

Sigma Rules for Detection Engineers

SEC408

Write a detection once in Sigma's vendor-neutral YAML and run it on any SIEM. Author rules with durable detection logic and honest false-positive profiles, convert them to Splunk, Microsoft, and Elastic with sigma-cli, extend them with correlation for multi-event attacks, validate them against data, and ship them as a maintained rule library. You finish able to carry a threat from a report to a deployed, portable detection.

Modules	13
Lessons	54
Phases	5
Free preview	Course Orientation

The method

A Sigma rule is a claim that a behavior is visible in a log source. This course runs the same loop for every rule it writes, because the difference between a rule that works and a rule that exists is the last three steps.

1. Name the behavior, not the tool. A rule matching an executable name breaks when the attacker renames it. A rule matching what the technique has to do survives.
2. Write against a log source you actually have. The most elegant rule in the world is inert if your estate never collects the field it matches on. Establish the source before the logic.
3. Render it to the backend you run. Sigma is a portable format, and portability is only useful if you check what the converter produced. The same rule becomes different queries in different backends.
4. Test both directions. Fire the behavior and confirm the rule matches. Then run it against a week of normal activity and count what it returned. A rule tested only positively is half tested.
5. Ship it with its false positive documented. Every rule has one. Writing it down is what stops the next analyst deleting the rule instead of tuning it.

What this course assumes

No minimum experience and no prerequisite course. YAML, log sources, field mappings and the backend model are all explained where they first appear.

What makes it go faster: any prior exposure to a SIEM query language, and a log source of your own to test against. Neither is required, and the course provides sample data for every rule it writes.

What this course does not cover: operating a SIEM, incident response, and the detection engineering program around the rules. This is the rule-writing craft, taught deeply, and the program that consumes those rules is a separate course.

Full syllabus

Course Orientation

Course Orientation [FREE PREVIEW](#)

What Sigma Rules for Detection Engineers teaches: write a detection once in Sigma's vendor-neutral YAML and deploy it to any SIEM.

Phase 1: Writing Rules

The Sigma Model

What a Sigma rule is as an object you author.

- 1.1 The Anatomy of a Sigma Rule
- 1.2 Logsource: Category, Product, and Service
- 1.3 The Detection Block in Outline
- 1.4 Metadata That Matters: id, status, level, and related
- 1.5 Tags and ATT&CK Mapping
- 1.6 Reading SigmaHQ Rules as a Peer
- Module Summary
- Check My Knowledge

Detection Logic

The detection block in depth. How a selection matches, the full set of field modifiers from contains and startswith through regex, CIDR, base64, and windash, the condition language with its quantifiers and operator precedence, and the exclusion logic that carves known-good activity out of a...

- 2.1 How a Selection Matches
- 2.2 String Modifiers
- 2.3 Transform and Type Modifiers
- 2.4 Encoding and Evasion Modifiers
- 2.5 The Condition Language and Precedence
- 2.6 Filters, Exclusions, and Composing a Rule
- Module Summary
- Check My Knowledge

Phase 2: Production Quality

Writing Rules That Survive Production

The gap between a rule that is correct and a rule that survives production.

- 3.1 Why Good Rules Get Switched Off
- 3.2 Durable Detections: Stable vs Volatile Fields
- 3.3 The Specificity Dial
- 3.4 False Positives and the Tuning Loop
- 3.5 Rule Quality and Review
- 3.6 From Noisy to Production-Ready
- Module Summary
- Check My Knowledge

Phase 3: Conversion

Conversion Across Backends

How one Sigma rule becomes a query on any SIEM.

1. 4.1 What Conversion Actually Does
2. 4.2 Targets and Pipelines: The Two-Part System
3. 4.3 Field and Logsource Mapping
4. 4.4 What Converts Cleanly and What Breaks
5. 4.5 Reading and Verifying Converted Output
6. 4.6 One Rule Across Three Backends
7. Module Summary
8. Check My Knowledge

Phase 4: Validate and Ship

Validate, Correlate, Ship

Turning rules into an operational detection practice.

1. 5.1 Validating a Rule Against Data
2. 5.2 Beyond One Event: The Correlation Model
3. 5.3 Counting Correlations
4. 5.4 Sequence Correlations
5. 5.5 Shipping: The Rule Lifecycle and Detection as Code
6. 5.6 Course Capstone
7. Module Summary
8. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The rule anatomy, the modifiers, what survives conversion, and the correlation types with their limits.

1. The Rule, and the Fields That Decide Its Fate
2. Detection Logic and the Modifiers
3. Conversion, and What Does Not Survive It
4. Validating, Correlating and Shipping

Cookbooks

Ordered procedures for writing a rule from a report, adopting a community rule, taking a noisy rule to production, and building a repository.

1. Writing a Rule From a Threat Report
2. Adopting a Community Rule
3. Taking a Noisy Rule to Production
4. Standing Up a Rule Repository

Walkthroughs

Four cases reasoned end to end, including the rule that converted perfectly and matched nothing.

1. The Rule That Converted Perfectly
2. The Rule That Was Broader Than Anybody Read
3. The Rule Nobody Should Have Tightened
4. The Correlation That Never Correlated

Playground

sigma-cli, the public rule repository, and log data of your own to validate against.

Operational Reference

The full rule anatomy, every modifier, the condition and correlation syntax, the sigma-cli conversion and validation commands, and the rule-quality conventions from the course in one place, organized by task.

1. Operational Reference

References & Further Reading

The Sigma specification and documentation, the pySigma toolchain and backends, ATT&CK, Atomic Red Team, and the backend platform documentation used throughout the Sigma Rules course, organized by category.

Course Completion

Course Exam

Sigma Rules for Detection Engineers end-of-course exam: one rule, two backends, clean conversion on both, and only one that ever fires.

1. Course Completion. Sigma Rules for Detection Engineers

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/sigma-rules/