SECUVANT
Cyber Security | Risk Management

FAQ FOR MSP’s

1. What is SolarWinds Threat Monitor™

   a. SolarWinds Threat Monitor™ empowers companies of all sizes by reducing the complexity and cost of threat detection, response, and reporting. You get an all-in-one security operations center (SOC) that is unified, scalable, and affordable.

2. What is a Threat Managed Service Provider (TMSP)?

   a. The SolarWinds Threat Monitoring Service Program is designed to support MSPs who have purchased Threat Monitor, but prefer to partner with one of the SolarWinds Threat Monitoring Service Providers (TMSPs) to deliver tandem managed security services to their customers with all the advantages of a full-service Security Operations Center.

3. What is a Security Operations Center (SOC)?

   a. A full-service, staffed operation center employing security analysts and technologies such as SIEM, advanced threat detection (NIDS and CIDS), as well as other layered technology services. The people, process, and technology deployed in a SOC enables the provider to detect threats, alert to breach conditions, assist with remediation, and provide log information for forensics purposes.

4. I am an MSP, why not build our own SOC?

   a. The cost and expertise required to stand up a full-service SOC consisting of certified security analysts and engineers, multiple security and operational tools, and the required processes and procedures to run an effective security operation poses a significant barrier to entry for MSP’s. SOC is not synonymous with NOC. Secuvant has done all the heavy lifting and provides to MSPs a mature security operation that can delivery value to an MSP client immediately.

5. How do I Partner with Secuvant?

   a. Select Become a Partner to be contacted by a Secuvant MSP Partner Manager.

6. Does Secuvant Provide Other security Services?

a. In addition to services built around the SolarWinds Threat Monitor™ software, Secuvant also has full Managed Detection and Response capabilities, comprehensive Security Gap and Risk Assessment services, Cyber Risk Program Management services, Penetration Testing and Vulnerability Scanning, Virtual CISO services, and access to teams that deliver full Digital Forensics and Incident Response (IR) services.

7. What are examples of how this service benefits my clients?

a. Increased visibility into threats
b. Leverage investments in current security controls (firewalls, IDS, AV, etc.)
c. Lower costs related to security operations
d. Decreased risks related to insider threat, malicious actors and exploits
e. Compliance to regulatory and legal requirements (PCI, HIPAA, FFIEC, etc.)

8. What are Real-World Scenarios that Help Demonstrate the Value of the Service:

a. Russian hackers took advantage of a client's vulnerable and outdated server. Under the service, Secuvant quickly saw the bad traffic, notified the MSP, advised on solutions, and together they resolved the breach quickly and effectively.
b. Client IT Director clicked on what appeared to be a good DocuSign link. Secuvant immediately saw the link as bad, notified the client, and negated the breach and in partnership with the MSP, preventing the threat from propagating to new users hroughout the organization.

9. Who Manages the Client Relationship?

a. The end-user is the client of the MSP; therefore, the MSP is Secuvant's Client. Secuvant understands the importance of its role to add security value to the MSP in protecting the Client from security threats. Both financial and account relationships are owned by the MSP, supported by Secuvant.

10. How does the licensing work?

a. The MSP procures SolarWinds Threat Monitor SIEM software licenses directly from SolarWinds, and the SOC services directly from Secuvant. The MSP then provides a single service price to the Client at a monthly rate.

11. How much does the client pay for the service?

a. There are multiple service bundles an MSP may offer its Client. Service bundles have been designed to address various needs of a prospective client, from a small 20-person company up to larger organizations consisting of several hundreds of employees.