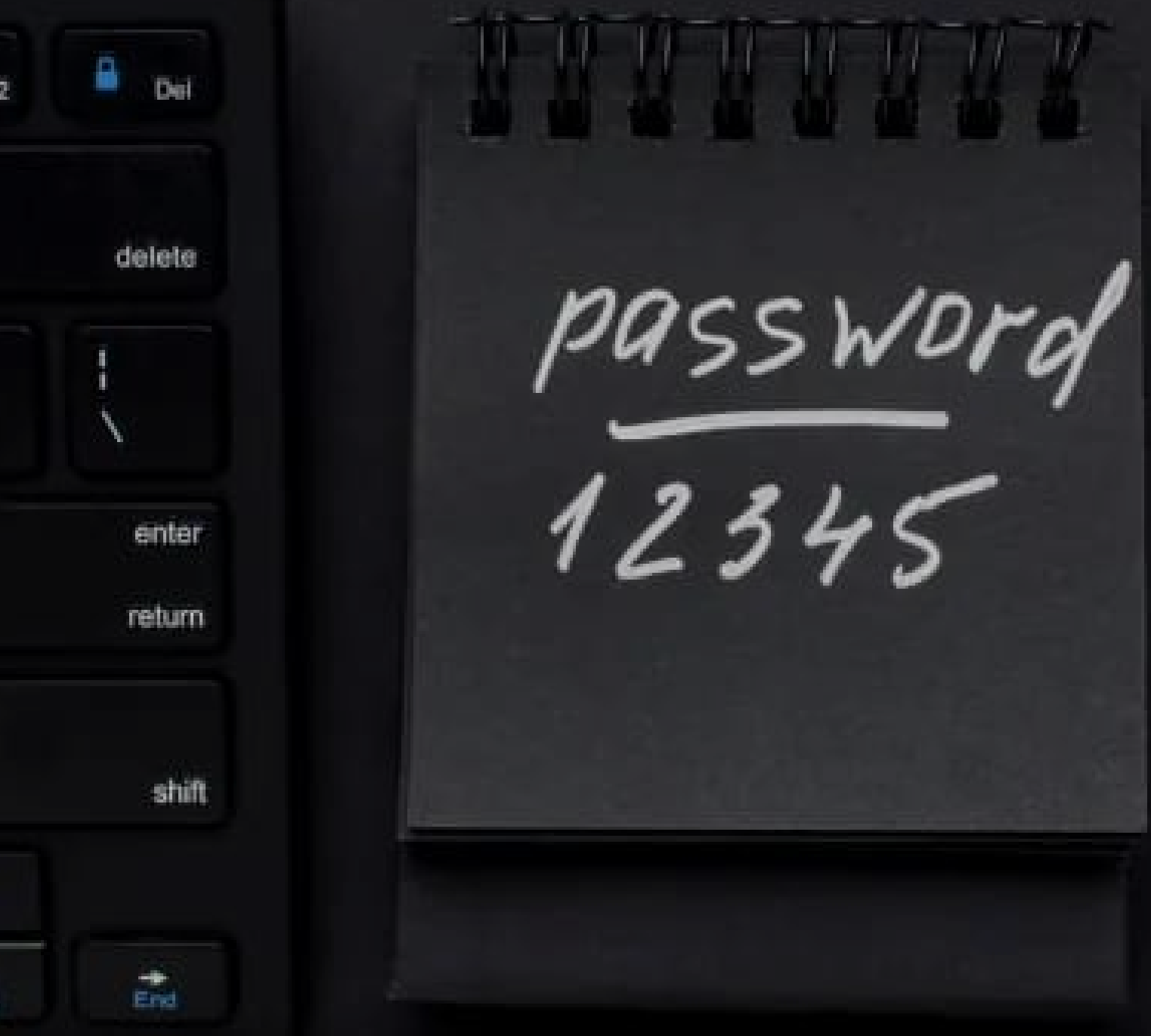




IT MANAGEMENT AND CYBER SECURITY | IMCS-015

Security Information and Event Management (SIEM)

Contact

+31 85 7444446
info@aractech.com
<https://aractech.com>

Address

Waarderweg 50, 2031PB Haarlem - Netherlands.

Course content

Why Attend

SIEM platforms collect and correlate security events across the organisation, enabling detection of threats and supporting investigations and compliance. However, many SIEM deployments generate noise rather than value.

This Aractech course covers SIEM architecture, log source onboarding, parsing and normalisation, correlation rules and detection use cases, alert tuning, dashboards, investigations, compliance reporting and SIEM programme management. Participants design detection use cases and tuning approaches.

Course Methodology

- Architecture presentations
- Use-case design workshops
- Demonstrations
- Tuning exercises
- Case studies

Course Objectives

- Explain SIEM architecture and capabilities
- Plan log source onboarding
- Develop detection use cases
- Tune alerts to reduce noise
- Use SIEM for investigations and reporting
- Manage and improve SIEM programmes

Target Audience

- Security analysts and engineers

Course content

- SOC staff
- IT security managers
- System administrators

Course outline

Detailed course outline

Day-by-day outline for Security Information and Event Management (SIEM).

Day 1 - SIEM Fundamentals

- 09:00-09:39 | Purpose of SIEM
- 09:39-10:18 | Architecture
- 10:18-10:57 | Deployment options
- 10:57-11:00 | Licensing and cost
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Licensing and cost (continued)
- 12:05-12:43 | Selection
- 12:43-14:00 | Exercise: Requirements

Day 2 - Log Management

- 09:00-09:39 | Log sources
- 09:39-10:18 | Onboarding
- 10:18-10:57 | Parsing
- 10:57-11:00 | Retention
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Retention (continued)
- 12:05-12:43 | Data quality
- 12:43-14:00 | Workshop: Log source plan

Course outline

Detailed course outline

Day-by-day outline for Security Information and Event Management (SIEM).

Day 3 - Detection Use Cases

- 09:00-09:39 | Use-case frameworks
- 09:39-10:18 | Correlation rules
- 10:18-10:57 | Threat mapping
- 10:57-11:00 | Behaviour analytics
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Behaviour analytics (continued)
- 12:05-12:43 | Testing
- 12:43-14:00 | Exercise: Writing use cases

Day 4 - Operations

- 09:00-09:39 | Alert triage
- 09:39-10:18 | Tuning
- 10:18-10:57 | Dashboards
- 10:57-11:00 | Investigations
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Investigations (continued)
- 12:05-12:43 | Compliance reports
- 12:43-14:00 | Demonstration: Investigation

Course outline

Detailed course outline

Day-by-day outline for Security Information and Event Management (SIEM).

Day 5 - Programme Management

- 09:00-09:45 | Metrics
- 09:45-10:30 | Governance
- 10:30-11:00 | Automation
- 11:00-11:30 | Coffee break
- 11:30-11:45 | Automation (continued)
- 11:45-12:30 | Improvement
- 12:30-13:15 | Roadmap
- 13:15-14:00 | Capstone: SIEM improvement plan

Seminar dates

Available seminar dates

Live dates and pricing for Security Information and Event Management (SIEM) generated from the course details page.

Date	Location	Format	Fee
16 - 20 November 2026	Frankfurt	Classroom	€1,875
7 - 11 December 2026	Rome	Classroom	€3,460
11 - 15 January 2027	Cape Town	Classroom	€1,625
8 - 12 February 2027	Barcelona	Classroom	€2,815
8 - 12 March 2027	Paris	Classroom	€3,825
12 - 16 April 2027	Frankfurt	Classroom	€1,875
10 - 14 May 2027	Barcelona	Classroom	€2,815
14 - 18 June 2027	Frankfurt	Classroom	€1,875
12 - 16 July 2027	Rome	Classroom	€3,460
9 - 13 August 2027	Vienna	Classroom	€3,225

Seminar dates

Available seminar dates

Live dates and pricing for Security Information and Event Management (SIEM) generated from the course details page.

Date	Location	Format	Fee
13 - 17 September 2027	Barcelona	Classroom	€2,815
11 - 15 October 2027	Paris	Classroom	€3,825
8 - 12 November 2027	Frankfurt	Classroom	€1,875
13 - 17 December 2027	Barcelona	Classroom	€2,815
16 - 20 November 2026	Online / Live	Online / Live	€1,815
7 - 11 December 2026	Online / Live	Online / Live	€1,815
11 - 15 January 2027	Online / Live	Online / Live	€1,815
8 - 12 February 2027	Online / Live	Online / Live	€1,815
8 - 12 March 2027	Online / Live	Online / Live	€1,815
12 - 16 April 2027	Online / Live	Online / Live	€1,815

Seminar dates

Available seminar dates

Live dates and pricing for Security Information and Event Management (SIEM) generated from the course details page.

Date	Location	Format	Fee
10 - 14 May 2027	Online / Live	Online / Live	€1,815
14 - 18 June 2027	Online / Live	Online / Live	€1,815
12 - 16 July 2027	Online / Live	Online / Live	€1,815
9 - 13 August 2027	Online / Live	Online / Live	€1,815
13 - 17 September 2027	Online / Live	Online / Live	€1,815
11 - 15 October 2027	Online / Live	Online / Live	€1,815
8 - 12 November 2027	Online / Live	Online / Live	€1,815
13 - 17 December 2027	Online / Live	Online / Live	€1,815