Objective

What are we trying to achieve?

Justification

Why are we trying to detect this activity?

Analysis

How should the event be analysed?

Key Fields

SIEM Fieldname	Raw Log	Description

Correlation Criteria

Description of how it detects.

Limitations and Bypasses

Any known limitations or bypasses.

Allowlisting

How should entities be allowlisted?

Event Sources

List the event sources required.

Testing

Document testing and results.

References