DevOpsSchool

SYLLABUS · LEVEL 01 OF 04 · FOUNDATION

Microsoft Sentinel Foundation Training

Microsoft Sentinel technical training · Foundation level · Day 1

CORPORATE TRAINING (DAY-WISE)	ONLINE LIVE & INTERACTIVE	SELF-PACED VIDEO	CURRICULUM EDITION
1 day · Day 1	Max 8-10 hours	1-year LMS access	2026-11-01

Format: Day-wise agenda only; no hourly schedule
Delivery: Instructor-led explanations, demonstrations, guided labs, assessment, and case studies
Primary experience: Microsoft Sentinel in the Microsoft Defender portal

Level structure and cumulative inclusion

Level	New instruction	Cumulative days (corporate)	Entry requirement
Foundation	Day 1	Day 1	No prior Sentinel experience required; basic Azure and security literacy helpful.
Essential	Day 2	Days 1-2	Foundation (Day 1) completed.
Intermediate	Day 3	Days 1-3	Completion of the Essential practical progression gate.
Advanced	Days 4-5	Days 1-5	Completion of the Essential and Intermediate practical progression gates.

This syllabus: Foundation level, covering Day 1. Each level includes every earlier day in full so the syllabus is self-contained; in delivery each topic is taught once, and later days build on earlier lab artifacts.

Delivery formats: Corporate training runs day-wise (Foundation 1 day, Essential 2 days, Intermediate 3 days, Advanced 5 days, cumulative). Online live and interactive sessions are a maximum of 8-10 hours. Self-paced video includes one year of LMS access.

Lab baseline: An approved Azure subscription and workspace, instructor-seeded synthetic logs where needed, Microsoft Defender portal access, and permission to create test artifacts. Additional Azure/Logic Apps ingestion and retention costs may apply. Preview or license/region-dependent features should be demonstrated only when available, with a prepared example otherwise.

Reference alignment note: Microsoft Learn currently states that the Azure-portal Sentinel experience will stop being supported after **March 31, 2027**; the course therefore teaches the Defender portal as the standard experience. Feature availability, costs, and licensing should be checked again before delivery. Source

Five-day learning progression (no repeated teaching days)

Day	Level	Principal new capability	Deliverable
Day 1	Foundation	Explain the platform and deploy a working workspace	Architecture and initial telemetry evidence
Day 2	Essential	Explore logs, enable a basic detection, and triage an incident	Query pack and first incident record

Day	Level	Principal new capability	Deliverable
Day 3	Intermediate	Ingest more complex data, correlate, enrich, and tune	Correlated custom detection and case automation
Day 4	Advanced	Engineer normalized detections, hunt, and orchestrate response	Hunt report and approval-gated playbook
Day 5	Advanced	Operationalize at enterprise scale and demonstrate readiness	Architecture, CI/CD, monitoring, and final capstone

Day 1 - Microsoft Sentinel Essentials, SOC Context, Architecture, and Initial Deployment

Level: Foundation | **Day outcome:** Understand where Sentinel fits in security operations, explain its architecture, and establish a working lab environment.

Day-specific 5W1H

Lens	Questions answered through Day 1 content
What?	What are SIEM, SOAR, XDR, security events, alerts, incidents, and Microsoft Sentinel?
Why?	Why centralize security telemetry, detection, investigation, and coordinated response?
Who?	Who owns the platform, operates the SOC, triages alerts, investigates threats, and governs access?
When?	When is SIEM useful for monitoring, compliance, detection, and incident response?
Where?	Where does Sentinel run, and where do Microsoft, multicloud, and on-premises signals originate?
How?	How do data sources, ingestion, Log Analytics, Sentinel, and the Defender portal work together?

Day 1 agenda - unique topics

ID	Topic	Coverage
F01	The security operations problem	Security visibility gaps, alert fatigue, SOC mission, and lifecycle of a security event.
F02	Fundamental security terminology	Telemetry, log, event, indicator, detection, alert, incident, case, false positive, and response action.
F03	What Microsoft Sentinel provides	Cloud-native SIEM capabilities, unified security operations experience, key benefits, and fundamental limitations.
F04	People and responsibilities	SOC L1/L2/L3 analysts, threat hunters, security engineers, cloud administrators, and service owners; basic ownership boundaries.
F05	Where Sentinel fits and when to adopt it	Microsoft/Azure, multicloud, hybrid, and on-premises contexts; common organizational use cases.
F06	Comparison with alternative approaches	SIEM versus endpoint-only monitoring, EDR/XDR, log management, and traditional SIEM; complementary rather than mutually exclusive tools.
F07	Foundational platform architecture	Data sources → connectors → ingestion/Log Analytics → analytics → incidents → investigation and response; Defender portal interface.
F08	Azure resource dependencies	Microsoft Entra tenant, subscription, resource group, Log Analytics workspace, region, and workspace association.
F09	Prerequisites and deployment planning	Lab scope, account requirements, region selection, permissions, sample data, safe test practices, and awareness of ingestion costs.
F10	Baseline access permissions	Least privilege concepts; basic Azure and Microsoft Sentinel roles; why owner and analyst access differ.
F11	Initial workspace setup	Create or select a Log Analytics workspace, enable Sentinel, connect it to the Microsoft Defender portal, and confirm navigation.
F12	First data connection	Activate one instructor-approved, straightforward Microsoft data source (for example Azure Activity, subject to access), observe connection status, and verify sample events arrive.

Practical exercises

1. Sketch the foundational Sentinel architecture and identify the responsibility of each component.

2. Provision or access a dedicated training workspace, enable Microsoft Sentinel, and open the Defender portal experience.
3. Connect an approved starter data source and record evidence of incoming events; use instructor-provided synthetic telemetry when a licensed source is unavailable.

Best practices, limitations, and troubleshooting focus

- **Best practices:** Use an isolated lab; apply least privilege; document subscription, workspace, and region; start with a small, known log source; use synthetic data instead of confidential real incidents.
- **Common errors:** Incorrect tenant or workspace, insufficient permissions, unsupported source prerequisites, no events yet, and confusion between portal views.
- **Advantages and limits:** Rapid cloud-based deployment and integration versus ongoing data charges, source-specific prerequisites, and the need for ongoing SOC processes.

Real-world case: A small enterprise needs one place to view identity and Azure administration events before developing a full detection program.

Day 1 evidence: Architecture sketch, working Sentinel workspace, documented access model, and proof of first successful data ingestion.

Official reading: What is Microsoft Sentinel? | Deployment guide | Sentinel in the Defender portal

Training quality and assessment design

Stage checkpoint	Evidence used for assessment	Next-step rule
End of Day 2 (Essential)	Setup and ingestion evidence, basic KQL, starter alert, incident triage	Pass before entering Day 3.
End of Day 3 (Intermediate)	Second-source collection evidence, correlation, enrichment, tuned rule, safe case automation	Pass before entering Day 4.
End of Day 5 (Advanced)	ASIM/hunt/response demonstration, enterprise blueprint, governed deployment, cost/reliability plan	Final program completion.

Recommended instructor assessment approach: use checklists and observable lab artifacts, not attendance alone. Allow a supervised remediation attempt for learners who miss a prerequisite. Reuse one synthetic incident storyline throughout the course, but introduce **new skills** on each successive day.

5W1H and requested topic coverage map

Requested training lens	Primary day where it is introduced and assessed
What / Why / Who / When / Where / How	Applied to the **distinct new capability on every day**, in each day's 5W1H matrix.
Architecture	Day 1 - core flow; Day 4 - SOAR workflow architecture; Day 5 - enterprise multiworkspace design.
Installation and setup	Day 1 - core workspace; Day 3 - AMA/DCR source integration; Day 4 - playbook setup; Day 5 - automated deployment.
Practical examples and real-world use cases	Fresh scenario and hands-on evidence on every day.
Best practices and troubleshooting	Specific, level-appropriate guidance and failure modes on every day.
Advantages and limitations	Basic platform evaluation on Day 1; feature-specific tradeoffs in later days.
Comparisons with alternatives	Day 1 - SIEM/XDR/log-management choices; Day 3 - ingestion/detection choices; Day 4 - NRT/scheduled and manual/automated actions; Day 5 - architecture and data-tier choices.

Scope note: This is an instructional **agenda**, not a time-blocked schedule or operational authorization to connect production sources. Changes, connector selections, and automated responses must be adapted to the actual tenant, entitlements, and security policy.

Enroll or ask for a corporate batch: https://www.devopsschool.com/courses/microsoft/sentinel/foundations.html
contact@DevOpsSchool.com · +91 99057 40781 · +1 469 756 6329 · www.devopsschool.com