Getting data into UBA

Learn how to add various data types to UBA and validate ingestion.

Introduction

- Understand data flow in Splunk UBA
- How data gets from the Splunk platform to Splunk UBA
- Use connectors to add data from the Splunk platform to Splunk UBA
- Which data sources do I need?
- Add Windows events to Splunk UBA

Prepare to add data to Splunk User Behavior Analytics

- Get data into Splunk UBA
- Add file-based data sources to Splunk UBA
- Add data sources to Splunk UBA in test mode
- Filter events analyzed by Splunk UBA for anomalies

Add HR data to Splunk User Behavior Analytics

- Why Splunk UBA requires HR data
- Get HR data into Splunk UBA
- Add custom attributes to your HR data
- Validate HR data configuration before adding other data sources
- Make changes to your HR data

Add assets data and identify assets to exclude from detections

- Identify assets in your environment
- Exclude identity resolution for devices or users
- Use allow and deny lists to generate or suppress anomalies
Add data from the Splunk platform to Splunk User Behavior Analytics

- Add CIM-compliant data from the Splunk platform to Splunk UBA
- Add raw events from the Splunk platform to Splunk UBA
- Add custom data to Splunk UBA using the generic data source
- Send data from the Splunk platform directly to Kafka
- Splunk UBA category to Splunk CIM field mapping reference
- Send notable events from Splunk Enterprise Security to Splunk UBA

Add other data to Splunk User Behavior Analytics

- Configure PowerShell logging to see PowerShell anomalies in Splunk UBA
- Configure the VirusTotal script to see VirusTotal anomalies in Splunk UBA

Review and verify your Splunk User Behavior Analytics data

- Verify that you successfully added the data source
- Monitor the quality of data sent from the Splunk platform
- Review and edit existing data sources in Splunk UBA
- Validate data availability