Getting help with ES

Training

Splunk offers a number of EDU training courses to help you get up to speed on how to make the most of your deployment. Completion of these courses to some effect is an essential building block to success. If you’d like to explore education options here, please get in touch with us via this contact form or get in touch with your account manager.

- Using Splunk Enterprise Security
- Administering Splunk Enterprise Security

Technical help - OnDemand Services

Engage our experts directly to help clarify our documentation or enablement, get answers to technical questions, or to get started quickly. Most customers have OnDemand Services included as a part of their license purchase. Getting help is easy! Follow these instructions from the OnDemand Services Portal End User Guide:

1. Open a request under the product Enterprise Security (ES)/UBA.
2. Select the task Ask a Security Expert.
3. Wait for the consultant to reach out to you directly to help.

If you cannot open a case, reach out to OnDemand@splunk.com and they can look into the issue for you.

<table>
<thead>
<tr>
<th>Plan</th>
<th>Implement</th>
<th>Use/Adopt</th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use Case Advisory Discussion</td>
<td>• Splunk Enterprise Security Use Case Implementation Guidance</td>
<td>• Getting Started with Security Cloud Suite or Splunk Security Analytics for AWS (SSA4AWS)</td>
<td>• Enterprise Security/UBA Technical Assessment</td>
</tr>
<tr>
<td>• Architecture Diagram Creation</td>
<td>• Post Implementation Review</td>
<td>• Data Model Review</td>
<td>• Upgrade Readiness Assessment</td>
</tr>
<tr>
<td>• Data Readiness</td>
<td></td>
<td>• Asset Identification</td>
<td>• Scaling Advisement &amp; Expansion Readiness Assessment</td>
</tr>
<tr>
<td>• Security Maturity Guidance</td>
<td></td>
<td>• Data Source Review</td>
<td>• Security Integrations Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Index and Retention Review</td>
<td>• Report or Dashboard Optimization</td>
</tr>
</tbody>
</table>
**Project-based services**

Project-Based Services are much more involved, typically larger-scale services engagements compared to ODS. With these, you will work with a Splunk Engagement Manager to determine and finalize the scope of the project. Once everything is signed off, we will work with you in lockstep to deliver on the agreed-upon project. If you'd like to explore options here, please get in touch with us via this [contact form](#) or get in touch with your account manager.

**Support**

Even the most savvy customer will need a little help. Whether it’s error messages, unexplained or unexpected behaviors, or incidents and outages, Technical Support is the first line of defense for all of your post-sales issues. Splunk Support Engineers will partner with you to ensure your environment is optimized to drive your journey with a focus on long-term technical health, so you can realize your ROI as soon as possible.

To review what is included with the Standard and Premium support programs, click [here](#).

The Support Portal can be accessed from the [Splunk.com home page](#) for logged in users, or from the Splunk product application user interface. Bring up the navigation menu, scroll to the bottom of the side-bar, select **Help & Support**, and then select **Support and Community**. From there you will be able to open a support case.

**Splunk Enterprise Security Tech Talks**

- What’s new in Splunk Enterprise Security 6.6
- Best practices for maturing Your SOC (part 1 of 4)
- Detecting Trickbot with Splunk
- Hunting for malicious PowerShell using script block logging
- Protecting against crypto-jacking malware with strong DevSecOps practices and Splunk

**Splunk Enterprise Security Documentation**

- [Enterprise Security](#)

**Other Splunk Enterprise Security Content and Useful Links**

- Security Maturity Model (S2M2) & Prescriptive value path
- [Threat Research Team home page](#) (STRT)
- [Introduction to Splunk Enterprise Security Content Updates](#)
• Security blog
• Introduction to Boss of the SOC (BOTS)
• Boss of the SOC
• Splunk Intelligence Management (TruSTAR) + Splunk ES Demo