FortiSIEM Parser

In this two-day course, you will learn how to create custom parsers to extend FortiSIEM's scope to as-yet unknown devices and custom applications whose log formats would not otherwise be understood by FortiSIEM.

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 5.2

Formats

- Instructor-led classroom
- Instructor-led online
- Self-paced online

Agenda

1. Introduction
2. Regular Expressions
3. Parser Recognizers
4. Collect Fields by RegEx
5. Switch Construct
6. Adding Events to the CMDB
7. Choose Construct
8. Handling Key Value Pair Logs
9. Handling Value List Logs
10. Advanced Features

Objectives

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

- Describe the steps to create a parser
- Create simple regular expressions
- Use local and global patterns
- Identify what information to extract from the log
- Recognize different log formats
- Extract data and map it to variables and attributes
- Understand pattern matching
- Understand the switch construct
- Understand the choose construct
- Add events to CMDB
- Understand key value pairs
- Work with sets of key value pairs
- Handle value list logs
- Understand parser order
- Clone a system parser
- Add different languages

Who Should Attend

Anyone who is responsible for day-to-day management of FortiSIEM.

Prerequisites

A basic understanding of programming languages and regular expressions would be an asset. It is also recommended that you have an understanding of the topics covered in NSE 5 FortiSIEM, or have equivalent experience.

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
  - HTML5 support
  - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled in your web browser

You should use a wired Ethernet connection, *not* a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Certification

There is no certification for this course at this time.