 03:45
Recon	RPC Targeted Recon	70	95	Feb 27th 2021 03:02	Feb 27th 2021 03:02

Key Takeaways:

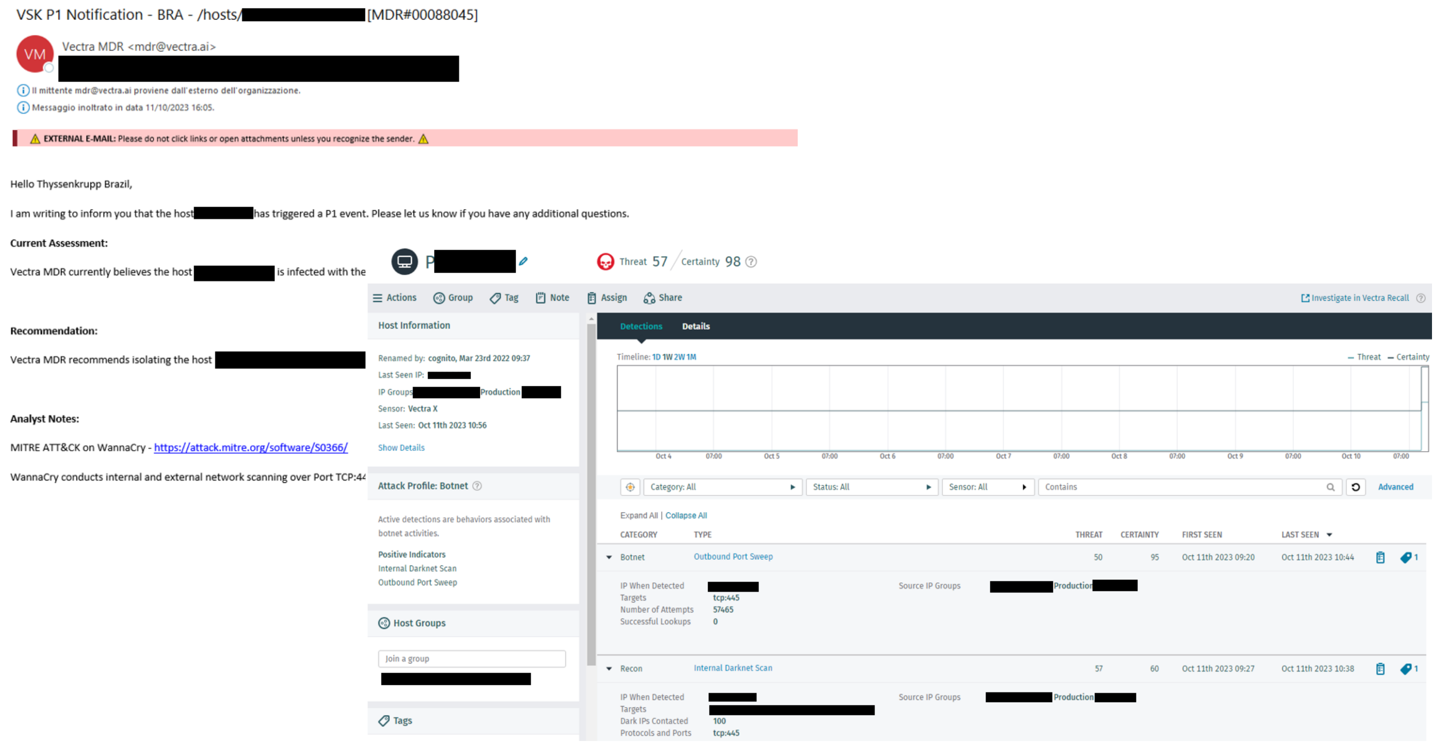
- Vectra's AI-driven signal detected attacker activity, notifying the SOC team that there was an urgent matter.
- A path of 9 detections detailed attacker behavior including lateral movement and ransomware.
- With the full attack details, quick action from the SOC team confirmed there was no exfiltration and they were able to execute a recovery plan.

2023 OT Ransomware Attack in Brazil

Incident details:

Vectra AI detected new attacker activity in the company's Brazil environment. The company was notified by Vectra MDR (a newly added service for the company) that the detected activity is a potential WannaCry ransomware attack.

11th of October	Comment
3:56 PM CEST+1	MDR Mail Escalation + Phone call for stange detections in Brazil (OT area), possible WannaCry
4:21 PM CEST+1	Device isolation (Switch port block)
12th of October	Remediation USB block, patch for wannacry, full scan and device clean up (source of the attach was a USB stick)



VSK P1 Notification - BRA - /hosts/[redacted][MDR#00088045]

Vectra MDR <mdr@vectra.ai>
[redacted]

Il mittente mdr@vectra.ai proviene dall'esterno dell'organizzazione.
Messaggio inoltrato in data 11/10/2023 16:05.

⚠ **EXTERNAL E-MAIL:** Please do not click links or open attachments unless you recognize the sender. ⚠

Hello Thyssenkrupp Brazil,

I am writing to inform you that the host[redacted]has triggered a P1 event. Please let us know if you have any additional questions.

Current Assessment:

Vectra MDR currently believes the host [redacted] is infected with the

Recommendation:

Vectra MDR recommends isolating the host [redacted]

Analyst Notes:

MITRE ATT&CK on WannaCry - https://attack.mitre.org/software/S0366/

WannaCry conducts internal and external network scanning over Port TCP:44

P[redacted]

Threat 57 / Certainty 98

Host Information

Renamed by: cognito, Mar 23rd 2022 09:37
Last Seen IP: [redacted]
IP Groups[redacted]Production [redacted]
Sensor: Vectra X
Last Seen: Oct 11th 2023 10:56
Show Details

Attack Profile: Botnet

Active detections are behaviors associated with botnet activities.

Positive Indicators
Internal Darknet Scan
Outbound Port Sweep

Host Groups

[redacted]

CATEGORY	TYPE	THREAT	CERTAINTY	FIRST SEEN	LAST SEEN
Botnet	Outbound Port Sweep	50	95	Oct 11th 2023 09:20	Oct 11th 2023 10:44
Recon	Internal Darknet Scan	57	60	Oct 11th 2023 09:27	Oct 11th 2023 10:38

Botnet – Outbound Port Sweep:
IP When Detected [redacted]
Targets tcp:445
Number of Attempts 57465
Successful Lookups 0
Source IP Groups [redacted]Productior[redacted]

Recon – Internal Darknet Scan:
IP When Detected [redacted]
Targets [redacted]
Dark IPs Contacted 100
Protocols and Ports tcp:445
Source IP Groups [redacted]Production[redacted]

Key Takeaways:

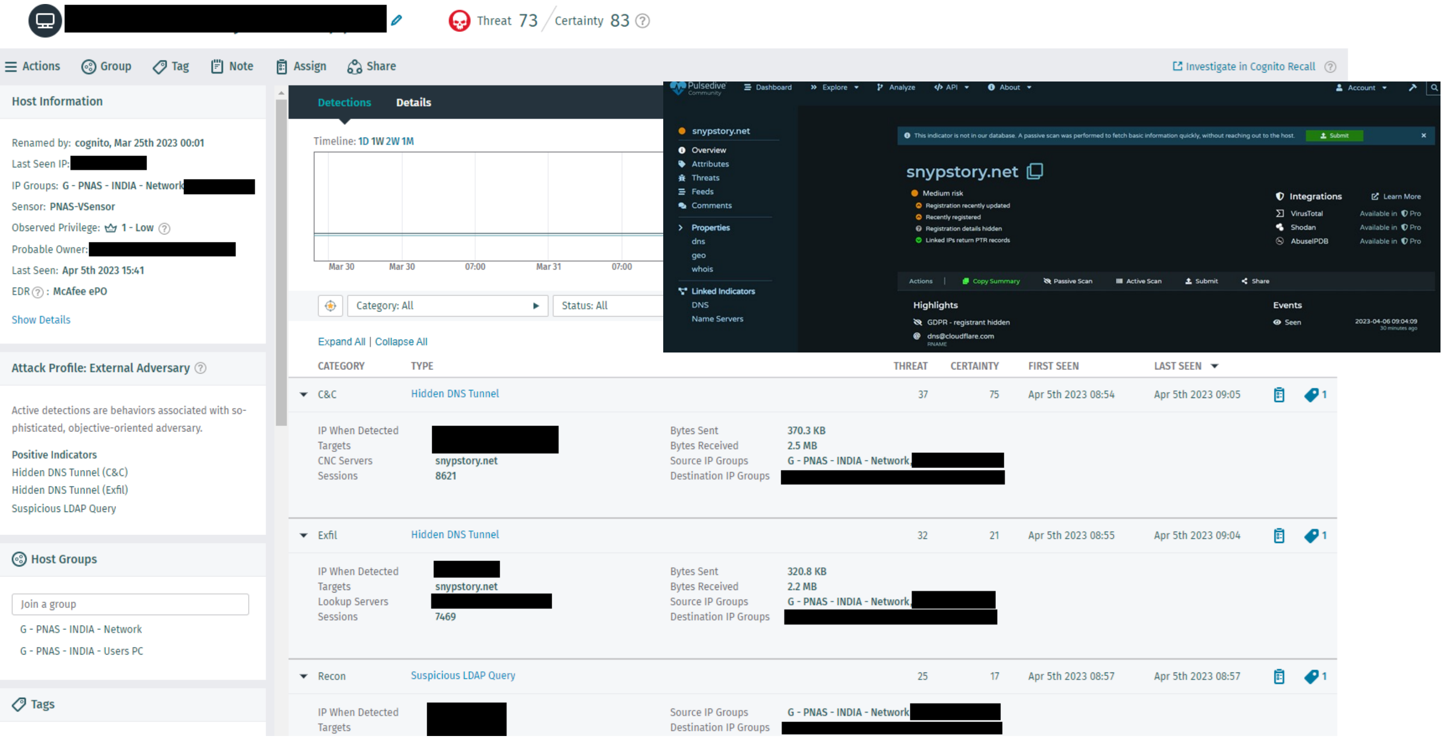
- Two years prior to the attack, the company expanded their NDR deployment in Brazil.
- In addition to the expanded coverage, the company also deployed Vectra MDR to make sure they have 24x7x365 detection, investigation and response coverage.
- Vectra MDR escalated the incident and recommended isolating the infected host to remediate the issue.

2023 Email Malware Attack in India

Incident details:

An incident was escalated by Vectra MDR via email and phone after detections signal possible Command and Control (C2) and exfiltration activity.

6th of April	Comment
8:30 PM	MDR Mail Escalation + Phone call for stange detections in INDIA
9:00 PM	Devices isolation
7th of April	Device clean up (source of the attach was a phishing e-mail, site was blocked)



[redacted]

Threat 73 / Certainty 83

Host Information

Renamed by: cognito, Mar 25th 2023 00:01
Last Seen IP: [redacted]
IP Groups: G - PNAS - INDIA - Network [redacted]
Sensor: PNAS-VSensor
Observed Privilege: 1 - Low
Probable Owner: [redacted]
Last Seen: Apr 5th 2023 15:41
EDR : McAfee ePO
Show Details

Attack Profile: External Adversary

Active detections are behaviors associated with sophisticated, objective-oriented adversary.

Positive Indicators
Hidden DNS Tunnel (C&C)
Hidden DNS Tunnel (Exfil)
Suspicious LDAP Query

Host Groups

Join a group
G - PNAS - INDIA - Network
G - PNAS - INDIA - Users PC

Tags

Category: All
Status: All

CATEGORY	TYPE	THREAT	CERTAINTY	FIRST SEEN	LAST SEEN
C&C	Hidden DNS Tunnel	37	75	Apr 5th 2023 08:54	Apr 5th 2023 09:05
Exfil	Hidden DNS Tunnel	32	21	Apr 5th 2023 08:55	Apr 5th 2023 09:04
Recon	Suspicious LDAP Query	25	17	Apr 5th 2023 08:57	Apr 5th 2023 08:57

C&C – Hidden DNS Tunnel:

IP When Detected Targets	[redacted]	Bytes Sent	370.3 KB
		Bytes Received	2.5 MB
CNC Servers	snypstory.net	Source IP Groups	G - PNAS - INDIA - Network [redacted]
Sessions	8621	Destination IP Groups	[redacted]

Exfil – Hidden DNS Tunnel:

IP When Detected	[redacted]	Bytes Sent	320.8 KB
Targets	snypstory.net	Bytes Received	2.2 MB
Lookup Servers	[redacted]	Source IP Groups	G - PNAS - INDIA - Network [redacted]
Sessions	7469	Destination IP Groups	[redacted]

Recon – Suspicious LDAP Query:

IP When Detected Targets	[redacted]	Source IP Groups	G - PNAS - INDIA - Network [redacted]
		Destination IP Groups	[redacted]

snypstory.net

This indicator is not in our database. A passive scan was performed to fetch basic information quickly, without reaching out to the host.

snypstory.net
- Medium risk
  - Registration recently updated
  - Recently registered
  - Registration details hidden
  - Linked IPs return PTR records

Integrations	
VirusTotal	Available in Pro
Shodan	Available in Pro
AbuseIPDB	Available in Pro

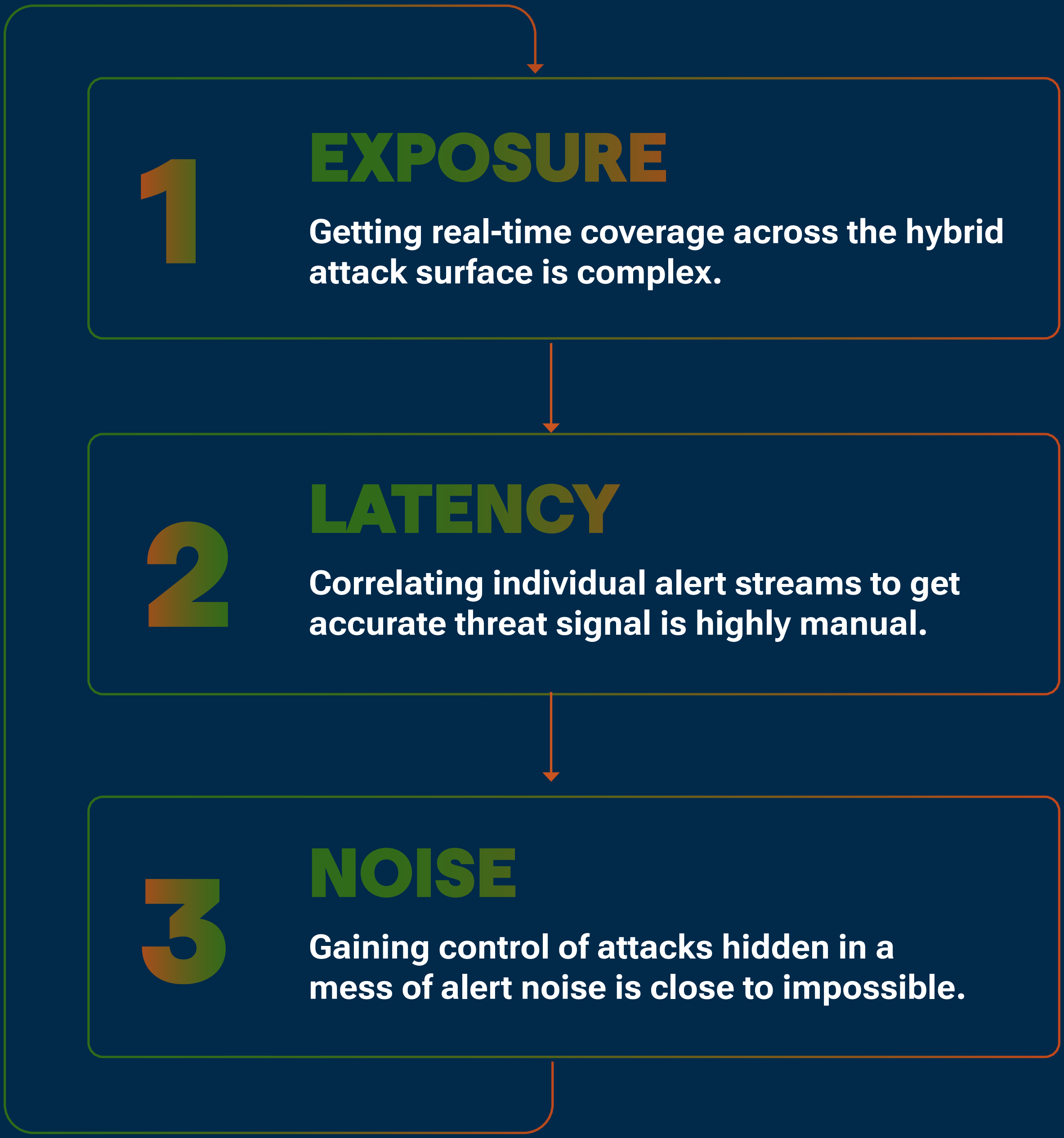
Highlights
- GDPR - registrant hidden
- dns@cloudflare.com RNAME

Events
- Seen 2023-04-06 09:04:09 30 minutes ago

Key Takeaways:

- The attack appeared to be initiated from a phishing email that was used to help the attackers gain access and bypass prevention controls.
- Suspicious LDAP Query detection indicated reconnaissance behavior where attackers are searching for administrative privilege to help them advance.
- Vectra MDR was able to isolate the infected device within 30 minutes of escalation.

What makes defending against today's hybrid attacks so hard?



1 EXPOSURE

Getting real-time coverage across the hybrid attack surface is complex.

2 LATENCY

Correlating individual alert streams to get accurate threat signal is highly manual.

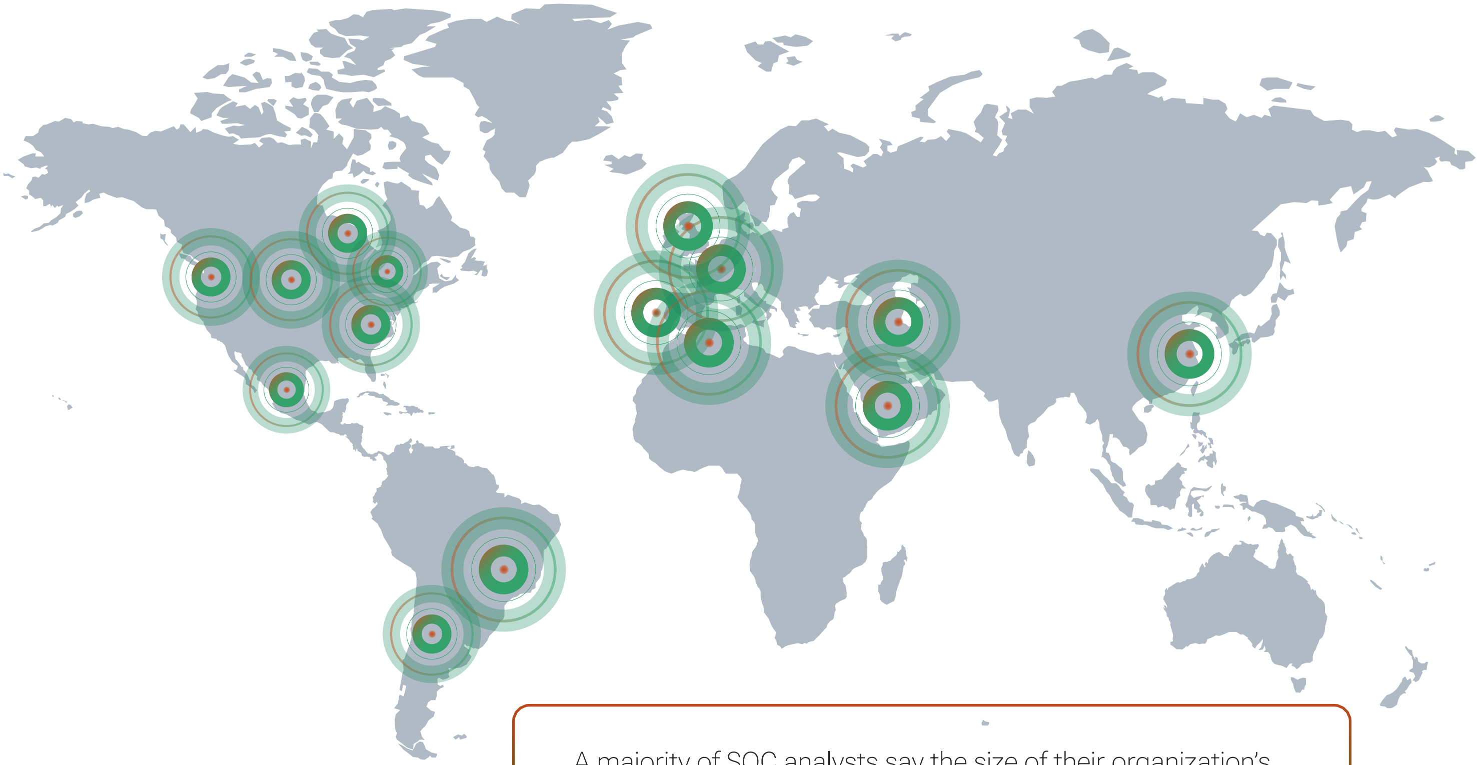
3 NOISE

Gaining control of attacks hidden in a mess of alert noise is close to impossible.

Three keys to stopping hybrid attacks

Coverage:
Can we see the attack?

✓ After each attack, they were able to utilize an integrated attack signal that delivered coverage across each surface — identifying what was happening in real-time with prioritized detections. They also recognized that as their environment and workloads expanded, their exposure increased as well and required that their coverage across each new attack surface needed to expand.

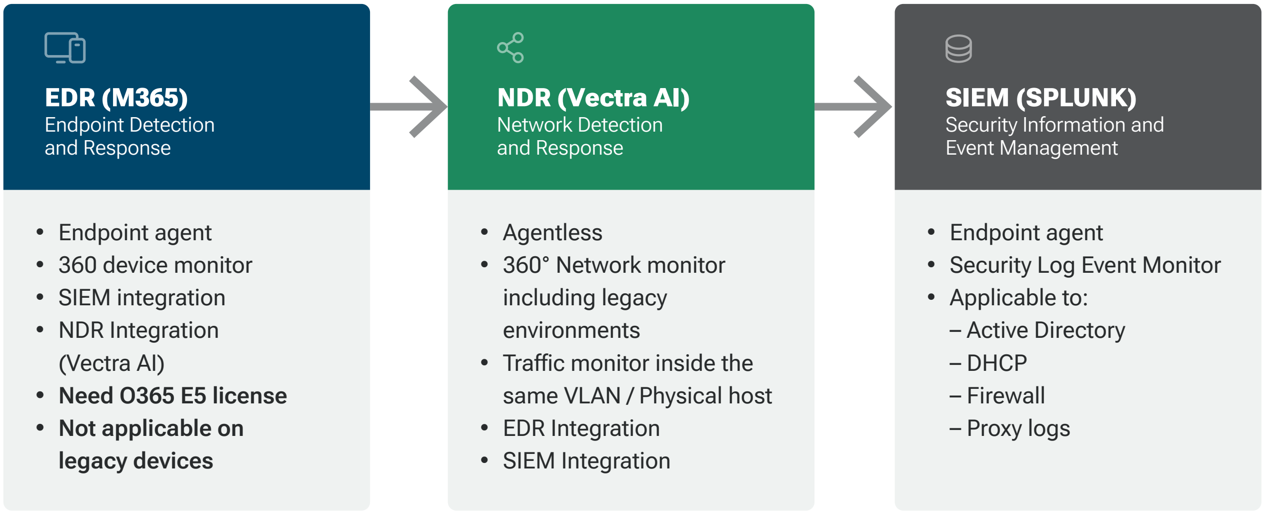


A majority of SOC analysts say the size of their organization's attack surface (63%), the number of security tools (70%), and alerts (66%) they manage have significantly increased in the past three years.[1]

Source 1: 2023 State of Threat Detection Report: The Defenders' Dilemma

Clarity:
Can we keep pace with attackers?

In addition to having coverage across all hybrid attack surfaces, this organization prioritized an AI-driven attack signal that provides clarity into post compromise attacker behavior (what activity is malicious and requires urgent attention). They designed their environment so the tools work together to close exposure gaps. The real-time signal removes any latency around detecting events, while the integrations between EDR, NDR and SIEM technologies gives the team clear context about attacks in one place, eliminating the effort it takes to gather information across siloed signals.



EDR (M365)
Endpoint Detection
and Response

- Endpoint agent
- 360 device monitor
- SIEM integration
- NDR Integration (Vectra AI)
- **Need O365 E5 license**
- **Not applicable on legacy devices**

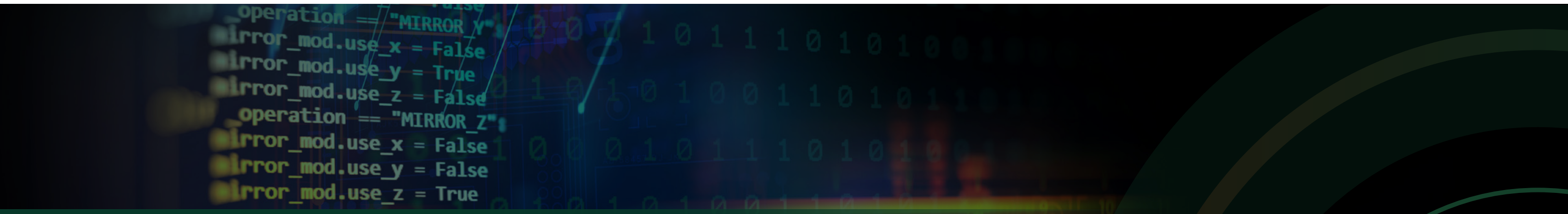
NDR (Vectra AI)
Network Detection
and Response

- Agentless
- 360° Network monitor including legacy environments
- Traffic monitor inside the same VLAN / Physical host
- EDR Integration
- SIEM Integration

SIEM (SPLUNK)
Security Information and
Event Management

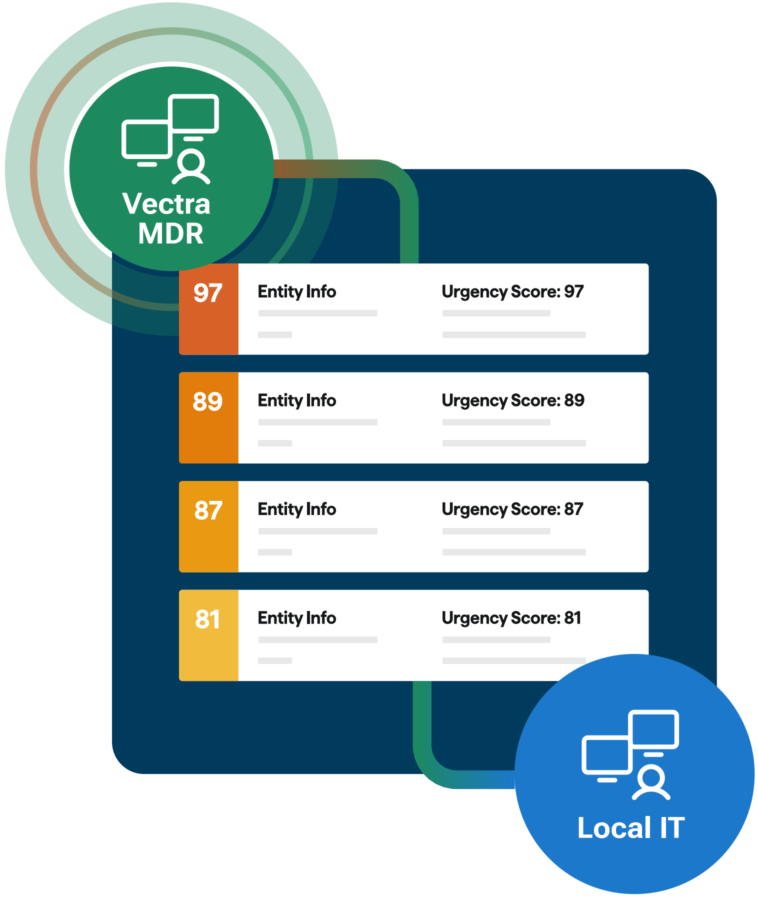
- Endpoint agent
- Security Log Event Monitor
- Applicable to:
  – Active Directory
  – DHCP
  – Firewall
  – Proxy logs

> “NDR complements EDR by closing the agent gaps. The combination of EDR and NDR enlarges and enforces the security level of the environment, giving the SIEM and the SOC more complete data.”
>
> **IT MANAGER**
> Cybersecurity



Control:
Can we stop the attackers?

As the attack surface expands, exposure grows, tools start to sprawl and the SOC workload increases. The SOC team recognized this and took action by deploying an MDR service as a way to maximize their current security talent and offload security operations where needed while gaining 24x7x365 coverage. This was key in stopping two of the attacks where the infected devices were isolated 30 minutes after escalation. Along with the full context of any incident that their tools provide, they now have the control to stop them efficiently.



> “In the last year we received at least four escalations at the beginning of an attack, one in India, one in Mexico, one in Brazil. And it was very interesting because we were able to apply our policy to isolate the device before it spread on the network. Each time, we were able to do a deep investigation and avoid any criticality for the business. The response time of the MDR service is within minutes. The communication goes to our local IT team then to an escalated response in less than half an hour.
>
> **IT MANAGER**
> Cybersecurity

Staying ahead of hybrid attacks

Today's hybrid attackers will keep trying to find new ways to expose organizations — they will compromise identities, elevate and hide in privileges, move laterally across domains until they find what they're searching for and ultimately cause damage. These real-life examples show the relentless nature of attackers, but also how a diligent SOC team can put their organization in position to successfully defend against them.

The SOC team and their approach to defending their organization highlights the path to finding the hybrid attack needle. They use an AI-driven attack signal to build the confidence and competence of their SOC talent. The challenges discussed that make stopping hybrid attacks so difficult — exposure, latency and noise — are eliminated so the team is able to use their talent to focus on what really matters — stopping attacks.

Learn more about an AI-driven SOC →

VECTRA®

For more information please contact us:
Email: info@vectra.ai | vectra.ai