# FortiSIEM Parser

***In this course, you will learn how to create custom parsers to extend the integration capability of FortiSIEM to a wider range of devices and custom applications. You will learn how parsers recognize the type of device or application that sent the data, extract and save key information from the log, and map the device type and log information to an event type.***

## Product Version

- FortiSIEM 6.3

## Course Duration

- Lecture time (estimated): 4 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 10 hours/2 days

## Who Should Attend

Cybersecurity professionals responsible for creating custom parsers on FortiSIEM should attend this course.

## Certification

There is no certification for this course at this time.

## Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- *NSE 4 FortiGate Security*
- *NSE 4 FortiGate Infrastructure*
- *NSE 5 FortiSIEM*

It is also recommended that you have knowledge of programming languages and regular expressions.

## Agenda

1. Introduction
2. Regular Expressions
3. Event Format Recognizers
4. Parsing Instructions
5. Switch-Case Constructs
6. Custom CMDB Event Types
7. Choose-When Constructs
8. Key Value Pair Logs
9. Value List Logs
10. Advanced Features

## Objectives

After completing this course, you will be able to do the following:

- Examine how FortiSIEM determines which parsers to use
- Review parser terminology and steps to create a parser
- Identify different log types and structures
- Review basic and advanced regex patterns
- Use tools for regex validation and development
- Identify appropriate uses of global and local patterns
- Define local and global patterns
- Identify common string patterns in event logs
- Create event format recognizers
- Configure parsing instructions to extract and map data
- Build `collectFieldsByRegex` functions
- Build `setEventAttribute` functions
- Add comments to parser code
- Build conditional matching logic capabilities in parsers
- Parse and normalize date and time from logs
- Add, categorize, and query the CMDB for new parser events
- Create parsers for various log types
- Manipulate extracted strings from logs
- Perform calculations on variables or attributes
- Calculate event severity with syslog priority values
- Use advanced functions to parse JSON logs
- Enable FortiSIEM support for logs in other languages

## Delivery Options and SKUs

**Instructor-Led Training**

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Contact your Fortinet Resellers or Authorized Training Partners to purchase this course.

**Self-Paced Training**

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using a purchase order (PO) through Fortinet Resellers or Authorized Training Partners.

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

For training and lab SKUs, or additional purchasing information, refer to Purchasing Process.

## (ISC)$^2$

- CPE training hours: 4
- CPE lab hours: 6
- CISSP domains: Security Operations

## Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.