OPTIMIZE YOUR SOC

Guide to Optimizing a Physical Security Operations Center

DATAMINR PULSE

Introduction

You're managing a well-run physical security operations center (SOC) that has an established technology stack, an experienced team, and predefined workflow processes. While your SOC has demonstrated value on multiple occasions, it's been challenging to justify further investment in the program.

Conversations with company leadership inevitably lead to questions about the program's budget. Questions like, Does it make sense to outsource parts of the physical security function? Will using a managed security services provider offer similar security coverage at a fraction of the cost?

This guide is designed to share best practices for optimizing an existing SOC, based on Dataminr's experience working with hundreds of the world's leading physical security teams and SOCs.

At their core, physical security operations centers do five things:

- **Real-time information** flows into the security team and forms the basis for all decision-making
- **Analysts** process real-time information and decide how to take action to mitigate risk
- Risk mitigation actions enter **workflow processes** that are repeatable, scalable and measurable
- The team **reports its impact** back to the business, to justify continued investment in the program
- Build toward the **converged security** future

To optimize a SOC's performance, SOC managers must closely examine these five major functions to identify ways to improve each individual function.

Optimize the SOC's access to real-time information

Physical and cybersecurity operations centers are powered by real-time information. Giving SOC analysts access to real-time information results in more consistent outcomes, as measured in response time and the impact of actions taken.

SOC managers want to consistently be informed about emerging risks first, before other groups inside the company. SOC managers tell us that the phone call they dread the most is from their CEO, calling to ask about a risk incident that the SOC wasn't previously aware of.

Several years ago, the greatest technical challenge facing SOCs was inconsistent access to real-time information. The SOC would get phone calls and messages from employees about potential risks in their area, and analysts would work to gather enough corroborating information to put together a risk mitigation plan. During large-scale or complex risk incidents, SOCs had difficulty consistently building a complete picture of the risk environment.

In other cases, SOCs would set up keyword watch lists inside social media monitoring tools, in hopes that they'd catch the majority of emerging risks in near-real time. Those tools were incredibly noisy, surfaced volumes of irrelevant content—and often missed actual risks entirely, especially those that had not been predefined.

Today, artificial intelligence is capable of processing massive volumes of data at scale, to give SOCs more consistent access to relevant, real-time information, often within seconds of a risk incident occurring.

Let's take a closer look at the three major sources of information available to SOCs today, and how they can be optimized.

Internal communication tools

When they need help, how do employees currently communicate with analysts inside the SOC? Consider investing in communication tools that are easy to use, and automatically trigger workflows inside the SOC's ticketing system. Take a closer look at:

- 24/7 phone services that transcribe and log incoming calls into the incident management system
- Messaging software that allows for two-way, mass communication with employees and SOC analysts
- An email alias that automatically classifies incoming messages and logs them into the incident management system
- Purpose-built security apps for travelers that allow them to proactively check in and see real-time information relevant to their current location

Automated internal security sensors

How many internal IoT sensors communicate directly with the SOC? Take a closer look at:

- Identity and access control systems that go beyond simple employee badges and passwords, and instead provide a second layer of identity verification, like biometric scanners or mobile device management
- Automated building management systems that communicate directly with the SOC, notifying analysts to alarms, broken glass, open doors and power outages
- Location tracking systems on company-owned cars and trucks as well as personal distress devices for field personnel that communicate directly with the SOC
- Software that delivers a single pane of glass that displays all internal IoT sensor data in one place

Access to real-time information

Is the information coming into your SOC delivered in real time? How quickly is your SOC notified when an unexpected risk incident occurs that could impact business continuity? If you're currently using an all-in-one risk management platform, the answer is likely "not fast enough."

Does your existing alerting platform contain enough contextual information for SOC analysts to take decisive action?

Dataminr uses artificial intelligence to process public data from more than 150,000 sources in real time, consistently finding the earliest indicators of emerging risk incidents worldwide. Artificial intelligence is faster and more comprehensive than competing information sources manually processed by analysts.

Real-time information from Dataminr Pulse frees up valuable analyst time, so analysts can spend more time mitigating risk, rather than searching for it.

Learn how Ellie Mae used Dataminr to protect their employees in the Midwest, following a devastating cyclone in 2019.

READ THE CASE STUDY

Optimize how the SOC processes information

SOCs are fueled by real-time information, but still require an intermediary—either by analysts, automated software, or a combination of both—to process the information and make a binary decision: Is this risk something that we need to take action on? From there, many other decisions will be made.

Information analysis at scale represents one of the greatest areas for innovation in the physical security industry today. **This innovation is happening on two fronts:**

Improved relevance of real-time information

Measure the volume of information currently coming into your SOC, and what percentage of that information is relevant and useful. Take this data back to the information platforms that power your SOC. Analysts who spend the majority of their shift processing consistently irrelevant information are more prone to make mistakes or miss early signals about an emerging risk.

Real-time information platforms should give you the flexibility to tailor incoming alerts to your company's specific risk profile—your physical locations, brands, the names of your executives, competitors, and other relevant risk focus areas.

Automated decision-making

Artificial intelligence will eventually be capable of automatically triggering workflows without the SOC's direction or intervention. Forward-looking SOCs are already beginning to adopt automated workflows, which allow the SOC to take action more quickly.

For example, a SOC might get a real-time alert that there's been a major earthquake near one of their satellite offices. This immediately triggers the automated software to issue a mass notification message to employees assigned to that office, asking them to communicate back to the SOC that they're safe and don't need immediate help.

Optimize how the SOC turns alerts into action

You've optimized your information sources and have taken a closer look at how your SOC is processing that information. Now it's time to ask: How efficiently are alerts turned into action?

Workflow processes, such as after-action reviews, should be examined after every major risk incident, to find areas where they fell short and can be better optimized. The incident management software you use should be set up to measure the SOC's performance—data that can serve as the basis for ongoing reports about the SOC's effectiveness and value:

- How many alerts are processed every hour?
- How many of those alerts do SOC analysts take action on?
- How long does it take for the SOC to receive a notification of an incident, analyze it, and take action?

Make it a best practice to close the feedback loop on actioned alerts, measuring the positive impact of early action.

Some SOCs use tools more commonly found on customer service teams, to measure how quickly analysts are responding to internal communications. A small group of high-performing SOCs take this concept one step further, sending out employee satisfaction surveys after every interaction with the SOC, asking employees to rate their experience and provide feedback.

Optimize how the SOC reports its impact back to the business

SOCs perform mission-critical work for the organizations they serve, and SOC managers should look for ways to better market their team's impact internally. Make it a habit of packaging measurement results, after-action reports, and employee satisfaction survey data into a quarterly presentation aimed at the C-suite.

Focus on risk incidents where the SOC provided outsized value to the organization, by either using real-time information to alert early on a previously unknown risk, or where departments might have had trouble coordinating action without the help of the SOC.

Consider measuring success across three areas:

- Improved productivity: SOCs help deliver improved productivity across the business, due to their unique ability to process real-time information
- Reduced costs: SOCs provide timely intelligence around risk, helping business units reduce costs by mitigating risks early
- Reduced risk exposure: SOCs increase risk awareness at the earliest point of detection, to help the business quantify and proactively reduce its risk exposure

Look for ways to provide more value to the business, by using real-time information and the SOC's internal knowledge, to help leaders make decisions that proactively mitigate risk. For example, here at Dataminr, we've seen SOC managers use security data to help operations teams choose the best location for their next satellite office or distribution center. We've also seen SOC managers use security data to help risk managers identify which markets to enter or divest from.

Plan for the converged future of risk management

At most organizations, specific teams own well-defined areas of risk:

- The physical security team is responsible for employee safety, executive safety, travel safety and physical asset protection
- The cybersecurity team is responsible for information security
- The legal team is responsible for compliance and regulatory risk
- The marketing team is responsible for brand and reputation risk
- The risk management team is responsible for long-term planning and proactive risk mitigation

These risks are increasingly converging, and forward-looking organizations should break down operational silos to manage risk more holistically.

In practice, that means disparate teams have access to the same real-time information, communicate regularly, and build operational workflows that encourage collaborative risk management decisions, rather than singular decisions in silos.

A small number of organizations are adopting true, converged security operations centers, where teams—physical and security but also liaisons from across the business such as HR and legal—sit together, share tools, and report to the same manager.

Even if your organization decides to keep its security operations centers separate, make it a best practice to adopt elements of a converged risk management framework by sharing information, intelligence, and visibility into shared risks.

Creating the Security Operations Center of the Future with Real-time Information

READ HERE

These best practices are aimed at helping you optimize your current SOC, and build in the flexibility and adaptability needed to future-proof it.

Dataminr Pulse forms a crucial building block for hundreds of SOCs globally.

Learn more at dataminr.com/pulse

Learn more

Request a demo

Book a demo to see how you can gain earlier insights into high-impact events and emerging risks.

BOOK A DEMO

Contact us

General | info@dataminr.com

Support | support@dataminr.com

Learn more about SOC at our Security Operations Center hub