

Detection posture summary

Sample enterprise estate | Splunk structural assessment | 24 October 2026

1,006 rules assessed

Enabled, deployed and in scope. 1,054 imported; 48 excluded.

759

CAN FIRE

133

CANNOT FIRE

114

INDETERMINATE

75.4% meet the assessed structural prerequisites. Broken and indeterminate rules receive no credit.

SELECTED FINDING

35 rules affected by one confirmed issue

A confirmed blocker prevents these rules from firing within the assessed scope.

Decision: prioritize these rules for remediation before relying on them at cutover.

Included in the 133 CANNOT FIRE total. Technical evidence omitted from this preview.

WHAT YOUR TEAM RECEIVES

The full assessment identifies affected rules, supporting evidence, limitations and verification steps for your engineers. A fresh assessment after remediation supports comparison with the baseline.

READING THE VERDICTS

CAN FIRE - Required conditions within the stated structural scope are verified.

CANNOT FIRE - Evidence establishes a blocker within the assessed scope.

INDETERMINATE - Available evidence does not support a definitive verdict.

SCOPE AND LIMITATIONS

Input completeness: partial. Results apply to the supplied evidence at the assessment time. No attacks were run or customer code executed. The assessment does not establish rule quality, tuning, attack coverage, scheduling or alert delivery. CAN FIRE does not prove that a matching attack would be detected.