McAfee Enterprise Security Manager (SIEM) Learning Path

Frequently Asked Questions

Q: What has changed in the course offerings?

A: We recently replaced SIEM 101 and 201 courses with role-based courses, introducing Analyst and Engineer tracks. The new courses continue to provide a comprehensive overview of McAfee® Enterprise Security Manager—our security information and event management (SIEM) solution—through multiday courses with hands-on labs.

Q: What is the difference between an Engineer and an Analyst?

A: While the functions of an Engineer and Analyst will look different at each organization, for the purposes of the Enterprise Security Manager courses, an Engineer is responsible for configuring the Enterprise Security Manager and an Analyst is responsible for analyzing events and identifying incidents.

Q: How does the Engineer-I course differ from the Analyst-I course?

A: Many of the same topics are covered in both courses, but the focus may be different. The Engineer-I course covers configuring the feature in more depth, while the Analyst-I course covers how to use the feature in more depth. The following modules are significantly different in depth:

- McAfee Enterprise Log Manager.
- Devices.
- Policy Editor.
- Correlation.

Q: What topics are covered in Engineer-I that are not covered in Analyst-I?

A: Most topics that are covered in Engineer-I are also covered in Analyst-I with a different focus. However, Engineer-I includes the following modules that are not covered in Analyst-I, including:

- Installation and Configuration.
- Redundancy.
- Troubleshooting.

Q: What topics are covered in Analyst-I that are not covered in Engineer-I?

A: Most topics that are covered in Engineer-I are also covered in Analyst-I with a different focus. However, Analyst-I includes the following topics that are not covered in Engineer-I, including:

- Robust Correlation.
- McAfee Application Data Monitor and McAfee Database Event Monitoring.
- Parsing.

Q: My co-worker previously took the SIEM 101 course and recommended I take it. Which course is the best replacement for that course?

A: Both the Engineer-I and the Analyst-I course used the SIEM 101 course as a starting point. The courses were updated to the current version and then modified to focus on either the Engineer or Analyst role. Therefore, either the Engineer-I or Analyst-I course would be recommended. Compare your job duties to our definition of an Analyst and Engineer to decide which course is best for you.

Q: My co-worker previously took the SIEM 201 course and recommended I take it. Which course is the best replacement for that course?

A: The Engineer-II course was based off of the SIEM 201 course. There were many additions and updates so it is not simply updated for the current software version. Please note that it is recommended that you take the Engineer-I course prior to attending the Engineer-II course.

Q: How does the Engineer-II course differ from the Analyst-II course?

A: With the exception of the overview modules, there is no similarity between the Engineer-II course and the Analyst-II course. The Engineer-II course covers advanced configurations and troubleshooting while the Analyst-II course covers use cases.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com