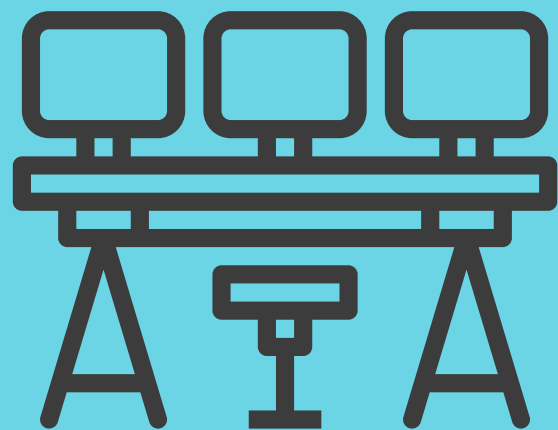


How to Operate a Security Operations Centre (SOC)



The role of the Security Operations Centre in managing operational security risk

Forty-two percent of security professionals are concerned with their organisation's inability to secure physical spaces, according to the Ponemon Institute. That's not surprising. Buildings, sites, plants and equipment, materials, and other physical assets tend to be largescale, creating a larger physical environment to secure. What's, then, to be done if your organisation finds it difficult to protect physical assets and people as well as coordinate speedy responses? The answer is clear: build a robust Security Operations Centre to improve your operational security posture.

What's a Security Operations Centre, exactly? Definitions vary. Broadly speaking, though, a Security Operations Centre provides a platform for detecting and reacting to security incidents.

The actual Security Operations Centre is a facility (physical, virtual, or hybrid) that houses an organised, highly skilled security team. That team relies on operational security management software and well-honed processes to achieve top-line, security objectives.

Who staffs the Security Operations Centre and what do they do?

The security team responsible for carrying out the Security Operations Centre core mission usually includes the SOC manager who heads up operations, engineers, and security analysts. That team will also work closely with the organisation's Crisis, Emergency Management, and Business Continuity teams to coordinate responses to physical security incidents that become critical events.

The primary duties the team discharges include regularly monitoring and analysing the organisation's operational security posture. More specifically, the Security Operations Centre team detects, investigates, responds to, and reports on security incidents.

It's important to note that the Security Operations Centre is an operational unit. That means it's not responsible for developing security strategy.

In essence, the Security Operations Centre works continuously to manage risks and threats. Of course, those responsibilities don't cease when the office closes down. And that's why most Security Operations Centres are open around the clock.

What's the benefit of the Security Operations Centre?

This kind of set up offers a key benefit in terms of centralising security arrangements. It's clear that advanced equipment and technology alone aren't enough to achieve operational security goals. If they were, there'd be far fewer physical security incidents, as security procurement went up. Instead, mitigating risks and improving incident preparedness and response call for a security apparatus *specifically* dedicated to preventing damage, theft, and intrusions, as well as protecting people.

And that's precisely what Security Operations Centres do so well. They consolidate security expertise and reporting into one centralised location.

Security Operations Centres receive physical security data from the field to furnish a real-time picture of security threats and vulnerabilities. This centralising approach cuts down on the siloing characteristic of security incident management in most large enterprises.

Rather, the Security Operations Centre delivers noticeable gains in visibility, increasing situational awareness of security incidents. Also, when it comes to those security incidents, a Security Operations Centre will help communicate to and interface with other parts of the business who need to be on high alert if a security breach does occur, e.g., Legal and PR.

Another thing: recently, lawmakers and regulators have mandated aggressive security measures, especially in critical infrastructure sectors. A robust Security Operations Centre might go a long way towards ensuring compliance with those mandates, as well as easing any reputational damage that might come following a physical security incident.

What are the challenges of setting up a Security Operations Centre?

Despite the benefits, Security Operations Centre adoption isn't universal. In fact, 48 percent of companies still don't have a Security Operations Centre, according to EY's Global Information Security Survey, 2017-2018.

48% of companies still don't have a Security Operations Centre

What's going on, here? Well, for starters, upfront capital costs for furnishing a Security Operations Centre can be considerable. On balance, though, that financial investment pays for itself in the lower incidence of security mishaps down the line.

There's also the complexity of conforming with multiple regulations (external as well as internal), as organisations do build out their Security Operations Centre. Lastly, qualified security analysts can be hard to come by.

Overcoming the challenges to operating a successful Security Operations Centre

Overcoming those challenges won't be a walk in the park. But they are surmountable with the right practices.

As mentioned, security strategy doesn't come out of the Security Operations Centre. However, the aims of the Security Operations Centre should be consonant with those of the organisation's overall, operational security strategy – we've provided some examples below.





In other words, for the Security Operations Centre to be successful, it must address specific, clearly defined company (and customer) needs. It should also scale to the organisation's footprint.

C-suite sponsorship of the Security Operations Centre helps in this regard. Though operational security focused, the Security Operations Centre is a cross-functional operation. Typically, only senior executives can ensure that business-specific goals from various departments are incorporated into the Security Operations Centre's mission. Also: that the Security Operations Centre gets the necessary visibility across a defensible perimeter, be that perimeter comprised of doors, walls, or other physical barriers.

Context-aware threat intelligence helps, here. A Security Operations Centre that first undertakes a detailed site vulnerability assessment is far more likely to be successful than one that doesn't.

The vulnerability assessment will help Security Operations Centre staff discover gaps in need of greater focus (and protection). The vulnerability assessment will also give the organisation at large more granular knowledge into layout and how employees act within the physical environment.

Further, the vulnerability assessment games out the impact of potential security incidents and their possible effects on security personnel and process operators. Those potential impacts, in turn, help determine your operational security requirements. Those requirements might include:

-  Identify and control individuals who enter and exit the facility
-  Track movements of building occupants and assets
-  Control access to restricted areas
-  Track and locate equipment, products, and other resources
-  Track the location of personnel on site in the event of an incident
-  Integrate control and security systems for greater speed and efficiency
-  Protecting process automation networks and systems from potential intrusion
-  Respond quickly to alarms and events

To be sure, those requirements should be part of the organisation's incident response framework, upon which the Security Operations Centre will play a key role executing.

What's more, the most effective Security Operations Centres are governed by established, rigorous processes. Their staffs are engaged in continuous training that keeps pace with the evolving threat picture.

The Security Operations Centre is one component of a best-practice operational security management program. Here are some of the other best practices for planning and managing your operational security resources.

- Physical security programs should be holistic, and the allocation of resources should be integrated into the organisation's mission, objectives, goals, and budget process.
- Physical security functions should be consolidated within an internal security office, led by a Director of Security (i.e., CSO), who reports to a high-ranking senior executive official who has ready access to the agency head, as needed.
- Director of Security (i.e., CSO) should be responsible for managing and allocating physical resources based on risk assessments and using performance measures to justify security resources across the organisation's facilities.
- Development and implementation of the physical security program should involve collaboration among top management, security, facilities management, emergency preparedness, budget, health and safety specialists, and other stakeholders.
- Physical security programs should be aligned with the organisation's mission, strategic goals, and budgetary requirements.
- Physical security programs should meet the cost-effective expectations of the organisation's leadership in terms of totally integrated security support and safety services rendered.
- Physical security programs and countermeasures should be balanced with other operational needs and competing interests.
- Physical security resource allocation should be periodically assessed, including historical spending records, which may be useful in future resource allocation considerations.

Source: Department of Homeland Security

Simply building and staffing a Security Operations Centre doesn't ensure zero physical security incidents. Organisations will still need to take a best-practice approach to operational security management, committing to constant training, developing rigorous processes, implementing standards, and procuring the right integrated risk management and operational security management technology.

Security Operations Centre operators, in particular, often have to manage multiple technology sets at once. But there's a means of easing the burden. Operational security management software not only keeps operations secure but Security Operations Centre humming along. Just look for the following features when procuring:

- Manage all operational security incidents and major events in a single system
- Perform security investigations
- Centralise, track, and manage security information, checklists, and actions
- Task and dispatch security staff to respond to any event
- Manage lost and found property
- Schedule security escorts
- Fully integrated mapping to visualise locations of incidents, hazards, people, and assets
- Perform hazard and risk assessments
- Automatically generate security statistics on dashboards and security reports
- Easily capture rich logs for patrols, shift-changes, parking infringements, and other security activities
- Integrated communication templates: email, SMS, voice, and more
- Conduct alarm tests and inspections
- Monitor persons of interest
- Manage security staff and contractors
- Built-in dashboard analytics, structures, and ad-hoc reporting
- Automate and follow business procedures with fully configurable workflows
- Collect intelligence from the field via mobile apps

That's not all, though. Looking for the right operational security management software solution? Download our purchaser's guide, which takes you through all of the capabilities you'll need to reduce security incidents and keep people and assets safe.



Like what you read? Follow Noggin on social media



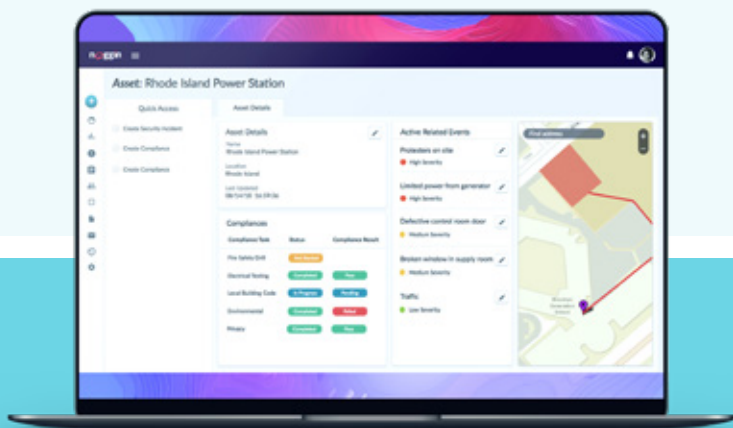
@teamnoggin



facebook.com/teamnoggin



linkedin.com/company/noggin-it



noggin

for Security

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Security gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Security solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: www.noggin.io
or contact: sales@noggin.io