modiqo

Modiqo Rote for Security Operations (SOC)

Turn Repetitive Investigations into Deterministic Plays

Use AI to investigate once. Use Rote to execute every time.

Rote captures successful AI-assisted investigations and converts them into reusable Plays that execute consistently, reduce analyst effort, and continuously improve over time.

AI discovers.
Rote remembers.
Your SOC stays ahead.

01 / THE CHALLENGE

Every investigation starts from scratch.

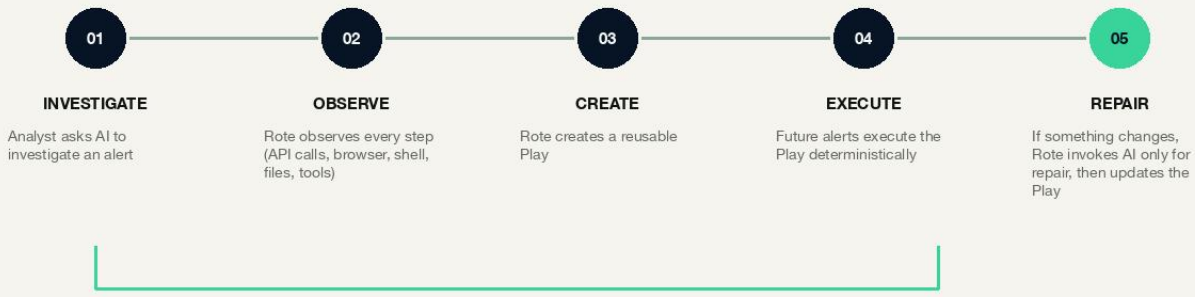
SOC analysts spend most of their day repeating the same investigative workflows across SIEM, EDR, threat intelligence, identity, cloud, and ticketing systems.

Each investigation starts from scratch:

01 Different prompts
02 Different steps
03 Different results
04 High AI cost
05 Inconsistent outcomes

This slows down triage and creates risk.

02 / HOW ROTE WORKS



03 / BENEFITS

- **Deterministic Investigations**
  Execute the same investigation consistently across every analyst.
- **Reduce AI Cost**
  Eliminate repeated reasoning. Run Plays instead of rediscovering workflows.
- **Faster Triage**
  Reduce investigation time from minutes to seconds.
- **Capture Analyst Expertise**
  Senior analysts build Plays once. The entire SOC benefits immediately.
- **Self-Healing Automation**
  When APIs, schemas, or workflows change, Rote repairs the Play and versions the update.
- **Continuous Improvement**
  Every repaired or enhanced Play becomes better for the next investigation.

04 / EXAMPLE SOC PLAY

Investigate suspicious shell execution

COLLECT	ENRICH	ACT
01 Retrieve Falcon endpoint telemetry	01 Query threat intelligence feeds	01 Generate investigation summary
02 Collect process tree and parent process	02 Pull recent DNS activity	02 Create ServiceNow incident
03 Check user identity and account details	03 Collect network connections	03 Attach evidence and artifacts
04 Query Active Directory / Entra ID	04 Retrieve recent authentication events	04 Notify responders (Slack / Teams)
05 Check VirusTotal and reputation	05 Correlate with SIEM alerts	05 Store Play for future use

THE CONTRACT No prompt engineering. No repeated reasoning. Same investigation every time.

05 / INTEGRATES WITH YOUR EXISTING SECURITY STACK

- CrowdStrike Falcon
- Microsoft Defender
- Microsoft Sentinel
- Splunk
- IBM QRadar
- Google Chronicle
- Palo Alto Cortex
- Okta / Entra ID
- ServiceNow
- Jira
- Slack / Teams
- Threat Intelligence Platforms
- Any REST API
- Browser, shell, files, tools

Bring your stack. Rote works with it.

06 / IDEAL SOC USE CASES

- Alert triage
- Cloud security investigations
- IOC enrichment
- Compliance evidence collection
- Incident investigation
- Vulnerability validation
- Malware analysis
- Case preparation
- Identity investigations
- Executive incident summaries
- Insider threat
- SOC runbooks
- Threat hunting
- Shift handoff automation

AI discovers.
Rote remembers.
Your SOC stays ahead.

WHY MODIQO ROTE?

Rote combines the power of AI with deterministic execution to turn how your team works today into automated Plays you can trust tomorrow.

01	02	03	04
Discover once.	Execute forever.	Operate with confidence.	Continuously improve.