eciperon
MV Group

SAC

Strategic Awareness Cell

SAC creates an awareness in your digital environment where we detect the threats and act to counteract the intrusions before they occur and reduce the damage once the intrusion is a fact.

SAC is a staffed service with Nordic staff where you subscribe to a trained high-performance Cyber Team with many years of experience.

You get a Cyber Team with routines, daily trained and educated operators, external surveillance.

SAC

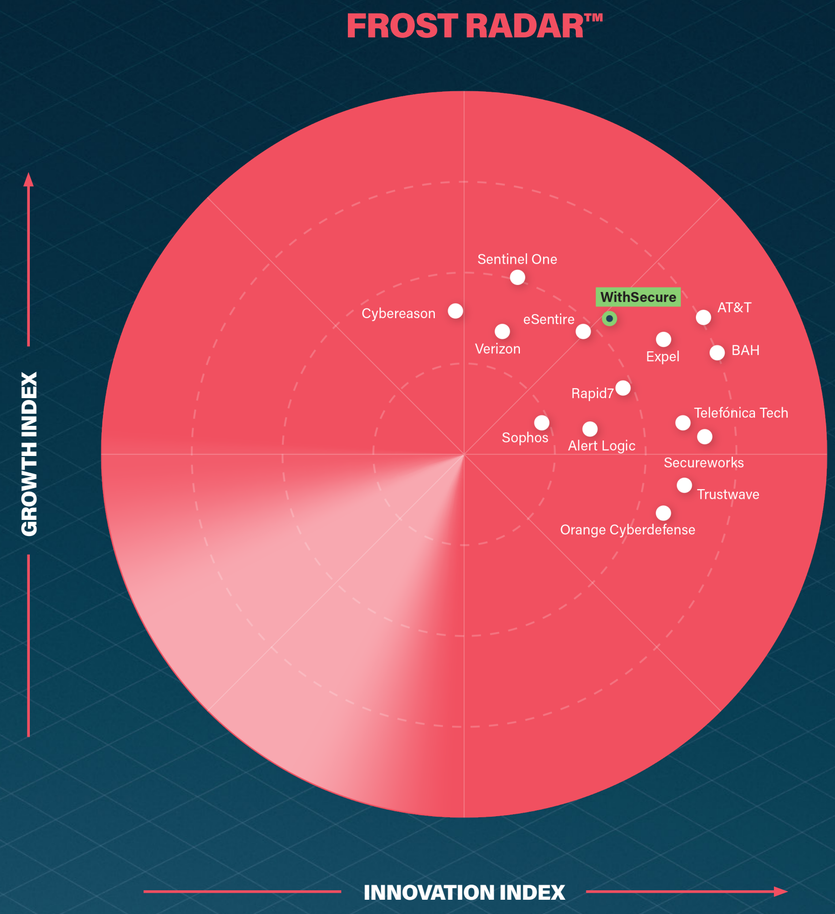
Strategic Awareness Cell

The Future of MDR

Global Managed Detection and Response Market (Frost)

Organizations will increasingly make use of MDR services, relying on the service providers' vast knowledge, expertise, and monitoring capabilities. Due to this, they will be able to allocate their resources to other, more strategic tasks.

The new generation of solutions and services promises to deploy machine learning and artificial intelligence, automating decision making to improve the overall performance of the security stack. In the next five years security services and solutions that provide a combination of human teams and automation will thrive in the market.



SAC

Strategic Awareness Cell

SAC architecture

A managed detection and response (MDR) solution built by attackers for defenders

Effective Attack Detection and Response

SAC dedicated attack Detection and Response team deals with potential cyber threats to your organization in minutes.

SAC acts as an extension to your cyber security team, sharing our threat hunting expertise, helping your team learn and grow and supporting continuous improvement of your security posture.

Peacetime Value

SAC provides cyber security insights that support continuous security posture improvement.

We help you improve your security posture and meet your compliance obligations.

SAC

Strategic Awareness Cell

eCiceron SAC and common D&R solutions compared

The service's utmost goal is True Partnership to act as an extension of the client's security team.

Even when there are no alerts to report WithSecure aims to deliver peacetime value via telemetry driven insights to increase security posture and improve the customers' readiness

WithSecure's SAC works in Windows, macOS, or Linux operating systems. This makes it more broadly appealing and gives it a reach advantage over other competitors.

Based in Stockholm and Helsinki, Finland, with mostly European customer base.

	Common D&R solutions	eCiceron SAC
Time to value:	Months	**Days**
Logs consumed per month:	Billions	**Millions**
Alerts per month:	100,000s	**1000s of relevant alerts**
Alerts investigated by experts:	0 - 10%	**100%**
Investigation time:	<1 minute	**As longs as necessary**
Solution efficacy: *	<50%	**>95%**
Responder profile:	Analyst	**Threat hunter**

** % of actions that produce a desired result*

SAC Solutions

Install xDR Platform

Supported systems:
Windows, Mac, Linux, Android, iOS

Protection against threat vectors:
Malware, Ransomware, Advanced Persistent Threats, Zero Day Exploits, Phishing Attempts, Business Email Compromise (BEC), Brand and Domain Infringement.

Subscription:
(Per client/month)

24/7 Detection & Response Team

Detect breaches quickly:
Detect targeted attacks quickly thanks to immediate alerts with minimal false positives.

Protection against threat vectors:
Built-in automation and intelligence that support a swift response to the real advanced threats and targeted attacks. SLA 1 hour.

Subscription:
(Per client/month)

(08.00-17.00). Contact us for a quotation on extended responses.

Incident Response meeting

Bi-annually meeting
Bi-annual meeting to discuss eventual alerts that occurred and to update the Incident Response Plan.

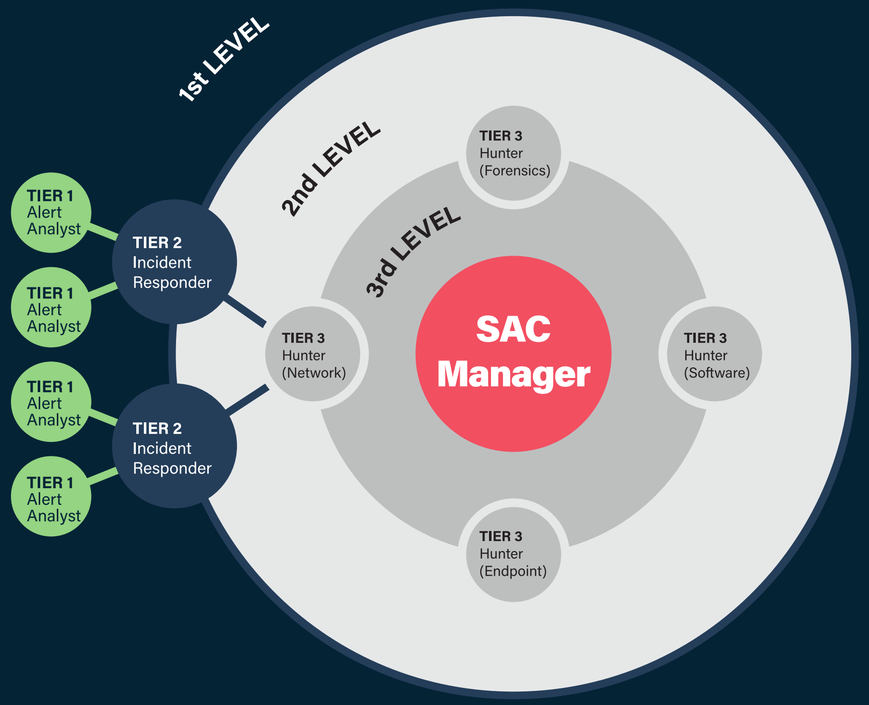
Threat Intelligence report
Summery of actual Global and local attacks from the SAC Threat intelligence team

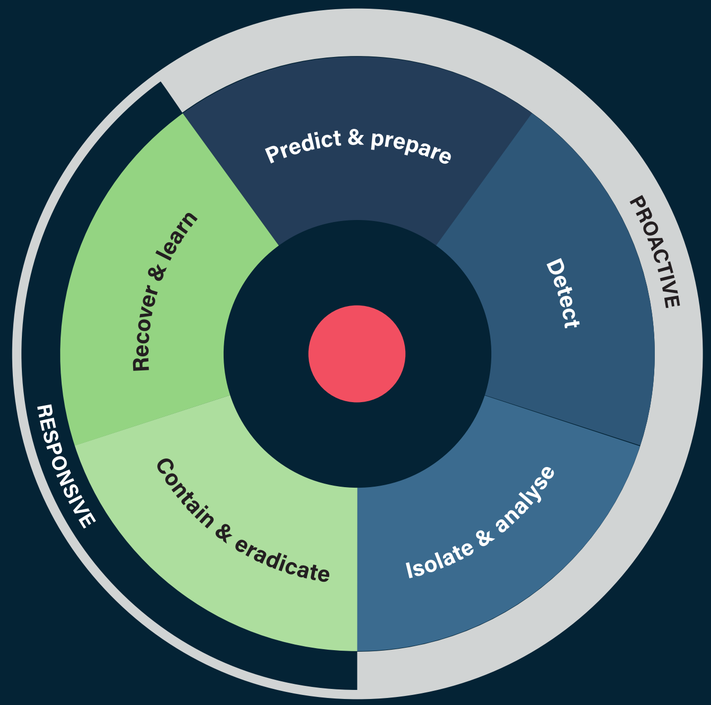
Subscription
(Per client/month):

Included. Contact us for a quotation on extended services.

SAC: Organization Chart

Strategic Awareness Cell





TIER 1
- Limited access
- Removal of false positives
- Act accord. IRP

TIER 2
- Customer contact
- Analysis
- Respond accord. IRP

TIER 3
- Strategic decisions
- Reports
- Board level discussions

IRP - Incident Response Plan