solarwinds msp

SolarWinds Threat Monitoring Service Program

Streamline your security operations with SolarWinds® Threat Monitor

Customers expect you to safeguard their businesses from security threats. This means continuous focus on better security services and expansion beyond basic security services. We know implementing a rigid security posture and full-fledged security team can be challenging. With SolarWinds® Threat Monitoring Service Program, getting into managed security services is easier than you think.

Q. What is SolarWinds Threat Monitor?

SolarWinds Threat Monitor is a cloud-based security-information-and-event-management (SIEM) tool designed to help you detect, respond to, and report on threats to your managed networks.

Q. What is the Threat Monitoring Service Program?

The SolarWinds Threat Monitoring Service Program provides services and tools to implement threat intelligence as part of your security offering. SolarWinds facilitates your introduction to a SolarWinds-approved Threat Monitoring Service Provider (TMSP), who will provide you with a support structure to implement and deploy Threat Monitor for your customers—so you don't have to do the heavy lifting yourself.

Q. What are the benefits of using a TMSP?

SolarWinds-approved Threat Monitoring Service Providers have security tools and operations in place to help ensure onboarding and adding new customers to Threat Monitor is simple and scalable. They have in-house, certified security experts in place who know what to look for and do when a threat is identified. In a nutshell, the TMSP will offer you advanced monitoring, analysis, and investigation of threats in your managed networks—giving you the flexibility to manage your customer relationships and win new business.

Q. What are the TMSP's responsibilities?

The TMSP provides a security operations center (SOC), proactive security monitoring, and alerting to ensure you have full visibility of threats and incidents in your managed networks. The TMSP assists with onboarding, including:

- Gathering information about your network, systems, IPs, people, tools, and environments in collaboration with you
- Creating log collector(s), NIDS, and agents
- Setting up the escalation process with your contacts (e.g., your team's contact information and alert-notification order)
- Turning up the log sources, NIDS feed, alert setup, rules and dashboards in Threat Monitor
- Enabling your security operations center (SOC)

Q. What are my responsibilities as the MSP?

You maintain customer relationships and handle all direct communication. To enable the TMSP in assisting you with onboarding, you are responsible for the following:

- Providing the TMSP information on your network, systems, IPs, tools, environments, and contact information of your team, including alert-notification order
- Installing the VMs, span ports, and agents—including configuration of logs and forwarding for log sources, such as firewalls

Q. Who responds when a breach or threat is uncovered?

Your TMSP partner will notify you when a breach or threat is uncovered, so you can provide a response to your end customer.

Q. Will Threat Monitor automatically respond to revealed threats?

Threat Monitor is a threat-detection tool designed to identify and report on potential security breaches. Response and remediation will be handled by you.

Q. How does the reporting work?

Threat Monitor is designed to help you gain a better understanding of your customer's security postures with detailed reports. Reports itemize security-related events and threats identified across your managed networks to give you insights, so you can provide your end customers with visibility over incidents and assist in their efforts related to regulatory and compliance audits.

Q. Will I receive reports regarding my customers' networks from my TMSP?

Yes, your TMSP will provide you with reports. The frequency can be discussed with your TMSP and determined during your introductory meeting(s).

Q. How does alerting work?

Threat Monitor is designed to alert you only to relevant threats, based on user-configured thresholds and rules. Alarm engine rules can be tweaked to make sure only the right alerts are received while minimizing false positives. The TMSP will set up these thresholds and rules and notify you when potential breaches or threats are detected.

Q. What are the costs associated with a TMSP?

Costs for the program are broken down by licensing for Threat Monitor and SOC service fees. Licensing for Threat Monitor is based on the count of log-emitting devices (LED), including a monthly charge per collector needed. Note: Each end customer requires at least one collector, but this also depends on the network configuration, and in some instances, additional collectors may be required. The SOC service fees are paid to the TMSP. Your sales representative will be happy to provide a detailed breakdown of costs.

Q. What is my business opportunity?

Providing proactive security monitoring to safeguard your customer environments opens a new line of revenue for you and gives you competitive advantage. Meeting customer's security requirements and expectations demonstrates brand value and generates opportunity for you to upsell.

Q. What are the first steps I need to take as an MSP?

1. Gain familiarity with SolarWinds Threat Monitor by signing up for an interactive demo
2. Meet with your TMSP
3. Review your customer base and identify opportunities
4. Create a plan in collaboration with your TMSP
5. GO WIN THE BUSINESS!

Q.Where can I learn more about SolarWinds Threat Monitor?

Visit **solarwindsmsp.com/products/threat-monitor** or sign up for a demo at **solarwindsmsp.com/products/threat-monitor/demo?pid=threat_monitor&poi-tm=1**