Analytics Rule Blindness

“ARB”

A term that analytics will encounter during work with network sensors

Made by
Lenny Hansson
Senior Security Analyst @ Networkforensic.dk

Date: 12/28/23

Description

During my many years of work with network-sensors systems listening into traffic on many types of different networks, I have always missed a term like this I could explain to new analysts. The term is “Analytics Rule Blindness” and all network analysts need to know and understand the term and its effects.

Both new and experienced cyber security analysts who study network traffic need to be aware of a potential blind spots that can result in making inaccurate judgements on alerts/noteables. A side effects can also be “analyst fatigue”

Challenge

When analysts are reviewing network traffic, the traffic is captured onto a network sensor of some sort, either from network taps, monitor ports, forward traffic from an application on a server system and so on. Meaning the analyst can only see what have been send to the sensor for monitoring. The analyst is often not aware of what filters have been put into place, before or after the sensor received the traffic. This is where many hours can be wasted on validating with the possibility of making wrong decisions if traffic can be harmful or not.

When analyst are doing analytic on network traffic, the traffic is captured onto a network sensor of some sort, either trough the means of network taps, monitor ports, forward traffic from an application on a server system and so on. The analyst can only see what have been send to the sensor for monitoring. The analyst in often not aware of what filters have been put into place, before ore after the sensor received the traffic. The is also where many hours can be wasted on validating with the possibility of making wrong decisions if traffic can be harmful ore not. Even worse, someone can have manipulated the traffic in order to save money for reasons like trying to save money on license fee for a SIEM systems. Some side effects can also lead to things like “analyst fatigue” But the worst part is bad judgments on alerts/notables and wasted hours on validating the traffic.

Explanation

When traffic is coming from a network-tap, and the network-tap is placed “in front” of a firewall , then the analyst see all the traffic hitting the outside of a firewall/router including the traffic passing trough the firewall and “drop traffic” is also visible. However the analyst can never see what firewall rules are in place inside the firewall and how they are formatted. The same thing apply also for sensors placed behind a firewall.

However, the analyst can say that a full TCP/IP connection was created or not, and thereby say something about that there might be a firewall rule that allow that traffic to go though the firewall or not. The analyst can’t see rules in the firewall that might apply to that traffic, that could be things like “point to point” firewall rules, where traffic is only allowed between two or more IP addresses, or other things like IDS/IDS, Content filtering, and so on that the firewall might have. Even scheduling on when ports are open from the outside to the inside here traffic is only allowed on a certain time of the day/week/years. That could also be true for Geo-filters, where traffic is only allowed to come from a specific country.

The analyst can even be prohibited from being allowed to see traffic, this can be filtered on the sensor itself or from somewhere in the ISP’s network. So there are a large number of unknown factors that can come into play, when the analyst makes judgments on performing analysis of network traffic. Besides all that, there is a large amount of protocols most sensors ore SIEM systems don’t even understand.

Examples

Lets say that the analyst see traffic that could be related to what the analyst might think is bad policy “bad policy'” (Yes..define bad policy's) like a clear text protocol as HTTP, Telnet, FTP, DNS and so on, that are triggering any form of rule on the sensor.

The analyst will never know if that if part of a firewall rule already in place, that are either intentionally placed or a possible misconfiguration in the firewall rule-set. The analyst know that the traffic is running though the firewall, that can be based on a large number of factors. A simple example can be based on connection flags in the traffic. It is quite easy to see if the traffic between of one more IP’s have communications and connection, and what port it runs on, but he can never see the firewall rule that could be performing any of this filtering.

So it all boils down to that the Analyst can’t see firewall rules in network traffic or what he has been prohibited to see. The analyst will thereby often never know what to expect. It is important for the analyst to have some sense of what to expect before making any judgment calls if it is good or bad. It often leads the analyst to have to contact customers or firewall operators and start asking questions. (The clock is ticking here and is bad for businesses)....

I have seen that someone thinks it is wise to allow FTP traffic between 2 IP' addresses controlled by a firewall rule. The analyst can't see the firewall rule that only allow the 2 IP-address to talk FTP. Is the traffic in any danger? Maybe?

Lets say that the one IP is from the inside to a system outside is a controlled network in a foreign country ore just another network, then there could really be a danger of letting this happen, because anywhere on the route, the traffic can be intercepted and passwords, files and so on can be extracted from traffic.

What about encrypted traffic ? Agencies and others around the world are working by the term "Harvest now – Decrypt later" that refers to a proactive approach taken by potential adversaries who compromise systems to collect encrypted data today with the intention of decrypting it in the future when quantum computers are powerful enough to break existing encryption methods ore some vulnerability is discovered that makes decryption "easy".

You should really be aware that all your network traffic is always intercepted somewhere on the wire.

The analyst has to make a lot of judgments during a normal work day. There are many scenarios where this can be very important to know what the sensor is covering and where it may be located in the network or in the world.

Another example is where the analyst sees someone logging on to a firewall from some "strange" IP to a web-interface on a firewall with a self signed certificate. How should the analyst ever say that this is bad if there haven't been some sort of documentation on what the analyst could expect ? Again this could simply be covered by a "point to point" firewall rule allowing the traffic to happen between two trusted IP's.

What about allowed services ? This could also be a service someone have that is put into place, like vulnerability scanners, that test all vulnerability's on the IP-range that the sensor is covering, this will be setting off alerts in all directions, and make it hard to see if this is someone is attacking or not. This quite often lead to bad judgment, simply because it was not documented for the analyst. The analyst will start making phone calls to customers and say they are under attack.

So there is a lot of potential issues that the analyst will see every day, and it can really help to have some documentation for every sensor you might have to make things easier for the analyst.

There can be many scenarios where it might be good for the analyst to known what a sensor is covering, and have some sense of what firewall rules there might be in place. A lot of misinterpreted alerts can be stopped before it leads to phone calls to customers.

Mitigating Analytics Rule Blindness

Mitigating this issue can be quite easy for most running sensor-systems. It is always a good idea to have some sort of sensor documentation to explain what the analyst can see from a given sensor and how and where the sensor is placed.

Know the term “Analytics Rule Blindness” (ARB) to explain why you are asking for some documentation and then create some guidelines from what you already know. What’s expected to see on the sensor, is there placed anything in front that can manipulate what traffic you are allowed to see? What systems are running through the sensor.

Is it only Clients, Servers, IOT systems and so on. Is there any IP ranges where only servers will be running from ? It could just be an open wireless guest network of some sort. Any special type of traffic to any partners that are allowed. Make basis documentation for any sensor you monitor.

Understanding ARB can help an analyst from wasting hours/weeks/years trying to figuring it all out , help new analyst making good judgment, getting rid of analyst fatigue, and even getting the right analyst person/skills that know a “special way” to monitor the system. You might not even have the right filters in place on the sensors if you want to monitor the QUIC protocol.

I believe the most important thing can be to create some PCAP’s from the Sensor and store them for references, when you need to validate the system down the road. Test some created IDS/ SIEM rules, that have been validated as well. Store them on a system that is not the sensor and document what you can see and not see.

Get this in place before you consider a network sensor to be fully implemented. Let some else test the documentation before production. And always be aware of “ARB” If you encounter them then document them.