Vectra and Endace

The Right Data with the Right Context

VECTRA®

Challenge

Despite multiple layers of cybersecurity defense such as next-generation firewalls, IDSs, and AI security solutions, cyberattackers still get past to gain access into enterprise networks. Without visibility into what's happening inside the network perimeter, it's impossible to detect and defend against these attacks.

Solution

Together, Vectra and Endace provide rich insight into attacks across cloud, data centers, IoT devices, and enterprise networks.

Vectra's threat detection and response platform delivers powerful analysis and detection that perfectly complements the EndaceProbe™ Analytics Platform's always-on packet capture. By combining Vectra's Platform and EndaceProbes, analysts have powerful threat detection coupled with the detailed forensic evidence they need to detect, investigate and respond to cyberthreats and attacks quickly and definitively.

Vectra's platform leverages a unique combination of data science, machine learning, and behavioral analysis to detect attacks at all phases – such as internal reconnaissance, command and control, lateral movement and data exfiltration. Over time, Vectra's platform understands the naturally occurring communities in the network and continuously listens, thinks, and learns to adapt to the ever-changing threat landscape.

Vectra's platform automatically detects cyberthreats – even those hidden in approved applications or encrypted traffic – and correlates these threats to the hosts that are under attack, delivering unique context about what attackers are doing. This gives IT security teams the insight they need to quickly identify, prioritize, and respond to the threats that pose the greatest danger.

The EndaceProbe Analytics Platform's always-on network recording captures, indexes, and stores a 100% accurate record of traffic on the network. This comprehensive, packet-level forensic evidence lets security teams quickly investigate the threats that the Vectra platform detects so they can respond faster to stop attacks.

Efficient Investigation and Threat Hunting

The Network History recorded by EndaceProbes can be fully integrated into the Vectra platform's workflows using the EndaceProbe's Pivot-To Vision™ integration. This integration lets security analysts pivot from alerts in Vectra's platform directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the packet-level Network History related to the event. Pivot-to-Vision uses the IP address and time range of the trigger event to rapidly dissect, review, and extract the relevant traffic from amongst petabytes of Network History recorded on the network. It supports analysis to microsecond level detail, with views filtered by Application, IP, Protocol, Top Talkers, and many other parameters, providing rapid insights and enabling accurate conclusions.

Directly accessing the related packets with a single click lets security analysts quickly discover the root cause of issues as they are threat hunting in their environment. They can respond rapidly to threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of security threats from escalating to become more serious breaches.

PRODUCTS

- **Vectra Threat Detection and Response Platform**
- **EndaceProbe Analytics Platform**

BENEFITS

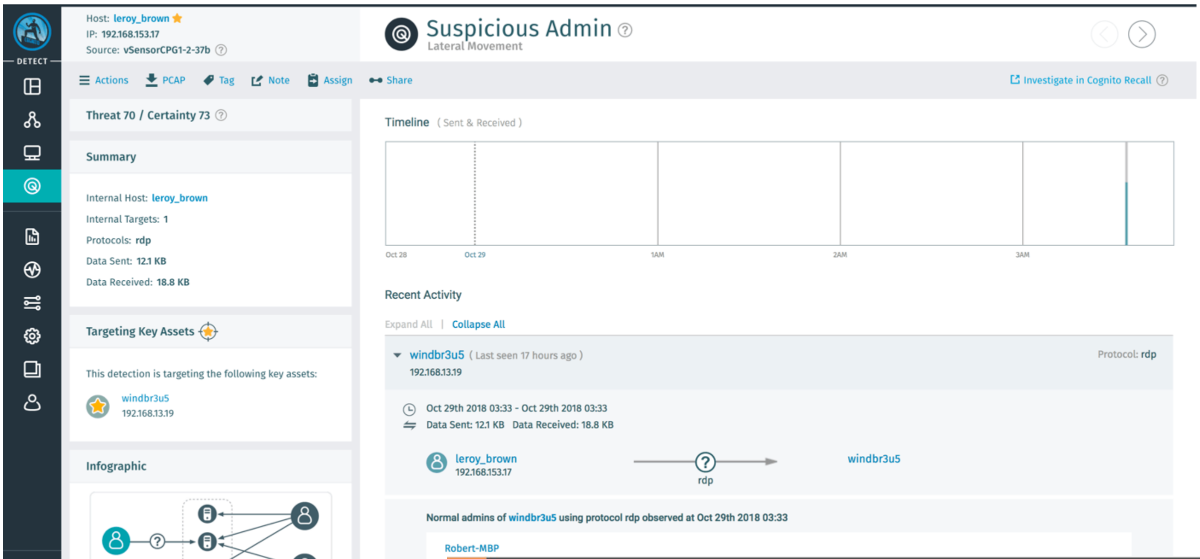
- Vectra's platform automatically and in real time, detects in-progress cyber attacks that evade prevention security defenses and spread inside networks.
- Vectra's platform combines data science, machine learning, and behavioral analysis to detect all phases of a cyber attack.
- Streamlined investigation workflows give SecOp teams one-click access to definitive evidence, accelerating the investigation and remediation of threats.
- Definitive evidence trail with an accurate record of all relevant packets.

Conclusion

Combining the Vectra platform with the EndaceProbe's 100% accurate Network History delivers more effective threat detection, greater visibility into attack activity, and definitive evidence that enables SecOps teams to combat numerous and sophisticated attacks.

Integrating the two technologies empowers security teams to respond to alerts and investigate threats with speed and confidence.

How It Works



Host: leroy_brown
IP: 192.168.153.17
Source: vSensorCPG1-2-37b

Suspicious Admin
Lateral Movement

Threat 70 / Certainty 73

Summary

Internal Host: leroy_brown
Internal Targets: 1
Protocols: rdp
Data Sent: 12.1 KB
Data Received: 18.8 KB

Targeting Key Assets

This detection is targeting the following key assets:

windbr3u5
192.168.13.19

Infographic

Attack Phase

Timeline (Sent & Received)

Recent Activity

Expand All | Collapse All

windbr3u5 (Last seen 17 hours ago)
192.168.13.19
Protocol: rdp

Oct 29th 2018 03:33 - Oct 29th 2018 03:33
Data Sent: 12.1 KB Data Received: 18.8 KB

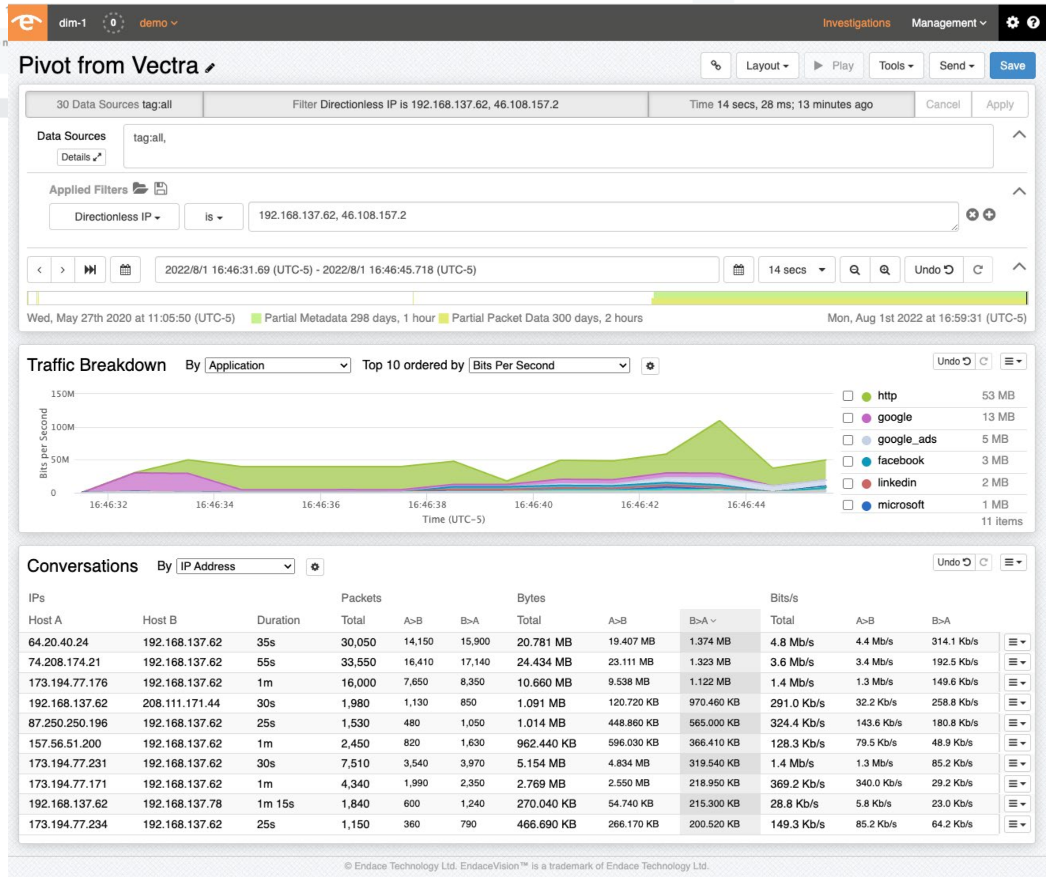
leroy_brown
192.168.153.17

windbr3u5

Normal admins of windbr3u5 using protocol rdp observed at Oct 29th 2018 03:33

Robert-MBP

Figure 1. From alerts in the Vectra platform, you can drill-down directly to related packets in EndaceVision.



Pivot from Vectra

30 Data Sources tag:all | Filter Directionless IP is 192.168.137.62, 46.108.157.2 | Time 14 secs, 28 ms; 13 minutes ago

Data Sources: tag:all,

Applied Filters: Directionless IP · is · 192.168.137.62, 46.108.157.2

2022/8/1 16:46:31.69 (UTC-5) - 2022/8/1 16:46:45.718 (UTC-5) · 14 secs

Wed, May 27th 2020 at 11:05:50 (UTC-5) · Partial Metadata 298 days, 1 hour · Partial Packet Data 300 days, 2 hours · Mon, Aug 1st 2022 at 16:59:31 (UTC-5)

Traffic Breakdown By Application · Top 10 ordered by Bits Per Second

□	● http	53 MB
□	● google	13 MB
□	● google_ads	5 MB
□	● facebook	3 MB
□	● linkedin	2 MB
□	● microsoft	1 MB
		11 items

Conversations By IP Address

IPs			Packets			Bytes			Bits/s		
Host A	Host B	Duration	Total	A>B	B>A	Total	A>B	B>A	Total	A>B	B>A
64.20.40.24	192.168.137.62	35s	30,050	14,150	15,900	20.781 MB	19.407 MB	1.374 MB	4.8 Mb/s	4.4 Mb/s	314.1 Kb/s
74.208.174.21	192.168.137.62	55s	33,550	16,410	17,140	24.434 MB	23.111 MB	1.323 MB	3.6 Mb/s	3.4 Mb/s	192.5 Kb/s
173.194.77.176	192.168.137.62	1m	16,000	7,650	8,350	10.660 MB	9.538 MB	1.122 MB	1.4 Mb/s	1.3 Mb/s	149.6 Kb/s
192.168.137.62	208.111.171.44	30s	1,980	1,130	850	1.091 MB	120.720 KB	970.460 KB	291.0 Kb/s	32.2 Kb/s	258.8 Kb/s
87.250.250.196	192.168.137.62	25s	1,530	480	1,050	1.014 MB	448.860 KB	565.000 KB	324.4 Kb/s	143.6 Kb/s	180.8 Kb/s
157.56.51.200	192.168.137.62	1m	2,450	820	1,630	962.440 KB	596.030 KB	366.410 KB	128.3 Kb/s	79.5 Kb/s	48.9 Kb/s
173.194.77.231	192.168.137.62	30s	7,510	3,540	3,970	5.154 MB	4.834 MB	319.540 KB	1.4 Mb/s	1.3 Mb/s	85.2 Kb/s
173.194.77.171	192.168.137.62	1m	4,340	1,990	2,350	2.769 MB	2.550 MB	218.950 KB	369.2 Kb/s	340.0 Kb/s	29.2 Kb/s
192.168.137.62	192.168.137.78	1m 15s	1,840	600	1,240	270.040 KB	54.740 KB	215.300 KB	28.8 Kb/s	5.8 Kb/s	23.0 Kb/s
173.194.77.234	192.168.137.62	25s	1,150	360	790	466.690 KB	266.170 KB	200.520 KB	149.3 Kb/s	85.2 Kb/s	64.2 Kb/s

© Endace Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd.

Figure 2. From EndaceVision you can use filters and views to analyze the traffic related to the event, zoom in or out on the timeline to view precursor or post-event activity and decode and analyze packets in a hosted instance of Wireshark direcly on the EndaceProbe without needing to download a pcap.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com