Tarun yadav

IDEAS FOR DEVELOPMENT TEAM

1.IMPLEMENTATION OF ACTION MATRIX

Action Matrix for alert triage ,proposed to a development team as part of an alert-handling workflow, with benefits and future extensibility (AI enrichment) .The **Action Matrix** is a **decision framework** that converts raw security alerts into **guided, prioritized responses** using a calculated **Action Score**.

Instead of analysts manually interpreting every alert, the system :

- Scores each alert
- Sorts alerts by urgency
- Maps each score range to a predefined guided response .
- **Action Score** = Severity × Attack Vector Risk × Instant Attention Score

So , severity wise (Business impact ,Data loss, service disruption, compliance risk) generally from detection logic or SIEM rules.Attack Vector Risk (External vs internal ,Known exploit availability ,Exposure surface).Instant Attention Score (Time sensitivity ,Indicates how quickly action is required).

Example:

- No urgency = 1
- Needs review today = 3
- Immediate response required = 10

The **Guided action** can comprises of various task based on the score calculated like review any queue , investigate SLA , immediate containment or eradication and log analysis only no action required.

So, this reduces analyst decision fatigue ,Ensures consistent response quality and makes action explainable.

Benifits to development and security teams are :

- NO analyst dependent , priority based objective
- Reduce alert fatigue
- Faster responses
- Built in documentation for response and audit.

We can use AI for pattern recognition across alerts , False-positive suppression using historical outcomes , guided response by AI , adaptive playbooks and automation.

2.RBAR – ROLE BASED ALERT RESOLUTION

It introduces **role-aware alert delivery and resolution workflows** integrated with the SIEM and the goal is to ensure **the right alerts reach the right analysts at the right time**, based on priority, complexity, and risk .

So , This model directly improves:

- SOC productivity
- Resolution accuracy
- Response time reduction
- Analyst utilization across Tier 1 / 2 / 3

When alerts are generated and are enriched (Action Matrix, asset context, threat intel) they will be classified according to the score.RBAR logic assigns alerts to Appropriate **SOC tier** ,Appropriate **role level** (Junior / Senior) or Appropriate **resolution workflow** .

So, The alert delivery will not be broadcasted to everyone but assessed based on rules and priority.Despite that correlation could be performed if access granted. The distribution will be based upon **Action score , Alert category , Required Expertise and business criticality.**

For example junior analyst handling Initial triage ,alert validation while senior handling **deep investigation ,correlation across alerts** , root cause analysis and response recommendations and Exper Incident Response Team handling Malware analysis , advance threat hunting and stratergic containment decisions.

This type of architecture performs segregation of duties which reduces operational risk , supports audit and compliance requirements and **prevent single point decision failure**. So , juniors can focus on repeatable tasks , seniors focus on complex cases and expertise is applied efficiently.

Result

- Better resolution quality
- Faster response times
- Improved analyst confidence & growth

So Action matrix determine what is urgent and RBAR defines who should handle it.