Infigo
Managed SOC

Let professionals worry about your IT security so you can focus on your core business

MANAGED SECURITY OPERATIONS CENTER

Atop of every problem a modern business has, there is also **ever-looming threat of cybercriminals**. They are relentless, they can come from anywhere, and **they can strike with impunity**. We can't help you with pure business problems, but **we can do wonders for cybersecurity woes with our managed SOC**

Cybersecurity is expensive. It is hard. It is constantly changing trying to be one step in front of cybercriminals. Security specialists are almost impossible to find, and when you find them, they have to continuously learn new things, and again, that is expensive. **And time-consuming**.

That is where Infigo Managed SOC, Security Operations Center, comes into play. As the term says, Security Operations Center is a department in the organization that is constantly monitoring the organization's security posture, tracking suspicious events, analyzing a high volume of data, trying to prevent security breaches. **SOC is made up of people, technology, and processes** – just having one isn't helpful, it has to be the right mix of all three. And that takes us back to the start and shows why it is expensive. To counter that, **managed SOC is a SOC you rent and skip all that pain of setting it up** by yourself.

Experience shows

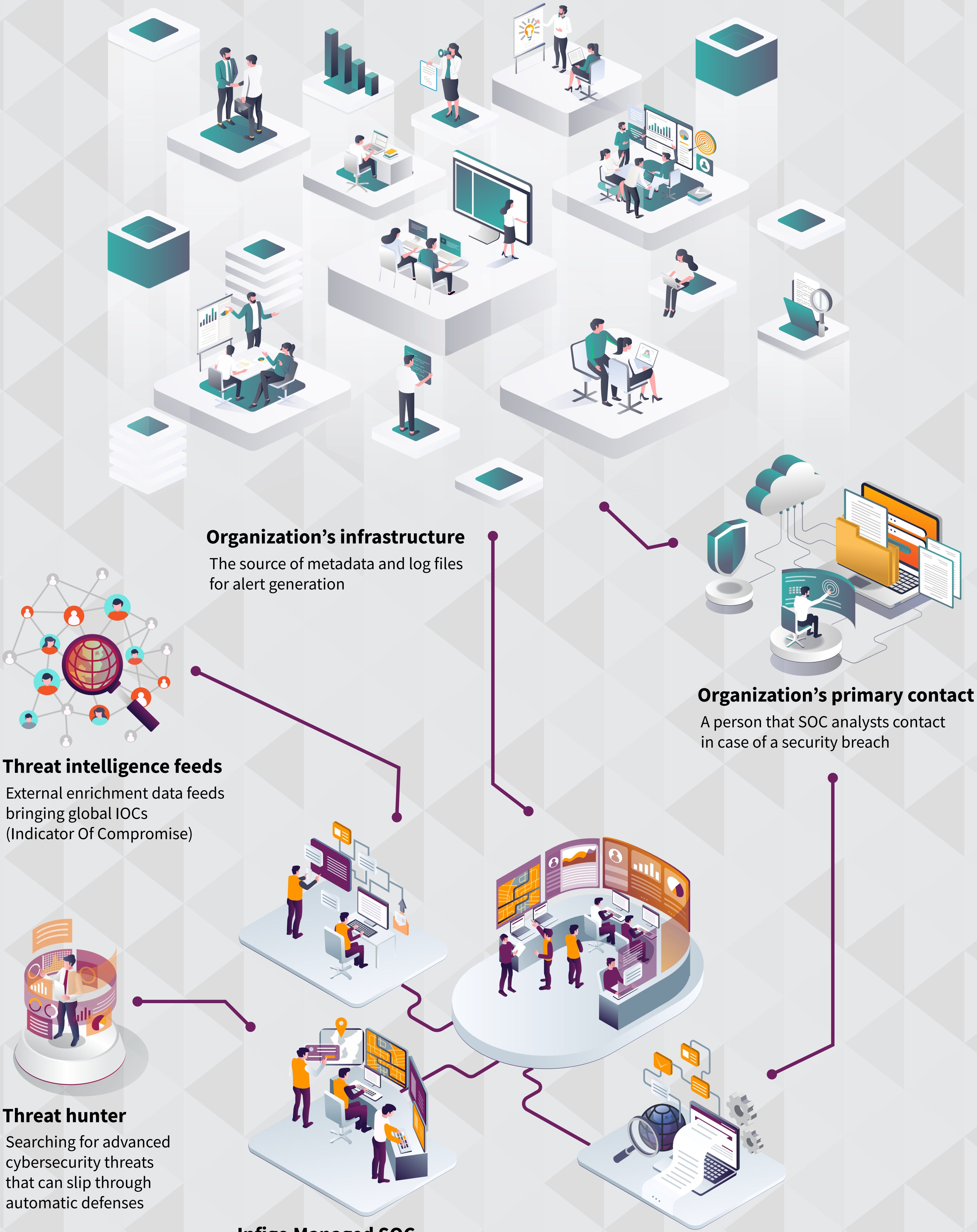
Organizations come to Infigo IS because of our more than 15 years of experience in IT security. During that time, we have established our processes, gathered a thriving team of security specialists, worked with numerous organizations on three continents, and built our own SOC. **We rent our SOC to organizations so they instantly get expertise, maturity, and processes**.

Infigo Managed SOC encompasses our every department – risk and compliance helped with their **extensive knowledge of business processes and regulatory demands**; cybersecurity assessment, better known as the red team, employs **real-world hacking techniques** in their security engagements that enables SOC analysts to see what the "enemy" is doing; security solution implementation, with their massive **experience in mission-critical environments**, refined various procedures that made implementing SOC an ease when compared to other vendors. We have more than 500 years of cumulative experience in every facet of cybersecurity and that shows in our products and services.

So, how does this work?

First, we have preparation and kick-off – we agree on the scope, designate primary contacts, and we go to work. We deploy needed infrastructure, and after that do technical and process onboarding. This step is vital because **your organization is our focal point** and your business policies and procedures should reflect what we see in the SOC – **for Infigo, the client always comes first**. Then it is time for acceptance testing, training, and service activation.

While all that is happening, **we are already monitoring security events on your system**, providing service. Full activation takes about two months. Yes, some claim their service is instantaneous, but that means it is fire and forget, and they expect you to adjust to them. After years of Infigo's integration department fixing implementations of that kind, we have decided we will never allow ourselves to put a client through that ordeal.



Organization’s infrastructure

The source of metadata and log files for alert generation

Organization’s primary contact

A person that SOC analysts contact in case of a security breach

Threat intelligence feeds

External enrichment data feeds bringing global IOCs (Indicator Of Compromise)

Threat hunter

Searching for advanced cybersecurity threats that can slip through automatic defenses

Infigo Managed SOC

Three tiers of security analysts monitor alerts 24x7x365

Key Features

Flexible solution

Except for the Core SOC, which is a basic building block, everything about managed SOC is flexible. We are aware we are coming into a complex system with a lot of existing technologies; we can integrate with them, working with something that you have already paid for. That means that your SIEM, EDR, vulnerability management, or anything in between, can stay.

We offer value-added services that are basically missing components to your system; if you lack, for example, EDR (Endpoint Detection and Response), a critical piece that would boost your security posture, we can offer one.

Three tiers of analysts

Other than SOC manager, and a lot of supporting engineers from other departments, Infigo Managed SOC at its core has three tiers of analysts.

Tier 1 (triage) sees only alerts coming from the client's system so they can do response and triage. If they suspect something more serious is happening, they escalate the problem.

Tier 2 (incident response) can connect to the client's system, but only the specific component to expand their investigation through additional logs.

Tier 3 (forensic) does a complete forensic investigation and helps with remediation if there is a confirmed security breach.

Threat hunting

With data coming from the client's infrastructure in combination with threat intelligence feeds, our analysts do proactive threat hunting. There are many advanced threats, attacks from highly sophisticated bad actors sometimes sponsored by the states (North Korea has many state-sponsored hacking groups), that can slip through defenses.

Highly trained analysts use available data, specialized techniques, and their vast experience to expose stealthy intruders or to spot a complex cyberattack that still hasn't reached its full potential and can be stopped before it does damage.

ABOVE INDUSTRY STANDARDS

Infigo IS, and its products and services, are ISO 9001/27001/22301 certified, GDPR and SOC 2 (System and Organization Controls 2) compliant. ISO and SOC 2 aren't necessary by law, but we like to go above and beyond.

ANALYST CERTIFICATION

Our analysts have certificates from leading international security organizations like ISC2, ISACA, and SANS, that prove they are trained and experienced to monitor and remediate any kind of cybersecurity threat they encounter.

Multiphase enrichment

Security Operations Center gets thousands or even millions security of events per day. It is crucial to filter them to see what is relevant and what is not.

We don't believe in filtering in one go – that means that at the start you lose many events that can become valuable with the right enrichment. Infigo Managed SOC filters events in multiple phases; every phase has an enrichment part where data gets more data points from external or internal sources that transforms it into actionable information. We repeat that process multiple times so in the end, we get highly relevant and focused events.

Managed SOC compatible services

As Infigo IS is a one-stop-shop for your every IT security need, you can rely on us for more than just the managed SOC. If your organization has a problem with IT security or would like to boost it to another level, or has a new compliance problem it has to solve, we are here to help!

With managed SOC in place, you could do a red team exercise where we test the whole organization, trying to break your security on every level possible. Or you maybe have the need for specialized penetration testing service because of PCI DSS? Or you need a custom security solution that we can develop? You have a problem, we'll provide the solution.

Incident reporting

Through managed SOC, we monitor the infrastructure, user behavior, network data, and during an investigation we record the network data from devices in the incident range (for evidence collection or incident investigation).

From all that the client (all relevant shareholders) receives a clear description of the incident, incident categorization according to common incident management procedure defined during the onboarding phase, and a precise description of recommended measures that will ensure this kind of incident doesn't happen again.

24x7x365

Your IT environment never sleeps. Cybercriminals never sleep. That is why our Managed SOC is up and running every second of every hour of every day. Our Tier 1 analysts are always on the lookout, and Tier 2 and 3 are on standby.

FIXED COST

Infigo Managed SOC is a service that has no variable or hidden costs; each organization pre-arranges the scope and price and can be confident in the financial construction from day one without fear of unexpected expenses.

Problem, meet Solution

We don't have enough security specialists!

You and everybody else. There is **a shortage of millions of security specialists** around the world and it is not getting better. That is why managed SOC is such an attractive proposition; you don't have to suddenly have a bunch of specialists for your non-core business. Security is our core business so you don't have to worry about it.

We have a strict policy about data privacy!

That's great! Everybody should have one of those. And that is why **managed SOC doesn't handle your data** – we don't see what is in your documents, we don't hear what you are talking about, **we only handle metadata and log files**. With that we can get a picture about your systems, generate alerts, do threat hunting, everything we need to do our job without infringing on your privacy.

We don't have time to implement managed SOC!

We are aware of that, and that's why we, after agreeing on the scope of work, take over end to end onboarding process. We need around two weeks from kick-off to start security events monitoring, and if all goes to plan, we can deliver the full service within two months.

Truthfully, we don't have a single security specialist!

Again, that is why we're here. **You only need a standard IT department** that handles your day-to-day operations; anything dealing with security is on us, from implementation to monitoring. And in the case of a confirmed security breach, we help your IT department to remediate the problem with our Tier 3 analysts in charge of forensic investigation.

We want assurances we are never going to be hacked!

Unfortunately, **nothing is 100 percent certain** except death and taxes (and some creative accounting practices can help with the latter). As the best and the safest car can't guarantee you will never be in a car accident, the best-managed SOC in the world can't guarantee you will never get hacked. But it can drop the chance of that happening to a manageable minimum.

We can't allow any business slowdowns!

And why should you? During the onboarding phase **there is never any disruption to daily business processes or their continuity** – SOC setup is **completely non-invasive** to the everyday business. The whole point of managed SOC is to protect your business, not disrupt it.

Why us?

Experience

Infigo IS has more than 15 years of experience in the security arena, tested procedures, a long list of certifications and past projects that confirm we are the real deal.

Deep knowledge

Our company is made of different departments, every dedicated to one aspect of IT security; we combine all that knowledge to form balanced products and services.

Big guns

It is often a problem to speak about our projects in the public due to confidentiality clauses, but we can tell you our threat hunters are invited every year to NATO's cyber threat exercise.

40% of the organizations say they struggle with SOC staff shortages and finding qualified people. It is better to rent one than to build one

What happens next is up to you - let us make your life easier

www.infigo.is

INFIGO IS d.o.o.

Karlovačka 24a
10020 Zagreb
Croatia
+385 1 4662 700
info@infigo.is

INFIGO IS d.o.o.

Hasana Brkića 2
71000 Sarajevo
Bosnia and Herzegovina
+387 33 821 245
info@infigo.ba

INFIGO Software Design LLC

2902, Level 29, Marina Plaza
Dubai Marina, Dubai
PO Box 5000307
United Arab Emirates
+ 971 4 512 4081
info@infigo.ae

INFIGO IS d.o.o.

Tivolska cesta 50
1000 Ljubljana
Slovenia
+386 1 777 89 00
info@infigo.si

INFIGO IS d.o.o.

Ul. Metodija Shatorov Sharlo br. 30/2-17
1000 Skopje
North Macedonia
+389 (0)2 3151 203
info@infigo.mk