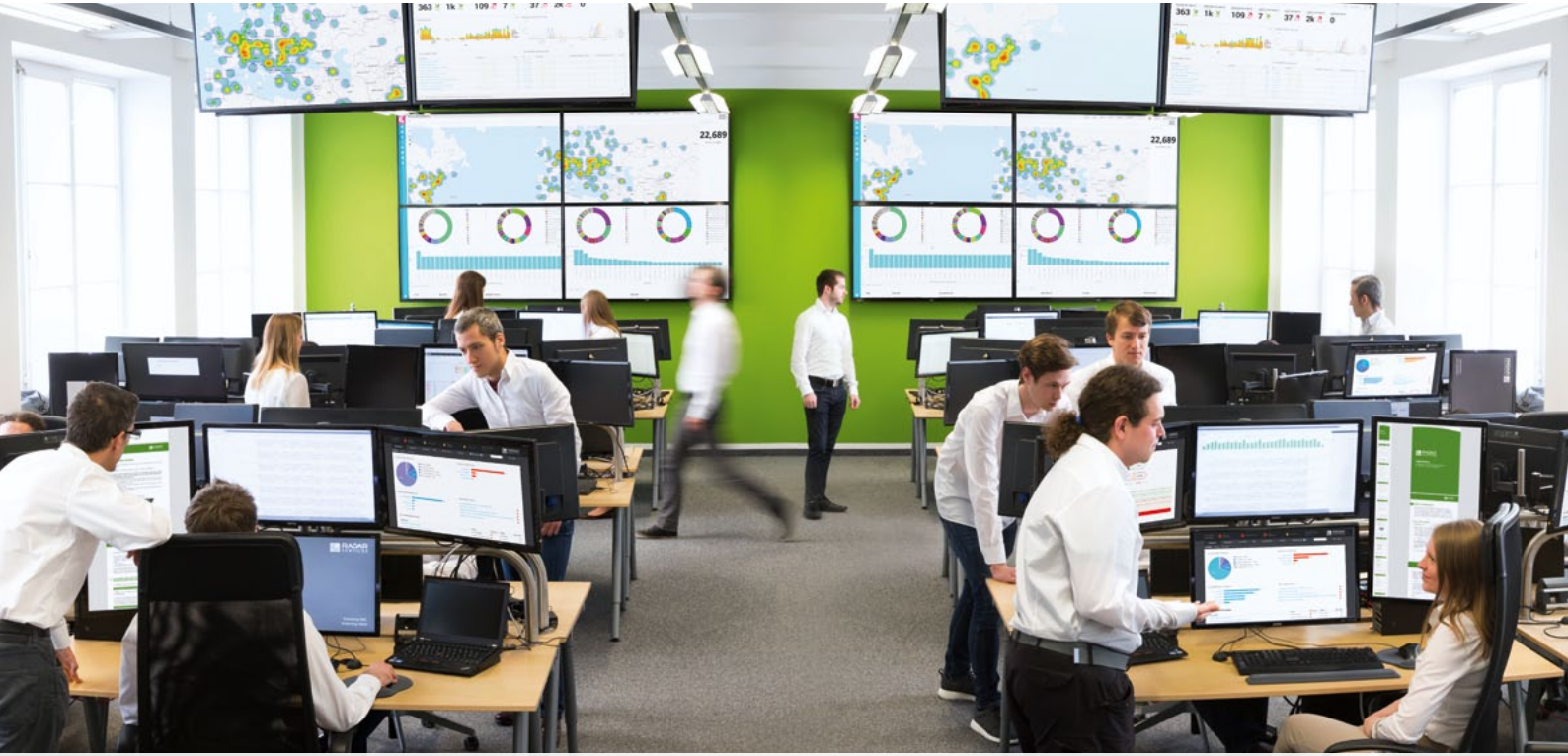
Competence Series

SOC as a Service

Decision Criteria for a Provider Selection



IT Security
made in Europe

RADAR SERVICES

SOC (Security Operations Centre) as a Service versus running your own SOC

Ongoing and extensive monitoring of IT security is a crucial part of an overall strategy aiming at protecting your organisation against attacks, data exfiltration and business disruptions.

Establishing and setting up the right hard and software tools, highly qualified experts, and processes that work perfectly in an emergency within an organisation requires substantial human and financial resources.

There is an alternative, however: SOC (Security Operations Centre) as a Service. Buying in external services is an effective and efficient alternative to running your own SOC. Yet it is essential to choose the right service provider.

This guideline is meant to support you in choosing the right provider by means of a list of criteria.

Criterion 1:
How do you rate the provider's SOC-related expertise and experience?

A

How significant is "SOC as a Service" in the provider's overall range of services?

The answer to this question will vary strongly depending on the provider: **big consultancies provide these services among many others, but they are the core expertise of specialised providers.**

In light of this, it is important to know that "**SOC as a Service**" is not an easily standardisable service. To work effectively, it actually has to be **adjusted to a large degree the individual requirement of a customer's organisation**, especially in cases of acute danger. If, during the selection process, it becomes obvious that the provider lacks capacity for customisation, this signifies a medium-term risk for the customer.

B

Are adequate customer credentials available, allowing to rate a provider's experience for a specific project?

Since SOC providers should offer their customers the highest possible degree of confidentiality regarding cooperation, customer credentials are frequently not available to the public, but are provided **in personal contacts between IT security officials** of the interested company and the provider's customer.

If you are provided with such customer credentials, you will benefit from very individual and thorough feedback from an existing customer of the service provider.

Make sure that the customer credentials originate from **organisations similar to your organisation regarding size, sector or other essential features**.

C

Expressed in figures, how much experience does the provider have?

Indicators for estimating the size of an SOC are the **volume of (1) analysed data, (2) events and (3) vulnerability information, and (4) incidents identified** over the past years. The number of customers and experts is equally revealing.

A SOC's size is not only decisive for rating the SOC provider's experience: In particular, large SOC sites also attract the best security analysts in the world, who in turn influence the work quality of SOCs.

Criterion 2:

Is the technology used future-proof, and does it optimally meet your current and future requirements?

A

What gateways for cyber attackers are identified by the provider's risk detection modules, and how does correlation of Big Data work?

Based on trillions of events originating from various sources, **a simple Cyber Risk Management process** should be created, identifying **decisive risks** by means of the service provider's tools and operations. To achieve this goal, the underlying technology has to work properly for in-depth and in-width analyses.

An optimally integral solution (vs. isolated solutions for various sub-areas) has to be **based on correlation of a wide range of events, originating from both IT itself and the environment in which the IT systems are operated. Correlation has to take place not only within individual risk detection modules** but simultaneously also as **cross-correlation** involving a variety of risk-detection modules, in order to effectively draw conclusions.

B

Does the provider use proprietary or third-party technology?

Another distinctive differentiator between "SOC as a Service" providers is the technology they use: this may be **proprietary technology or a (mostly foreign) third-party technology**.

Technology developed in-house provides three major advantages: (1) The **analysts** processing the results of the automated detection modules, executing configurations making daily adjustments to your needs **understand the technology and its proper use to the smallest detail**. (2) You as the customer can **follow the development of the technology used** and, as the case may be, discuss features that are important to you with the developing experts. (3) Moreover, you can track **software quality to the smallest detail** and examine it any time, if you wish to do so.

C

How efficiently and quickly are recent research findings integrated into technology development and thus into the services provided?

Always up to date with the latest trends: providers using proprietary technology can make themselves stand out with a distinct quality feature in terms of their services' future viability: **their own research department**. The advantage of this is that highly-trained experts can efficiently advance technological trends and their implementation in their own technology. Their **findings are continuously integrated into the services provided** – for instance in the field of machine learning.

Machine learning uses algorithms in order to identify patterns or correlations in existing data. These are underpinned by statistical methods, including classic inference statistics, Bayesian models or clustering. On this basis, systems referred to as "self-learning" or also "behaviour-based" automatically draw conclusions, calculate probabilities for different scenarios and make predictions – these being key features of advanced security technologies.

Criterion 3:

Do you trust the professional skills of the experts working for a service provider, and are they easy to reach even in urgent cases?

A

Who are your individual contact points?

Security is based on trust. Trust especially grows through personal contact, long-term collaboration and "a common language".

Therefore, inform yourself early on about your individual contact points, i.e. the **analysts at the SOC**. Talk with them, **preferably in person**, **request credentials** of and information on their **experience** as well as their **education and training activities**.

B

How is the organisational framework of the SOC expert team designed?

In your evaluation, pay special attention to two **basic organisational factors: the availability of your personal contact points, and low turnover within the analysts team**. Both factors form an important basis for continuously high service quality that you can trust.

Criterion 4:

Do the work and information processes run smoothly within the service provider's organisation as well as in cooperation with your IT (security) experts?

You best assess the functionality of processes by means of a trial run (**Proof of Concept**/POC). After a reasonable period, evaluate: (1) the provider's daily **operations** and **work results** (2) the **granularity of results** that works best for you as a basis for future processing (including reduction of false positives and false negatives) and for the information to all stakeholder groups (3) if the risks are **presented as needed and in a well-structured manner** for critical business processes, IT services and legal as well as regulatory requirements and (4) the **experts' availability and response capacity**.

Criterion 5:
How secure is your data with the service provider?

A

Where is your security-relevant data located?

SOC providers offer various models for handling your security-relevant data which they analyse: in the most secure version, **all your security-relevant data remain at your organisation in physical form**. **Cloud-based services**, however, **give priority to efficiency features**.

B

How highly developed are the service provider's physical and IT security measures, and how are they implemented by its employees?

Quality features for the SOC provider's own physical and IT security should be evaluated as well, for example certification of the entire organisation according to ISO 27001, strong organisational security measures such as isolation of the SOC, access controls, screen recordings or video monitoring, awareness training and reliability tests for employees, and technical security concepts for the use of hard and software as well as encryption within the organisation.

Criterion 6:
How high do you estimate your actual return on investment?

The efficiency of your IT risk detection system should in any case be a top priority, since in an emergency the early warning system has to work perfectly for your IT. However, basic economic requirements must be met as well: is the service provider's **offer competitive**, and will it allow for the flexibility, among other things, you may need in the future? Keywords in this context a are "**pay as you grow plan**" or **adjustment to changed general conditions**, new sites, new system platforms or new applications.

Conclusion

The highly specialised service "SOC as a Service" is an efficient alternative to running your own SOC. At the same time, selecting a SOC provider for trustful, reliable and long-term cooperation is of major importance. Its know-how, experience, technology, experts, processes and its own security should be evaluated in order to make the right choice.

RADAR SERVICES

The European Experts
in IT Security Monitoring
and IT Risk Detection

RadarServices is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client's Security Operations Center (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT security monitoring and an overview of security-related information throughout the entire IT landscape of an organization.

RadarServices
Zieglergasse 6
1070 Vienna
Austria

Phone: +43 (1) 929 12 71-0
Fax: +43 (1) 929 12 71-710
Email: sales@radarservices.com
Web: www.radarservices.com

RadarServices Germany
Taunustor 1
60310 Frankfurt a. M.

Phone: +49 (69) 2443424 655
Email: sales_germany@radarservices.com

RadarServices Middle East
A110-1, DSO HQ Building
Dubai, VAE

Phone: +971 (4) 501 5447
Email: sales_me@radarservices.com

ISO 27001 CERTIFIED

PUBLIC