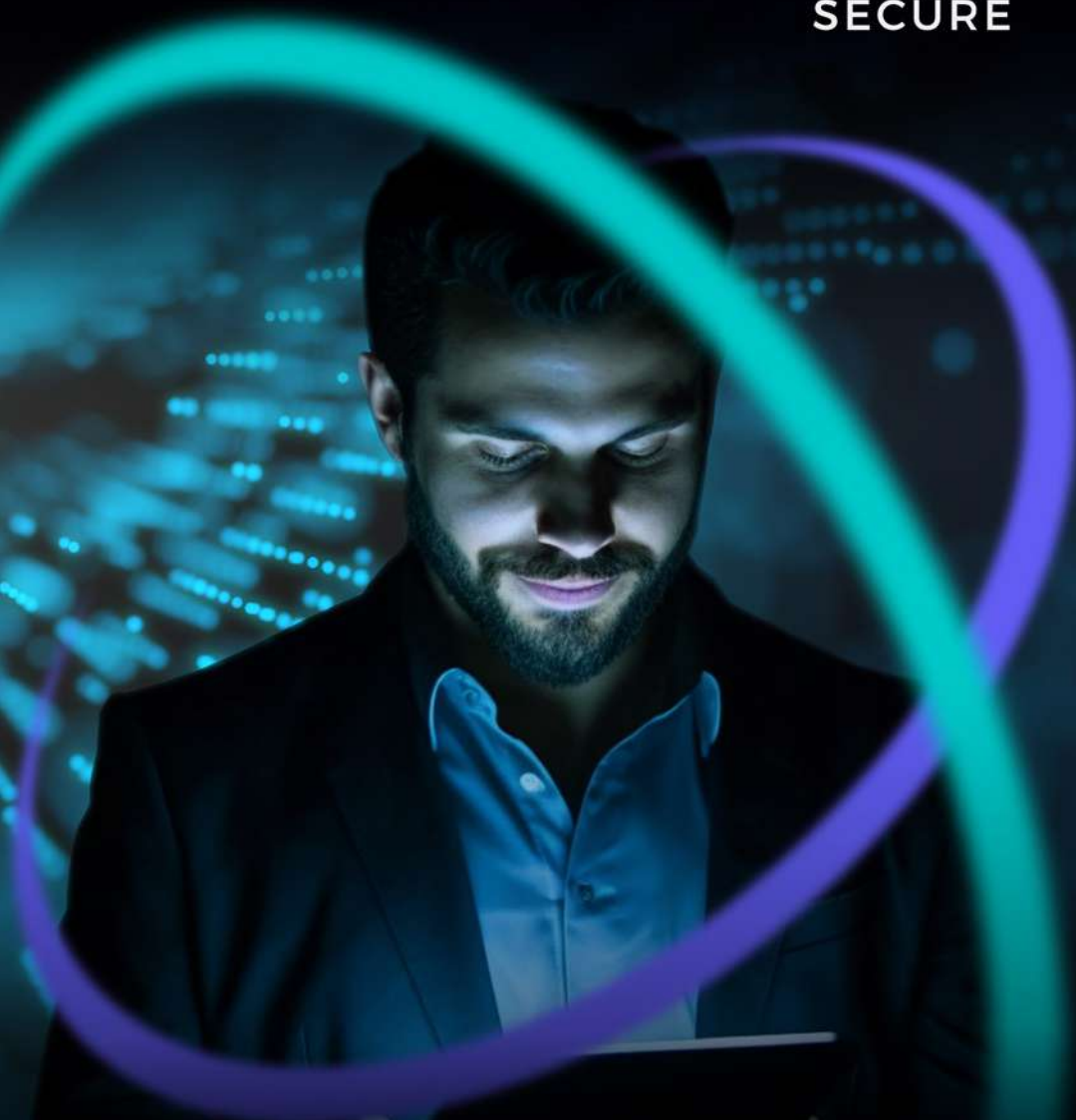




MAIDAR

SECURE



Tailor-made SOC Solutions



MAIDAR
SECURE

WHAT MAKES US

More than your average SOC-as-a-Service provider



We're here for the **Journey**

At Maidar Secure, we believe that cybersecurity should never be a one-size-fits-all solution. Every organisation is unique, with its own specific vulnerabilities, risks, and security landscapes.

That's why we don't just provide cyber threat protection - we craft tailored defences designed to meet the precise needs of each client. Our process begins with a deep dive into your organisation's security requirements. We work side by side with you, identifying potential weaknesses and understanding your unique challenges. From there, we develop customised strategies, whether you need a thorough vulnerability assessment, enhancement of your existing security infrastructure, or a review of your incident response plan.



**Skilled & Experienced
Personnel**



**Comprehensive
Security Infrastructure**



**Scalability &
Flexibility**



**Advanced Threat Detection
& Incident Response**



**ISO 27001:2013
Certified Company**

24/7
SECURITY MONITORING

100 000
END POINTS

25+
YEARS OF EXPERIENCE

But what truly sets
Maidar Secure apart
is our **flexibility**

Unlike many providers who push generic solutions, we adapt our services to seamlessly integrate with your organisation's structure and team dynamics. Our expertise spans a wide range of cybersecurity domains and technologies, ensuring that we've got you covered, whatever the need may be. At Maidar Secure, we're building a security partnership that evolves with you. Your security is our priority, and our tailored approach ensures you get exactly the protection you need.



Whatever the problem,
consider it solved.

Our Global Services

Let's build the SOC solutions you need together.

1 Basic SOC as a Service

Our entry-level SOC service offers continuous monitoring, available either 8x5 or 24x7, supported by an advanced tech stack and a team of seasoned cybersecurity experts. This service lays the groundwork for your cybersecurity monitoring, providing you with peace of mind as your business grows, knowing your digital assets are under constant, vigilant protection.

- ✓ 8x5 OR 24x7 SLA-based Detect & Notify
- ✓ Threat Hunting and Advisory
- ✓ High-level support on customer-owned SIEM and SOAR Solutions
- ✓ SLA Reports
- ✓ Executive Reports
- ✓ Compliance Reports

2 Standard SOC as a Service

Our Standard SOC service is specifically designed for small to medium-sized businesses (SMBs) that require real-time visibility, monitoring, and expert guidance on remediation. This service features an integrated tech stack, bolstered by automation to streamline repetitive analyst tasks, along with continuous tuning of detections and alerts for optimal security.

- ✓ Basic SOC as a Service + SIEM as a Service
- ✓ Log Management with 400 Days Live Log Retention
- ✓ Platform Administration
- ✓ Daily Health Check Reporting
- ✓ Activeboardxs (Real-Time Dashboards)
- ✓ Collaboration Integrations
- ✓ SecOps DFIR Triaging
- ✓ SecOps DFIR Entity Analytics
- ✓ Compliance Use Cases



3 Advanced SOC as a Service

This SOC bundle includes SOAR-as-a-Service (SOARaaS) seamlessly integrated with our SIEM solution to automatically respond to alerts, drastically reducing response times. Custom automations and workflows are tailored to your specific environment and threat landscape, ensuring that automated responses are both fast and precise.

- ✓ Standard SOC as a Service + SOAR as a Service
- ✓ 750+ integrations
- ✓ 680+ content packs
- ✓ Workflow automations for active response
- ✓ Security-focused automated case management
- ✓ Threat intelligence management
- ✓ Network security automation
- ✓ Cyber security vs. operations integration and automation
- ✓ Machine learning-based playbooks
- ✓ Scheduled reporting
- ✓ Consolidated dashboards for incidents,
- ✓ SLAG and collaboration

4 Enterprise SOC as a Service

Designed for enterprise companies, this advanced SOCaaS package combines all the benefits of our top-tier SOC services with the power of external threat intelligence. This integration enables the identification of external threats while actively monitoring internal behaviours through UEBA (User and Entity Behavior Analytics) and custom detection use cases tailored to your specific log sources. This comprehensive solution offers unparalleled protection for your organisation.

- ✓ Advanced SOC as a Service + C.E.R.U. (CIRT)
- ✓ Cyber Emergency Response
- ✓ Standard 15 hours support per month
- ✓ Co-managed SOAR management and collaboration
- ✓ Unlimited use case development
- ✓ SIRP (Security Incident Response Program) Management
- ✓ Training (5 hours per month)
- ✓ Preparation (13 hours per month)
- ✓ Testing (Red-Teaming) 6 hours per month)

5 SIEMaaS

Traditional log management falls short against today's sophisticated threats. SIEMaaS provides advanced threat detection through predictive analytics, pattern recognition, and machine learning. This enables your team to identify and connect anomalous or dangerous behaviours across your organisation's network, enhancing your ability to respond to emerging threats effectively.

6 XTI (External Threat Intelligence)

XTIaaS harnesses a broad array of intelligence from diverse sources, including proprietary research, to deliver tailored threat intelligence feeds. These feeds are customised based on your industry, geographic location, and technology stack, providing a clear view of your external footprint and enabling swift reduction of your attack surface.

7 Vulnerability Management

Identifying vulnerabilities across both external and internal infrastructure can be daunting without proper prioritisation. VMaaS simplifies this process by using automated scanning and advanced analytics to detect vulnerabilities in your IT environment. Our service provides detailed reports and actionable remediation guidance, enabling your team to address the most critical issues first and efficiently manage your security efforts.

8 Cyber Incident Response Team

Our CIRT team stands ready to respond to incidents around the clock. Our incident responders deep dive into investigations and digital forensics with robust tooling and comprehensive experience. Unused CIRT resources can be used for proactive development and refinement of incident response plans, conducting simulation exercises, and providing training, all to ensure your team is prepared for any cybersecurity eventuality.



MAIDAR

SECURE





MAIDAR

SECURE

Peace of mind starts
with taking the first step.
Talk to our team today.

info@maidar.io

maidar.io

