What is detection rule validation?

Detection Rule Validation (DRV) proves that the detection rules in your SIEM and EDR actually fire on real attacker behavior and produce an alert an analyst will see. It tests the full detection pipeline: is the right telemetry being collected, does the rule trigger on the behavior, and does it generate a high-fidelity alert. DRV exists because most detection failures are silent, a rule that looks fine can fail because a log source is missing, coalesced, or misconfigured. Independent research repeatedly finds that far more attacker activity is logged than is ever alerted on, and DRV is how that gap gets found and fixed.

HOW IT WORKS

01 Why do detection rules fail silently?

Detection breaks in quiet, unglamorous ways. Independent analysis of detection-rule failures consistently finds that log-source problems are the single largest cause: telemetry that is unavailable, broken, inactive, or improperly coalesced so that critical events are dropped or merged before the rule ever sees them. Configuration and performance issues add more silent failures, rules that exist but never trigger in production because content drifted away from the infrastructure.

The result is a wide gap between what is logged and what is alerted. Teams believe they have detection coverage, but the alert that should fire during a real intrusion never does. DRV surfaces those failures before an attacker relies on them.

02 How does DRV work?

DRV validates the whole detection lifecycle, not just the rule text:

- Telemetry check. Confirm the log sources the rule depends on are present, complete, and not coalesced away.
- Trigger check. Run the attacker behavior and confirm the rule actually fires on it.
- Alert check. Confirm the trigger produces a high-fidelity alert that reaches an analyst, not noise that gets buried.
- Fix and re-test. Tune the rule or the pipeline, then re-run to confirm the detection now works.

SOURCES

[1] MITRE ATT&CK Framework

[2] NIST SP 800-115 Technical Guide to Information Security Testing

Running this continuously catches regressions the moment a log source or rule change breaks coverage.

03 The gap between logged and alerted

The most important thing DRV measures is the difference between a behavior being logged and being detected. Logging is necessary but not sufficient. Telemetry can reach the SIEM and still never produce an alert, because the rule is missing, misconfigured, or tuned so loosely that the signal drowns in noise.

This is where security control validation and DRV meet: prevention validation asks whether the attack was blocked, and DRV asks whether, when it was not blocked, anyone would actually know. Both are part of adversarial exposure validation.

04 How do you get started with DRV?

Start with the detections that matter most, the behaviors tied to your highest-risk attack paths, and validate the full pipeline for each: telemetry, trigger, and alert. Fix the log-source and configuration issues first, since they cause the majority of silent failures, then re-test.

DRV can be driven by a continuous automated validation platform that exercises detections on a schedule, or as part of a human penetration testing engagement that checks whether your team actually saw the attack. The goal is the same: no detection you rely on should be unproven.

Logged is not detected. Prove your alerts fire.
securelayer7.net/learn/pentest/what-is-detection-rule-validation

Open online