sumo logic Academy

Cloud Security Architect Learning Path

This guide lays out the recommended Sumo Logic Academy course sequence for Cloud Security Architects and SOC Administrators. It starts with onboarding and moves through Cloud SIEM administration, automation, and hands-on certification.

➤ **Recommended:** take this path step-by-step in the Sumo Logic Learning Portal — Cloud Security Architect 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	Admin config & Dojo AI	Administration, Hands on with Mobot and Dojo AI	~4 hrs
3. Advanced	SIEM, search, automation, extensibility	Cloud SIEM, Search Mastery, Logs for Security, Automation Service, Extending Sumo Logic with MCP/API/Terraform	~10 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

Hands-on administration and Dojo AI fundamentals.

Administration

Configure sources, users, RBAC; FERs, Partitions, Scheduled Views.

Free live instructor-led class: Register here · Watch recording · ~3 hrs
Free self-paced course: Access course · ~3–4 hrs
Target role: *System Administrators, IT Ops*

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

Cloud SIEM, search efficiency, and automation for security operations.

Cloud SIEM

Comprehensive Cloud SIEM course covering both practitioner and admin topics; turns raw logs into actionable Insights.

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

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*

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*

Automation Service

Configure Automation Service integrations; create playbooks; automate insight and alert management without Cloud SOAR. Prereq: Fundamentals + Cloud SIEM recommended.

Free live instructor-led class: Register here · ~1 hr
Free self-paced course: Access course · ~1–2 hrs
Target role: *Admins, SOC Admins, Cloud Security Architects*

Extending Sumo Logic with MCP/API/Terraform

Learn ways to extend Sumo Logic platform functionality through MCP, Terraform, or API commands.

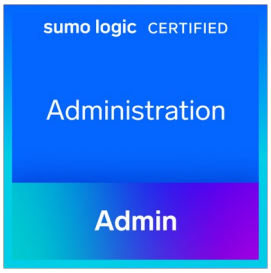
Free self-paced course: Access course · ~1–2 hrs
Target role: *All Sumo Logic users interested in extending the platform via MCP*

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.
- **Administration Exam** — $150, requires Fundamentals. Leads to the Sumo Logic Certified Administrator 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.



Administration badge

Optional resources

Supplementary content for deeper exploration and self-directed learners.

Optional self-paced courses

- Cloud SIEM: User Interface Configuration — deep dive into the Cloud SIEM Configuration Page (~1 hr)
- Cloud SOAR Administration Self-Paced — configure data sources, custom fields, incident templates, playbooks, automations (~2 hrs)
- The Sumo Security Pipeline — overview of Sumo Logic's security tools: CIP, Cloud SIEM, Cloud SOAR (~1 hr)

Microlessons — Administration

- Administering Roles (3:29 min)
- Administering Policies (CloudFlex) (4:13 min)
- Tool Consolidation Overview (4:17 min)

Microlessons — SIEM

- Rule Tuning in Cloud SIEM (2:27 min)
- Cloud SIEM Global Intelligence for Security Insights (3:06 min)
- Cloud SIEM Automation Service (2:39 min)

Expert sessions

- Cloud SIEM Rule Tuning
- Cloud SIEM Entity Groups
- Elevating Security Posture to Maximize Threat Response

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