SANGFOR CYBER GUARDIAN

Managed Threat Detection & Response

Market Challenges

Today's threat landscape has grown more advanced and more damaging to organizations. Employing the latest security technologies alone is no longer sufficient to prevent attackers from causing havoc. The has shifted the onus onto security operations to play a bigger role in keeping organizations safe. However, establishing effective security operations is not without its challenges.

Challenge #1

24x7 SecOps is expensive and difficult to maintain

Challenge #2

High alert volume leads to alert fatigue and high staff turnover

Challenge #3

Cybersecurity talent difficult to find and retain

Challenge #4

Ineffective / non-existent SecOps processes and procedures

Sangfor Cyber Guardian MTDR

In order to assist the market with addressing these challenges, Sangfor has launched Sangfor Cyber Guardian MTDR, a round-the-clock managed threat detection and response service designed with our customers in mind.

Value Proposition

Sangfor Cyber Guardian Managed Threat Detection and Response (MTDR) Service helps customers improve their security operations efficiency through a threat monitoring, detection, analysis, and response service. Cyber Guardian MTDR leverages the concept of Human-Machine Intelligence to accurately detect threats and effectively eradicate and mitigate those threats.

01 Combine state-of-the-art AI-powered threat detection technologies with the most up-to-date global threat intelligence to detect and identify known and unknown threats.

02 Employ human logic and professional scepticism in threat analysis to provide context-relevant threat notifications and alerts.

Contact Us To Know More marketing@sangfor.com sales@sangfor.com www.sangfor.com

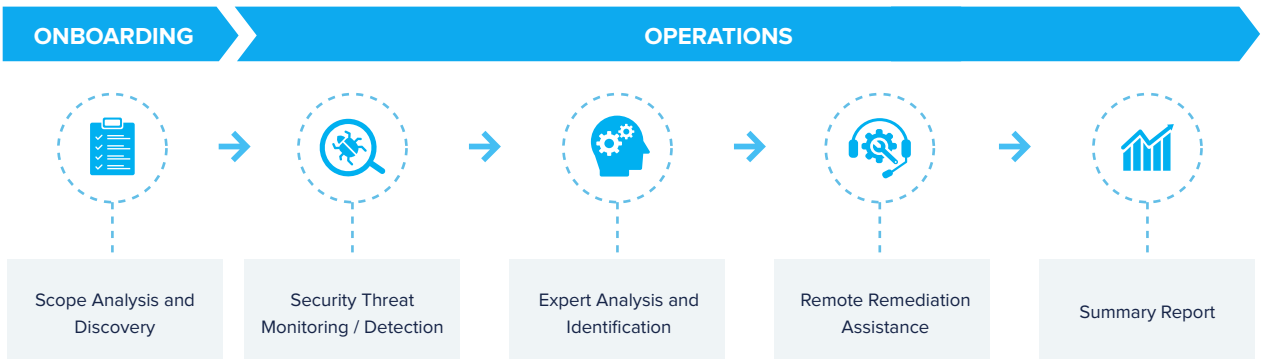
03 Enhance the effectiveness of security operations by leveraging the know-how and expertise of seasoned security professionals to respond to threats.

04 Gain peace of mind with continuous, round-the-clock threat detection and response operations.

Delivering Relevance

This service aims to deliver contextual relevance to our customers, that is, providing accurate and relevant threat notifications and response assistance when credible threats are identified in the customer's environment. This is achieved through our two-stage service process.

- ***Pre-service Onboarding:*** Assessing the environment to understand the context in which the service will be rendered.
- ***Service Operations:*** Continuous threat detection and response operations including the necessary reporting and communications between customers and our SOC team.



Human-Machine Intelligence

Using processes and procedures optimized through years of rich industry experience, Cyber Guardian MTDR takes the best of two worlds and merges them together to deliver a best-in-class threat detection and response service. Our dedicated team of security experts, combined with our leading-edge technology, is solely focused on ensuring our customers are protected against the most sophisticated and stealthiest of threats.

Experienced Security Professionals

- Round-the-clock monitoring, detection and analysis
- Timely and relevant alerting
- Context-relevant advisory and guidance
- Actionable response assistance
- Optimized SecOps processes and procedures
- Proven threat detection and investigation techniques

State-of-the-Art Detection Capabilities

- Cloud-based XDR platform
- Network + endpoint telemetry
- AI-powered detection algorithms
- User and entity behavior analytics
- Global threat intelligence
- Intuitive security platform built and improved to deliver value

Cyber Guardian MTDR Benefits

- Enhance your security operations with round-the-clock monitoring less the technology overheads and hiring difficulties.
- Strengthen your organization's overall security posture and architecture with expert advice and recommendations.
- Leverage the expertise of seasoned professionals to assist your in-house team in defending your organization.
- Establish optimal organizational security policies and processes based on proven effectiveness.

Cyber Guardian MTDR Service Elements

Service	Description
Threat Analysis and Identification	24x7 threat detection, analysis and verification, leveraging AI-enabled detection capabilities and experienced security professionals to accurately identify and analyse threats and provide notifications in a timely manner.
Threat Response and Remediation	Context-relevant threat response assistance rendered remotely by our team of security experts to help customers manage and eradicate detected threats. Covers emergency containment assistance, detection and impact analysis, traceability investigations and hardening recommendations.
Device Management	Regular assessments and reviews of our security technologies to optimize their effectiveness at securing your environment.
Asset Tracking	Initial and regular reviews of in-scope assets to track and identify unauthorized changes and provide valuable context to the service.
Expert Services	A dedicated security professional assigned to every customer to ensure continuity in communications relating to threat notification, response assistance as well as any related advisory or recommendations included in the service. Quarterly threat hunting exercises are also conducted by your dedicated security professional.
Customer Portal	Gain access to a real-time security overview of your environment, including open and closed cases, security view of monitored assets as well as access to regular reports.