Problem context

Modern SIEM platforms already collect and correlate vast amounts of logs, but analysts still face high alert volume, noisy rules, and slow investigation cycles in the SOC.
Static correlation rules often fire in isolation, miss slow or multi-stage attacks, and generate false positives that exhaust Tier-1 teams.

At the same time, many organizations run a “20-rule” baseline pack that covers critical use cases such as brute-force authentication, privilege abuse, lateral movement, malware detections, and data exfiltration, but these rules are rarely tuned continuously.

Proposed solution: SIEM Co-Pilot Agent

The mini project proposes a “SIEM Co-Pilot” made of a small set of AI agents that sit on top of an existing SIEM and SOAR stack and operate on alerts generated by the standard 20 SIEM rules.
Instead of replacing correlation rules, the agents consume them as input, enrich them with context, and then decide whether to escalate, suppress, or auto-respond.
The system is organized into three logical agents: a Detection Triage Agent, a Context Enrichment Agent, and a Response Orchestration Agent, each communicating with the SIEM and security tools through APIs.

The Detection Triage Agent continuously monitors alerts produced by the 20 baseline rules, clusters similar alerts, and calculates a simple risk score using features like asset criticality, user role, and number of correlated events.
This risk scoring reflects SIEM best practices of prioritizing high-impact, high-likelihood events while reducing noise from low-value detections.

The Context Enrichment Agent automatically calls external systems such as asset inventory, vulnerability scanners, EDR, and threat-intel feeds to gather additional evidence for each high-risk alert.
This mirrors how human analysts investigate alerts but compresses the time by automating repetitive “swivel-chair” lookups across multiple consoles.

The Response Orchestration Agent uses predefined playbooks to propose or execute actions such as isolating an endpoint, disabling a compromised account, blocking an IP on the firewall, or opening an incident ticket.
In low-risk or uncertain cases, it only drafts a recommended response for human

approval; in high-confidence cases (for example, malware plus confirmed C2 traffic), it can trigger fully automated containment through SOAR integrations.

Applying the 20 SIEM rules

The project treats the 20 SIEM rules as the “signal layer” and focuses on making them smarter rather than rewriting them.

For authentication-focused rules (password spray, unusual login locations, impossible travel), the agents correlate identity logs with VPN, IAM, and endpoint data to distinguish real attacks from user error, tuning thresholds over time.
For privilege-escalation and admin-activity rules, the agents cross-check change windows, known maintenance tasks, and vulnerability context before deciding if an event should be escalated as suspicious.

For malware and EDR-driven rules, the agents combine SIEM alerts with endpoint process trees and sandbox verdicts to raise the risk score only when there is evidence of execution or lateral movement, cutting down on noisy detections.
For data-exfiltration and network-anomaly rules, the agents factor in business context like normal data transfer patterns for that host or user, aligning with behavior-based SIEM best practices.
Over time, feedback from analysts (marking alerts as true or false positive) is fed back into the agents so they learn to prioritize which of the 20 rules matter most in that specific environment.

Evaluation and project scope

The mini project can be scoped to a lab SIEM (or a cloud SIEM trial) with a limited data set such as VPN, Windows AD, and EDR logs, plus a small SOAR or scripting layer for automated actions.
Success can be measured by comparing before-and-after metrics: alert volume from the 20 rules, percentage of alerts auto-closed as benign, time to triage high-severity alerts, and number of incidents where the agent triggered a correct automated response.
By the end, the outcome is a working prototype that demonstrates how AI agents can sit on top of a traditional rule-based SIEM, make the canonical 20 rules more effective, and move the SOC towards an autonomous, agent-driven operating model.