Tarun yadav

Alert-Triage-Workflow

Goal - Demonstrate alert detection, prioritization, investigation, containment, and remediation in a cloud SOC workflow.

As Cloud environments are dynamic and complex,making it difficult for security engineers to quickly detect, investigate, and remediate attacks and cloud security engineer often face problems and challanges of handling numerous alerts at same time , which leads to missclassification of incidents and delayed response due to no clear triage path. The lab simulates multiple attacks (IAM enumeration, SSH enumeration, bucket enumeration, API fuzzing, unauthorized S3 upload) against a LocalStack environment monitored by Wazuh.Flow is designed to mirror an actual **SOC workflow.**

Alert → Triage → Investigation → Correlation → Remediation → Post-Incident Learning.

We used various proposed features like **Alert Dashboard** (Centralized view of all alerts with severity, resource, timestamp, and status.**Alert Details & Correlation Panel** (Drill-down to logs, source IP, affected resources, and timeline view to correlate multiple attack vectors).**MITRE ATT&CK Mapping** (Automatic tagging of alerts with relevant cloud MITRE techniques to guide investigation). **Post-Incident Notes & Rule Tuning** (Record findings, update detection rules, and suggest preventive measures for future attacks).

High Priority features directly reducing response time and risk (Alert Dashboard, Investigation Timeline, Response Actions) ensures the engineer can detect and mitigate attacks efficiently and **Medium Priority** features that improve understanding and long-term effectiveness (MITRE mapping, post-incident notes). They enhance strategic security posture but are not critical for immediate containment and **Low Priority (optional for future)** Automation and predictive recommendations, which are innovative but require mature data and integration .

For **Priortity decision making** severity is very importrant as if there are **multiple intentional attacks** at the same time in complex enviornment ,then impact is propotional to risk involed and criticality.So choosig Critical over informatives and Action priortization - Containment of attack rather than going for patching single vulnerability. So **action plan and guided response action** become very useful.

I have also proposed two ideas from development point of view ,which I think can enhance the action plan and decision making become more efficient in a **SOC or SIEM** enviornment. First is **Action Matrix** (Listing down a guided response or action list based on action score) and second is **Role based access resolution** (integrating Role based Access model to solve the alerts through a multi tier , multi level or by multi role capabilities.

So ,There is a need for a **UNIFIED alert triage workflow** that helps security engineers to quickly investigate, assess impact, and remediate cloud security incidents , performing Containment actions , Root cause analysis and eradication.