SAGA new frontier group

Security Operations Center

DIGITAL SECURITY

Security Operation Center - flexible outsourcing IT security service

IT security or Cyber security nowadays is not only one of the functions of IT operations, but the key element important for the entire company's business. In addition, threats and challenges in this area are becoming more complex and require constant "awareness" and ongoing investment in the form of human and technical resources. Outsourcing IT security service could represent an optimal response to these challenges, reducing business risks while reducing both capital and operational investments.

Zašto je bitan IT security?

IT security or Cyber security nowadays is not only one of the functions of IT operations, but the key element. Our esources can be made available to the whole world, without physical or territorial limitations. It also means that they can be easy object of an attack, even the larger number of attacks at the same time.

It is estimated that the Cyber-crime is "more valuable" and "more profitable" than illegal narcotics. The additional difficulty presents the fact that data can always have a value. That is evidenced with frequent Ransomware attacks (software/virus/malware that encodes/encrypts the data on PC, with the offered price for its unlocking)..

Why SOC?

A few years ago, security in IT was mostly reduced to firewall and antivirus solutions. This was enough as there was less exposed information, cyber-crime market was underdeveloped, threats were less sophisticated. This is best evidenced by the fact that in the last two years a larger number of different types of malware/virus have been detected than in the previous 10 years combined.

Constant changes and new challenges require not only large investments in human and technical resources, but also constant monitoring and adjusting the same. For these reasons, the capital and operating costs of IT security are becoming larger and larger and more difficult to fit into the available budgets.

SOC, as a partial or complete security outsourcing, may represent an optimal, efficient and cost effective approach in response to these challenges.

Powered by INOVENTICA

SAGA new frontier group

BENEFITS OF USING SOC:

Dedicated security experts

one of the most important benefits is a **dedicated security team of experts**. Larger companies may have dedicated teams and expertise in this area, but in this case Saga SOC team may represent an effective supplement to the internal team in areas that internal teams can not cover. SOC's expert team is working with several companies and is cooperating with many institutions concerning IT security and thus their broad experience may represent a significant advantage.

Lower costs and scalability

Saga SOC offers **24/7 monitoring** and mitigation of incidents. Within most companies there is no dedicated SOC, with a team that is able to work in three shifts. While internal approach requires continuous 24/7 monitoring, Saga SOC provides 24/7 monitoring without the need for expansion of internal teams. This approach is also scalable, infrastructure and processes are provided from the start as part of the services, and resources are adapted to the needs and growth without need for additional capital investment.

Awareness and focus

Experience gained in a larger customer data base provides a much wider view than internal resources have. Similar or even the same threats can occur at more customers' and thus acquired specific experience can be applied for faster and more efficient detection and remediation (repair) thereof. IT and security solutions in companies often represent isolated islands both in terms of technical integration and of jurisdiction of the various teams and individuals. Saga SOC is able to monitor the entire IT system with efficient correlation of events into really recognized incidents, on the basis of which the next steps can be taken.

What Do You Get From Saga SOC?

Basic operating step in increasing the security of the system (and thus reducing the risk in business) is achievement of high level visibility of the entire system. Visibility is the key factor in all stages of a potential attacks/incidents - prevention, detection and response i.e. mitigation. Achieving visibility is not an easy task - it is not merely monitoring of all parts of the system, but filtering, correlation and focusing on true incidents, which is a continuous "search for a needle in a haystack.

Saga SOC service is adapted to that particular environment and specificities. It is able to track the systems which are composed of solutions from different manufacturers. Prior to the implementation phase, our team actively works with the customer to analyze requirements and the overall system.

By 2020, 75% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2012.

„Five Golden Rules for Creating Effective Security Policy", Gartner security report, septembar 2014.

SAGA
new frontier group

Saga d.o.o. Beograd
64a Zorana Djindjica Blvd.
11070 Belgrade, Serbia
www.saga.rs

By 2018, more than half of organizations will use security services firms that specialize in data protection, security risk management and security infrastructure management to enhance their security postures.

Gartner's 2014 Security and Risk Management Summit, London, septembar 2014.