From Cloud Compromise to Lateral Movement: A Mixed-Method Analysis of Detection Fragility in Open Sigma Rules

Tayyip Ozturk
Department of Computer Engineering
TOBB University of Economics and Technology
Ankara, Turkey
tayyipozturk@etu.edu.tr

***Abstract*—Modern cyber operations typically follow a hybrid kill-chain: gaining initial access via cloud services before pivoting laterally through on-premise infrastructure. Despite this established reality, open-source detection engineering efforts appear unevenly distributed. This study presents a quantitative analysis of public Sigma detection rules mapped to MITRE ATT&CK, specifically comparing the "Cloud Compromise" and "Lateral Movement" phases. We introduce a "Detection Health Framework" that evaluates rule repositories not just by coverage, but by structural fragility and temporal evolution. Our results reveal a paradoxical inversion of detection maturity: Cloud techniques exhibit significantly higher rule density (mean 6.32) and coverage (56%) compared to Lateral Movement (mean 3.53, 50%). However, advanced metrics indicate that this cloud dominance is fragile. Cloud detection rules show extreme distributional inequality (Gini Coefficient: 0.78) and high technique coupling (2.06), suggesting a reliance on a narrow set of standardized APIs. Conversely, Lateral Movement detection is numerically weaker but structurally more stable. We conclude that the community has prioritized the "breadth" of cloud detection over the "resilience" of lateral movement detection, creating a "Fragile Giant" posture where critical pivots in the hybrid kill-chain remain exposed.**

***Index Terms*—Cybersecurity, MITRE ATT&CK, Sigma Rules, Cloud Security, Lateral Movement, Detection Engineering**

I. Introduction

Hybrid cyber operations increasingly span both cloud and on-premise environments. Attackers often gain initial access via cloud misconfigurations or stolen credentials before executing lateral movement through internal systems. While numerous commercial and academic works analyze endpoint detection coverage, few provide an open, data-driven comparison of detection rule representation across these two critical phases.

The detection engineering community increasingly leverages the MITRE ATT&CK framework to evaluate visibility [1]. However, current assessments often treat "detection" as a binary metric—either a rule exists, or it does not. This binary approach fails to capture the *quality* and *fragility* of the underlying logic.

This study addresses this gap by analyzing open Sigma detection rules mapped to MITRE ATT&CK. We aim not to simulate specific attack paths, but to quantify the "Detection Health" of the community's response to hybrid threats. Our contribution is threefold:

- A quantitative comparison of rule density and coverage between Cloud and Lateral Movement phases.
- A novel "Detection Health Framework" that measures structural fragility (coupling) and inequality (Gini coefficient).
- A temporal analysis revealing the divergent evolutionary paths of cloud vs. endpoint detection logic.

II. Related Work

Prior research has primarily focused on endpoint visibility. Virkud et al. [1] conducted a comprehensive empirical study of commercial Endpoint Detection and Response (EDR) products, revealing that coverage averaged only 48-55% even in mature tools. Similarly, Rahman and Williams [2] mapped NIST SP 800-53 controls to adversarial behaviors, identifying significant gaps in unmitigated techniques.

Visualization-oriented approaches have also emerged to address these gaps. Shete [3] proposed interactive visualizations to depict organizational coverage, while Datadog's Cloud SIEM Map [4] demonstrates how commercial platforms align telemetry to cloud-related techniques. However, such tools often remain proprietary. In the broader cloud domain, the Cloud Security Alliance (CSA) and McAfee [5] found that defenders struggle to adapt on-premise strategies to cloud telemetry, though their study lacked quantitative rule analysis.

III. Methodology: The Detection Health Framework

We extracted data from the official MITRE ATT&CK Enterprise JSON and the SigmaHQ repository [6], utilizing its ecosystem of converters (e.g., Panther [7]) to parse logic. Techniques were classified into "Cloud" (platforms: AWS, Azure, GCP) and "Lateral Movement" (kill-chain phase: lateral-movement).

To move beyond simple counting, we developed a **Detection Health Framework** (see Table I) comprising both quantitative and qualitative metrics.

TABLE I
THE DETECTION HEALTH EVALUATION FRAMEWORK

Metric	Qualitative Attribute	Security Implication
Rule Density	Defense Maturity	High density implies defense-in-depth against evasion.
Technique Coupling	Systemic Fragility	High coupling indicates reliance on single points of failure (e.g., one log stream).
Log Diversity	Detection Complexity	Low diversity implies simple, brittle logic; High implies rich correlation.
Gini Coefficient	Strategic Bias	High inequality reveals "Tunnel Vision" on popular techniques.

A. Metrics Definition

- **Rule Density:** The mean number of detection rules per technique.
- **Coverage Ratio:** The percentage of techniques with ≥ 1 rule.
- **Gini Coefficient:** A statistical measure of inequality (0 to 1), where high values indicate that rules are hoarded by a few "celebrity" techniques.
- **Technique Coupling:** The average number of *other* techniques a rule detects. High coupling implies "fragility."

IV. QUANTITATIVE RESULTS

A. The Density Inversion

Contrary to the assumption that endpoint security is more mature, our analysis reveals that **Cloud techniques significantly outperform Lateral Movement** in raw metrics (Fig. 1).

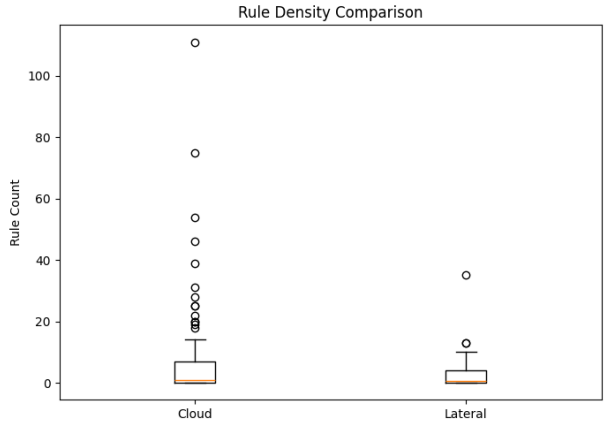

Fig. 1. Comparison of Mean Rule Density. Cloud techniques show nearly 2x the rule volume of Lateral Movement techniques.

- **Cloud:** Mean Rule Density of **6.32** rules/technique; Coverage of **56%**.
- **Lateral Movement:** Mean Rule Density of **3.53** rules/technique; Coverage of **50%**.

This suggests the open-source community has aggressively prioritized cloud visibility, likely driven by the standardization of cloud APIs which simplifies rule creation compared to fragmented endpoint logs.

B. Distributional Inequality (Gini Analysis)

While the average density is high, the distribution is deeply unequal (Fig. 2). We calculated the Gini Coefficient for both domains:

- **Cloud Gini: 0.78** (Extreme Inequality)
- **Lateral Gini: 0.75** (High Inequality)

A Pareto analysis confirms this imbalance: **62%** of all Cloud detection rules are concentrated in just the top **10%** of techniques. This indicates a "bunching effect" where defenders over-optimize for common behaviors (e.g., *T1078: Valid Accounts*) while leaving the "long tail" of 45% of cloud techniques completely uncovered.

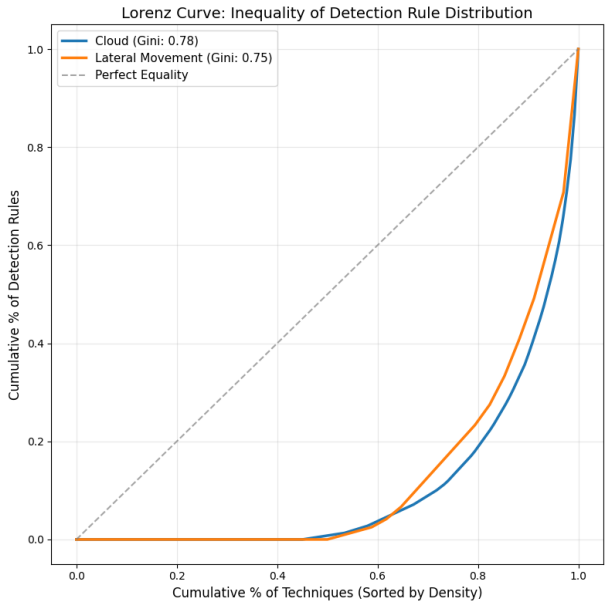

Fig. 2. Lorenz Curve of Rule Distribution. The nearly identical curves illustrate that both domains suffer from severe inequality, with a small percentage of techniques capturing the majority of detection rules.

C. Temporal Evolution

To understand if this disparity is historical or emerging, we analyzed rule creation timestamps (Fig. 3).

- **Validation:** The dataset effectively begins in **2017**, correlating with the public release of the Sigma standard.
- **Trend Analysis:** Lateral Movement rules exhibit a linear, stable growth pattern, characteristic of a mature field. In contrast, Cloud rules show an **exponential "boom" starting circa 2020**.

This 3-year "Adoption Lag" (2017–2020) likely reflects the industry's transition period to standardized cloud logging (e.g.,

AWS CloudTrail maturity) before portable detection logic could be authored at scale.

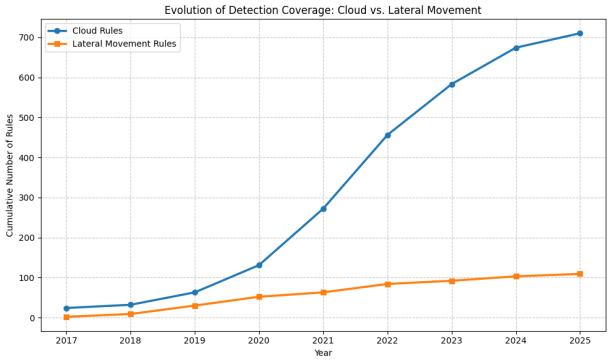

Fig. 3. Temporal Evolution of Detection Coverage. Note the "Cloud Boom" post-2020 compared to linear Lateral Movement growth.

V. Discussion: Qualitative Health Analysis

A. The Fragile Giant Phenomenon

Our analysis uncovers a critical distinction in detection maturity. Both domains exhibit similar levels of bias (Gini ≈ 0.78), indicating that defenders largely focus on the same "top 10%" of techniques regardless of the platform. However, the operational risk of this bias is asymmetric.

In **Lateral Movement**, this concentration is supported by loosely coupled, diverse logs (Coupling: 1.29); a failure in one detection logic does not necessarily cascade. In contrast, the **Cloud** domain operates as a "Fragile Giant." It possesses immense rule density and coverage (Quantity), but these rules are tightly coupled (Coupling: 2.06) to a narrow set of API logs. Consequently, the Cloud's high detection numbers mask a systemic vulnerability: a single evasion technique targeting a key log source (e.g., disabling CloudTrail) has a significantly higher "blast radius," potentially blinding the majority of the detection rulebase simultaneously.

B. The Telemetry Gap

We observed a critical gap between rule availability and operational utility. Cloud rules have high **Logsource Diversity** (mean 2.68), often requiring verbose data events (e.g., S3 object-level logging) that are frequently disabled by default due to cost. Conversely, Lateral Movement rules (mean 1.59 sources) rely on endpoint telemetry that, while harder to standardize, is often more persistently available on high-value assets. Thus, the 56% Cloud coverage figure likely represents a "theoretical maximum" rather than an operational baseline.

VI. Reproducibility

To facilitate future research and validation, the complete source code, parsing modules, and dataset generation scripts used in this study have been made publicly available. The repository includes the Jupyter notebooks for the Gini and Coupling analysis, as well as the raw CSV outputs used to generate the figures in this paper.

Code Availability: The fully reproducible codebase is accessible at: https://github.com/tayyipozturk/Detection-Coverage-Across-Hybrid-Attack-Paths

VII. Conclusion & Recommendations

This study quantified the detection disparity between the two critical pivots of hybrid cyber warfare. We found that the open-source community has pivoted aggressively toward the cloud, achieving nearly double the rule density of lateral movement techniques. However, this quantitative lead conceals a qualitative fragility.

Our "Detection Health" analysis demonstrates that cloud detection is highly coupled and unequal—reliant on a narrow set of "super-logs" and concentrated on "celebrity techniques." Meanwhile, the Lateral Movement phase remains a "legacy" problem: stable, but stagnant.

We recommend distinct strategies for each domain:

1) **For Cloud:** Focus on **Decoupling**. Reduce fragility by developing redundant detection logic that does not rely solely on single-stream management APIs.
2) **For Lateral Movement:** Focus on **Standardization**. The gap in coverage is a data problem, not a logic problem. Unifying endpoint telemetry schemas is a prerequisite for closing the density gap with the cloud.

References

[1] N. Virkud, S. Upadhyaya, and V. Ganesh, "How does endpoint detection use the mitre att&ck framework? an empirical analysis," in *USENIX Security Symposium*, 2024.

[2] M. A. Rahman and L. Williams, "An investigation of security controls and mitre att&ck techniques," *arXiv preprint arXiv:2211.06500*, 2022.

[3] S. Shete, "Visualizing cybersecurity coverage using MITRE ATT&CK Framework," *ResearchGate*, 2023.

[4] Datadog, Inc., "Identify gaps to strengthen detection coverage with the datadog cloud siem mitre att&ck map," 2025.

[5] CLTC and McAfee Enterprise, "Mitre att&ck as a framework for cloud threat investigation," 2023.

[6] SigmaHQ Community, "Sigma: Generic signature format for siem systems," *GitHub*, 2025.

[7] Panther Labs, "Your guide to the sigma rules open standard for threat detection," 2025.