SECURITY OPERATIONS CENTER

SOC

Security Operations Center

abbreviated as SOC, provides an opportunity for security professionals to monitor the organization’s equipment, defend it against threats, and proactively reduce their destructive effects.

The more information we store on the Internet, the greater the risk of being hacked. The cyber threat landscape is rapidly evolving, and protecting against potential cyberattacks requires monitoring and rapid response. Cyberattacks have been ranked as the fifth threat in 2020 and have become the new norm in the public and private sectors.

It is said that all types of cybercrimes have increased by 600% in the past two years, and it is predicted that the damages of these crimes will reach 10.5 trillion dollars by 2025, but this number was three trillion dollars in 2015. The risk of cyberattacks and hacking is lurking for every organization and business, and no matter how much you spend to protect and defend your organization, these risks still exist. As defense and security methods become more advanced, attackers' methods become more complex. For this reason, organizations and businesses should look for new, fast, and up-to-date strategies and solutions to identify risks and threats in the shortest possible time and respond to them appropriately and on time; this is the responsibility of the security operation center team of the organization.

Organizations use superior macro-level security technologies to prevent all kinds of attacks, timely detection and provide optimal solutions. Considering the existing limitations organizations are trying to reduce risks in the organization as much as possible by implementing security controls.

Introducing the Security Operations Center (SOC)

The Security Operations Center (SOC) is the foundation where the organization’s information security teams operate. The term SOC refers to both the physical center and the security team that detects and analyzes security incidents and ultimately responds to them. In other words, the Information Security Operations Center (SOC or ISOC) allows security professionals to monitor the organization’s equipment and defend it against security threats, proactively identifying and reducing their destructive effects.

SOC teams usually consist of a manager, analysts, and security engineers. In the past, only large organizations were able to set up SOCs; still these days, many small and medium-sized companies are implementing lighter SOCs with the help of technical solutions, including managed security services.

Different types of services available in the Security Operations Center

	Service name	Description
1	Security monitoring	Continuous monitoring of possible security events in the organization and general security situation
2	Security event analysis	Analyze and review the identified events and provide reports to explain the events to different layers of the organization
3	Malware and forensics analysis	Establish a mechanism to deal with threats or notify relevant departments to take the necessary action
4	Threat Intelligence	Gathering evidence and In-depth analysis of the security incidents
5	Threat Intelligence	Utilize the information published by various references on the Internet about various cyber threats
6	Vulnerability management and security setting	Continuous identification and evaluation of potential misconfigurations and vulnerabilities on various organization assets
7	Threat hunting	Proactive search for threats that existing security solution has failed to detect

Solutions and technologies used in SOC

Routers/Switches	SIEM	Ticketing & KB Management
L4/L7Firewall	IDS/IPS	FPC
PAM	Vulnerability Scanner	UEBA
Asset Management	TI	SOAR
Antivirus	Security Configuration Management	Forensic Tools
EDR	NTA	Malware Analysis Tools

Challenges of Traditional Security Operations Center

- Traditional Security Operations Center
  - Focus on data collection and normalization
  - Use of threat intelligence resources
  - Correlation rules

Challenges:

- The High volume of logs and generated data
- The High volume of generated alerts
  - According to surveys, SOC analysts can only review up to 10% of the generated alerts
  - No action is taken on 64% of the produced security tickets
  - The High costs of SOC experts
- Diversity of threat intelligence sources

Next-generation security operations center (NGSOC)

- High scalability and use of big data solutions
- Use of artificial intelligence and machine learning algorithms
  - Reduce false positive rates (FP)
- Utilizing SOAR technologies
  - Automation in the incident handling process
- Reduce the human resource workload and Focus on important operations instead of repetitive ones
- Increase the usability of threat intelligence resources through artificial intelligence technologies

SOC Benefits

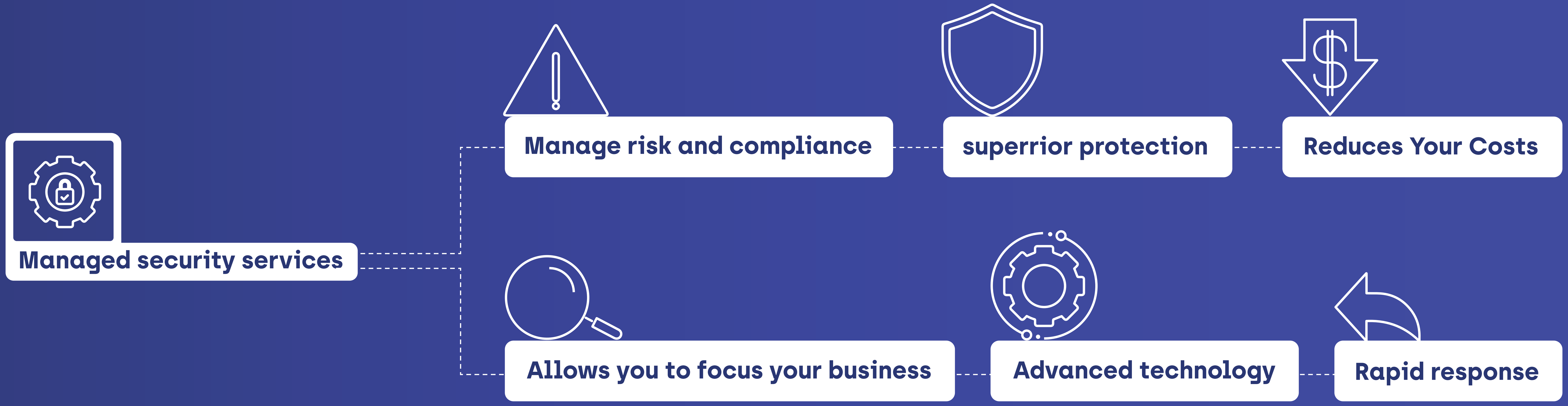
- Reduce the time required to collect information, incidents, and alerts in an emergency
- Reduce the costs of service interruption

SOC implementation steps

- Planning the Security Operations Center
- Designing a security operations center
- Installation and implementation
- Setting up and integrating tools
- Establishing processes and security cases
- Advanced measures (establishment of SOAR, diagnoses based on behavioral abnormalities, etc.)

Managed security services and security operations center as a service

Given the valuable experiences of the SOC experts in Spara Group, without a doubt, one of the best ways to use these experiences and reduce concerns related to human resources is to outsource security services entirely to the Spara security team. With the development of cloud computing services worldwide and the advantages of this technology, outsourcing security services to specialized businesses in this field has also become more popular. One of the most important benefits of outsourcing security services is the focus of businesses on their technical activities and the use of experienced and specialized external teams in cyber security. Other benefits of getting security services from security service providers are listed below:


Managed security services

Manage risk and compliance

superrior protection

Reduces Your Costs

Allows you to focus your business

Advanced technology

Rapid response

SOC is suitable for which businesses?

Deploying a security operations center can be effective for small and large organizations.

About Spara

Today cyber risks are a critical threat to all organizations worldwide. In the past, organizations tried to provide their cyber security only by using the security equipment and software available in the market. But today, cyberattacks have a very complex structure, so it is no longer possible to deal with them using traditional methods. Therefore, to deal with advanced cyber threats, organizations need to use advanced detection and prevention systems to identify them in the shortest possible time in case of cyber penetration.

In this regard, “Spara” company and a group of the best cyber security experts in the country have produced new products, diverse services, and comprehensive cyber security solutions. “PAM”, “EMS” and “EDR” are the most important products of Spara. Spara’s security services and solutions also include a wide range of security services such as “Security Operations Center”, “Penetration Test”, “Threat Hunting”, “Red Team”, “Governance, Risk Management, and Compliance”, “Incident Response”, “Consulting” and “Training”.

We have been trusted by:

بانک پاسارگاد

TEJARAT BANK بانک تجارت
بانک تجارت

فناپ
زیرساخت

فناپ تلکام
FANAP TELECOM

فناپ تک
FANAP TECH

بانک آینده
AYANDEH BANK

ریاست جمهوری
معاونت علمی و فناوری

سایپا

MIDHCO

پست بانک ایران

همراه اول

SHATEL
شاتل

شرکت سپرده گذاری مرکزی
اوراق بهادار و تسویه وجوه (سهامی عام)

شوکا

شرکت فناوری اطلاعات ناواکو

pod
پایگاه اطلاع رسانی پشتیبانی پاد

داتین
شرکت نرم‌افزاری داتیس آرین قشم

سازمان فناوری اطلاعات ایران

نماوا
NAMAVA

ایرانسل
MTN

اسپارا
SPARA

☎ +98(0)21-22275003

✉ info@spara.ir

www www.spara.ir