Trantor®

SECURITY OPERATIONS CENTER · TURNKEY

Turnkey SOC

The Security Operations Center that arrives ready to use.

One rack cabinet, three servers plus a malware lab, four operator stations plus a malware lab station, and the video wall: a complete SOC, delivered turnkey into your datacenter.

TURNKEY · ON-PREMISE · ONE SINGLE CONTACT · ASSEMBLY INCLUDED

FEW COMPANIES HAVE ONE, MANY NEED ONE

The sheer complexity of ordering and configuring a SOC room inside your own company has always been a deterrent, even for organizations to which an operations center is fundamentally important.

trantor.it · info@trantor.it

10 August 2026

THE BACKGROUND

What is a SOC for?

01

A Security Operations Center (SOC for short) is the part of a company tasked with monitoring the security of the corporate infrastructure and keeping up with the latest developments in vulnerabilities and attacks.

Who is responsible for the SOC?

The person who sets the SOC's direction is usually the same one responsible for information security across the organization. A SOC is built to be autonomous, but a degree of coordination is needed in order to establish the guidelines to adopt, and to define the department's duties properly.

Who works inside the SOC?

SOC operators are IT technicians, often specialized in cybersecurity or otherwise trained for the role. Their purpose is to use the tools at their disposal to monitor the company's security, to design and improve it, to respond to and investigate incidents, to keep up with the latest vulnerabilities and attacks, and to make sure the company is ready to face them.

Which tools are used inside a SOC?

Besides the physical tools (the video wall and the operator stations), the main software tools are: an event and alarm management system (a SIEM, for instance), a network monitoring system for anomaly detection, tools for forensic analysis of disks and network traffic, a system for tracking the latest vulnerabilities and attacks worldwide, and a defence system to act when an attack is detected.

How does the SOC connect to my infrastructure?

The software installed inside the SOC can connect to the company in several ways: if the company already has systems and appliances monitoring alarms, events, logs or network traffic, the SOC can attach to them; in addition, the security applications the company already uses (firewalls, endpoint protection, and so on) can be operated by the SOC for monitoring and for response when an attack occurs.

What difficulties could I run into?

If your company is short of technical staff to run the SOC, we can supply trained operators remotely or on site, or train technical staff you already have. If the company lacks configured monitoring software, we can help setting up a new monitoring system inside the SOC so that the most important data starts being collected. And if the company has no well-defined security policies, or somewhat vague procedures for hardening the infrastructure, we at Trantor® help you put it all down in writing.

WE STAY WITH YOU THROUGH THE PROJECT

The team behind Trantor® is trained to support companies as they set out to build an in-house SOC. The Trantor® solution exists to shorten the time to a working SOC and to train the people who will run it.

THE EQUIPMENT

An entire SOC, in one cabinet

02

The SOC does not arrive as a list of separate orders: it arrives as a system. Trantor® handles transport, assembly and configuration, and you find everything standing and working in your datacenter. This is the standard supply, item by item.

The standard supply	
19-inch rack cabinet	32 units: the entire SOC infrastructure arrives cabled and tested inside it.
3 TVirt© servers	The SOC platform: the applications and the operator VDIs run virtualized on Trantor® TVirt©.
1 TVirt© malware-lab server	The laboratory where potentially malicious software is examined and tested: separate by design.
2 switches in HA	The SOC's internal network, redundant in high availability.
2 firewalls in HA	The SOC's perimeter, redundant in high availability.
2 cabinet UPS units	Power continuity for rack, servers and network. Redundant in high availability.
4 + 1 operator stations	Five operator stations, one of which is the malware-lab station. Each one: a thin client reaching its own VDI through Trantor® VDesk, two 28-inch 4K 60 Hz monitors, speakers, mouse and keyboard.
1 UPS for the stations	Power continuity for the five operator stations.
Video wall	Four 75-inch 4K 60 Hz screens with a video matrix: the situation always in view of the whole team.

THE PROMISE

«The SOC is not an integration project: we assemble it, cable it and commission it ourselves. Turnkey.»

HOW IT ARRIVES

Transport, assembly, training

03

Transport is our business

A whole SOC cannot travel assembled, and that is not your problem: components and machines travel with us, all the way to your datacenter.

Assembled and cabled on site

Rack, servers, network, stations and video wall: the Trantor® team assembles and cables everything on the spot, down to the last cable. The malware lab stays on separate machines, separate by design.

Delivered and commissioned

We leave only once the system is standing: configured, tested, working. On-premise, inside your perimeter: the operations room is yours from day one.

Training on site or remotely

Our team trains the staff who will run the SOC, so that you end up completely self-sufficient.

How the rack cabinet is built

32 units, one single system: redundant firewalls and switches at the top, the four TVirt© servers in the middle together with the malware lab, power at the bottom. This is what gets assembled in your datacenter.

THE NEXT MOVE

Let's talk.

A session on your perimeter: what the SOC needs to see, who will operate it, where the cabinet will stand. All tailored to your company.

trantor.it

info@trantor.it