White Paper

Top 8 CISO Challenges Solved

Eight of the most pressing questions CISO's are asking, answered, as businesses continue their journey of digital transformation and cyber threats continue to rise.

securityhq.com

SecurityHQ

Table of Content

Executive Summary

As a global Managed Security Services Provider (MSSP), with clients ranging from small businesses to corporate giants, SecurityHQ have worked with multiple industries and have witnessed for many years the changes in security needs. Throughout these years, we have discussed with each client their greatest security challenges and, from these discussions, a trend has emerged with regards to the questions CISO's have been asking.

Cyber-attacks are the greatest risk to a company's operational capacity, as well as its revenue and brand value. With the digital transformation, and with it an acceleration of modern technology, there has been a vast increase of security issues that Chief Information Security Officers (CISO's) have had to face. This is especially true for small to medium business, as these companies have accelerated straight through to the Cloud and experienced at full force all the new and developing related issues. Similar issues face larger corporations, but at differing degrees. Which has led to a list of frequent questions being asked.

> **'96% of CISOs stated that they face well-organized cybercriminal attacks motivated by financial gain. Nearly 72% of them said adversaries are moving faster than they are, and a similar number (69%) say their adversaries have improved their attack capabilities in the last 12-18 months.'**
>
> \- CISO Mag

The following **eight questions** discussed in this paper are some of the most asked questions by CISO's that we receive. These questions are based on challenges we have seen CISO's deal with, have helped CISO's overcome, and get asked daily from businesses around the world who are looking to increase their security posture.

1. **Speed of Detection.** How do I go from detection taking days/weeks even months, to seconds and minutes?
2. **Speed of Response.** How do I go from speed of response taking days/weeks even months, to seconds and minutes?
3. **Round-the-Clock.** How do I move from 9-5 monitoring, detection, and response to 24/7/365 monitoring, detection, and response? Why is it important?
4. **Detect Complex Threats.** How do I go from the detection of simple security events to the detection of complex and sophisticated events?
5. **Skills and Expertise.** How do I move from a team with a basic understanding of threats, to using highly skilled expertise?
6. **Risk Visualised.** I have zero visibility, but I want highly visual risk interpretations, how do I get these?
7. **Governance of Sec Ops.** How do I move from no/little standardisation and lack of controls to complete OLA, SLA, KPI and metrics enforced?
8. **Cost Certainty.** How do I move from ad-hoc expenditure to clear operational costs?

By understanding what is needed, respondeding to these 8 elements correctly and iniciating the right practices, a complete security web is created.

1 Speed of Detection

CISO: How do I go from detection taking days/weeks even months, to seconds and minutes?

The first section of the web that needs to be considered is speed of detection. A CISO needs to be able to detect threats in minutes and seconds. The concept of hours or even days is simply not good enough if you want to successfully react to threats.

When it comes to enhancing security, the reality is that you have to have detection and response. The majority of our clients that we take on will already have invested in their Firewalls, their Intrusion Detection Systems, (IDS), their Intrusion Prevention Systems (IPS), their anti-virus, and all the latest and greatest tools that they have accumulated. But they still lack the speed. We have even seen businesses taking months to detect threats. Which is far too long.

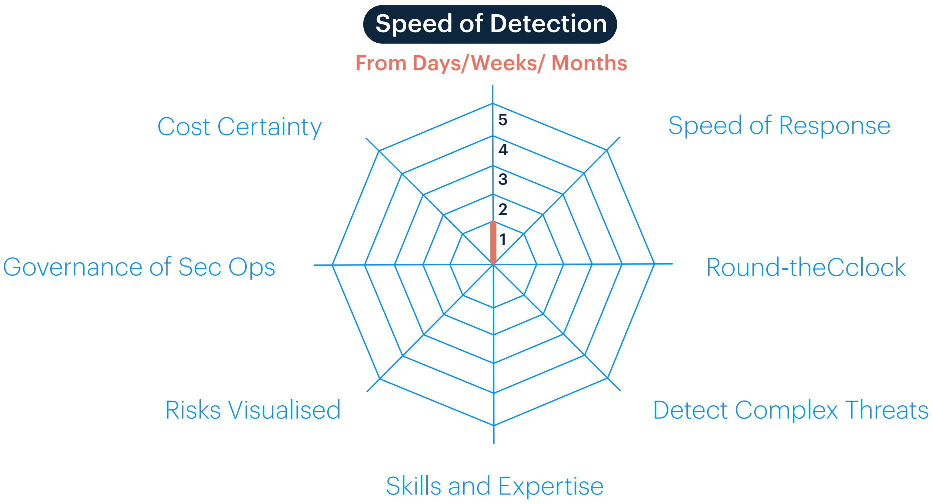
Once the data is collected from these sources, it can be analysed, and the response can be actioned.

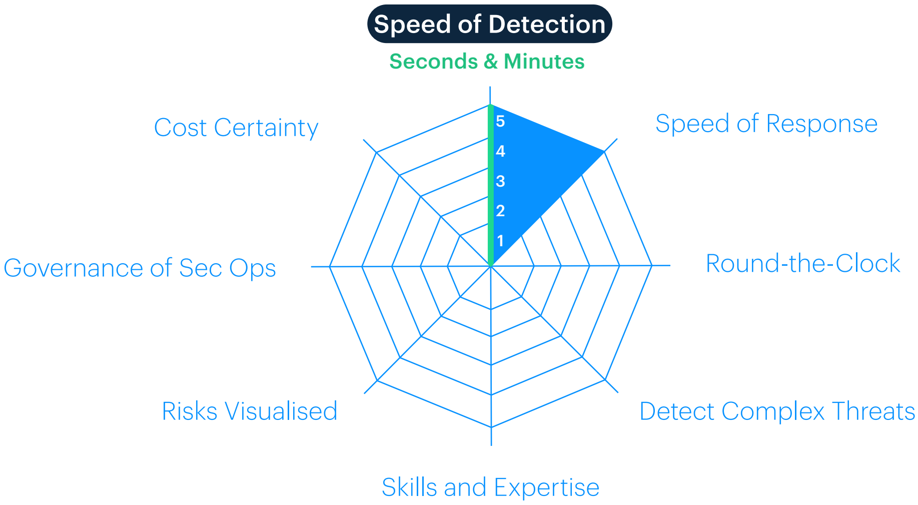
By using an MSSP, you can speed up detection time. And, with technology such as a QRadar SIEM based service, you are going to get a detection time in seconds and minutes as standard. An MSSP takes a complex tool, such as QRadar, and operates it on behalf of the client. That way, experts are monitoring 24/7 and can, consequently, detect threats every second of every minute of every day.

Experts should be monitoring your networks continually, and you should be able to call the SOC at 4am, and someone should be there to answer your call.

Watch out for any automated services, these do not bring the same level of care, nor will they answer your specific security needs.

On top of this, elements such as Threat Hunting can significantly increase the speed of detection. Learn more about Threat Hunting with our white paper on 'The Fundamentals of Threat Hunting. Hunt Like a Pro.'





The Outcome of Improved Speed of Detection

The outcome of improved speed of detection means spotting attacks and vulnerabilities before they become a significant problem, the faster you detect something, the faster you can put in place steps to reduce the impact of the issue, and often stop threats in their tracks altogether. This not only saves time and resources, but also significant financial implications involved if breached. If you can reduce your risk level altogether by detecting incidents faster, you can reduce the risk of a breach, and all the issues that come with that.

2 Speed of Response

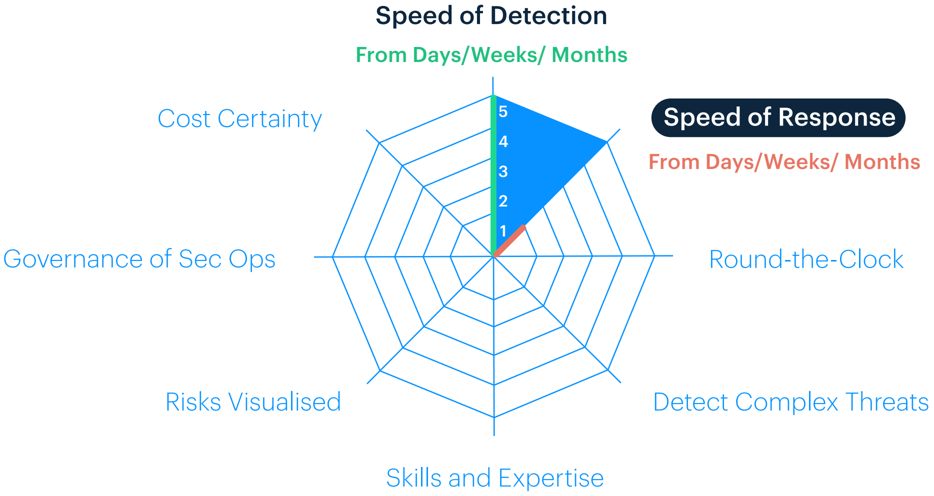
CISO: How do I go from speed of response taking days/weeks even months, to seconds and minutes?

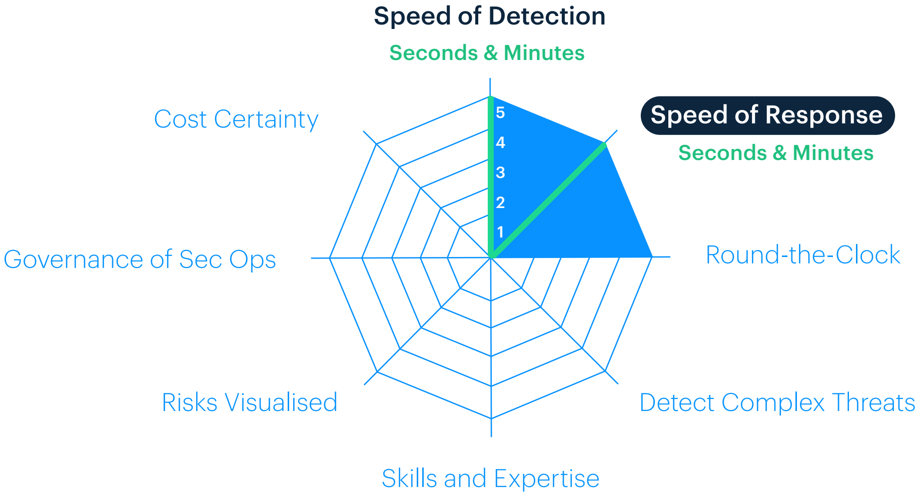
A CISO needs to be able to have the capability to respond in minutes. And respond with the right processes in place.

When SecurityHQ clients join us, their capability of response usually takes days, weeks and sometimes even months. We often see the issue whereby the business may have an incident, so they go to IT, and IT looks at it, and they are not sure what to do, so they google it, and weeks later they respond, and often incorrectly. Which is just not acceptable. There is no point knowing that your house is on fire if you are not able to grab that bucket of water and put it out. Otherwise, you are just going to sit there and watch it burn.

Incident response requires advanced analysis, combined with an accurate assessment, categorisation, and a playbook for investigation and response. That is where the use of technology, such as IBM Resilient via an MSSP, shines. With Resilient, response takes seconds and minutes rather than days and months.

Your MSSP should have a hotline number if you suspect an incident, or indeed for anything urgent. They should also have an App you can contact the team directly on, and a designated Service Delivery Manager (SDM) to call upon once signed up.





The Outcome of Improved Speed of Response

The outcome of improved speed of response means responding to and blocking attacks before they have the chance to develop further. If you can respond to a threat in rapid time, before it has the time to implement further actions, can mean the difference between a breach or securing your assets in time. If you can reduce the time it takes to respond to threats, the greater chance you and your security professionals have at responding to the threat correctly, meaning a reduction in the chance of further escalations.

3 Round-the-Clock Monitoring

CISO: How do I move from 9-5 monitoring, detection, and response to 24/7/365 monitoring, detection, and response?

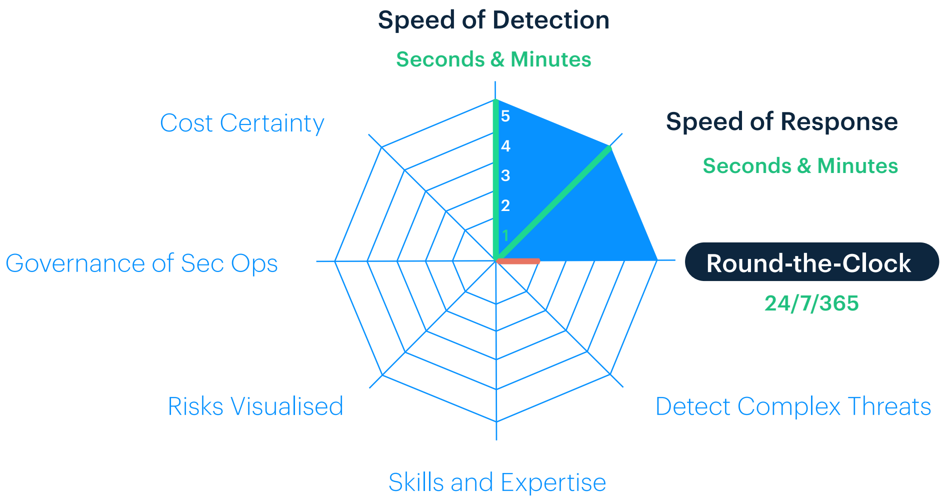
A CISO knows that cyber never sleeps. They need the capability to monitor 24/7. Our clients, and questioning CISO's, tend to work a nine-till-five workday. Which means that few have a full 24/7 capability if they are only covering this period.

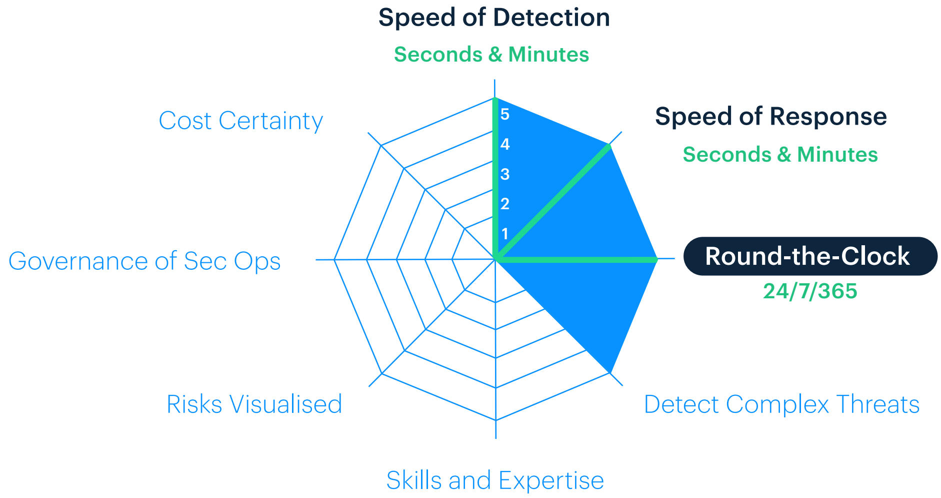
If an attacker or a perpetrator was to attack them, they would learn about the working hours and shift patterns, when people are in and when people have left for the day. Same thing goes for physical theft/crime. A thief operates during the hours you are not there to protect and guard your data, people, or processes. Which means businesses need protection during the weekends, in the evenings, on bank holidays, every second of every day.

To operate a Security Operations Centre (SOC) it takes a minimum of eleven people to cater to 24/7. It must be human driven. And highly trained analysts are rare. To get a highly trained analyst available to detect an incident, drill down into the details, to understand the details and what to do next, every second of the day, is costly. And this number only takes into consideration the SOC analysts, let alone the content team, infrastructure, and any other support services.

An MSSP works as an extension of your team, to provide just this. While your team may work the usual Monday to Friday, 9-5 hours, your networks, data, and everything that goes into your business requires 24/7 security. Which is why it is necessary that your MSSP provides full security, 24/7, every day of the year, regardless of holidays, working schedules or natural disasters. 24/7 means supported by humans, not automated machines.

Again, you should be able to call the SOC at 4am, and someone should be there to answer your call. Watch out for any automated services, these do not bring the same level of care, nor will they answer your specific security needs. You need humans there, every day, every second.





The Outcome of Round-the-Clock Monitoring

The outcome of round the clock monitoring means continuous detection and response. If threats are left undetected because you do not have a team of analysts 24/7, then your people, process, technology, and data is left at risk, regardless of the systems you have in place. If you can monitor 24/7, you can detect and react to threats every minute of every day, leaving no time for threats to go undetected.

4 Detection of Complex Threats

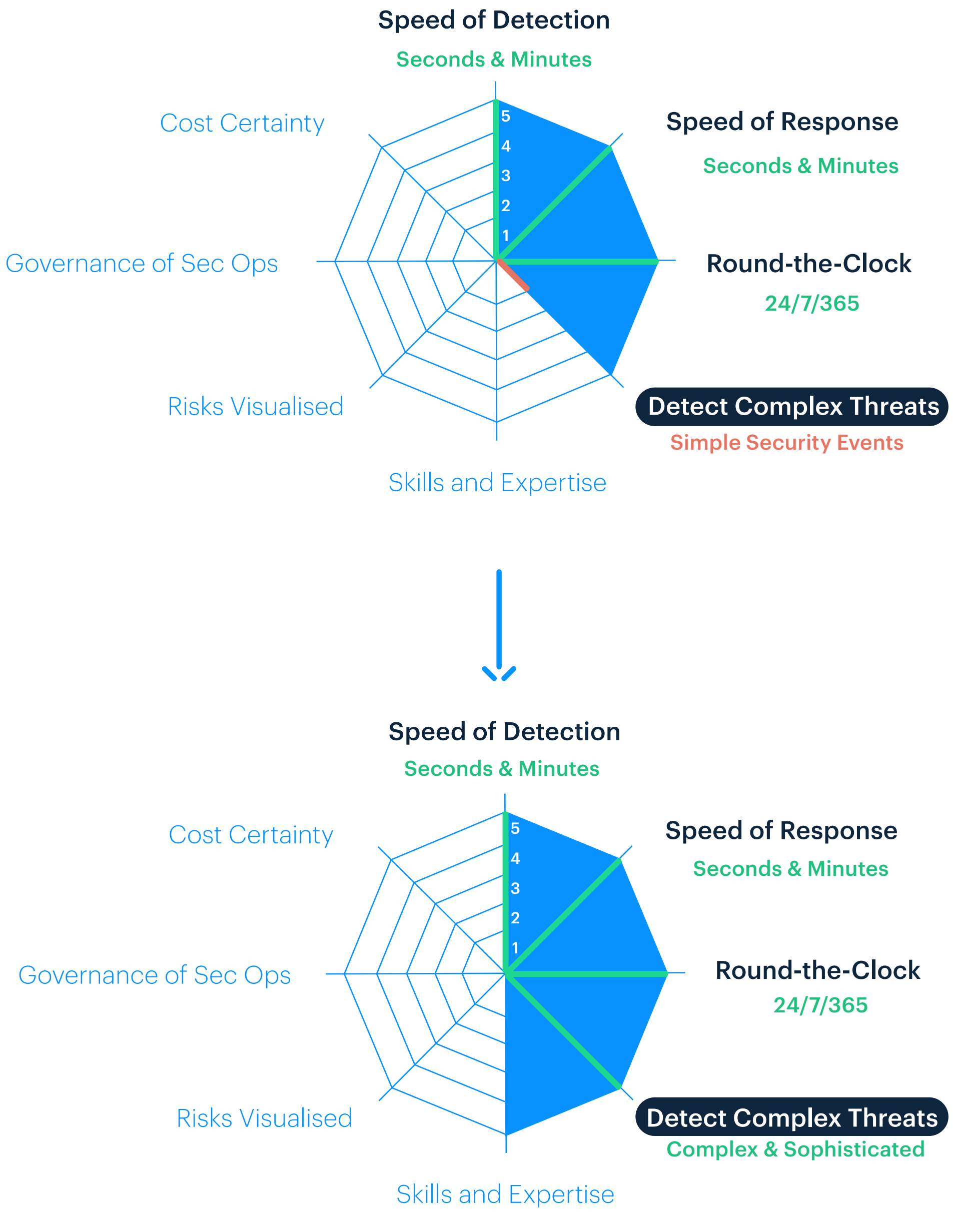
CISO: How do I go from the detection of simple security events to the detection of complex and sophisticated events?

CISO's must have the capability to deal with and respond to complex threats. Some of the ransomware we are seeing today is exceedingly complicated, in a way that when we look at it, we say 'Wow, how are they doing this?'. This is not glorifying their efforts, but rather highlighting the fact that when we go to government agencies, which we often do, and show them what we find, nine times out of ten they have not seen the threat either. They say, 'That's really amazing, send it to us because we have to learn how to deal with this.'

We are all living in a world of Zero Day.

Advanced Correlation & ML can be used to detect complex threats. Organisations struggle with the rapid identification of malicious behaviour. This identification requires a matured SIEM, with advanced correlation, anomaly, and user behaviour analysis, together with continuous monitoring.

SecurityHQ applies advanced correlation & machine learning to expose patterns of illicit behaviour. SOC immediately investigates the extent of an event, and its context, to derive a complete analysis with mitigation and risk quantification.



The Outcome of Detecting Complex Threats.

Complex threats often go undetected, IT teams alone do not have the capability to detect them. But, if you can use a security expert combined with the right systems to spot such threats, you can secure your business from some of the most harmful attacks, including the increase in ransomware targeting businesses.

5 Skills and Expertise

CISO: How do I move from a team with a basic understanding of threats, to using highly skilled expertise?

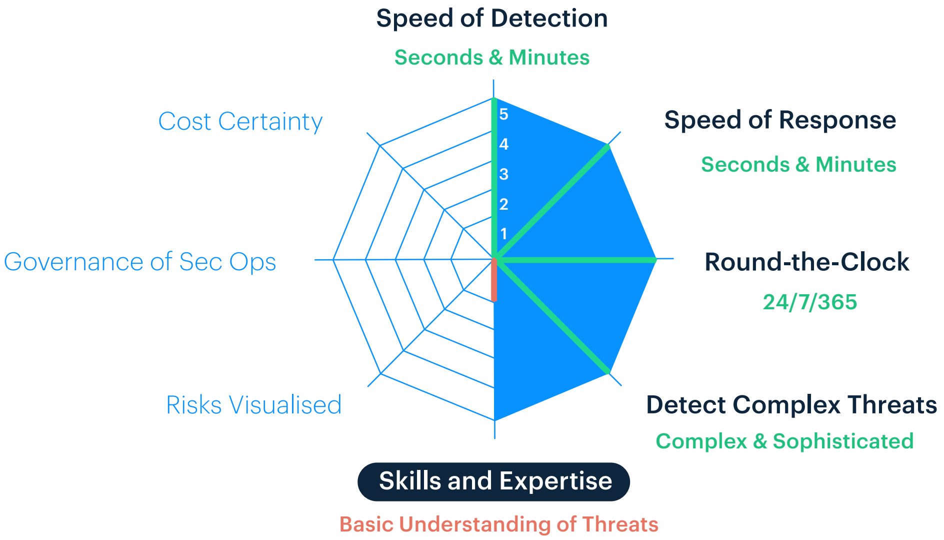
When you are running a business, security is not the primary focus, which means organisations often consider it as a secondary function, to do as and when other priorities are done. But this should not be the case. As mentioned previously, it takes a minimum of eleven security professionals to run a SOC. And it takes a vast amount of management time to recruit the right people, retain them and motivate them. And that is not going to get easier. This is a real, continuous challenge for our clients.

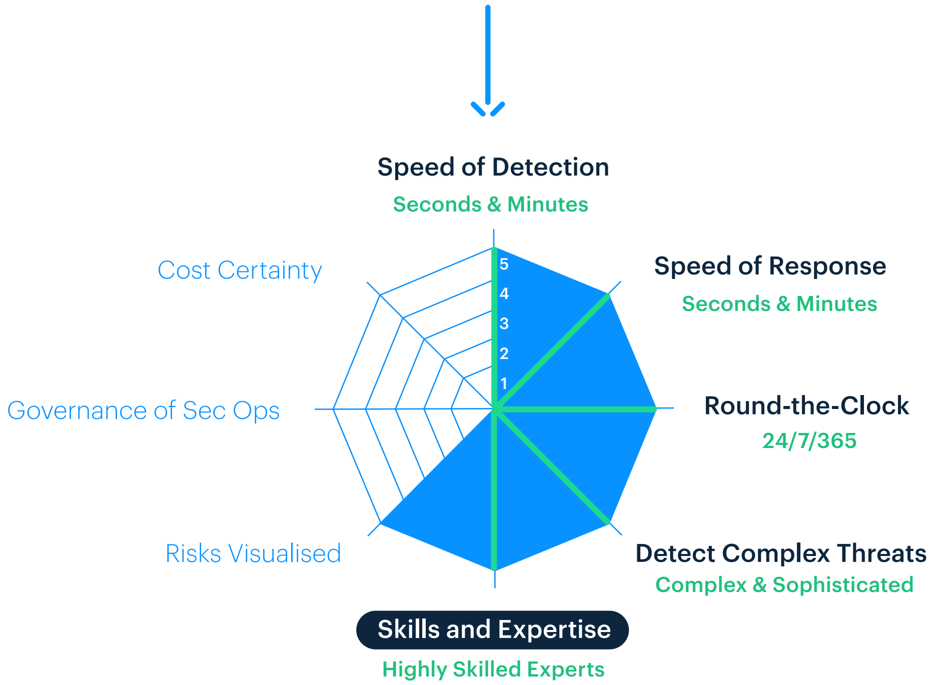
Everyone struggles with skills and expertise. Businesses will have some basic understanding, and they have a few people to go to, but what they need is a complete skill set from low, medium, to high-level, available 24/7.

With an MSSP, you have access to trained analysts, available to detect an incident, drill down into the details, to understand the details and know what to do next, every second of the day.

‘Businesses often only jump on security when there is an issue. With an MSSP, experts will be able to push your business to continually make the right updates, and proactively search out issues, before the issues are found by the wrong people and used against the business. Your MSSP should tell you what to focus in on. Watch out for the alerting services, this is not what you want, you want someone to raise the tickets, act on the tickets, and be with you and advise you.’

- Eleanor Barlow, 'Choosing Your Managed Security Service Provider'





The Outcome of Utilising Skills and Expertise

If you use the skills and expertise of experts within the field, it means you and your team can continue doing what you do best, continue running and increasing your business and growth, while the experts monitor and act on threats, so that you do not have to. Peace of mind is the main outcome here, knowing that the experts have your back, have your security under control and increase the safety of your people, processes, and data while you continue to run your business.

6 Risk Visualisation

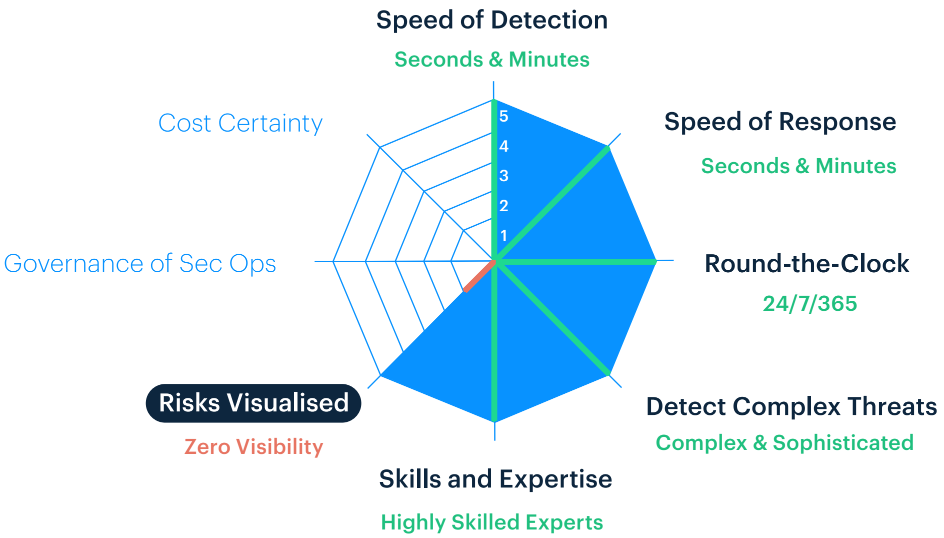
CISO: Zero visibility, but I want highly visual risk interpretation, how do I get this?

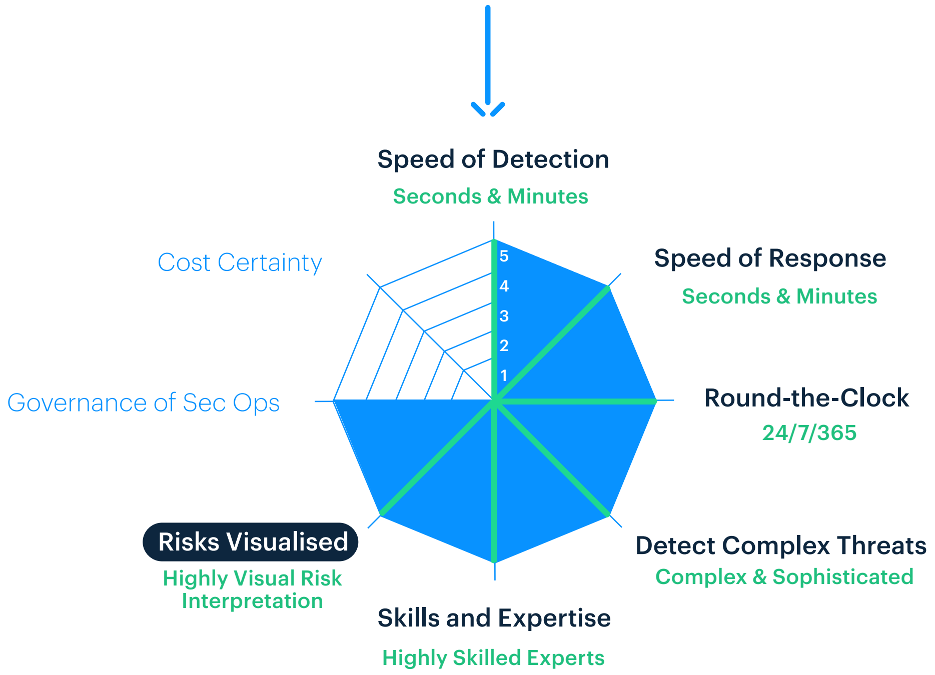
As a business, you must have complete visibility of your risks. What keeps most CISO's up at night is the fear of the unknown. Knowing that what they deal with is only a fraction of the threats targeting them. That is the frightening factor that must be faced head-on.

As an example, if you are seeing the beginning of an encryption happening on a server, and that server happens to be your CRM payment gateway, you start to quickly realise the risk to the business, the risk to your client base, and supply base. You can see that you are about to get locked out of your business. You need to visualise this event before it happens, so you know how to react when it does.

At the same time, if you see something happening in the distance, then you have a different risk, but you need help identify the risk in the first place. The IT teams and cyber teams within our clients' organisations need help to visualise risks, so that they can talk to their management, or their own colleagues about it and understand the level of severity.

That is important as part of the requirement of building a SOC. By visualising risky behaviour and misconfigurations, we target the threat at its source. Our customers receive detailed weekly reports with granular statistical analysis to illuminate risky behaviour, security posture issues and security incident metrics.





The Outcome of Risk Visualisation

The key outcome of successful risk visualisation is having a clear view on what would otherwise be unknown. Knowing what to deal with, how to deal with it and how to prioritise threats is crucial to face attacks head-on.

7 Governance of Security Operations

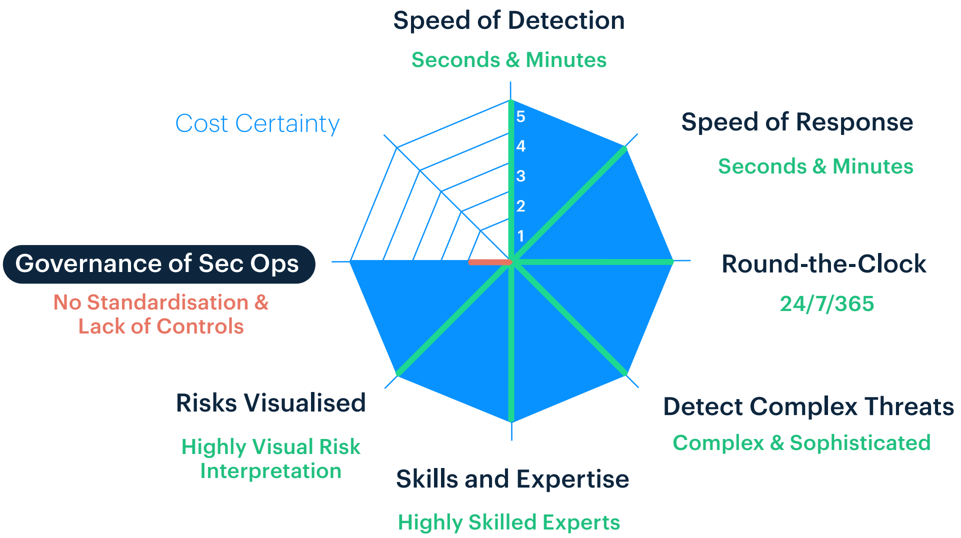
CISO: How do I move from no/little standardisation and lack of controls to complete OLA, SLA, KPI and Metrics Enforced?

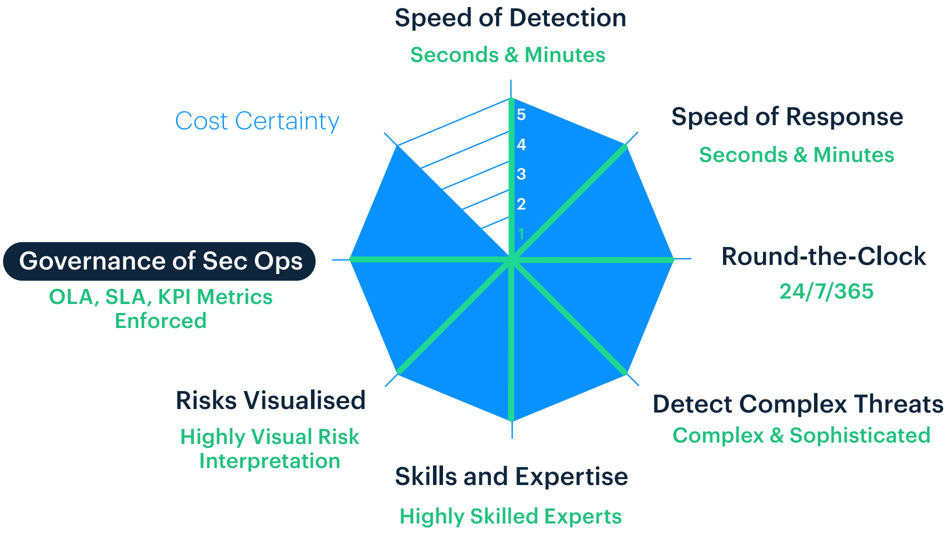
Most clients have some form of requirement with respect to compliance. Many have government best practices and their own internal compliance rules like ISO 27001 as part of Managed Detection & Response (MDR). But whatever your compliance requirements are, controlling the users, the logs and the security is crucial to meet compliance requirements.

With compliance, you must also have some form of standardisation. And you must have the controls. Controls are there because they are important. When you are playing a sport, for instance, you must know the size of the field you are playing on to create a strategy. In cyber, you must measure the journey to understand that your capability to detect and respond is working. You need to know how much has changed in a year, in a month, in a week. Having the ability to look at logs from a year ago, with the intelligence that you have today, is not only unbeatable, but necessary.

You must have compliance ideally integrated within OLA's, SLA's, KPI Metrics enforced and measurements.

> **'Regardless of how good your internal team may be, the experts within security operation centres are the ones with their eyes on the glass, who can rank issues, order and separate the major events from the minor concerns. By dealing with issues that are a high priority first, you deal with the challenges that have the biggest impact on closing out security loopholes and protecting your organisation.'**
>
> - Eleanor Barlow, 'How MDR is Used to Spot Third Party Risks, Insider Threats and More'.





The Outcome of Governance and Security Operations

Having the right security operations and governance in place not only means improved processes for you and your team, but it also means that you are working within the law.

8 Cost Certainty

CISO: How do I move from ad-hoc expenditure to clear operational costs?

'Technology is continuously evolving, which makes setting aside a security budget challenging. Your MSSP, however, must look out for your interests. The right MSSP will discuss and provide options for your security needs, alongside your own workforce, and explore what yearly planning looks like for your business to save money and improve efficiency. They should also provide fixed pricing. You need a single point of contact not only technically with delivery, but also commercially.'

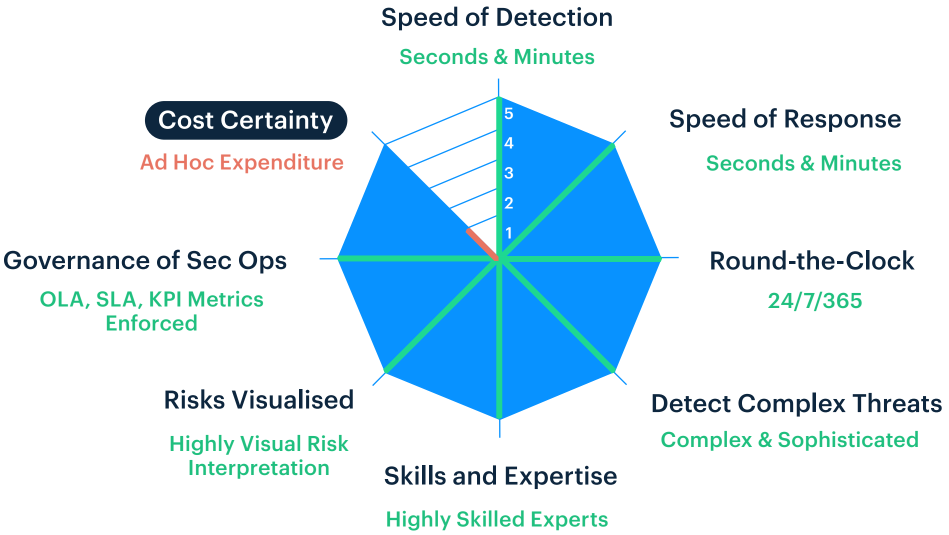
If you have a provider, you need a Service Level Agreement (SLA) to provide cost certainty. You must know:

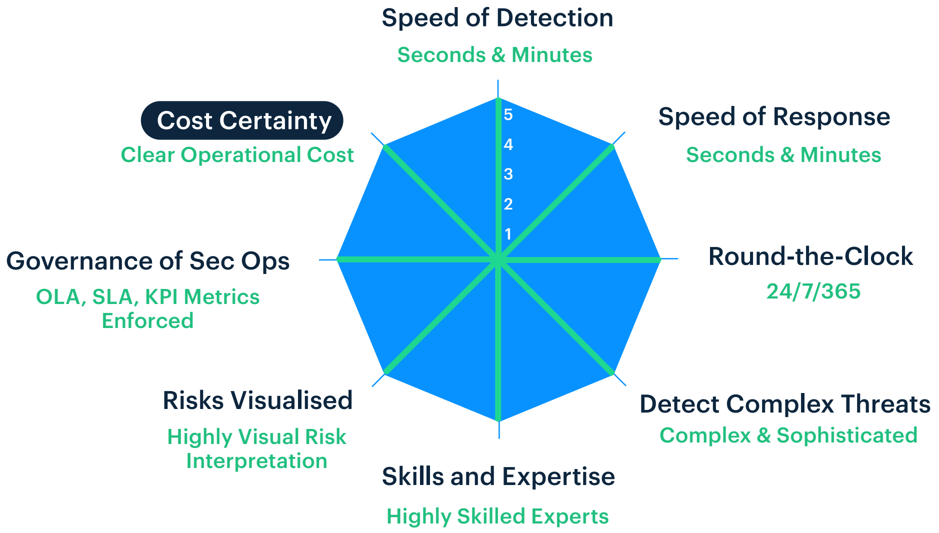
a) What is the cost of the service/services supplied?

b) What is it going to cost every month?

And you must try to narrow it down, so it does not change too much.

If a client does not expand their infrastructure significantly, we provide cost certainty with fixed pricing.





The Outcome of Cost Certainty

Fixed pricing means no nasty surprises. You know what you need, you know how much it will cost you, you get the job done, without expensive additions and contract changes.

Closing Statement

At the end of the day, you must have in mind the outcomes of what you want, and work towards those.

A lot of people make the fundamental mistake that when they buy a SIEM, they believe that 90% of building a Security Operations Centre (SOC) is done. But buying a SIEM does not even cover 15% of what a SOC incorporates, and the work involved. A SIEM is a highly complex tool, which looks for unusual incidents, which needs to be used every second of every day, it needs to be correlated and alarmed, so that it becomes the heart of your SOC.

Many make the mistake of thinking about a SOC purely as a tech purchase, and they go ahead and they do their analysis, and they put out an RFP, but they have no plan in place for the purchase. The scope always creeps up, incomplete visibility and the failure to define the context is what is most damaging.

In fact, the majority, when using a SIEM, go into auto pilot mode because, let's be honest, a lot of people in sales make the sale in the first place by highlighting how the SIEM will do everything for you, will contain and correlate for you and magically sort out all your problems in an instant. This means that people get lazy when it comes to using and configuring all the features, and often don't stop to understand all the features in the first place.

Others use it solely for compliance purposes, which is a poor way to observe your security, as you will never react to threats properly if you just have it sat there as a tick-box exercise. And you still need the expert analysts and team to get the most out of it. Every second of every day.

The right MSSP should improve business efficiency by saving you time, by utilising the right resources, and putting into action the services most appropriate for you. An MSSP can ensure that you are legally compliant, help mitigate threats, and reduce costly disaster repairs if attacked. But, most importantly, an MSSP will support your foundations, so that your business can keep on building and growing, without the constant worry that your security will cause its collapse, both from inside and from external threats.

SIEM is the heart of our SOC, and, in some environments, it is right. But understand what you are buying. We have clients who have a SIEM, and we manage it for them. In that case there are certain requirements. But do not go into the vortex of chasing after the latest feature or the latest technology. At the end of the day, you want clear tickets, clear responses, to enhance your speed of detection and speed of response.

To learn more about SecurityHQ's award winning Incident Management Platform, our services, or to speak with an expert, contact our team.

Author

Barlow, Eleanor

Content Manager, SecurityHQ

As an experienced named author and ghost writer, Eleanor specialises in researching and reporting on the latest in cyber security intelligence, developing trends and security insights. Eleanor holds a first-class degree B.A. (Hons) in English Literature, and a master's degree (M.A.) from the University of Bristol.

How Does SecurityHQ Differ?

SecurityHQ is a Global Managed Security Service Provider (MSSP) that detects, monitors & responds to cyber threats 24/7, to ensure complete visibility and protection.

The right combination of tools, skills, people, and processes is essential to manage, detect and defend your environment from all malicious activity proactively and effectively. Our mission is to provide world-class security operations, to empower our clients and partners, to integrate processes seamlessly, and act as an extension of our user's own teams to address specific risks and challenges and improve security posture.

Which is Why...

We are enabling
the security of clients across the globe in every vertical.

We are collaborating
with partners to provide enterprise grade solutions tailored to client and industry specific needs.

We are helping
businesses feel protected, by delivering **24/7** visibility, every minute of every day, 365 days a year.

We are supporting
organisations with a team of **260+** experts available on demand.

Integrity & Transparency

Our code of ethics is fundamental, not only to our business success, but to the growth of all that we value. We place the power of our SOC team into the client's hands, providing complete visibility of the digital footprint, systems and processes, specific threats, and security posture.

Incident Management Platform

Collaboration is critical for effective security operations. Our incident Management & Analytics Platform provides a single pane of glass for incident workflows, SLA management, data visualisation and document repository.

Innovation

Cyber threats are increasing, both in terms of volume and sophistication. Which means that traditional approaches need to be re-evaluated. SecurityHQ combines best-in-business technology, processes, and expert minds to provide solutions to your security needs.

Bespoke & Engineered

Every client is different. Your risks, geolocations, regulatory requirements, and processes demand a bespoke response. We provide tailored services based on clients' specific needs. Built from the foundation up, our team of expert engineers know exactly what is required.

Have a question? We would love to hear from you.

Safeguard your business, people and processes with SecurityHQ.

Reach us

sales@securityhq.com | +44 (0) 20 332 70699

Americas	+1 312 544 0538
APAC	+91 9359609941
Europe	+44 20 332 70699
Middle East	+971 4354 9535

Follow us f in 🐦 ▶