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.

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

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

1. 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.
2. Employ human logic and professional scepticism in threat analysis to provide context-relevant threat notifications and alerts.
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.

Using processes and procedures optimized through years of rich industry experience, Cyber Guardian MDR 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.

**Delivering Relevance**

**Human-Machine Intelligence**

Using processes and procedures optimized through years of rich industry experience, Cyber Guardian MDR 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.
## Cyber Guardian MDR 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 MDR Service Elements

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Analysis and Identification</td>
<td>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.</td>
</tr>
<tr>
<td>Threat Response and Remediation</td>
<td>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.</td>
</tr>
<tr>
<td>Device Management</td>
<td>Regular assessments and reviews of our security technologies to optimize their effectiveness at securing your environment.</td>
</tr>
<tr>
<td>Asset Tracking</td>
<td>Initial and regular reviews of in-scope assets to track and identify unauthorized changes and provide valuable context to the service.</td>
</tr>
<tr>
<td>Expert Services</td>
<td>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.</td>
</tr>
<tr>
<td>Customer Portal</td>
<td>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.</td>
</tr>
</tbody>
</table>