PLAN AND BUILD YOUR SOC

Best Practices for Building a Physical Security Operations Center

DATAMINR PULSE

Introduction

You and your team have been tasked with building your company's first physical security operations center (SOC). The project has an executive sponsor, a strong business use case and budget, and you're eager to build a high-performing SOC that can handle the increasingly sophisticated risk landscape facing your company today. This eBook is designed to help you think through the people, processes, technology and key performance indicators necessary to build a leading SOC.

Risk incidents as a catalyst for action

Before making the decision to build their first SOC, many companies have already experienced a risk incident—one that their existing physical security team struggled to respond to effectively. Those incidents can spur a company's leadership team to action, and form the basis for the business case for added investment in the company's security function.

Here are some examples of risk events we've seen from our customers, all of which led them to build their first SOC:

- A company's CEO was in a meeting at a satellite office when they heard gunshots outside the building. Contract security officers onsite locked the office doors and told people to stay inside, but the response was chaotic and employees were scared. The CEO later called into their company's corporate security team, which had no idea there had been a shooting near the office.
- A major earthquake rocked Mexico City in 2017, toppling dozens of buildings and killing several hundred people. A major American company had multiple office locations in Mexico City, and needed to quickly account for employees and executives. News reports were slow, and didn't contain the granularity the security team needed to plan evacuation efforts.
- During the early weeks of the COVID-19 pandemic, retailers faced a rapidly shifting patchwork of state and local health regulations. One major American retailer struggled to build a complete picture of the regulatory restrictions affecting their stores across the country. Separately, the retailer's leadership team asked the security team for daily situation reports on COVID-19 case counts, which were difficult to manually compile from public sources.

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

How you design your security operations center will depend on the budget, risk profile and goals of your organization. Every centralized corporate security team shares four common characteristics, no matter its size, industry or area of responsibility:

- **Real-time information** flows into the security team and forms a crucial input for decision-making
- **Analysts** investigate real-time information and decide whether to take action to mitigate risk
- Risk mitigation actions enter **workflow processes** that are repeatable, scalable and measurable
- The team **reports the SOC's impact** back to the business, to drive further investment in the program

Despite those similar characteristics, there is no one-size-fits-all approach to designing or scaling a centralized security function. The size and responsibilities of your organization's centralized security function will depend on the unique risk profile facing your company, its risk tolerance, leadership, corporate culture and other factors.

Dataminr works closely with hundreds of the world's top-performing SOCs, providing them with a unique view into best practices across the industry.

We've seen companies of a similar size, in the same industry, and with a similar risk profile, design their centralized security team in dramatically different ways. In one example, Company A opted for a large global security operations center, while Company B opted for a decentralized approach with small, regional teams working largely independently from one another.

Despite those stark operational differences, real-time information is a crucial component in how security teams act to keep their people and assets safe.

Let's take a closer look at the individual components of a centralized security team.

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

Real-time information

Real-time information, from internal and external sources, forms the cornerstone of a high-performing security team. Real-time information is information about a specific risk incident delivered as quickly as possible after the initial event; in many cases, within seconds.

Information comes from multiple sources:

- Internal tools:
  - Access control systems
  - Video surveillance
  - Network security appliances
- Rapid lines of communication with the business:
  - Dedicated security email alias
  - Security apps
  - Chat tools
  - 24/7 phone number
- External news and information sources:
  - Social media monitoring tools
  - News feeds
- Real-time information platforms like Dataminr Pulse

Together, these real-time information sources give security teams—from the analyst to the chief security officer—a comprehensive picture of the current set of risks facing their organization. During a crisis, security teams are evaluated on the quality of the real-time information at their disposal, and how quickly they can process and act on that information to protect business continuity.

Real-time information is fed into other technology platforms inside the SOC, such as:

- Risk monitoring platform with locations of interest
- GIS mapping and data visualization
- An incident response ticketing and workflow management system
- Mass communication tools
- Travel information platforms
- Cybersecurity alerting software

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

Key Considerations When Building a Security Operations Center - Plan and Build Your SOC

READ HERE

Artificial intelligence inside the SOC

How much time do your security analysts spend gathering information? Dataminr Pulse uses artificial intelligence to help your analysts spend less time searching for information, and more time acting on it.

Dataminr's AI platform processes more than 150,000 public information sources—social media content, internet-connected sensors, news sites, audio feeds, and the deep and dark web—at scale, delivering the earliest indications of emerging risks to business continuity.

The platform is highly configurable: Identify your organization's physical locations and specific topics of interest, to zero in on the alerts that are most relevant to your organization's needs.

Dataminr is trusted by hundreds of the world's leading global security operations centers, government agencies, humanitarian groups and journalists working at more than 650 leading news organizations.

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

People

Security operations centers are staffed by analysts and managers, who work together to make recommendations to protect employees and executives, partners and clients, and company assets.

SOCs vary in physical size. In our experience, we've seen:

- Smaller companies with a centralized security function of as few as three people, who work 9-5 and rely on a managed security service provider for coverage outside of traditional working hours, or during an all-hands-on-deck crisis
- Midsize companies with a centralized team of as few as five people, many times working without a physical SOC, who provide 24/7 security coverage to the business, and rely on regional security managers for support
- Larger companies with a dedicated global security operations center, staffed by as many as 30 people, working around the clock and directing efforts with regional SOCs and regional security managers

SOC managers are responsible for overseeing and improving the SOC's workflows and processes and measuring success. They are calm and measured under pressure, with the added responsibility of taking appropriate action on real-time information during a risk incident.

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

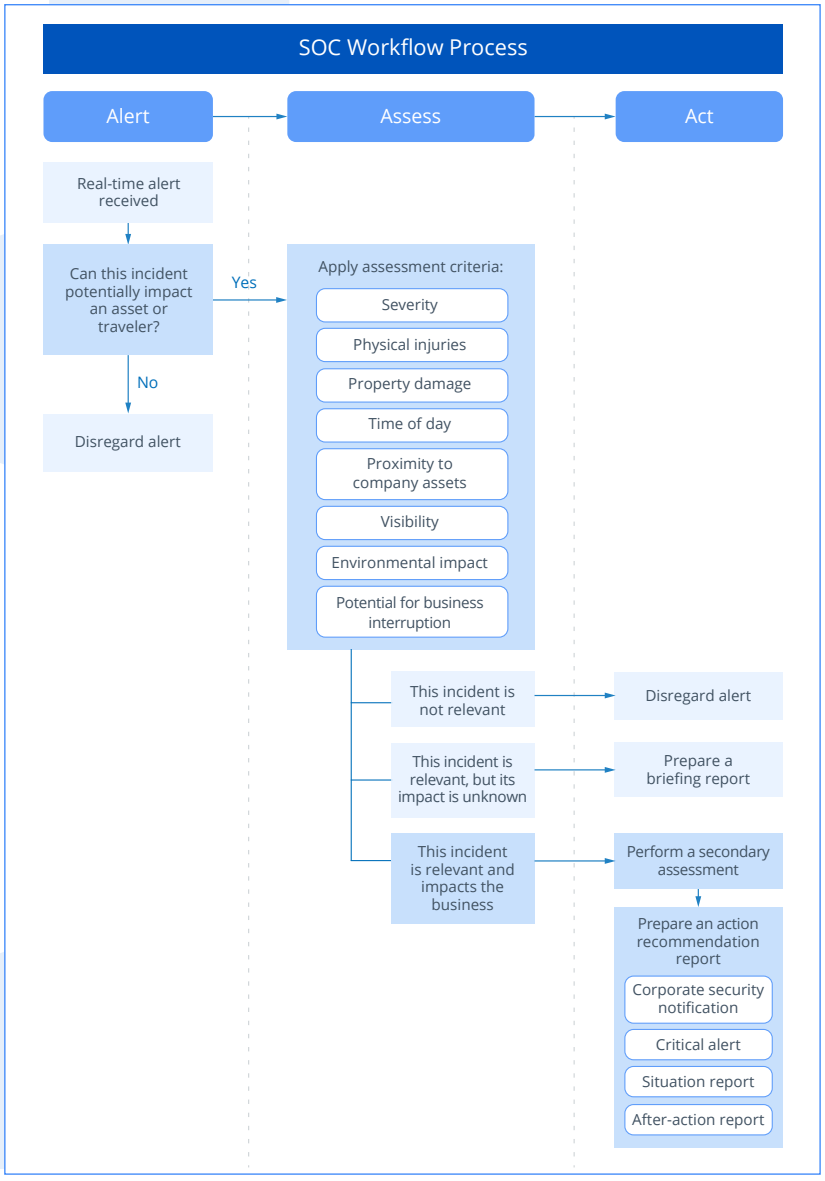
Planning for the future

Learn more

Workflow processes

Fundamentally, all centralized security teams turn real-time information into actionable intelligence. Predefined workflows formalize the information-into-action process, and contain tools that can measure the workflow's performance.

SOC workflows can be grouped into three major steps: Alert, assess and act. **Here is an example workflow that we've seen in use across multiple SOCs today:**



Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

Workflows are mapped out using an incident management system, which contains tools that measure a team's average response time and performance. Separately, some SOCs use other measurement tools to gauge team effectiveness and impact, such as employee satisfaction surveys.

5 Pitfalls to Avoid When Setting Up Your Security Operations Center

WATCH THE VIDEO

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

Reporting impact

Security teams do not generate revenue for the business, so it's important to devote resources toward measuring a SOC's positive impact, and make a case for continued investment in the program.

SOC managers who want to see increased investment in their program need to design measures of effectiveness and reporting tools from the outset, regularly updating their leadership team on the SOC's impact and performance.

Security teams face a unique challenge that comes with measuring the value of a risk that was mitigated. The potential scale of the impact will never be fully realized, making it difficult to estimate the cost of an action that was avoided, or a risk that was otherwise minimized.

Key performance indicators to consider measuring include:

- Total number of real-time alerts processed by the SOC in the reporting period
- Total number of risk mitigation actions taken by the SOC during the reporting period
- A select number of high-impact risk mitigation actions from the reporting period
- Employee satisfaction scores

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

Planning for the future

When planning for the future, there are two things that SOC managers can do to ensure continued investment in their team.

First, uplevel the security operations center's work, moving away from reactive risk response, and toward proactive risk management and business resilience. Use available real-time information and historical risk data to help company executives make better-informed decisions.

Share access to real-time information with other teams in the organization that are responsible for mitigating risk, such as the cybersecurity team and the risk management team, so they can use that information to better anticipate future risks.

Second, approach risk management, business resilience/continuity, cybersecurity and physical security holistically. Each of these teams is focused on a similar goal: Anticipating, planning for, and mitigating risk. However, running these teams in operational silos can inadvertently create risk blind spots.

Cybersecurity and physical security risks are increasingly converging, and many companies are exploring ways to adopt converged security best practices to eliminate risk blind spots.

Security operations centers are crucial for modern enterprises that want to approach risk management in a measured, repeatable and scalable manner. Real-time alerts from Dataminr Pulse form the cornerstone for hundreds of high-performing corporate SOCs around the globe today.

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more

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

Introduction

4 major areas:
1. Real-time information
2. People
3. Workflow processes
4. Reporting impact

Planning for the future

Learn more