IS A SOCAAS USEFUL TO BUSINESSES?

The advantages of a SOCaaS solution

Telsy

TABLE OF CONTENTS

INTRODUCTION

The fact that a company does not have cyber security as its core business does not mean that **it does not have to worry about hostile actions coming from the web.**
The correct management of IT infrastructures is essential to guarantee any organization's growth and evolution on the market, as well as obtaining those certifications required to have by law in the field of IT security.

Choosing the right technology is one of the most difficult choices faced by the corporate IT manager in the process of building a secure and resilient infrastructure resistant to cyber threats.

SOCAAS: WHAT IS IT?

An immediate solution to these problems would be to equip your organization with a **SOCaaS security service based on cloud technology.** SOCaaS reflects a service-based model; in particular, **a SOC as a Service outsources parts of the SOC (Security Operation Center) functions to an external supplier.**

Moving to the cloud means that security information, such as **alerts, telemetry, logs, and network information** become accessible through different channels rather than managed through on-premises environments.

The most sophisticated and modern SOCaaS solutions base their service **on the cloud. Cloud computing is a constantly evolving technology and its growing popularity among IT and cyber industry stakeholders** is attracting more and more companies to adopt it as a solution for managing their IT security systems.

The use of cloud technology enables oblique, on-demand and cost-effective network access for a shared pool of computer resources such as servers, networks, data storage, etc., which can be quickly configured **with a minimum level of interaction required with the service provider.**

In other words, cloud computing treats IT infrastructures, software and platforms as virtual units to which **the end user of the service always has access.**

THE 10 ADVANTAGES OF A SOCAAS SOLUTION

Having clarified what SOCaaS is and what technology it uses, we list the main advantages of adopting this solution:

1. **The customer at the center.** The service is aimed at satisfying the needs of the customer-end user. **The provider takes care of setting the line of defense, the customer chooses which are the most suitable lines of defense for his organization.**

In particular, the security manager allows users of the service **to choose** which security measures and protocols are **most suitable for their business or organization.** The security manager will take care of:

- Support the end user of the service in choosing security measures
- Support the configuration of the chosen security measures
- Provide the client with access to all the services provided in the contract

In short, users have various solutions to choose from. The service guarantees different lines of defense for different types of attacks (example: protection of cloud assets, data, programs and virtual machines)

2. **Flexibility.** Some SOCaaS providers offer full coverage, while others unpack their services. **The customer can choose which level of support to request and adapt the service to their needs.**

3. **Cost optimization.** SOCaaS services have a **fixed cost** and do not require additional expenses: the introduction of **SOCaaS lowers operating costs** of the organization that adopts it. The management and maintenance of a local SOC is particularly expensive, especially for small to medium-sized companies.

   Furthermore, the management of your local SOC implies maintaining a relationship with your suppliers: **the SOCaaS service absolves the customer of any management burden.**

4. **(Almost) unlimited storage**. It allows the management of **huge amounts of data** - a SOCaaS service allows the secure storage of this data and its management on a cloud.

5. **24/7 threat monitoring and analysis**. Many companies cannot afford a SOC that runs 24 hours a day every day. **The vast majority of companies in this sector offer SOCaaS services 24/7**, so as to **always** protect the customer against cyber threats.

   Monitoring allows **real-time monitoring** of the network and connected assets and the analysis tools allow **a reliable forecast of potential risks.**
   In particular, the monitoring allows the early detection of threats that have passed the first line of defense, the gateway and **the real-time observation of users** of the corporate network - **both before and during the use of the service** - to collect information and discover **the most sophisticated and evasive malware** nested in the IT infrastructure.

6. **Safety and competence.** A SOCaaS provides the **ultimate technology in cybersecurity** on the market. Outsourcing your SOC means taking advantage of the expertise of the best IT security professionals at **no additional cost.**

   A SOCaaS solution offers an excellent compromise between human and technological support: the service provides qualified and highly competent personnel who can promptly identify and resolve problems and disruptions that can interrupt or slow down company operations.

7. **Cutting-edge and instant threat management.** The use of a SOCaaS allows **significant and precious time saving** in data analysis and threat prediction.

   The AI software used by SOCaaS solutions allow intelligent **management of security alerts** and select the most relevant ones to conduct a threat analysis. Data selection prevents the security team from being flooded with information that could **delay the organization's response to a critical event.**

8. **End-point detection and protection.** Analytical tools based on **AI** monitor and record all the activities of the corporate network in real time, carrying out an assessment of potential threats **to discover its origin, objective and level of risk.**

9. **Reporting.** Many SOCaaS provide a reporting service on a regular basis to ensure **complete and constant monitoring.**

10. **Professional updating. Cybersecurity is a complex and vast subject** that requires **constant updating**. In the near future, technologies and associated technologies will increase exponentially.

    This will inevitably result in the need for **continuous professional updates** and a more specific training process to acquire the skills necessary to update and configure the components of your IT infrastructure. The majority of SOCaaS services meet this need, **offering the service to train the IT staff of contracting organizations.**

GOOGLE CHRONICLE AS A SOCAAS SERVICE

Google Chronicle Security is a cybersecurity company part of the Google Cloud Platform and born from an offshoot of **Google X; it intends to offer a SOCaaS service to its customers in the near future.**

As a partner of Chronicle, **Telsy uses YARA-L** rules-based security for its security protocols, **ready to be integrated into solutions aimed at searching and identifying threats.**

Data upload and management

Google Chronicle allows easy and highly secure uploading of telemetry data. Among its main features, Chronicle forwards data from any **sylog source, existing log aggregators, SIEM systems to its cloud platform,** allowing **immediate traffic analysis.**

Uploading telemetry data includes normalization, indexing and association with hostile events in progress in just a few seconds. Each time a user of an organization that uses Google Chronicle accesses a domain through a browser, **the DNS data is forwarded to Chronicle itself, which inserts, normalizes and indexes them and makes them available in the GUI with equal speed and automatically.** Therefore, analysts will always have at their disposal **the most up-to-date information on network activity** in real time.

Thanks to its dashboard, Chronicle allows **an almost instant understanding of a huge amount of data and activity** in progress on the network, facilitating the management of threats and reducing the time spent on security activities. **Chronicle saves a significant amount of precious time**: for example, if the Chronicle analysis classifies a domain as a threat, the platform will immediately identify all accesses to that domain.

Threat detection

To detect threats, Chronicle follows a process that begins with **the application of the UDM (United Data Model)**, a functioning and extensible scheme for any telemetry used for data security. The data processed through the UDM model are classified according to the context (example: type of asset and vulnerability).

Chronicle's engine allows analysts to easily build advanced and complex threat detection networks on the collected UDM data. Operators also have at their disposal a set of pre-established schemes that allow coverage **for numerous variants of malware, ransomware, trojans, suspicious activities, MITER ATT & CK techniques, lolbin attacks, etc.** Chronicle customers can also take advantage of the detection rules and threat indicators of **Uppercase, Chronicle's research team dedicated to threats.**

Chronicle aims to make it easier to analyze malware and bugs through new advanced tools that also include machine learning. Thousands of potential clues to hacker activity are ignored or discarded every day on average. Security teams usually filter out a few thousand that they think are worth investigating, but in a day's work they are lucky if they can go through a few hundred..

Storage capacity

As far as storage capacity is concerned, **Chronicle is designed to handle data up to over 100 petabytes, resulting in significant savings in economics and storage space.** Chronicle is, in fact, equipped with an unparalleled and state-of-the-art data infrastructure: it automatically resizes factors such as **calculation, memory, I / O** to ensure **optimal performance** regardless of the workload to which it is subjected.

BIBLIOGRAPHY

Alruwaili, Fahad F., and T. Aaron Gulliver. "SOCaaS: security operations center as a Service for Cloud Computing Environments." *International Journal of cloud computing and services science* 3.2 (2014): 87.

Furfaro, Angelo, Alfredo Garro, and Andrea Tundis. "Towards security as a service (secaas): On the modeling of security services for cloud computing." *2014 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2014.

Hussain, Mohammed, and Hanady Abdulsalam. "SECaaS: security as a service for cloud-based applications." *Proceedings of the Second Kuwait Conference on e-Services and e-Systems*. 2011.