

Sysmon Configuration and Tuning

SEC206

Turn Windows endpoints into a detection sensor you can trust. Build a tuned Sysmon config that captures attacker behavior without drowning your SIEM, deploy it across a fleet, feed its events to a SIEM, map them to Sigma detections and ATT&CK, validate coverage with atomic tests, and operate the sensor so your coverage stays real. Four modules, thirty sections, free preview.

Modules	12
Lessons	53
Phases	4
Free preview	Course Orientation

The method

Sysmon is a configuration file and a decision about what you are willing to store. This course runs the same four-step loop for every event type it covers, because a config written without it produces either a blind spot nobody knows about or a volume bill nobody predicted.

1. Know what the event actually carries. Each Sysmon event ID records a different set of fields, and the ones you can filter on are not always the ones you want to alert on. Read the schema before writing a rule against it.
2. Write the include and the exclude together. Every exclusion is a new blind spot, and a config that only includes is a config that fills a disk. The two halves are one decision.
3. Baseline before you tune. Deploy in a permissive state, measure what normal looks like in your estate, then cut. Tuning against an assumed baseline tunes against somebody else's environment.
4. Prove the event still fires. After every exclusion, re-run the behavior it was meant to catch. A config that stopped generating noise and stopped generating evidence look identical on a dashboard.

The output is a config you can defend line by line, and a written record of what each exclusion gave up.

What this course assumes

No minimum experience and no prerequisite course. Every concept is explained where it is first used, including what an event ID is and why Sysmon exists alongside the Windows Security log rather than replacing it.

What makes it go faster: a Windows machine you can install on, even a virtual one, and enough comfort reading XML to recognize a nested element. Neither is required, and the course walks through the install from nothing.

What this course does not cover: writing detection rules in a SIEM, which is a separate discipline, and endpoint forensics. Sysmon is the telemetry layer, and this course is about producing telemetry worth querying rather than about querying it.

Full syllabus

Course Orientation

Course Orientation [FREE PREVIEW](#)

What Sysmon Configuration and Tuning teaches: turn Windows endpoints into a detection sensor by building a tuned Sysmon config, deploying it across a fleet, feeding it to a SIEM, mapping its events to Sigma and ATT&CK, validating coverage, and operating it day to day.

Phase 1: The Telemetry

The Telemetry

What Sysmon records, event by event, before you decide what to log.

- 1.1 What Windows Misses, and What Sysmon Captures
- 1.2 The Architecture: Driver, Service, and Log
- 1.3 Process Events: Creation and Termination
- 1.4 Credential and Injection Events
- 1.5 Network and DNS Events
- 1.6 File and Registry Events
- 1.7 Image Loads, Drivers, Pipes, and WMI
- 1.8 The Remaining Events, and the Decision
- Module Summary
- Check My Knowledge

Phase 2: Configuration and Tuning

Configuration

How a Sysmon config actually controls what gets logged.

- 2.1 The Configuration File: Structure and Hashing
- 2.2 Include and Exclude
- 2.3 Condition Operators
- 2.4 Rule Groups and Combining Conditions
- 2.5 Precedence: How Conflicts Resolve
- 2.6 The Field Reference
- 2.7 Building a Config from Scratch
- Module Summary
- Check My Knowledge

Baselines and Tuning

Where a config meets a real environment. The community baselines and how to read one as a peer, the economics of noise, a repeatable measure-first tuning method, the over-exclusion trap that silently deletes detections, taming the loudest events, and tuning a config to each host role. The module...

- 3.1 The Community Baselines
- 3.2 Two Baselines Compared
- 3.3 Reading a Baseline in Depth
- 3.4 The Economics of Noise
- 3.5 A Tuning Methodology
- 3.6 Safe Exclusions and the Over-Exclusion Trap
- 3.7 Taming the Loudest Events
- 3.8 Environment-Specific Tuning
- Module Summary
- Check My Knowledge

Phase 3: Deploy, Detect, and Operate

Deploy, Detect, and Operate

Getting a tuned config off your bench and into a working detection capability.

1. 4.1 Deploying at Scale
2. 4.2 The Native Windows Sysmon Feature
3. 4.3 Getting Events to the SIEM
4. 4.4 Mapping Events to Detections
5. 4.5 Validating Coverage
6. 4.6 Operating Sysmon
7. 4.7 Capstone: Build, Deploy, Validate
8. Module Summary
9. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The event IDs, the config schema, the operators that behave unexpectedly, and the exclusions that quietly remove your coverage.

1. The Events, and What Each One Costs
2. The Config, and How It Actually Evaluates
3. Tuning Without Losing Coverage
4. Deploying and Proving It Works

Cookbooks

Ordered procedures for the work: first deployment, tuning a noisy estate, adding coverage, and updating a config safely.

1. Deploying Sysmon for the First Time
2. Tuning a Noisy Estate
3. Adding Coverage for a Technique
4. Updating a Config Safely

Walkthroughs

Four cases reasoned end to end, including the ones where the config was valid and collecting the wrong thing.

1. The Rule That Was Already Excluded
2. The Estate Running Four Configs
3. The Config Nobody Should Have Cut
4. The Gap That Was Not Sysmon's

Playground

One Windows machine, a config you write yourself, and the checks that make the practice real.

Operational Reference

Every Sysmon command, event type, condition operator, config idiom, and operational pattern from the course in one place, organized by stage: install and reconfigure, the event catalog, filtering, measurement, deployment, collection, detection, validation, and health.

1. SM99.1 Operational Reference

References & Further Reading

Microsoft and Sysinternals documentation, the community Sysmon baselines, the Sigma detection toolchain, Atomic Red Team, and MITRE ATT&CK: the external sources used throughout the Sysmon Configuration and Tuning course, with stable top-level locations.

1. SM100.1 References & Further Reading

Course Completion

Course Exam

Sysmon Configuration and Tuning end-of-course exam: a config review where the volume figures are accurate and all three submitted edits are wrong, testing whether you can read what an exclusion actually removes and find the change that silently inverts collection.

1. Course Completion. Sysmon Configuration and Tuning

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