## Anomalous File Creation Detection

# Fields and Their Use for Anomalous File Creation Detection

**1. File Metadata**

**File Path and Name**

:

Use location to determine the file's location.

Extract patterns from location to identify sensitive directories and unusual file paths.

**File Size**:

syscheck.size\_after and syscheck.size\_before track file size changes.

The absolute value of the size change (|size\_after - size\_before|) can be used as a feature.  **File Permissions**:

syscheck.win\_perm\_after and syscheck.mode provide insights into file permissions.

Anomalous changes in permissions could indicate potential security concerns.

1. **File Integrity Monitoring**

**File Hashes**

:

syscheck.md5\_after, syscheck.sha1\_after, syscheck.sha256\_after: Changes in hash values help detect unexpected modifications.

Comparing \*\_before and \*\_after values highlights suspicious activity. **File Attributes**:

syscheck.changed\_attributes and syscheck.attrs\_after: Indicate what specific attributes changed.

Use this to detect unexpected changes to critical file properties.

1. **User and Process Context**

**User Information**

:

syscheck.uid\_after

and

syscheck.uname\_after

:

Capture the user who

created or modified the file.

Anomalous user activity (e.g., privileged users creating files in nonstandard locations) is a key signal.

1. **Time-Based Features**

**Timestamp**

:

timestamp captures the time of the event.

Derive features such as "hour of the day," "weekday vs. weekend," or "time since last similar event."  **Modification Time**:

syscheck.mtime\_after and syscheck.mtime\_before provide file modification times.

Rapid or unexpected modification sequences could indicate anomalies.

1. **Alert Context**

**Event Metadata**

:

decoder.name identifies the source of the alert (e.g., FIM, syscheck). rule.firedtimes: Higher values indicate recurring patterns, which may help classify behavior as normal or anomalous.  **Rule Correlations**:

rule.groups, rule.mitre.id, rule.mitre.tactic, and rule.mitre.technique provide detailed context about the event's classification.

Use these to connect alerts to known tactics and techniques.

1. **Agent and Manager Information**

**Agent Details**

:

agent.id, agent.name, and agent.ip: Identify the source system of the event.

Correlate patterns across different agents to identify system-specific anomalies.

**Manager Details**:

manager.name: Helps correlate events across distributed setups.