



ROI from SOC Automation

Chronic Problems at Physical Security SOCs

False alarms in Physical Security SOCs¹ are a chronic issue costing organizations \$50,000-\$250,000/quarter² in wasted physical security resources. Within the United States alone, false alarms cost \$3.2B/year, in addition to causing mental fatigue for SOC operators and officers. The COVID-19 pandemic has forced organizations of all kinds to examine and define which core functions and services are truly essential. Physical SOCs is one of the most critical parts of business continuity. The tasks performed by SOCs include securing data centers from sabotage, restricting people from entering secure areas of critical infrastructure, preventing property/IP theft on a corporate campus, responding to natural disasters or pandemics, ensuring compliance, and much more. Physical security teams work around the clock identifying, analyzing, and mitigating threats facing their organizations. The job is even more difficult when teams are burdened with hundreds or thousands of point products and independent static security configurations with no orchestration between them. False alarms, nuisance alarms, and maintaining system/device health regularly overwhelms SOCs³ staff, distracting them from more risk remediation tasks. Many organizations do not have enough security personnel to thoroughly review the volume of daily security alarms/requests generated by these disconnected systems, and the result is often a growing alarm backlog and operator fatigue/high turnover.



¹ Security Operations Center, a.k.a GSOC, Fusion Center, Alarm Center, Command and Control Center, etc.

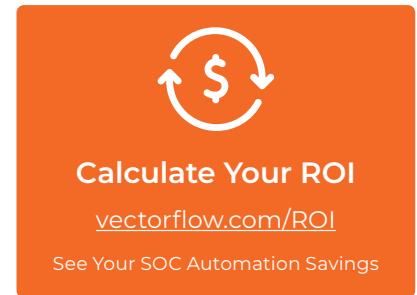
² <https://www.securityexecutivecouncil.com/spotlight/?sid=31426>

³ <https://www.osti.gov/biblio/1347158>

Cost of Manual Security Operations

To first understand the ROI benefits of Out-of-the-Box SOC Automation we first identify the costs that it takes to perform the operations manually. We identify them into three core sections:

- People
- Process
- Technology



People

Personnel costs still continue to be the most expensive portion of the security investment with average salaries ranging from a mid-Security/SOC Analyst (\$50/hour) to a Security Manager at (\$65/hour). Hiring security talent still remains a top problem with hiring managers reporting that it takes an average of 6 months to fill up open requisitions that require more than 5+ years of SOC experience. ROI Calculator tracks this as **'Hourly (fully loaded) cost of your SOC Operator?'**.

Process

It takes significant time to invest in a good security process that works consistently, automates tedious tasks that otherwise are done manually. For example, investigating a Door Forced Open (DFO) alarm (positive or false-positive) involves the SOC operator performing the following steps in serial order:

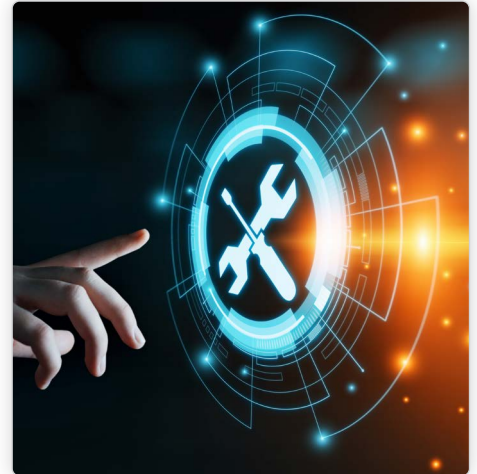
1. SOC Operator's Console receives a DFO (initiated from a device/sensor)
2. SOC Operator check if the Alarm is already acknowledged? If not, acknowledge the alarm
3. Identify the Door and extract all the details – Name of Door, Site, past history, any open service tickets
4. Watch Live Video and Recorded Video (before the Alarm) to investigate
5. Check card swipes and verify personnel who entered/exited prior-during-and after the alarm
6. If needed, dispatch a patrol officer to check the door, radio-call/create dispatch order
7. Check if the Door needs Repair or is already in Maintenance mode
8. Enter comments based on response and close the alarm
9. Finally, as needed create an Incident Report, or a repair work order and notify the team

Our customers reveal that it can take a very long time to define, train and mandate a well-defined SOC response. Often, SOC operators miss or skip few steps largely due to a high number of alarms, lack of context, or training – and the manual process steps can easily take up 5-20 minutes/alarm response. ROI Calculator tracks this as, **'Time taken by your SOC Operator to resolve an Alarm'**.

Technology

Finally, the choice of technology and supportive integrations play a role in the cost calculations. SOCs has a huge operating cost associated with running and maintaining SOC tools & technology. Unexpected downtimes, technical team costs, emergency repairs, tracking repair work orders across different system integrators, tracking repair SLAs are all manual – these significantly add up SOC costs. These are tracked in the ROI Calculator as:

1. **Number of Buildings where your organization conducts Alarm response?**
2. **Number of SOC operators that are part of your security Alarm response?**
3. **Number of Daily Alarms received globally across all SOCs?**



Cost with Out-of-the-Box SOC Automation

Vector Flow’s AI-Enabled SOC Automation Platform leverages Artificial Intelligence and Machine Learning (AI/ML) deep learning algorithms to process and evaluate the enormous data and automate SOC processes. Based on customer and industry results, ROI Calculator provides an estimate of **60% reduction in SOC Operator response time and associated costs** for a mid-size enterprise with 65 buildings, 16 SOC operators (to run 24x7x365 days operations) with an estimate of 1,000 alarms/day received. With Physical Security SOC Automation, they see:

SOC Cost Savings: \$3 → \$1 Per Minute	SOC Cost Savings: \$960,000 Per Year	Time Saved: 512 Man Days Per Year	FTE(s) Gained: 2
---	---	--	----------------------------

The SOC automation results in a reduced effort that can be realized as cost savings or increased SOC capacity for other duties including improving the service quality. The Full-Time-Equivalents (FTE) gained metric quantifies how the processing capacity of the SOC team has expanded with automation.

Conclusion

Via the ROI Tool, you can assess the benefits specific to your SOC team. Vector Flow SOC Automation Suite can bring quick value and demonstrate ROI within months. The Vector Flow SOC Automation Suite comes with easy Out-of-the-Box connectors and will automate all your security processes, without writing a single line of code. This will help you save time and money while increasing productivity and efficiency.

Please contact sales@vectorflow.com for further details.