sumo logic Academy

SOC/Security Analyst Learning Path

This guide lays out the recommended Sumo Logic Academy course sequence for SOC and Security Analyst teams. It starts with onboarding and moves through Cloud SIEM triage skills and hands-on certification.

➤ **Recommended:** take this path step-by-step in the Sumo Logic Learning Portal — SOC/Security Analyst Learning Path

⚠ **Before you begin:** the guided path above and the self-paced course links below both require signing in to the Sumo Logic Learning Hub.
View sign-in instructions

Core learning path

Phase	Focus	Courses	Time
1. Foundation	Platform basics	Fundamentals	~3 hrs
2. Operational Maturity	Triage & Dojo AI	Essential SIEM Skills for SOC Analysts, Hands on with Mobot and Dojo AI	~2 hrs
3. Advanced	Search efficiency & security logs	Search Mastery, Best Practices for Query Efficiency, Logs for Security	~6 hrs

Phase 1 Foundation

Platform basics before anything role-specific.

Fundamentals

Basic concepts: metadata, data types, dashboards, apps. Includes hands-on labs.

Free live instructor-led class: Register here · Watch recording · ~3 hrs
Free self-paced course: Access course · ~3 hrs
Target role: *All Sumo Logic users*

Phase 2 Operational Maturity

Day-to-day Cloud SIEM usage, incident triage, and Dojo AI.

Essential SIEM Skills for SOC Analysts

Focuses on using Sumo Logic's SIEM effectively within a SOC team responsible for identifying and managing cybersecurity incidents — the how's and why's of incident triage and best practices for using SIEM and Dojo AI capabilities.

Free live instructor-led class: Register here · Watch recording
Free self-paced course: Access course · ~1–2 hrs
Target role: *SOC Analysts*

Hands on with Mobot and Dojo AI

Mobot's core functionality and business value; writing effective prompts; best practices for using Mobot efficiently.

Free live instructor-led class: Register here · Watch recording · ~1 hr
Free self-paced course: Access course · ~1 hr
Target role: *All Sumo Logic users*

Phase 3 Advanced

Search efficiency, query optimization, and hunting through security logs.

Search Mastery

Advanced log operators, analytical functions, efficient queries, dashboards, alerts.

Free live instructor-led class: Register here · Watch recording · ~3 hrs
Free self-paced course: Access course · ~3 hrs
Target role: *Analysts, Admins who write queries*

Best Practices for Query Efficiency

Craft efficient log search queries by mastering performance efficiency, scope efficiency, and the Flex pricing model. Prereq: Fundamentals; Search Mastery recommended.

Free live instructor-led class: Register here · Watch recording · ~1 hr
Free self-paced course: Access course · ~90–100 min
Target role: *Analysts, Admins, DevOps/IT Contributors, Log Analysts/SREs, SOC/Security Analysts, System Admins*

Logs for Security

Use Logs for Security & Threat Intelligence; query AWS data; hunt for threats; build SOC dashboards.

Free live instructor-led class: Register here · Watch recording · ~3 hrs
Free self-paced course: Access course · ~2 hrs
Target role: *SOC Analysts*

Certification **Prove It**

Once the courses above are complete — and with roughly six months of hands-on product experience — these exams are directly relevant to this role:

- **Fundamentals Exam** — $100, no prerequisite. Leads to the Sumo Logic Certified Fundamentals User credential.
- **Cloud SIEM Exam** — $150, requires Fundamentals. Leads to the Sumo Logic Certified Cloud SIEM Practitioner credential.
- **Search Mastery Exam** — $150, requires Fundamentals. Leads to the Sumo Logic Certified Search Mastery User credential.
- **Logs For Security Exam** — $150, requires Fundamentals. Leads to the Sumo Logic Certified Logs for Security Analyst credential.

Kryterion proctors every exam. Certifications stay valid for two years and award a Credly digital badge upon passing.

Cloud SIEM Practitioner badge

Optional resources

Supplementary content for deeper exploration and self-directed learners.

Optional self-paced courses

- Cloud SIEM Training Self-Paced — comprehensive Cloud SIEM course covering both practitioner and admin topics (~2–3 hrs)
- The Sumo Security Pipeline — overview of Sumo Logic's security tools: CIP, Cloud SIEM, Cloud SOAR (~1 hr)
- Use Case: PCI Compliance — install and configure the PCI Compliance app; meet PCI DSS standards (~1 hr)

Microlessons — SIEM

- Threat Investigation with Cloud SIEM (3:59 min)
- How are Insights Generated in Cloud SIEM? (2:35 min)
- Cloud SIEM MITRE ATT&CK® Threat Coverage Explorer (2:56 min)

Microlessons — Dojo AI / Mobot

- Dojo AI SOC Analyst Agent (3:18 min)
- Introduction to Mobot (4:50 min)
- Using Mobot for Log Analysis (4:10 min)

Expert sessions

- Threat Hunting
- Threat Detection Investigation and Response (TDIR) with Sumo Logic
- Mastering Dojo AI: How Agentic Intelligence Transforms SecOps

More info

- Website detailing all Sumo Logic Academy offerings
- FAQ Training and Certification
- More info on Private Virtual and Onsite training
- Contact the Sumo Logic training team