Sectotem MSSP

securing your success

Who are we, what does
MSSP even mean

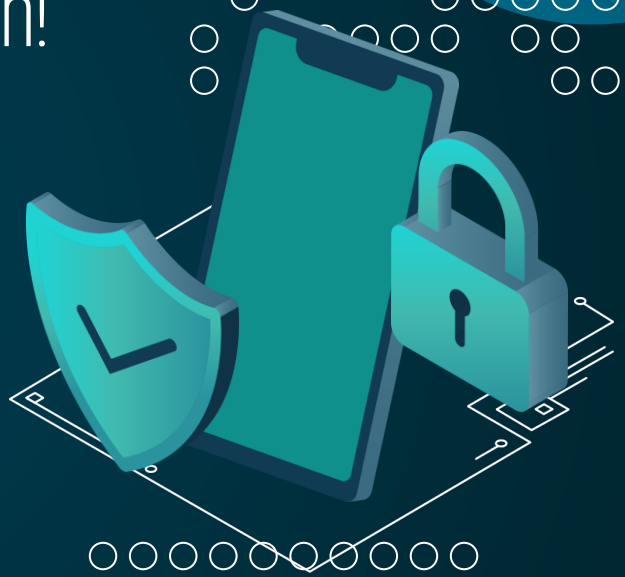
Table of content

01. MSSP ?!

Introduction to what MSSP means and what we do.

Your IT Team's Cyber Defense Extension!

- **We're a Managed Security Service Provider (MSSP)** — your outsourced cybersecurity partner.
  We act as an extension of your existing IT team — or as your entire security team if you don't have one.
- Our services include 24/7 threat monitoring, incident response, vulnerability management, and compliance support — all delivered through a scalable subscription model tailored to your organization's size and risk profile.



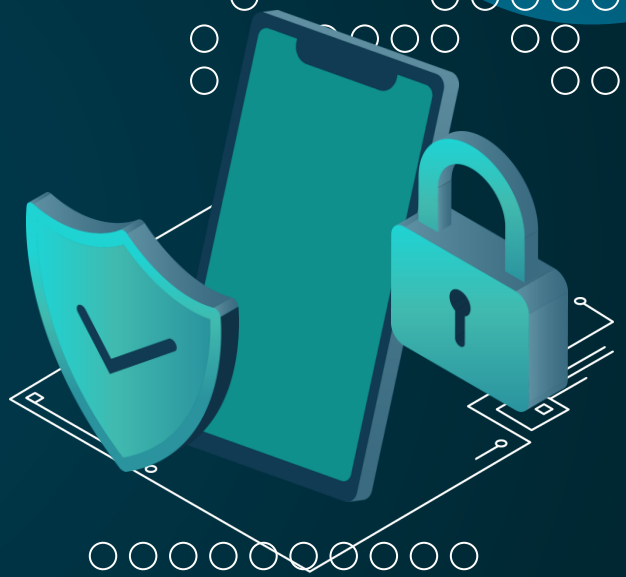
02

Why you need one

Why modern businesses rely on MSSPs to manage threats and ensure compliance

Why you need our services!

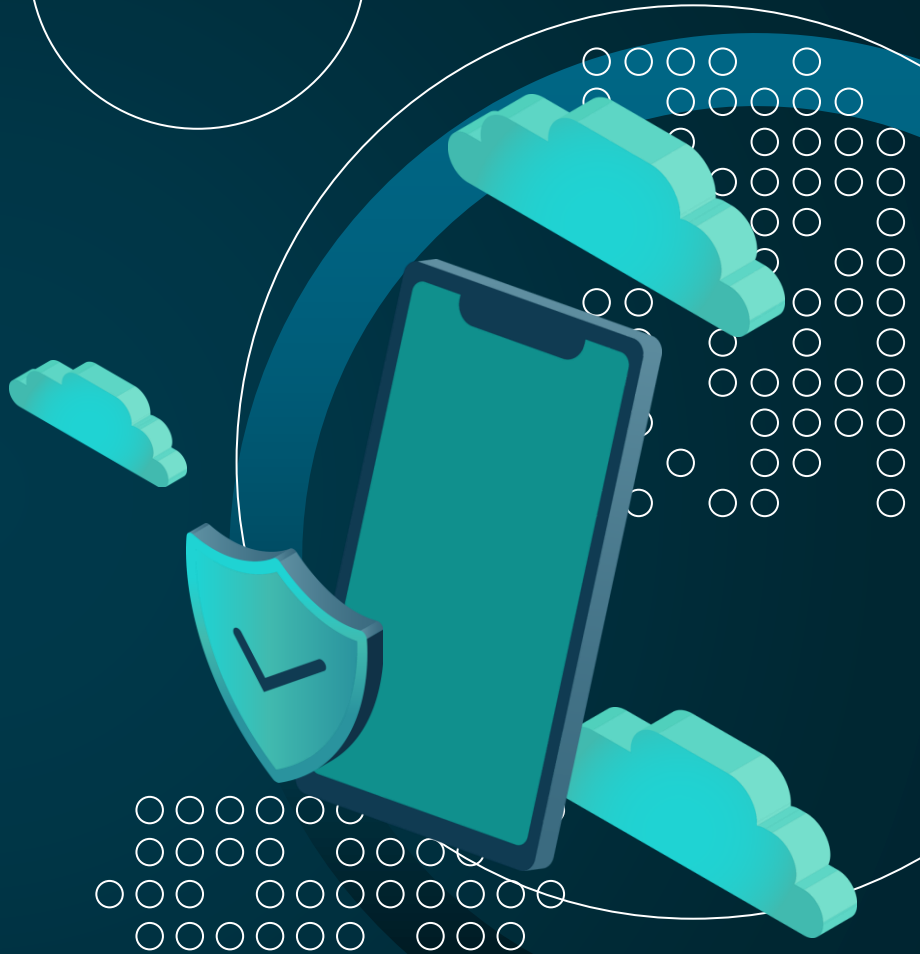
- **Evolving Cyber Threats**: Cyberattacks are becoming more frequent and sophisticated, putting constant pressure on internal IT resources.
- **Compliance & Risk Management**: Meeting security regulations and industry standards is complex and time-consuming without expert guidance.
- **24/7 Expertise & Monitoring**: MSSPs deliver around-the-clock protection, threat detection, and response from trained security professionals.
- **Proactive Defense**: MSSPs help prevent incidents before they happen, reducing downtime and ensuring business continuity.



03

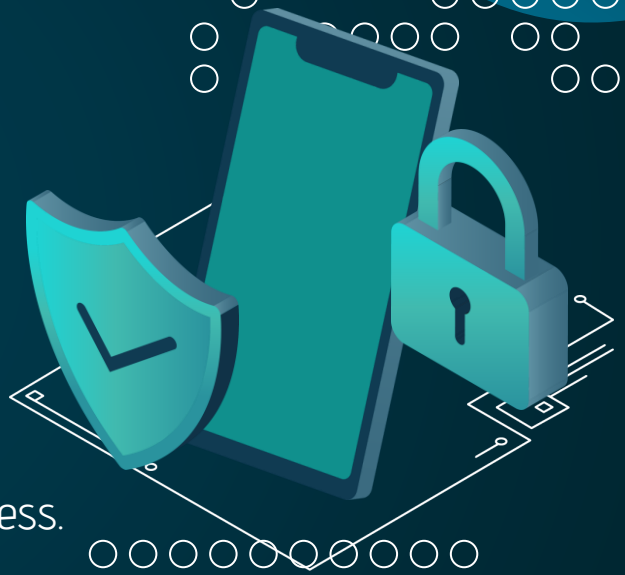
Our services and offers

Overview of our key security services



Everything you need in one package:

- Choose from individual services, tailored bundles, or a comprehensive subscription — and let us manage your security so you can focus on what matters most: your business.



Our Core Capabilities

01 Incident response

02 Security operation center (soc)

03 Threat intelligence

04 Penetration testing & redteam

Security Operations Center (SOC)

- Centralized team of security experts monitoring networks, systems, and endpoints.
- Operates around the clock to identify suspicious activities or breaches.
- Acts as the first line of defense against cyber threats.

Core function:

- **Threat Monitoring**: Continuous surveillance of network traffic, endpoints, and cloud environments.
- **Incident Detection**: Correlate alerts from multiple security tools (SIEM, firewalls, IDS/IPS) .
- **Incident Response**: Contain, eradicate, and recover from cyber incidents.
- **Reporting & Compliance**: Ensure regulatory and policy alignment.

workflow : *Monitoring → Detection → Analysis → Response → Recovery*

Incident Response

- **Immediate Threat Containment**: Rapid identification and isolation of security incidents to prevent further damage or data loss.
- **Root Cause Analysis**: Detailed investigation to understand how the breach occurred and what vulnerabilities were exploited.
- **Coordinated Response**: Expert teams work with your organization to manage communication, recovery, and remediation steps efficiently.
- **Minimized Downtime**: Swift action ensures business continuity and reduces operational impact.
- **Post-Incident Reporting**: Comprehensive reports and lessons learned help strengthen defenses and prevent future incidents.

Threat Intelligence

Overview:

Threat Intelligence involves the continuous collection and analysis of data on current and emerging cyber threats. It transforms raw information into actionable insights that help organizations anticipate and prepare for potential attacks.

How It Works:

- Gathers data from multiple internal and external sources.
- Analyzes threat patterns, indicators of compromise (IOCs), and attacker behavior.
- Feeds insights directly into the Security Operations Center (SOC) and Incident Response (IR) teams to enable proactive defense.

Penetration Testing & Red Teaming

Overview:

Penetration Testing and Red Teaming are proactive security assessments designed to identify vulnerabilities and evaluate real-world attack readiness. Both approaches simulate adversarial tactics to strengthen your organization's defenses before actual threats strike.

How It Works:

Penetration Testing: Controlled, targeted testing to uncover technical weaknesses in applications, networks, or systems.

Red Teaming: A broader simulation of real attacker behavior, testing both technology and human response capabilities.

Provides actionable reports and remediation guidance to enhance resilience.

Key Benefits:

Expose Weak Points: Discover hidden vulnerabilities before attackers do.

Test Response: Evaluate detection and incident handling effectiveness.

Enhance Preparedness: Build a stronger, more adaptive security posture.

NEXT STEP:
contact us

Contact us!

If have any questions or you need trusted professionals for your cybersecurity resilence, contact us:

info@sectotem.com
+216 20 171 019
sectotem.com