VECTRA
SECURITY THAT THINKS.®

Sanofi Webinar: Q&A

Unedited answers from Richard and Jean Yves at Sanofi to your questions during the Fireside Chat.

Question	Answer
What do typical EDR solutions miss that NDR's pick up?	Credentialed adversaries who are stealing data, preparing a ransomware etc. Once Credentialed traditional IPS goes quiet. That happens early in an attack.
What is the second part of the Zero Trust model?	1st line of defense = endpoints, second line is credential and access permission. A strong monitoring of lifecycle, usage and behaviour must be implemented : Active Directory monitoring + Bastion + User Behavior analytic
Hi Rich - do you use an EDR solution at Sanofi and did this miss all of the activity on the endpoint ? Great info here, thank you for sharing.	We use an EDR solution and it caught the WMI abuse. It is a very effective solution. But if an attacker is careful they might not trip it. Our EDR doesn't build a case over time, it triggers on a discreet event.
Very interesting presentation and attack. Out of curiosity, what do you use for EDR?	FireEye and it works very well.
What tool fired first between EDR & NDR ?	NDR Detected the scans and the Share enumeration first. EDR detected the WMI use next. NDR then detected the unusual account usage.
Just out of curiosity, how did you attribute to Lazarus?	TTPs, Government, Vendor and Law Enforcement contributions & MITRE
I'm guessing you get a lot of High and Critical alerts, what caught your attention that this was a serious threat and separates it from the rest	On the NDR side it was the threat and Certaity scores. They crossed a threshold and would have gone higher had we caught the C2. EDR WMI activity was enough by itself.
There may many network segments available in our network. So, is there any mechanism that we can use/to follow to make sure that all segments covered. For example, if the user to internet or user to server etc are not covered, there is high chances that we will miss attacks/malicious activities happening related to the same in our network.	Maybe a Netflow analysis might help to give some more visibility. This is challenge. How to get the sensors where they can have strong visibility
Did the 1st failure of the weaponized word document slow them down from making the progress that they might have otherwise made on a weekend?	Maybe, but the employee being phished was convinced and was not suspicious of the attacker. AV failed to detect.
Are you going to remove local admin accounts?	"Local Admin" in this case meant a powerful credential that was stolen, not an actual Windows Local Admin. We have strong controls around those passwords.

Question	Answer
Can you explain your containment and recovery? You mentioned detection net in this process. How was that used?	We did strong forensics and created new detection capability based on that detailed analysis.
Since Vectra is utilizing AI alogrithms that build baselines to detec deviations and therefore detects malicious activities, how long does it take so Vectra can really be effective at detecting malicious activities?	It depends on the complexity of the network but you might be able to get there in a few weeks of learning and tuning. We do have false alarms and we investigate and tune. We want that level of sensitivity though.
We Sanofi able to quantify how many Sanofi personnel were targeted by the fake LinkedIn recruiter messages – as this a highly targeted attack or a bit more indiscriminate? **Having identified a LinkedIn account as the attack source, did you notify LinkedIn and how quickly did they terminate the account?** **What was the time interval from the time the payload first got delivered to the client device to when you had a first detection by Cognito, and then to then you had the attack contained?**	We know that a handful of our employees were targeted and we know that other pharmaceuticals were targeted. When the payload was dropped the attacker did some basic recon, then a port scan. The EDR caught that port scan and share enumeration very quickly. But the attackers did take hours between actions.
How many people are working on tuning Cognito?	1 plus the team reaponds to detections and know how to tune the system after a false alarm.
Since Vectra is considered as NDR and 'R' here refers to 'Response', what is the role of Response Vectra can play here to contain attacks?	Vectra can interact with EDR, SOAR and other solutions to add automations and efficiencies. We don't have much maturity there though outside of detection
Can you describe what makes Vectra different from the competition? For example, Darktrace.	At the time of our POC, we looked a Darktrace and others. There were good things about all of them. But in our Red Team exercise that was going on at the time, with a credentialed adversary, only Vectra seemed to be in the game still. And we made a specific focus on the intensity of the relationship which is a strong promess for a continuous performance increase for the solution.
Can you elaborate on the timeline of the attack; when did you get indications and how fast did you respond and when did you feel safe the threat was contained? **How much time passed?**	it took a few hours of work for the attacker to get to activities that were dangerous and also firing alarms. There were hours sometimes between their actions. We believe the threat is still there. Not on our network but trying still to get in.
What, concretely, a NDR (vectra) can do better than an EDR? Sanofi's attack, EDR would have been able to detect it.	EDR could be NDR if every station is watching the network and reporting into an NDR like brain solution. For us, EDR is looking at running processes and command arguments. Our NDR, Vectra is looking at behaviour over time in an Infosec context.

Question	Answer
can you please elaborate a bit on the level of false alarms you get from your tools and how you deal with these?	We provide white listing like configurations to tell Vectra not to boose the threat or certainty for certain systems on certain rules. In a big complex network there is work here for sure.
Don't you think NDR can drive EDR but EDR can't really drive NDR ? So, NDR first ?	Not sure I understand the question, but I think that you need both. EDR can show you keystroke level precision of activity. NDR can perhaps resist attack better, assess the whole organization better over time
Including this recent breach that happened at Sanofi, how many days on average do they need to detect/respond to an incident and has Vectra helped to measurably reduce this time?	For me, we are not looking to Vectra to solve this particular problem. The problem we are trying to solve is when all other tech goes silent, when the attacker is a sophisticated, how can we detect?
Were you able to evaluate the return on ivestment you gain implementing Vectra and collaborating with Vectra Team	Our posture here is not to defend a "ROI" which will never statisfy the top management. We want be able to detect as fast as possible and react fast enough to avoid any damage. We are implementing a matrix approach to back-up each level of protection / detection with another one belonging to another technology (NDR versus EDR or NDR versus IPS/IDS for instance or NDR versus OT probes for instance). Duplicate the same capability withtwo vendors is not our vision of smooth spents
Do you use EDR, which one?	FireEye and we are satisfied with it
Do you plan to extend Vectra Detections to OT world?	Yes
How long did it take for Vectra's solution to "learn" normal behavior from Sanofi's network	Probably two months of tuning and we are continuing to tune over time with occasional FP.
How many people are operating the Vectra system at Sanofi and work on the alerts?	1 plus the team reaponds to detections and know how to tune the system after a false alarm.

For more information please email us at info@vectra.ai.

Email info@vectra.ai vectra.ai