SOC False Alarm Reduction

SOC False Alarms: A Huge Challenge

CSOs and Security Leaders rely on Physical Security Operation Centers (SOCs) to deter criminal activities and protect people, property and assets. SOC systems are designed so the security personnel are notified whenever an alarm or anomaly occurs across the local or global enterprise. Based on SOC procedures, each alarm typically requires up to 10 minutes of an operator's time for video verification followed by any needed investigation by dispatching a security officer, documenting the response, and creating an Incident or repair work order when warranted.

80-90% of all alarms are either false or nuisance alarms.

False alarms triggered by physical security systems pose a huge challenge due to the high costs they incur for all involved. False alarms waste expensive system operator and security officer resources as well as prohibit SOC operators from prioritizing important alarms. SOCs spend approximately $200,000/ quarter on managing false alarms.

Because 80-90% of all alarms are either false or nuisance alarms, they typically require a larger staff of system operators or security officers, disruptions to businesses, unnecessary hardware replacements, and increased MTTA (Mean Time To Acknowledge) Critical Alarms.

Addressing the Root Cause of the Problem

Vector Flow partnered with several customers and consultants to research the root cause of false and nuisance alarms, and determined that there are three recurrent themes:

1. **System Programming Issues:** Even though most organizations utilize high-quality (and expensive) equipment from leading manufacturers, most of that equipment is installed with default or sub-optimal settings. Because the settings are not tailored to the specifics of the installation, they are a big source of false alarms. Also, systems teams struggle to coordinate an endless array of physical security devices with an independent set of security controls – with no orchestration between them.

> "Every day SOC runs, 23 hours are wasted on False Alarms."
>
> - Security Manager, F100 Company

2. **Installation Issues:** When the security system is installed, it is critical that all sensors, resistors, wiring, timers, etc., are correctly aligned, and that they are installed, tested, and working per the manufacturer's recommendations. Most physical security devices have an electro- mechanical nature, and any improper assembly or inadequate pre-use testing will result in thousands of false alarms during daily operation.
3. **User/Human Error:** Another common cause of false/nuisance alarm is lack of alignment between security thresholds and business needs. Such misalignments are common in Data Centers, Customer Briefing Centers, Training Areas, Equipment Labs, Shipping/Receiving, and Freight Elevators, which are areas frequented by employees and non-employees.

Typical False Alarm Coping Strategies are Unacceptable

With a routinely high percentage of false and nuisance alarms, SOCs have been conditioned to either "mask" or "suppress" their false alarming devices to avoid dispatching officers to what they believe to be a false alarm. By literally ignoring or disabling alarms, SOCs risk failure to respond to a real alarm – thus creating a security hole. As the rate of nuisance and false alarms increases, the physical security system's perceived reliability decreases, causing SOC operators to lose trust in the system (the "cry wolf" effect).

The Solution: Implementing AI-Driven Vector Flow

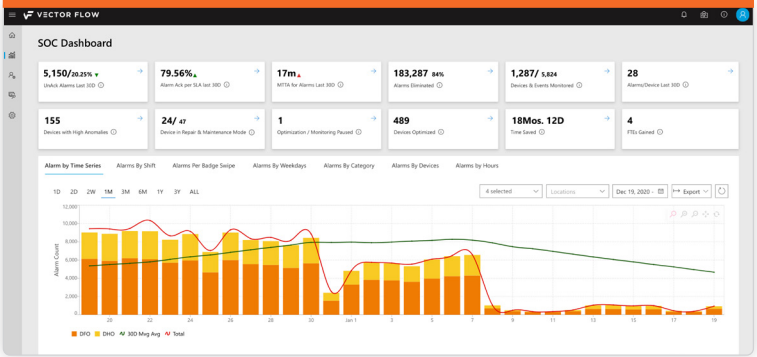
Vector Flow solves this problem by automatically analyzing thousands of security events in real-time, classifying false alarms with high accuracy and automatically fixing the system programming issues of alarm devices. This requires a combination of approaches - artificial intelligence (AI), stream processing, and analyzing real-time and historical data together.

> Vector Flow solution begins eliminating 30 to 50% of false-positive or nuisance alarms within 48 hours of deployment.

Historical event data helps build AI models for the behavior of every security device while real-time data ensures maximum relevancy in the present. We combine all three approaches into a single, real-world SOC Automation solution. Vector Flow automatically performs baseline physical security system assessments by understanding building or facility usage, conditions contributing to alarms, alarm thresholds for each sensor, device history, prior repairs, errors observed, users causing most alarms, and more. SOC Alarm Manager provides a quick return on investment (ROI) by performing real-time data analysis and then recalibrating the underlying security system to "optimize devices" thus eliminating false/nuisance alarms. This AI-driven automation reduces the SOC alarm workload while allowing SOC operators to spend their time proactively resolving real alarms, instead of masking or chasing false ones.

The ROI from such automation can be realized in just days because the Vector Flow solution begins eliminating 30 to 50% of false-positive or nuisance alarms within 48 hours of deployment. Vector Flow solutions require no new hardware equipment (cameras, etc) to be purchased or installed.

SOC Alarm Reduction



SOC Alarm Dashboard tells a straightforward story, including:

1. Alarms, devices, and locations that caused business interruption
2. What devices are causing alarm fatigue
3. What times of the day and what days of the week are most susceptible to high alarm rates
4. Forecast of alarm for the upcoming /day for better guard force management
5. Alarms that can be avoided from process, personnel improvements, or repairs

Vector Flow supercharges the scalability, performance, and speed of your SOC with the ability to process 50,000 security events per hour. Save time and money, all while increasing productivity, efficiency, and accuracy.