MSSP FAQ for Technical Sales Splunkers

FAQ for SEs, Architects, Specialist, PS when engaged with an MSSP on an opportunity

V1.0 Last updated: 9/12/18 by Vishal Nakra

Table of Contents

Somebody needs an MSSP…

Does Acme Inc. MSSP run Splunk in their offering?

First find out if they're a Splunk Partner. If they have an account in Salesforce and it designates them as a Partner – Partner Account are clearly marked vs Customer Account – then they have some kind of partnering relationship with Splunk. Note that many MSSPs are also Customers.

Contact the Partner Account Manager (PAM) or Alliance Manager for that MSSP to learn more, since MSSP offerings can be varied, and the same organization often has multiple relationships – they might buy and run Splunk under the MSP program, resell it to the customer under the Reseller program, or just take over running an existing Splunk deployment that the customer purchased themselves, in which case they have no partnering relationship with us at all.

Unwinding all this can take a while. Email msp-sme@splunk.com if you have more questions, but do some basic research in SFDC first. That's where everyone will start.

Customer wants to buy ES **from Splunk** and have an MSSP manage it. Whom can I talk to?

msp-sme@splunk.com is a starting point. Pure run-and-maintain is not a route to market for us, so you will probably end up talking to the Channels team or PS partners as well, whose ecosystem includes providers who may offer solely "run and maintain" services without any "Sell or Included" transaction. Some of the MSP world's ecosystem offers these services as well.

And yes, adoption can lead to future sales, but that's a different discussion. From an organizational standpoint, pure run-and-maintain providers are not usually handled by the MSP team. This is best addressed outside this FAQ.

Customer wants to buy ES **from an MSSP** and have them run it because they {want a single throat to choke | want to move to an OpEx model | have another reason }. Whom can I talk to?

Take a look at the MSP FAQ and MSSP Sales Primer and Sales Guide on the Field Enablement Portal to learn how an MSP transaction would work. Contact msp-sme@splunk.com to feedback on particular MSSPs, or if they want a recommendation.

Customer needs an MSSP to run and maintain their Splunk deployment, but their security team wants to use it too. How does that work?

This is what's called a co-managed SIEM offering. There are various models here. Sometimes the MSSP will do off-hours monitoring. Sometimes tier 1, 2, leaving the rest to the in-house team. Sometimes it's about use cases – the MSSP will deploy a battery of them (the customer can pick) and will triage alerts related to those only. The in-house security team handles the rest, as well as escalation on the things the MSSP is covering. MSSPs are familiar with all of these scenarios and will happily work with you to accommodate the customer.

Customer needs an MSSP to run and maintain their Splunk deployment, but non-security teams want to use it too. How does that work?

This is what's called a co-managed SIEM offering. All MSSPs offer this. The MSSP will handle the security usage, but since the customer owns it, they can use it for other things.

My customer already owns ES, but they have a tiny team and are getting no value. Can MSSPs help?

Yes. This a variant of the above. Since MSSPs focus on security maturity, not just SIEM use case maturity, they can often guide the customer well on this.

I have a large customer who wants to deploy ES globally. Can any of our MSSP partners do this?

Yes, the largest ones can, and they have SOCs globally. Contact msp-sme@splunk.com to talk about recommendations.

Can MSSPs do ES health checks?

Yes. This is common.

Do we have a combined table that ranks MSSPs by skills, #deployments, size of deployments etc.?

Sorry, not yet. It's one of the things we want to do.

My customer is looking at MSSPs-r-us for their MSSP. How good are they?

Contact the alliance manager or PAM for the MSSP. Sadly, there's no Yelp-like review for them yet.

Technical questions about MSSP offerings

How do MSSPs deploy Splunk? Is there a reference architecture?

This document is our reference architecture: Splunk for MSSPs – Technical Architecture

It describes what most people consider an MSSP-type deployment – a Splunk deployment *at the MSSP* that accepts logs and other data from the customer. There is another interpretation of "MSSP" that refers to somebody running and maintaining the customer's own Splunk installation at the customer's own premises. While this is not how Splunk and Gartner define the term, it is very common in the market. Many MSSPs offer both types of service, and there are many others offering only the second. Start with the paper above for these scenarios too, since it speaks their language, helps clarify the service offering by focusing on a particular architecture, sprinkles in differentiators, and addresses things that frequently come up –ES multi-tenancy, data segregation, getting data in, etc. Email msp-sme@splunk.com or Vishal Nakra directly if you need more.

Where do MSSPs deploy Splunk?

Classically, at their own data centers. Today, that normally includes any AWS, Azure or GCP space they have as well.

However, many MSSPs have two arms:

- Classic “run at MSSP” arm (datacenter or cloud).
- “Run at customer” arm, often under a different business unit called “Consulting”. This arm will run Splunk at the customer’s premises (Cloud BYOL or Splunk Cloud). They will also often be Resellers, so will sell, run and maintain.

What kinds of products do they deploy?

Usually Core and ES. SMB-focused MSSPs will sometimes deploy just Core, as will other MSPs who offer non-security managed services.

Many MSSPs are exploring the idea of using UBA. This will not be deployed in a multi-tenant fashion; strictly one UBA installation per-customer as is normal.

Phantom is also under consideration from many MSSPs. They’ve been reaching out to them since before they came on board Splunk and have independent or overlapping relationships in many cases. Contact Rich Hlavka and Don Leatham on the Phantom team to learn more.

Has any MSSP deployed ES in a multi-tenant fashion?

Yes, a few. Those deploying only Core have done it more than those deploying ES. Multi-tenant is very much in the eye of the beholder and means different things to different people, so a variety of flavors exist. As a general rule, we strongly urge them to deploy single ES instances per customer, but they have occasionally done truly multi-tenant deployments. See the Splunk for MSSPs – Technical Architecture whitepaper for the guidance we offer MSSPs. This is also useful if you came here looking for guidance on building an internal MSSP within your government, university or corporate customer.
Splunk for MSSPs – Technical Architecture

What does an MSSP’s Splunk setup look like?

Usually single ES instance per customer. MSSPs who focus on the SMB market will sometimes deploy only Core, and a single Core deployment in that case will service many customers. See link in previous question for the guidance we offer them.

Can MSSPs deploy in Splunk Cloud?

Yes, but the customer will have to purchase the Splunk Cloud license. The MSSP can run it afterwards just as a normal customer would (no special access to Cloud). They will have to be authorized by the customer to access the Cloud instance and to access Support, which means they'll need to be Authorized Contacts on the entitlement.

The MSSP cannot purchase Splunk Cloud directly, since Splunk Cloud is not included in the MSP Program. Under the MSP program, the MSSP buys the Splunk license and services a single, named customer using it. All Splunk software products can be deployed this way, but not Splunk Cloud, which is a service. However, there is work under way to make this possible. Contact the Global Strategic Alliances (GSA) team at gsasales@splunk.com for more. Also see the MSP FAQ for more on this.

How about AWS?

Yes. Many of their customers are asking about this, so they've been building capabilities. We don't have a good list of them, but we can ask.

How about Azure?

Yes. It's also picking up traction. We don't have a good list of them, but we can ask.

How about GCP?

Possibly. This doesn't come up that often, but I'm sure Google's sales team is hard at work convincing them.

So MSSPs don't have many Splunk instances, all sitting in Splunk Cloud and acting as one "combined Splunk" for all their customers?

That's correct. They don't have the ability to deploy multiple customers within a single Splunk Cloud instance. They manage each customer individually.

Do MSSPs get command-line access to Splunk Cloud?

No. The restrictions on command line access for SOC II compliance reasons remain in place.

I heard there were some MSSPs who got command line access to Splunk Cloud
This is a common misconception out there. MSPs do not get command-line access to Splunk Cloud. It is possible that PS subcontractors with a splunk.com email address and VPN access get PS-level access before production as our PS team does, but that disappears once it goes to production. The companies these PS subcontractors work for sometimes have some flavor of managed security services as well, so this detail tends to get lost and circulated as "ACME MSSP has command-line access". The short story is that MSPs do not get access to Splunk Cloud.

Do MSSPs have full access to Splunk Cloud as we do for a Cloud POC?

No.

Can we set up a Cloud POC environment for an MSSP who wants to run a POC ?

Yes. Follow the normal process for setting up a Cloud POC. Make sure to let the cloud team provisioning the POC environment know that external parties may be using the creds you receive, or have them generate separate credentials.

Does So-and-so MSSP have a preference on on-prem vs Cloud?

Generally speaking, MSSPs are open to both, and like the Splunk Cloud option for the fast time to value. (Though they don't like the lack of full access to the CLI).

Contact the Partner Account Manager (PAM) or Alliance Manager for that MSSP to learn more about any particular MSSP.

Tell me more about what MSSPs can and can't do with Splunk Cloud.

Take a look at this document on Pwny Portal. It was published with MSPs, PS partners and Resellers in mind.
https://splunk--simpplr.na57.visual.force.com/apex/sitepagesdetail?contentId=aCU0b000000TN31GAG&siteId=aCa33000000GmiKCAS

What does so-and-so MSSP use Splunk for?

There's no central repository of quick "About me" information on MSSPs – yet. Contact the Alliance Manager or PAM to learn more.

How does my customer send data from their on-prem Splunk environment to the MSSP?

Can customers log into the MSSP's environment and look at their data?

It depends on the MSSP's service offering. We usually allow them to do that. The decision is up to them, save in rare cases where Splunk prohibits it. Email msp-sme@splunk.com to get a firm answer.

Can the MSSP handle all these use cases/data sources/requirements the customer has?

Best to have a conversation with them. Email msp-sme@splunk.com to start this process.

What kinds of data sources do MSSPs usually pull in?

Network-based (firewall, proxy, WAF, IDS/IPS, sandboxes, flow data) would be a good start. We are generalizing out of necessity here since there are so many MSSPs. Authentication logs of all kinds. Windows Security Events are common.

It's rare for them to pull in asset/identity data, but this may be changing. Advanced Windows endpoint data like Sysmon is something they're all interested in. They also have relationships with EDR vendors so are also thinking about Carbon Black etc. Since the actual use cases they deploy are considered proprietary, it is difficult for us to know a lot about this.

Vulnerability data is also commonly used by MSSPs, but perhaps not in the way you expect. They have a range of forward-looking assessment services, including vulnerability management, penetration testing, red-teaming, and sometimes purple-teaming. These services are usually run out of a different group. Some of them are using Splunk. The MSSP (SOC) side may also be using vulnerability data for context, but again, this is difficult for us to tell.

Cloud data sources are becoming increasingly common. AWS, Azure and O365 come up most often.

Technical Sales Process

Do MSSPs do POCs?

Sometimes, for their own services. They may include a Splunk piece in that, but this decision is usually transparent to us at Splunk.

Who does the POC?

They do it themselves if needed. Support from Splunk is rarely needed, and our own POC process is not followed. They may come to us for advice, however. It is important to keep in mind that the team selling the service (AE, Solution Architect) is often different from the one running the actual MSSP service. The running side will be called in to do a POC, and you may not be engaged with them. If a POC is required, be sure to ask who is involved on their end, and sync up with your colleagues on the GSA team to work out a plan to support unusual circumstances as you learn about them.

How about demos?

This depends on the type of MSSP they are. Most MSSPs are demoing their service offering so will not just demo Splunk in the way we do. However, there are many types of MSSP, and those that are primarily reselling Splunk, not a shared managed security service, will often demo just

Splunk. When co-selling with an MSSP, they will sometimes ask the Splunk team to step in and demo Splunk to the customer.

How about workshops?

The MSSPs who are primarily Resellers may be trained to run workshops. Contact the “Partner SE” team that handles these relationships – pse@splunk.com to see if that’s the case. This is because they are often selling a piece or bundle of technology, so their sales motion is more similar to ours. The ones we consider classic MSSPs sell not a bundle of technology with additional services on top, but a service that happens to include various pieces of tech behind the scenes. Might want to re-read that. The latter are the ones doing MSP transactions, and they do not run any workshops.

Do they have access to our sales plays?

If they’re in the Partner Portal, yes. However, see next question.

Do they follow our sales plays, like SIEM replacements?

No. They are selling a service, of which Splunk is only a part, so their plays are different. It really depends on how you define MSSP though. If they’re more of a VAR or SI, maybe. See the MSP FAQ for more on this difference.

Who does the PS on an MSSP engagement? How would I “hand off” as an SE to them?

The MSSPs will usually handle it themselves. For the at-MSSP offering, they may subcontract to Splunk PS for complicated deployments or reach out to Support. Ditto for at-customer deployments. Their use of Splunk PS tends to be higher when they are still ramping up, and peters out eventually. There are plenty of places where they’d do better to use Splunk PS, but for many reasons it doesn’t work out that way.

The handoff process will be informal, depending on how involved you are with the sales cycle. Often, if will only be ad-hoc involvement.

How does Support work with an MSSP in play?

We urge them to get Premium Support to reduce the lag on responses. Since they own the Splunk license, they are the ones named on the entitlement and will open tickets themselves. They manage their tickets on splunk.com like normal customers.

See this doc: intended for MSSPs: How to work with Splunk Support
And this one, only for you (do not share with MSSPs) – How to work with Splunk Support – addendum for Splunkers

Okay, can you walk through a typical sales cycle with an MSSP – where do Splunk SEs/Architects/Specialists fit in?

The process starts when either the MSSP comes to us with a lead, or we reach out to them in response to an internal inquiry about a customer who's requesting help from an MSSP. The first thing is to get the two companies' alliance teams in the loop. They represent the companies overall. The Splunk Alliance manager/PAM for the MSSP in question will work with their counterparts connect the two account teams – the MSSP's and Splunk's.

This will be a co-selling engagement, with the MSSP carrying the majority of the load. They'll position the service and Splunk's place in it, and we'll speak to specifics technical strengths of Splunk if needed. Think of our technical sales team as an escalation point. You mightneed to demo Splunk, but you'll usually be answering questions from the MSSP and/or customer about data types the customer needs to ingest, and how much that works out to in GB/day. Data flow comes up when the customer already has Splunk. Things like deployment location, HA/DR etc. are relatively standardized at the MSSP. MSSPs will sometimes handle data volume sizing, but it may fall to you. The Splunk rep for the customer will need to generate a quote for the MSSP's sales team and help them with negotiations around that. More on the Account Manager's role can be found in the MSP FAQ.

The MSSP's account team will include an Account Manager, a Solution Architect (like an SE), sales overlays for the particular managed service being sold, and technical resources from the team that runs the managed security service. Their internal team will be their primary technical sales team, and the Splunk account team will be an escalation point.

The Splunkers on the Splunk alliance team for the MSSP (Account Manager, SE) for the MSSP will overlay over all of this, and will participate in many of the joint meetings you have with the MSSP's sales team. So will their counterparts from the MSSP's own alliances team. The Splunk alliance team is the your internal source of expertise on the MSSP's offerings and how they do business. They will also smooth over differences, serve as glue to make sure the sales process goes smoother, and support the account team in the deal. The alliance SE (from the GSA team) will be an overlay to the field SE, helping drive the deal where needed. Since the alliance SE team is small, it cannot be the primary driver of every deal with every MSSP, but it is very incented to close the deal with you. The field SE's normal escalation path remains in place – teammates, management, SME, Specialist, etc. The alliance SE is added to this mix to help with specific technical asks, cover when the field SE cannot, educate the MSSP partner where needed, and generally make sure the co-selling process works smoothly at the technical level and results in a technical win for Splunk.

Competing with MSSPs

What are some ways to co-exist with an MSSP?

Take a look at the last section of the Use Cases and Positioning document.

James Hanlon from the EMEA security specialists team also put together a deck for the EMEA field that covers most of what we would want to say about this scenario. It leaves out the Managed SIEM and Co-managed SIEM scenarios, and will be enhanced to cover all this by the GSA team in the future.
https://drive.google.com/file/d/1MMJXtxaHjSkQMpD4BGLJgN1KINZvswrt/view?usp=sharing

How do I compete against an MSSP?

First, go read the MSSP Primer and Sales Guide, which talks about this a lot. There are some additional musings in the Use Cases and Positioning Guide that we use when engaging with MSSPs on building their services using Splunk. If you have more questions, email msp-sme@splunk.com, competition@splunk.com or check out http://competitive-answers.splunk.com

Do I care that the MSSP that I am competing with is using Splunk or not?

Oh yes. If they're running Splunk, they will in the vast majority of cases be purchasing a Splunk license to service your customer, which means that your account team and you will be credited for that. MSSPs running Splunk will actually co-sell with you on this opportunity, and of course will be versed in what Splunk is, which means their own messaging will be consistent with yours, enhancing the value of the technology we bring rather than denigrating it in favor of people and process. All of this assumes that they're picking one or both as the source of the Splunk license they will be making use of (note not "purchase" – when an MSSP purchases it, they own it, not the customer). It is entirey possible that the MSSP chooses to contract with Splunk and the MSSP independently – product from us, services from them.

The short story is that MSSPs running Splunk are a friend, not a foe. If they're not running Splunk, the gloves are off. See question on co-existing with Splunk for more ammo.

How do I know if a MSSP I am competing with will manage customers Splunk or will insist on using their own tools?

No short answer. There's no table of capabilities anywhere, though we recognize the need for this. Reach out to msp-sme@splunk.com to know more about particular MSSPs.

What is the difference between a MSSP and MDR?

See the Use Cases and Positioning document.

How do I compete against an MDR?

This is a relatively new area, so there are no proven practices on this yet. In short, answer their people/process expertise with a Splunk-powered MSSP, and counter their big data platform (sometimes ELK) with Splunk.

First, understand that MDRs are not more comprehensive than MSSPs. If you strictly limit security to be proactive advanced threat hunting, ideally using endpoint data (which MSSPs typically don't get) and are ok living without SLAs, then yes, you could say that MDRs have more extensive capabilities in this one area. MDRs do no usually offer SLAs at all. Their "greater"capabilities are also driven by their focus – this is all they do. MSSPs, on the other hand, work with many vendors (not just their own technologies like the MDR guys) and have many service offerings, so even their larger resources are diluted. If you look at security more holistically, however, the MSSPs, GOSIs and consulting offerings would be more comprehensive, particularly if you include their consulting offerings that go beyond the cookie-cutter. They cover the whole spectrum of security.

Second, be wary of positioning MDR offerings as immature. They've been around for a while and the capability is part of the standard pitch any large outsourcer offers today. A sales rep from an MSSP partner who isn't aware of your previous de-positioning of MDRs would end up undermining what you said previously when they touted their own MDR capabilities.

Third, your best course may be to partner with a Splunk-based MSSP on this. Don't worry if they're an MSSP and not an MDR – they all have MDR offerings and are well-versed on this. Let's take a deeper look at this from an MDR point of view.

Looking specifically at the MDRs' extended capabilities, they're in four main areas:

- **Additional data sources, primarily endpoint.** MSSPs don't traditionally use this; this is true. They focus more on ingress/egress points. But a big reason is the lack of organizational access to sensitive data.
    - If the MDR uses this and the customer is willing to give this to them, they should be willing to give it to a Splunk-based MSSP who demonstrates that they can use it effectively. Our larger MSSP/SI partners come into this boat. MDR-style services are more similar to big MSSPs' custom on-prem offering, not their a shared, cookie-cutter services run out of their own premises, which are necessarily standardized and stripped down to achieve scale. All of our partners do these custom engagements, so they can certainly offer an MDR service to the customer as well.
    - If the MDR does NOT use this, they lack one of the main pillars of MDR services.

- **Big data platforms to look at large amounts of data or unusual sources like custom apps.** Some MDRs are using ELK. Others probably are too. They inherit all of ELK's weaknesses and cost structure, so leverage the ELK competitive information here. They may choose to make it more about the people and process, but if they are a pure-play MDR, not a vendor-led MDR (like Rapid7 for example), they not be very large organizations, and will have fewer resources to handle the drain that ELK will put on them. An MSSP running Splunk, on the other hand has a stronger big data platform behind their "MDR service", a different cost structure, and can afford to be a security expert rather than an ELK expert. Work with them to position these strengths.

- **Machine Learning**. MSSPs running Splunk probably have more extensive capabilities here. All major MSSPs are experimenting with ML in some way. This is not an easy one to comment on, but remember that ML requires skills. And "machine learning" could mean anything, as we well know from our UBA travails.

- **Access to the organization**. "Work closely in the trenches with you" etc. Key for any outsourced security offering to truly be valuable, and a key part of an MDR's value prop. "We don't just give you a dashboard, but work closely with you to fix the problem". Again, if they're willing to give the MDR access (particularly with no SLAs), they should be willing to give it to a custom engagement from a Splunk-powered MSSP.

In short, you could position one of our MSSP partners as well. They're all well aware of MDR offerings in the market, have included "MDR offerings" in their own positioning, and the more custom you go, the more they can actually provide it. The more custom offerings are more expensive, but that's for them to try and match.

Specific examples of MDRs in the market:

- Arctic Wolf Networks – Does not use Splunk.
- Alert Logic – Does not use Splunk.
- Cisco – Does not use Splunk. At the corporate level, of course, it's complicated ☺
- CrowdStrike – OEMs Splunk.
- eSentire – Does not use Splunk. But is interested.
- FireEye – Does not use Splunk, and competes.
- Mnemonic – Uses Splunk, but not as the core of their MSSP service.
- Morphick – Does not use Splunk, but was just acquired by Booz-Allen Hamilton, a major partner, so we'll see.
- Netswitch – Does not use Splunk.
- Rapid7 – Does not use Splunk, and competes.
- Raytheon Foreground Security – Use their own product and Splunk. We're quite engaged with them.
- Rook Security – Does not use Splunk.

Are there competing vendors that will sell products, and all be MSSPs at the same time?

The only one who really fits that bill is IBM. They are a full-fledged, Magic Quadrant-leading MSSP and SIEM vendor.

Vendors with services

There are plenty of competing vendors who are also MDRs, however, and offer services centered around their products. (Remember that MDR services are a subset of classic MSSP ones). The vendors led to the rise of MDR services to begin with, by offering services to help customers get value out of their products. Rapid7 and FireEye are MDRs. Securonix offers managed services for its products. another. Carbon Black and Crowdstrike also have MDR services, but they are not Splunk competitors, just examples of vendor-led MDR services.

All these services may be available to the customer via various channels, as MSSPs and MDRs do have channel partners who resell their services, so you may have to dig a couple layers deep to find out if you're up against a particular vendor competitor.

Services who become vendors

Sometimes, MSSPs will sell their homegrown platforms to the customer. These are often in cases where they have no on-premise delivery capability. These situations are not common and are the reason no MSSP-created SIEMs appear in the Gartner Magic Quadrant. If it does happen, the product becomes a much bigger part of the conversation, so counter as you would any other product.

Which MSSPs focus on SMB and which ones are more up-market?

The Gartner Magic Quadrant is a decent to this one, though it doesn't list anywhere near the universe of MSSPs out there. There is no general list within Splunk about this, so we suggest starting from the opposite end – asking msp-sme@splunk.com if a particular MSSP is SMB-focused or not.

Misc.

Can MSSPs get into Oxygen?

Yes, if they're Splunk Accredited Sales Engineers or Consultants. Simply being part of a Partner does not get them this privilege.

Can they read our SE or SME email lists?

No.

Slack?

No.

Competitive-answers?

No.

Confluence?

No.

JIRA?

Nope.

Field enablement portal?

Not all of it. They get a limited subset of the field enablement content in the Splunk Partner Portal.

Do MSSPs know about the PS splservices use case wiki? They're asking me a question that's answered there.

Many do. They're all entitled to access it provided they have a valid partner relationship with Splunk. Many MSSPs just run and maintain the customer's Splunk installation and do not buy, sell, or act as PS subcontractors for Splunk. These MSSPs are not Splunk Partners and will not have access to splservices. You can find out if they are indeed a partner from SFDC.

I think this MSSP needs some training. How would that work?

The account team handling the relationship with the MSSP can help them craft a plan for this. To find out who handles them, email msp-sme@splunk.com.

If you are handling the relationship with the MSSP yourself, send them this Excel sheet – it's a good starting point for discussions by laying out roles and responsibilities in the SOC, the recommended training for each, and how much it costs. MSSP Partner Training Recommendations

MSSPs have a mix of people with varying Splunk experience and are always looking for more, so some tailoring will likely be needed.

I'm talking to an MSSP who's asking about what training we recommend, how long it takes etc. Do we have a plan for them?

Sure do. See previous question.

I know an MSSP who would like to partner with us. Can you help?

Please ask them to apply for the MSP Program. Splunk is standardizing its process for recruiting MSSPs, so they must go through the process and qualify.

https://www.splunk.com/en_us/partners/become-a-partner/managed-service-provider-program.html

I have feedback on my last deal with an MSSP. Whom can I share this with privately?

Frank feedback is always welcome! Good or bad. The account team managing the relationship with the MSSP. Reach out to partner-se@splunk.com or Vishal Nakra directly.

What is Splunk doing with MSSPs in general?

Check out the Primer, the FAQ, and email msp-sme@splunk.com

References

The Field Enablement Page on MSPs is the best place to start for all MSP or MSSP questions. This doc should be there too.
https://fieldenablement.splunk.com/p/1/mssp/1_70381

[1] MSSP Primer and Sales Guide – On the Field Enablement portal here
[2] MSP FAQ – On the Field Enablement porta here
[3] Splunk for MSSPs – Use cases and Positioning – on Google Drive here
[4] Splunk for MSSPs – Technical Architecture – on splunk.com here

More resources can be found on Google Drive in a folder called MSSP Enablement Materials:
https://drive.google.com/open?id=1UVsK2qt-UHSXproZqF_R7VguyMb8uhWQ