Calipsa Resource

SECURITY OPERATIONS CENTER REPORT TEMPLATE

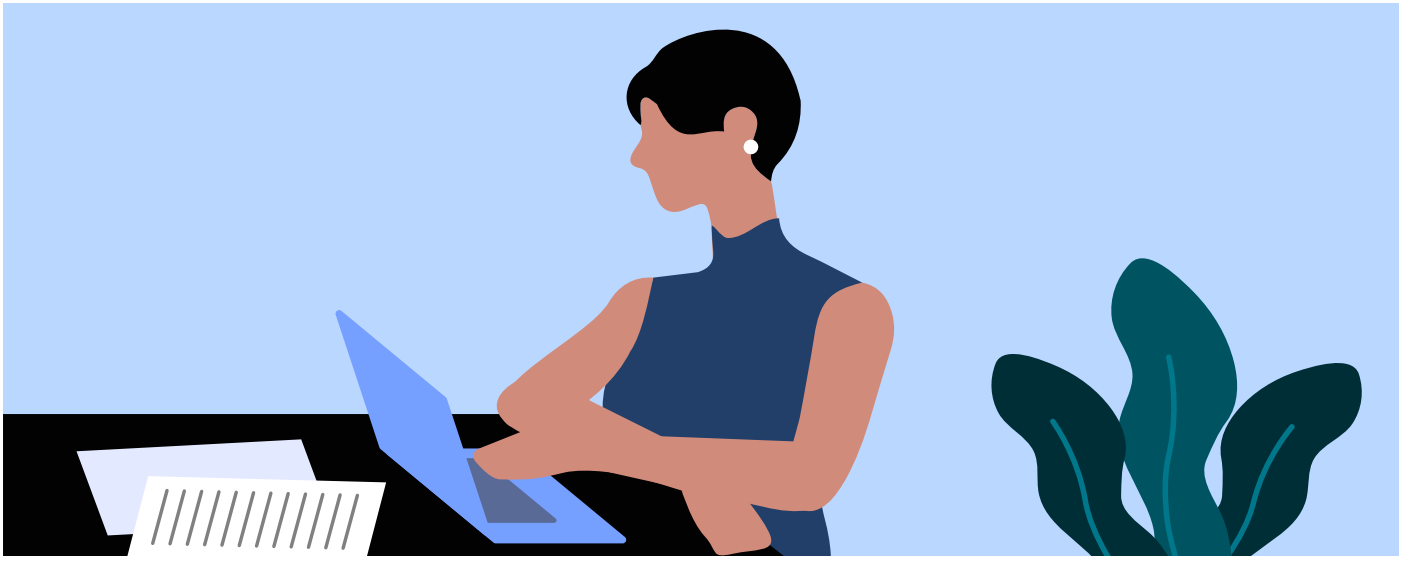
How to write a report for your SOC

CONTENTS

INTRODUCTION

Security operations centers (or SOCs) are vital to a company's physical security. So how do you demonstrate that your SOC team is doing a good job of protecting your company or client? How can you also explain your company's / client's current security status and risk profile? A detailed SOC report can help you to deliver all this information in a way that is easy for stakeholders or clients to understand. It also allows you to illustrate the great work your SOC is doing using data.

If you aren't sure where to begin, try this report template to give your results some structure. We have included all the key information a stakeholder or client should know to stay informed about your SOC's progress and performance.



Before you begin

The most important thing to remember when reporting to stakeholders and clients is: **keep it simple**. Try wherever possible to use non-technical language. When you do need to report something technical, do it clearly and explain any technical terms.

It is also useful to **explain things visually** for a non-technical audience. **Use graphs and charts** to visualize your results and highlight your most important figures. A little formatting can go a long way to making your report more accessible!

Focus on the most important things your stakeholders need to know: your results, your future requirements and any action points. If you are using this report to secure more budget, then it's crucial that you argue your case clearly and concisely.

You will also need to **contextualize your SOC's progress and performance** in relation to the rest of your organization (or your client's organization). How does security help the company to achieve its business goals? Are certain business areas particularly vulnerable to risk?

Remember that your **stakeholders want to know the key facts as quickly as possible.** If you want to include a more detailed analysis, add it as an appendix for future reference.

KEY FINDINGS

This opening section outlines your most important findings; it is also an ideal place to display some of this data visually: consider using graphs and charts to get your point across.

Here you should also provide an overview of your company's current security status and risk profile, summarizing the points in the following sections.

MONITORING DEVICE REVIEW

A site has many different security devices, all recording data. This section looks at how effective all of these devices have been. By completing the table below, you can investigate factors such as whether:

- Some locations have a higher proportion of incidents
- Some locations have devices that trigger a high volume of alarms
- Some devices trigger more alarms than others

Depending on your security system, you might want to categorize devices by type, e.g. security cameras, by a more granular type e.g. Pan-Tilt-Zoom security cameras, or as detailed as the brand and device model.

Device type (camera, motion detector, etc.)	Location	Total number of these devices at this location	Number of most alarming devices at this location	Number of most idle devices at this location	Number of incidents detected	Number of false positives detected

This section is also where you should also flag any devices or locations you chose to leave out of the report, and explain why you made this decision.

INCIDENT REVIEW

Moving on from an overview of devices in the previous section, here we delve into the alarms that turned out to be incidents. Below, we have included the key pieces of information you should include for each incident; this table will demonstrate how your SOC handles incidents and their severity.

Incident date	Incident handler (name + position)	Incident type	Number of most alarming devices at this location	How long to detect	How long to resolve	Severity level (1-10)	Actions taken

THREAT ANALYSIS

Of the incidents in the previous section, which posed a threat to the business? Here we look at the types of threats your SOC has encountered, including their severity, frequency and location. Using this information, you can look for trends; these trends can help you to predict whether certain types of threats are likely to occur again, and if so, how to prepare for them.

In this section you can also compare your company's threats with wider risk trends to see whether you are more or less at risk than other firms in your industry, in your region, or even globally.

Threat type	Threat description	Severity (1-10)	Frequency	Location(s)

RECOMMENDATIONS

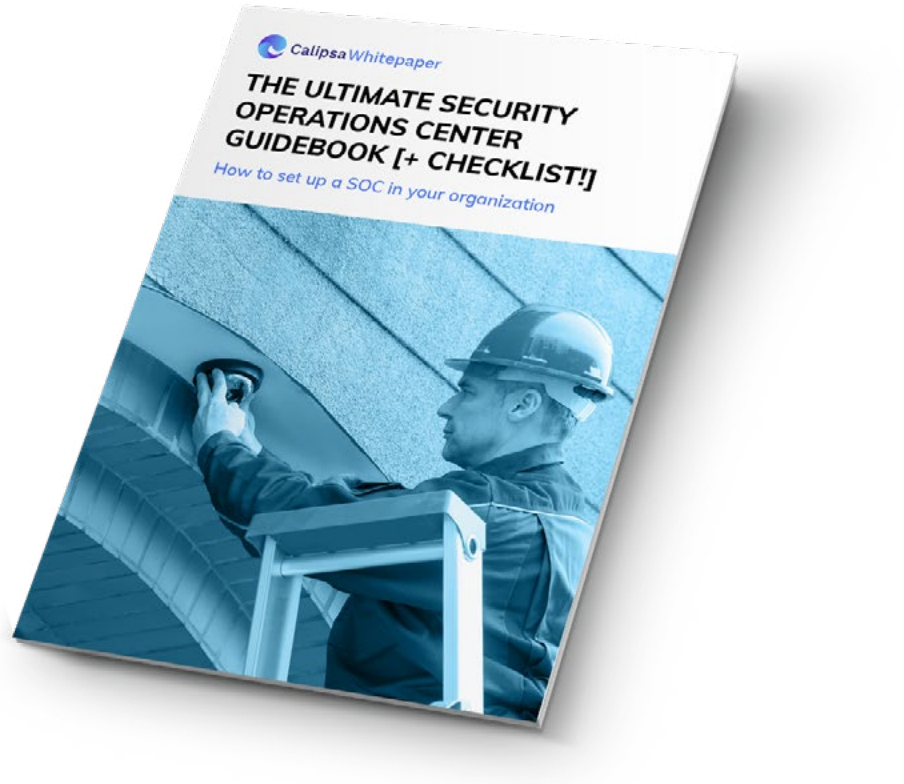
Based on all of the information above, you can now summarize all of your findings - this will be more thorough than the Key Findings section at the beginning.

Based on your findings, you can also suggest action points for members of the business to take. These can include further staff training, hiring more SOC team members, investing in security devices - or even upgrading your security system. Investing in software such as video analytics could help you to automate and improve some of your security functions, giving your employees more time to focus on incident handling. In many cases this can be more cost-effective than hiring extra staff or upgrading hardware, with similar results.

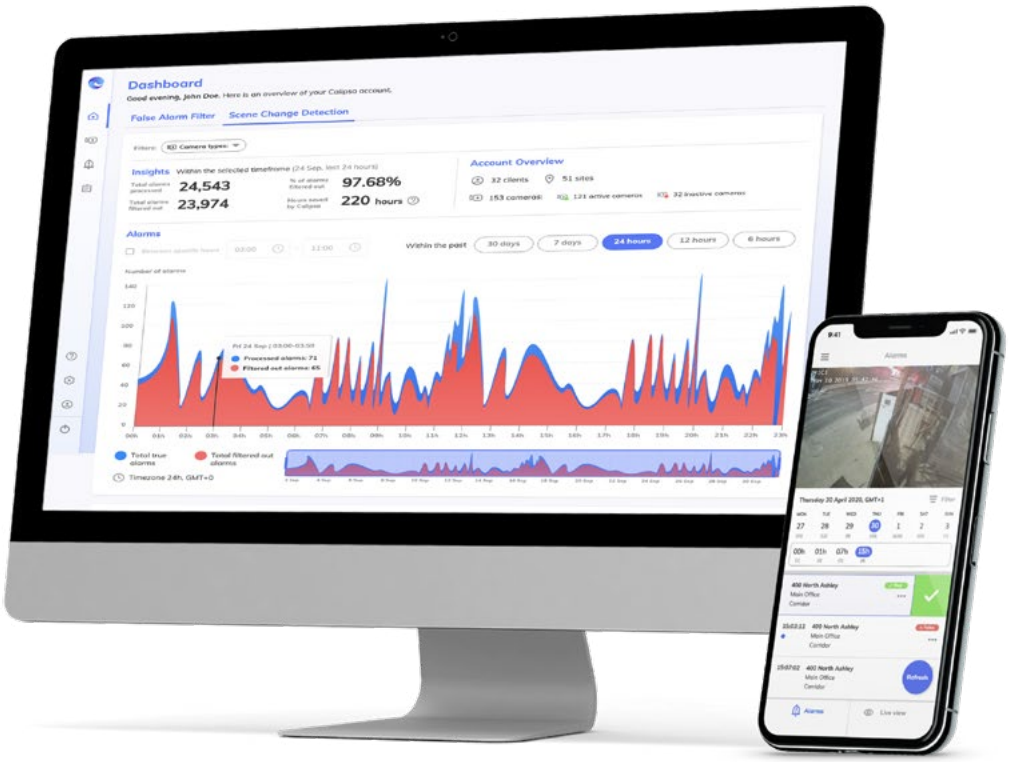
There might also be other, more targeted security recommendations - this might be because your report revealed that one particular location is more vulnerable than others, or that your business is susceptible to certain threats.

You might also suggest business-wide recommendations, such as better security awareness training for all employees to reduce certain security risks.

So there you have it - everything you need to create a SOC report. We hope you find this template useful, and if you want even more advice, check out our **Ultimate Security Operations Center Guidebook + Checklist.**



ABOUT CALIPSA



Calipsa helps companies extract more value from their new and existing video systems by turning video into data, and data into business intelligence. Calipsa Pro Analytics, advanced AI cloud video analytics for real-time and forensic analysis, leverage event-based video at scale to enable more effective and efficient security operations. Unlike other analytics Calipsa analyses frames, not video, saving on time and bandwidth; savings which we pass on to you.

Calipsa analytics are used today on over 130,000+ cameras on 22,000+ sites – spanning 6 continents – making it the leading global provider of cloud-based analytics for event-driven video. Whether you have a central monitoring station or an in-house security operation, Calipsa is here to help you do more with your video surveillance infrastructure.

Calipsa

www.calipsa.io
hello@calipsa.io

Find out how we can help you get more
from your video systems with Calipsa Pro Analytics