

## Enhancing Cisco Security Solutions with Splunk (CPLL-ECSS)

Duration: 180 Days

The Enhancing Cisco Security Solutions with Splunk (ECSS) Learning Path covers intermediate-level knowledge of Splunk, including its fundamentals, key components, and architecture so you can detect, investigate, and respond to security threats effectively. You'll learn to utilize various Splunk components, including Splunk Enterprise, Splunk SIEM, and Splunk SOAR. You'll also discover how to use and troubleshoot the Cisco Security Cloud App, Cisco Legacy Apps, and technology add-ons (TAs) for integrating Cisco security solutions with Splunk for enhancing user, cloud, and breach protections.

### Skills You'll Learn:

- Learn how to utilize Splunk to detect, investigate, and respond to security threats effectively
- Explore key components of Splunk, including Splunk Enterprise, Splunk SIEM, and Splunk SOAR
- Discover how to use the Cisco Security Cloud App, Cisco Legacy Apps, and TAs for Splunk integration

### Learning Path Objectives:

1. Basics of Observability: Outline the value, functionalities, and key components (forwarder, indexer, search head, Splunk Search Processing Language (SPL), Apps and Add-Ons, Dashboards and Reports) of Splunk Enterprise and Splunk Cloud.
2. Splunk Enterprise, Splunk SIEM, Splunk SOAR: Explain the use of XDR, SIEM, and SOAR as part of the modern SOC architecture to enhance the SOC's ability to detect, investigate, and respond to security threats effectively. Describe the functionality and use case of Splunk Enterprise, Splunk SIEM, and Splunk SOAR.
3. Cisco Security Cloud App: Implement Cisco security solutions to Splunk integration using the Cisco Security Cloud App.
4. Cisco Security Legacy Apps and Technology Add-Ons: Implement Cisco Security Solutions to Splunk Integration using Cisco Legacy Apps and TAs.
5. Cisco Security with Splunk Use Cases: Demonstrate the value of integrating Cisco security solutions with Splunk for enhancing user, cloud, and breach protections.
6. Cisco Apps Troubleshooting and Tuning: Troubleshoot the Cisco Security Cloud App and the Cisco Legacy Apps and TAs.