MSc Cybersecurity Privacy and Trust

EVALUATING OPEN-SOURCE XDR AND SOAR FOR APT DETECTION AND RESPONSE IN HYBRID CLOUD

Joe O'Shea C00326757@setu.ie | Supervisor: Dr Hisain Elshaafi

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

INTRODUCTION:

XDR (Extended Detection and Response) and SOAR (Security Orchestration, Automation and Response) are key for modern cloud security operations.

APTs (Advanced Persistent Threats) are stealthy, long running attacks that evade traditional security tools.

Hybrid cloud environments (public cloud + on prem) complicate log collection, visibility, and response coordination.

This research evaluates how open source XDR and SOAR tools can support APT detection and response in hybrid cloud environments.

80% The percentage of Companies in the past year that have been affected by Cloud Security Incidents

180days Organisations take an average of over 180 days to detect a cyber breach

60% Misconfigurations and lack of visibility account for over 60% of cloud related security incidents

KEY LITERATURE

Alshamrani et al. 2019 · ~195 cit.
Survey of APT techniques, attack stages, detection methods, and mitigation strategies that established the lifecycle framework referenced across the field.
Gap: no end-to-end detection

Kinyua & Awuah 2021 · ~100 cit.
AI/ML in SOAR - SOAR platforms to automate and accelerate security incident response in SOC environments.
Gap: no open-source SOAR eval

Jiang et al. 2025 · ~10 cit.
417 paper ATT&CK review - how the MITRE ATT&CK framework is applied across threat intelligence, incident response and attack modelling.
Gap: ATT&CK not live-tested

Ismail et al. 2025 · emerging
Hyper-automation SOAR architecture - that dynamically generates adaptive playbooks, replacing no-code workflows to improve SOC response precision.
Gap: no SOAR benchmark

Buchta et al 2024 · recent
A review of APT detection systems, comparing their evaluation datasets, and performance across detection approaches from ML to graph-based analysis.
Gap: no hybrid cloud scope

CONVERGING GAPS IDENTIFIED ACROSS THE LITERATURE

No hybrid cloud scope
All detection studies use on-premises or single-cloud environments

No open-source SOAR eval
Commercial platforms dominate; Shuffle has no academic treatment

No full kill-chain coverage
Existing tools detect 1–2 APT stages, not end-to-end campaigns

Legacy datasets
85%+ of IDS studies use DARPA 1998 — unsuitable for modern APTs

ATT&CK not validated live
Framework widely cited theoretically; rarely tested in real toolchains

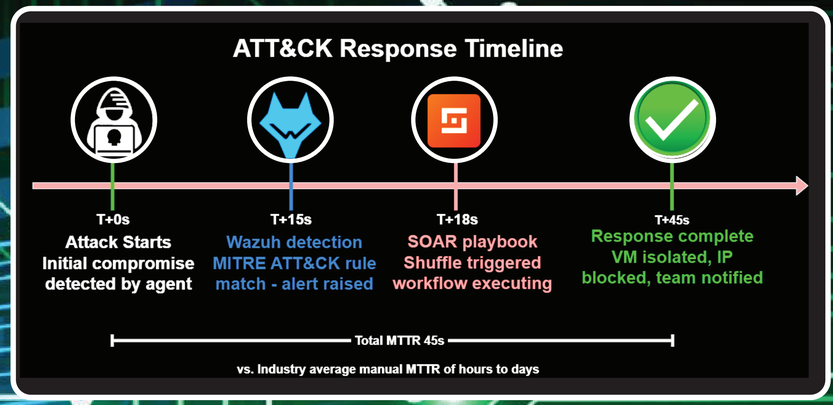
SOAR playbook rigidity
Rule-based workflows fail against novel or unseen APT techniques

THIS DISSERTATION'S CONTRIBUTION TO THE LITERATURE

RESEARCH GAP ADDRESSED

No published academic work has experimentally evaluated Wazuh (XDR) and Shuffle (SOAR) together for APT detection and automated response in a hybrid cloud environment, using MITRE ATT&CK-aligned simulation (Atomic Red Team) as the data source.

This study directly addresses all six converging gaps identified above.



RESEARCH QUESTIONS

RQ1 — Detection capability. How effectively does Wazuh detect multi-stage APT attacks across a hybrid cloud environment?

RQ2 — Automated response. To what extent does Shuffle SOAR automate incident response to APT alerts generated by Wazuh, and what are its limitations?

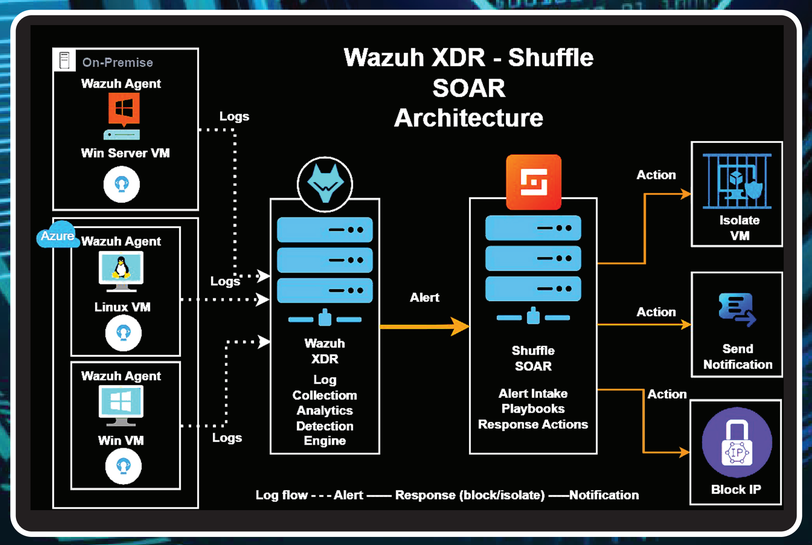
RQ3 — Commercial comparison. How does the Wazuh and Shuffle open-source stack compare to Microsoft Sentinel for APT detection and response in a hybrid cloud environment?

RQ4 — Hybrid cloud consistency. How consistent is APT detection and response when attack activity crosses the boundary between on-premises and cloud infrastructure?

Hypotheses
Open source XDR+SOAR can achieve detection coverage comparable to commercial tools, at lower licensing cost, but with higher configuration overhead.

REFERENCES

Alshamrani 2019
Kinyua & Awuah 2021
Jiang et al 2025
Ismail et al 2025
Buchta et al 2024



RESEARCH METHODOLOGY

Build a lab scale hybrid cloud environment (e.g., Azure + on-prem VMs).

Deploy selected open source XDR (Wazuh) and SOAR (Shuffle).

Simulate APT like behaviours using MITRE ATT&CK aligned techniques (e.g., via Atomic Red Team).

Collect logs, alerts, and response timings; measure detection accuracy, false positives, and response latency.

Technologies:
XDR: Wazuh
SOAR: Shuffle
Cloud: Azure
Simulation: Atomic Red Team

EARLY INDICATIONS:

"Initial tests confirm successful integration of XDR and SOAR components;
APT simulation runs are underway."

Next steps:

- Complete full APT simulation campaigns across multiple scenarios.
- Fine tune detection rules and SOAR playbooks.
- Analyse performance metrics and compare with commercial benchmarks or literature.
- Finalise findings and recommendations for practitioners.