HIVEWATCH

Developing a Strategy for Reducing Noise in Security Operations Centers

Developing a Strategy for Reducing Noise in Security Operations Centers

A step-by-step guide to tackling your false alarms

There's a huge misconception when it comes to handling noise in security operations. No two companies are exactly the same – and similarly, when it comes to noise reduction, there is no "one-size-fits-all" (or will quiet all) approach. Each company is dealing with their unique noise, which means customization is key to silencing alarms without suppressing the ones your team actually needs.

It's not enough to purchase the band-aid of an out-of-the-box noise reduction or false alarm detection software to solve these pains. Organizations must take steps to develop comprehensive strategies for reducing and understanding their noise in their security operations centers (SOCs) in addition to finding the right software.

But what does this kind of strategy entail? This eBook aims to explore some of the biggest noise perpetrators and give a step-by-step guide on how organizations can create a strategy to address these false alarms and other noise.

The Problem

Picture this: A typical global security operations center (GSOC), depending on the size of the organization it protects, might have dozens of operators and analysts, overseeing hundreds of locations around the world, and responding to hundreds, sometimes thousands, of alarms each day on numerous disparate platforms.

One of the main complaints heard in a GSOC is the overwhelming number of – mostly false – alarms that are coming in from a variety of sources at any given time. At times, there can be so much noise that operators miss an actual critical event, which can be dangerous and diminishes the value of the program and the organization's significant investment.

What is "Noise"?

"Noise" in a GSOC refers to the numerous false alarms coming in for operators to analyze and address. Amongst this "noise" are legitimate security alerts that need to be addressed immediately, crowded by completely false alarms triggered by faulty sensors, environmental factors (wind, rain, animals), and user error. When left unaddressed this noise problem can result in system overload, compromised security, high

One glaring cause for this is multiple security systems continually pushing streams of data for analysis – often across multiple platforms to manage. The majority of these systems don't "talk" to each other, which results in a level of difficulty for operators in a centralized SOC in achieving a streamlined workflow.

The "noise" from these disparate systems can become problematic and limit appropriate response, as well as increase the amount of time it takes to respond to and resolve incoming alerts.

Here's an example: A GSOC operator gets a "Door Forced" alert from an access control system. When an operator receives an alert of this happening, in many cases, that operator has to go in to look at the timestamp of the door forced within the access control solution, then access a different video system and search for the door that a specific camera is fixed on (this assumes that the disparate systems are properly time synced). Then they have to pull up the video manually in many cases to see who forced open the door and gather all the details of the incident.

In many organizations, various facilities are on different video platforms, which adds to the complexity and time in finding the right video clip. While there are some systems that integrate these two functions together, in the case of a centralized SOC with numerous locations and various solutions installed, there is a broader need for alignment between systems.

operator turnover, and complacency.

What Causes False Alarms?

The scenarios are endless, but here are a few common ones we've seen:

- Sensors not lining up
- Broken hardware
- Environmental factors such as wind or rain
- Shadows caused at different times of the day
- Animals being identified as humans/setting off motion detectors
- Janitorial staff pushing on doors to clean them
- User error

A New Strategy for Noise Reduction

As said in the introduction, an out-of-the-box solution alone might not be the best option for companies looking to adopt a noise reduction strategy for their operations center. Each company is dealing with their unique noise, meaning customization is key to silencing alarms, without suppressing the ones your team actually needs. In other words, one man's noise is another man's treasure. You need to have a plan to prioritize and complement the data you get from your chosen noise reduction solution.

Here are the steps to take when redefining your noise reduction strategy:

Step 1: Establish a baseline for your noise.

Essentially, you need to know where you're starting to know where you're going. Find out:

- Average number of alarms/month (this should not include all "events." Alarms include security events like doors held open, doors forced, etc.)
- How many alarms are considered "false"
- Average time it takes to respond to a false alarm

With this information, not only can you start to see the true impact of your problem, but also begin to quantify it by taking the wage of your operator, and calculating approximately how much these alarms are costing you. (If you're looking for a quick cheat sheet, you can use our noise reduction estimator at hivewatch.com/noise-reduction.)

Step 2: Figure out where your noise is coming from.

Before you can put together a strategy for reducing noise across your organization, you have to be able to identify where it's coming from. Are alerts coming from cameras? From access control readers? A mixture of both?

At this stage, it's all about determining what devices are triggering the most false positives and documenting when a false positive comes in. Chances are, most of your false alarms are consistently coming from the same places or are duplicative. (Duplicative alarms can be caused by faulty hardware that creates way more alarms in a timespan where it is not physically possible to have that many security incidents happen.)

Once you have that list, you are then able to prioritize which devices cause the most false positives so you can have the greatest impact.

Step 3: Understand why it's making the noise.

Some of the most common types of problems related to false alarms fall within three issue categories: hardware, software, and configuration. We've listed a few of the frequent malfunctions in each category here for your consideration:

Hardware:

- Contact connectivity

Common Challenges for Noise

Problem: I get too many false alarms.

Not only do teams who are burdened with excess noise face alarm fatigue, missed incidents, and additional employee turnover, but they're also losing focus on more critical security initiatives

- Device health
- Request to exit (RTE)
- Door forced open
- Door open too long
- Lock hardware not re-engaging/latching properly
- Use of keys as opposed to access cards (not recognized as a credentialed open)

Software:

- Camera setups that coincide with access alerts
- Analytics alerts
- Motion detection misfires

Configuration:

- Sensitive access control configurations and settings
- Sensitive camera and analytics configurations

This one may need a little more of an explanation. Businesses change – and configurations need to change with them. When a security system is set up there are some assumptions made to work with the flow of the business – but do those assumptions hold true today?

For example, a door may have been previously set up to alert when it's held open for 5 seconds. Now, you might know this door is routinely, and justifiably, held open for more than 30 seconds at a time. This needs to be adjusted as such.

which could ultimately improve the health and efficiency of their security program.

Problem: My noise reduction software doesn't understand the kinds of alarms I want to get.
What may be noise to one SOC could be music to another's. When overlaying an uncustomized, standard software there is a risk of losing or silencing real alarms.

Problem: Underperforming or offline devices add more noise to the equation.
Device health management is a critical piece of the puzzle for addressing noise reduction in a GSOC, which can contribute to lost time and resources triaging hardware issues. Quick identification and remediation is needed to help reduce the number of alarms incoming from these sources.

Step 4: Creating an action plan.

Now that you know where your alarms are coming from and why they are happening, you can create your strategy and action plan. Also assuming you did the baseline analysis in step 1, you should have a goal of what success looks like to you. The strategy should include addressing the ongoing noise, as well as choosing an appropriate noise reduction software so this problem doesn't spiral out of control again.

And as we all know, technology can't fix everything. There is a fair amount of training that can be done to address behavioral causes for false alarms across an organization, as well. Partnering together to align the two is essential.

The HiveWatch® GSOC Operating System

The **HiveWatch® GSOC Operating System (OS)** analyzes not only the systems being used, but individual customer data to determine the most accurate and productive path forward. This, combined with machine learning, allows HiveWatch to dramatically reduce false alarms and excess noise.

One HiveWatch customer saw a significant reduction of false alarms within the first 60 days. Through the data provided by device health monitoring within the HiveWatch® GSOC OS, the customer was able to have their systems team address the root cause of 30% of their false alarms.

Prior to implementing the HiveWatch platform, the same customer had so many incoming alarms that they determined the organization would need six times the number of operators they currently had per day to respond to every alarm as they scaled. Implementing the platform meant addressing false alarms and freeing up 57% of the operators' time, thereby saving a significant amount of money on additional headcount.

Another customer had a GSOC that oversees multiple facilities globally, which meant incoming alarms were (at times) overwhelming. Implementing the HiveWatch platform to identify device health issues that were causing so many of these alarms reduced false positives in the GSOC by 60% over five months.

HiveWatch facilitates this process through data-driven means that constantly learn and predict how an organization makes decisions. The rest? It's just noise.