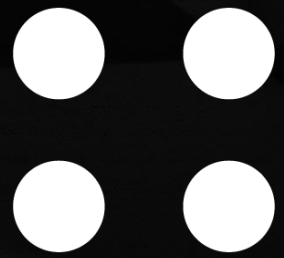


CYBEROO

SECURE SOUL

AN ATTACK EVERY 39 SECONDS

86%
attacks with cybercrime targets (vs 81% in 2020).

79%
attacks with high and/or critical impact in 2021 (vs 50% in 2020).

+58%
servers compromised by malware and botnets in Italy.

80%
very serious attacks in 2021 (vs 56% in 2020).

Sources: Clusit Report 2021; University of Maryland

WHAT DO YOU NEED TO PROTECT YOURSELF?

ADVANCED TECH

360-degree protection

PEOPLE

Cybersecurity Specialist

ALWAYS ON

Constant watch 24/7/365

YOU NEED AN ADVANCED SERVICE THAT COMBINES THESE THREE ELEMENTS:

According to Gartner, «By 2025, 50% of medium-sized enterprises will use MDR providers as their only managed security service»

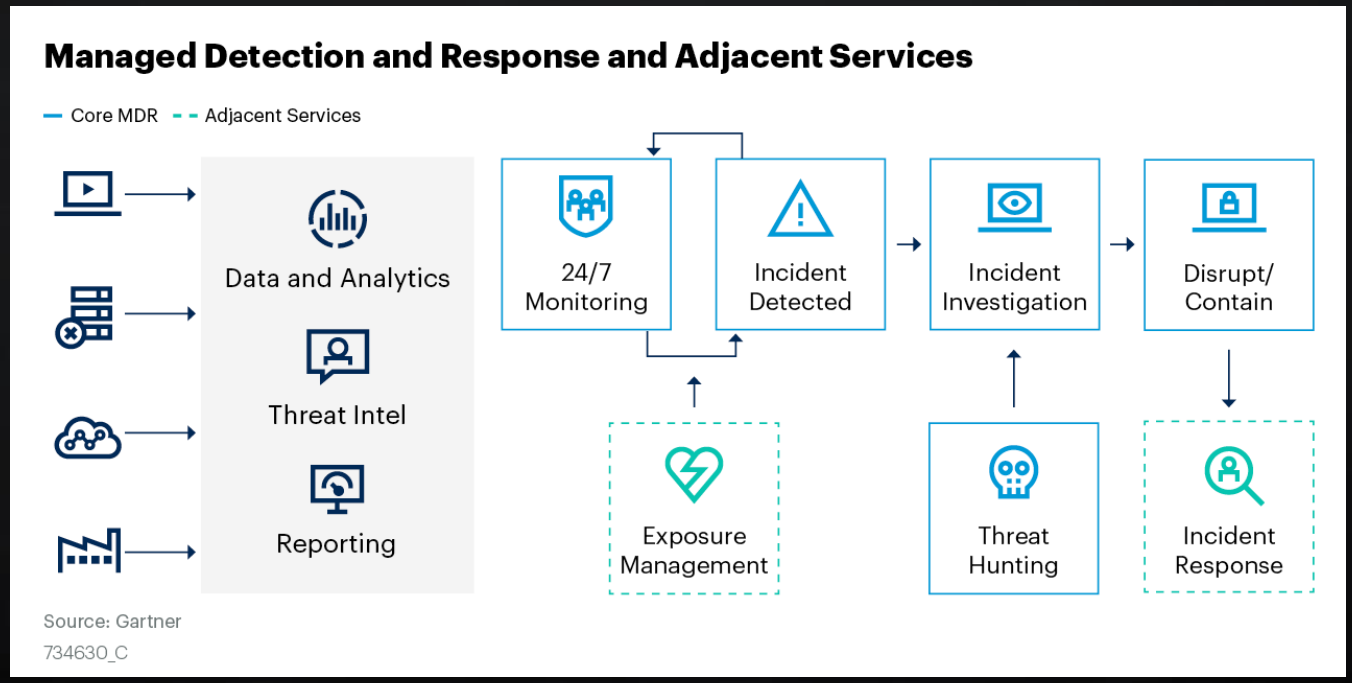
Scan the QR Code to download Gartner's «Market Guide for Managed Detection & Response Services 2021»

Notes: Gartner®, Market Guide for Managed Detection and Response Services, Published 25 October 2021 By Pete Shoard, Craig Lawson, Mitchell Schneider, John Collins, Mark Wah, Andrew Davies.

WHY AN MDR?

ACCORDING TO GARTNER ALL ENTERPRISE MIDSIZES SHOULD EMBRACE AN MDR

Different sources of information



Sources: Market Guide for Managed Detection and Response Services, Published 25 October 2021 By Pete Shoard, Craig Lawson, Mitchell Schneider, John Collins, Mark Wah, Andrew Davies.

WHY AN MDR?

BENEFITS

01 Strong **improvement in the technological capabilities of 24/7 detection** thanks to i-SOC and advanced technologies and thanks to the use of AI, Machine learning and behavior analysis and automatic remediation.

02 **Reduced time to identify threats** with a strong focus on those threats that bypass preventive security systems.

03 **Access to cyber security specialists that are still not very widespread on the market** today with a strong focus on identifying and resolving threats.

04 **Ease of installation:** the solution in fact requires an initial study lasting only a few weeks, followed by deployment. The solution is already working immediately after installing the agent.

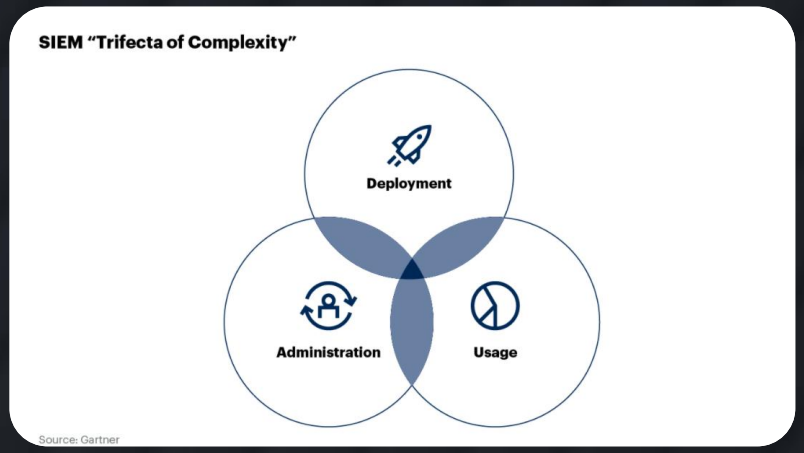
05 **Strong savings compared to building a 24/7 in-house team**, clear and well-defined costs with a monthly fee.

06 **Enhancement of investments already made in security systems** as MDR technologies adapt to the customer's existing eco system.

Source: Market Guide for Managed Detection and Response Services, Gartner, 25 October 2021

WHY NOT A MANAGED SIEM?

Gartner defines SIEM as a technology that supports threat detection and security incident response through real-time collection and **historical analysis** of events and that **supports compliance reporting and incident investigation through analytics historical data from these sources**



1

SIEM technology is a very common technology among large companies; however, it may not be the right approach for all organizations.

2

64% of midsize companies believe that SIEM is the answer for threat identification and detection. However, a SIEM solution could be difficult to implement and not be functional to the needs of detection and response.

3

To ensure that midsize companies can properly distribute and deliver value from a SIEM tool, they must have the appropriate resources and processes to support it, both internally and in case you choose an external SOC to manage it.

Source: Do Midsize Enterprises Need an SIEM to Have a Successful Cybersecurity Program? Gartner, 27 May 2020

MAIN PROBLEMS OF A MANAGED SIEM

01 COST

SIEM can get expensive quickly. Midsize companies need to plan future acquisition costs by analyzing the amount of data they are currently generating and anticipating the amount of data they can generate over time in order to adequately predict any increases in licensing capacity and / or underlying hardware purchases.

02 MANAGEMENT

Deploying a SIEM can be very complex. Make sure that the adequate amount of internal staff is available to support the soc at this stage.

03 RELIABILITY

Setup takes time. Midsize companies implementing SIEM technology must ensure that ingested log sources serve a purpose and are not collected for the sake of collection. Log sources must also be periodically checked and re-evaluated as to why those log sources are being collected. SIEM was created to provide a holistic view of an organization's IT security and create situational awareness. But it wasn't created to focus on detecting and responding to advanced cyberattacks.

04 SUSTAINABILITY

SIEM implementations are not just about technology, but also about its use. For example, your organization's use cases and log origins may change due to digital transformation and your SIEM must be able to evolve and be leveraged with business. Another common problem that occurs when SIEM technology is used is that there may be some analyst fatigue due to the amount of false positives.

05 SCALABILITY

For the correct use of a SIEM, midsize companies will need to collect, process, normalize, archive and log analysis of events relevant to security and other relevant data for the context, this often means the need to manage large amounts of storage. Furthermore, it is good to understand the flexibility of the SIEM to be implemented, verifying that the possibility of integrating data from new devices is foreseen in the future.

Source: Do Midsize Enterprises Need an SIEM to Have a Successful Cybersecurity Program? Gartner, 27 May 2020

CYBEROO,
YOUR ALWAYS ON
CYBER TEAM,
TO PROTECT YOU.

BECAUSE YOUR COMPANY IS VALUABLE.

CONTACT US

ADDRESS

Cyberoo S.p.A.
Via Brigata Reggio, 37
42124 Reggio Emilia

PHONE & E-MAIL

Tel. 0522.385011
Fax. 0522.382041

Mail: info@cyberoo.com

WEBSITE & SOCIAL

Web: www.cyberoo.com

LinkedIn: CYBEROO

Twitter: CYBEROO

YouTube: CYBEROO