# ALTER SOLUTIONS MANAGED SOC

Alter Solutions Managed SOC offers you a complete security incident detection and response service. We leverage the latest technological advances (UEBA, Machine Learning) and our experience to improve your detection capabilities, accelerate your incident response and reduce your costs.

## PREVENT

**Monitoring**
Our experts are continuously informed about new threats.

**Continuous improvement of detection rules**
We constantly update our detection rules according to the evolution of the threat and our customers' environments

**Automatic threat blocking**
Implementation of automatic responses on high-fidelity use cases (without false positives).

**Technology consulting**
We provide our clients the benefit of our expertise in cyber defense to guide them in their technological choices.

## DETECT

**24x7x365 detection**
Take advantage of our continuous detection capabilities for a fast and efficient response

**The right data, at the right time**
Advice on the collecting strategy to adopt and support in its implementation.

**Advanced detection techniques**
Artificial Intelligence, Machine Learning, UEBA, weak signal detection, Threat Intelligence.

## INVESTIGATE

**Contextualization**
Alerts are automatically enriched with data to contextualize and process them faster.

**Advanced investigation**
A manual investigation is made by our experts to conduct a deep analysis when necessary.

**Qualification**
Selection of true and false positives and determination of the criticality of the alert.

## RESPOND

**Fast and accelerated response through automation**
Response performed by our experts and supported by our SOAR platform.

**Incident Response Tracking**
Process of notification and follow-up of incidents allowing customers to track all stages of the response.

## Your security solutions orchestrated on a unique platform

All prevention, prevention, detection and incident response solutions managed from a single platform platform: SIEM / SOAR / EDR / NDR / UEBA.

## Freedom of choice of editors

With Alter Managed SOC, you have the ability to provide your own prevention, detection and response solutions that we integrate into our platform, or take advantage of our partners' solutions.

# THE OFFER ADAPTED TO YOUR NEEDS

## Co-Managed SOC

Alter Solutions assures the deployment and maintenance of your security solutions. This means that your teams can analyze security events without having to worry about maintaining the platform. In addition, they benefit from the panel of detection rules made available by Alter Solutions and regularly updated.

## Managed SOC Advanced

A complete detection service operated in 8x5 by our teams and with 24x7 supervision by our on-call teams of SOC experts.
In addition, you benefit from a remote incident response service allowing our teams to carry out the primordial response actions during a security incident.
The most suitable offer for any organization wishing to significantly improve their detection and incident response capacity.

## Managed SOC Essential

The basics of a detection service including the maintenance of your security solutions, but also a 5x8 supervision service monitoring by our SOC teams. Ideal for organizations wishing to implement an efficient detection service at a reduced cost.

## Managed SOC Elite

The most advanced incident detection and response offering including 24x7 detection service by our SOC teams as well as a remote incident response service. Take advantage of close monitoring of detection activities, as well as the inclusion of advanced markers dedicated to your environment (CTI) to detect the most advanced threats. An offer adapted to any organization with continuous 24x7 activity that wants to take advantage of the most in-depth and responsive detection and incident response capabilities.

## Compare our offers

| Components and features | Co-Managed SOC | Managed SOC Essential | Managed SOC Advanced | Managed SOC Elite |
|---|---|---|---|---|
| Integration of (EDR, NDR, XDR, etc) | ✓ | ✓ | ✓ | ✓ |
| Operational maintain | ✓ | ✓ | ✓ | ✓ |
| Detection maintenance | ✓ | ✓ | ✓ | ✓ |
| Detection services | | Business hours | 24/7/365 | 24/7/365 |
| Reporting | | Monthly | Bi-monthly | Weekly |
| Follow-up meeting | | Quarterly | Monthly | Bimonthly |
| Execution remote incident response | | Option | ✓ | ✓ |
| On-site incident response | On demand | On demand | On demand | On demand |