Alert Triage Workflow

Problem Statement

Cloud security teams receive a high volume of alerts, but triaging them is slow because context is scattered across tools (cloud logs, IAM, asset inventory, threat intel). Security engineers waste time figuring out: *Is this real? What's impacted? What should I do next?*

We need a workflow that helps engineers quickly:

1. validate if an alert is real,
2. understand blast radius,
3. take remediation action,
4. document resolution.

Personas

1.) Cloud Security Engineer (SOC / SecOps)

- Works in shifts, handles many alerts/day
- Needs fast investigation and clear next steps
- Values accuracy + speed
- Often suffers from alert fatigue
- Wants confidence before taking remediation actions

2.)Security Manager (cares about MTTR, SLA, reporting)

Pain Points (Alert Triage Workflow)

1. Too many alerts (Alert fatigue)

Security engineers receive hundreds/thousands of alerts daily, making it hard to focus on what is truly critical.

---

2. High false positives

Many alerts are not real threats, so engineers waste time investigating noise instead of real incidents.

---

3. Context is scattered across tools

To validate one alert, engineers must switch between:

- Cloud logs (CloudTrail / Azure logs / GCP audit logs)
- IAM console
- asset inventory
- SIEM tools
- threat intel sources
  This slows down investigation.

---

4. Hard to understand blast radius

Engineers struggle to quickly answer:

- What resources are affected?
- What data could be exposed?
- Is it limited to one account or spreading?

---

5. Slow investigation due to lack of timeline

Alerts don’t show a clear sequence of events, so engineers manually reconstruct what happened.

---

6. No clear “next step” guidance

Even if an alert is real, the tool often doesn’t suggest what action should be taken immediately.

---

7. Manual remediation is risky

Engineers hesitate to take action (disable key, block IP, rollback policy) because they fear breaking production systems.

---

8. Poor collaboration + handoff

When shifts change or alerts are escalated, important investigation details are lost due to missing notes and documentation.

---

9. Difficult to track ownership

Alerts may stay unassigned, duplicated, or ignored because it's unclear who is handling them.

---

10. Reporting and audit documentation is painful

Security managers need metrics like MTTR, SLA compliance, evidence logs, but engineers often don't document properly due to time pressure.

Proposed Features

1. Alerts Inbox / Alerts Dashboard

- Alerts list/table view (all alerts in one place)
- Severity tags (Critical / High / Medium / Low)
- Alert status (New / Assigned / Investigating / Resolved)
- Timestamp (when detected)
- Cloud account name + ID
- Region (AWS/GCP/Azure region)
- Resource affected (VM, bucket, IAM user, database etc.)
- Alert type/category (IAM, Network, Storage, Malware, Compliance)
- Confidence score (Real vs Possible False Positive)

2. Filtering + Sorting

- Filter by severity
- Filter by cloud account
- Filter by alert category/type
- Filter by time range (last 1 hr / 24 hr / 7 days)
- Filter by status (new/in progress/resolved)
- Sort by severity
- Sort by newest
- Sort by confidence score

---

3. Alert Preview Panel (Quick View)

- Quick summary in plain English
- Resource impacted
- Quick severity explanation
- Recommended next action button

Investigation / Alert Details Page

4. Alert Summary Card

- What happened (plain language explanation)
- Who triggered it (user/service account)
- Where (cloud provider + account + region)
- When it happened
- Severity + risk reason
- Confidence score
- MITRE ATT&CK mapping (optional bonus)

---

5. Evidence / Logs Viewer

- CloudTrail / Activity logs shown directly
- Log filtering inside the alert
- Raw log + simplified readable log view
- Download/export evidence logs

---

6. Attack Timeline / Event Timeline

- Timeline showing sequence:
  - login → policy change → resource access → suspicious action
- Highlight suspicious events in red
- Show exact timestamps

---

7. Blast Radius / Impact Analysis

- What resources are affected
- What data could be exposed
- Connected assets (network, IAM, storage)
- Dependencies map (resource graph)

---

8. IAM Context View

- IAM user/role involved
- Permissions summary
- Recently used permissions
- Policy diff (what changed recently)
- Risky permissions highlighted (AdminAccess, wildcard permissions)

---

9. Related Alerts / Correlation

- Group alerts that may be connected
- “Possible campaign detected”
- “Similar alert happened 2 days ago”
- Correlation based on:
  - same IP
  - same user
  - same resource
  - same account

Actions + Remediation

10. Recommended Actions Panel

- Disable access key

- Force password reset
- Require MFA
- Quarantine VM
- Block IP address
- Rollback policy change
- Remove public access from bucket
- Rotate secrets/keys
- Terminate suspicious session

---

11. One-click Playbooks

- Pre-built remediation workflows
- Confirmation popup before execution
- Auto-run scripts (optional backend)

Example playbooks:

- “Compromised access key response”
- “Public S3 bucket remediation”
- “Suspicious IAM privilege escalation”

---

12. Assignment + Escalation

- Assign to me
- Assign to teammate
- Escalate to Incident Response team
- Add priority / SLA tag

---

13. Collaboration Tools

- Comments section inside alert
- Mention/tag teammates (@name)
- Add investigation notes
- Attach screenshots/logs

Resolution / Closure

14. Resolution Screen

- Mark resolved / mitigated / false positive
- Add root cause category:
  - misconfiguration
  - compromised credentials
  - insider misuse
  - expected behavior
  - test activity

---

15. Audit Trail

- Record who took what action and when
- Track remediation history
- Evidence retention for compliance

---

16. Auto Incident Report Generator (Bonus)

- Generate a summary report:
  - what happened
  - impact
  - timeline
  - actions taken
  - recommendations

Reporting & Analytics

17. Metrics Dashboard

- Total alerts per day/week
- Alerts by severity
- MTTR (mean time to resolve)
- MTTT (mean time to triage)
- False positive rate
- Top alert categories
- Top risky accounts/resources

---

18. Continuous Improvement Suggestions

- Recommend detection rule tuning
- Recommend guardrails (ex: enforce MFA, restrict wildcard IAM)

Integrations (Bonus)

- Jira / ServiceNow ticket creation
- Slack / Email notifications
- SIEM integration (Splunk, Sentinel)
- Cloud provider API integration (AWS/Azure/GCP)

AI / Smart Features (Optional)

- AI-generated investigation summary
- AI-suggested severity adjustment
- AI anomaly detection (user unusual behavior)
- AI “next best action” recommendation

RICE Formula

RICE Score = (Reach × Impact × Confidence) / Effort

Assumptions:

- Reach = # of engineers / alerts impacted per month (scale 1–10)
- Impact = value delivered (0.25 low, 0.5 med, 1 high, 2 massive, 3 critical)
- Confidence = % confidence in estimate (50%, 80%, 100%)
- Effort = engineering/design effort in person-weeks (1–10)

RICE Prioritization Table (Alert Triage Workflow)

Feature	Reach (1-10)	Impact (0.25-3)	Confidence (0.5-1)	Effort (1-10)	RICE Score
Alerts Inbox + Severity Sorting	10	3	0.9	3	**90**
Alert Details Page (Summary + Context)	10	3	0.85	4	**63.75**
Filters (Account, Status, Time, Type)	9	2	0.9	3	**54**
Evidence Logs Viewer	8	2	0.8	4	**32**
Recommended Remediation Actions Panel	7	2	0.75	5	**21**
Investigation Timeline View	7	2	0.7	5	**19.6**
Assign / Escalate Workflow	6	1.5	0.85	3	**25.5**
Mark False Positive + Feedback Loop	7	1.5	0.8	3	**28**
Blast Radius / Impact Analysis	6	2	0.65	7	**11.14**
Related Alerts Correlation	5	2	0.6	7	**8.57**
Resolution Screen + Notes	6	1.5	0.85	4	**19.1**
Audit Trail (Actions Log)	6	1.5	0.8	4	**18**
Jira/ServiceNow Ticket Integration	4	1.5	0.6	6	**6**
AI Investigation Summary	4	2	0.5	8	**5**
Auto Incident Report Generator	3	1.5	0.5	7	**3.21**

Final Prioritization (Based on RICE)

P0 (Build First – MVP)

1. Alerts Inbox + severity sorting (**90**)
2. Alert Details page with context (**63.75**)
3. Filters (**54**)
4. Mark false positive + feedback loop (**28**)
5. Assign/Escalate workflow (**25.5**)
6. Evidence logs viewer (**32**) *(core for investigation)*

P1 (Build Next)

7. Recommended remediation actions (**21**)
8. Investigation timeline (**19.6**)
9. Resolution screen + notes (**19.1**)
10. Audit trail (**18**)

P2 (Later / Advanced)

11. Blast radius analysis (**11.14**)
12. Related alert correlation (**8.57**)
13. Jira integration (**6**)
14. AI summary (**5**)
15. Auto incident report (**3.21**)

Success Metrics

1. Speed / Efficiency Metrics

- **Mean Time to Triage (MTTT)**
  → Avg time from alert creation to first action (assign/investigate)
- **Mean Time to Resolve (MTTR)**
  → Avg time from alert creation to alert closure
- **Time spent per alert investigation**
  → Avg investigation duration per alert

2. Quality Metrics

- **False Positive Rate (%)**
  → % alerts marked as false positive
- **True Positive Detection Rate**
  → % alerts that resulted in real confirmed incidents
- **Repeat incident rate**
  → % similar alerts recurring within 7/30 days (should go down)

---

3. Workflow Adoption Metrics

- **% alerts investigated using the workflow UI**
  (instead of jumping to external tools)
- **% alerts resolved using recommended remediation actions**
  → shows usefulness of action panel/playbooks
- **Filter usage rate**
  → indicates whether triage filters are valuable

---

4. Collaboration Metrics

- **Escalation rate**
  → % alerts escalated to IR team
  (should decrease if triage becomes easier)
- **Average time to assign an alert**
  → measures workload distribution improvement

---

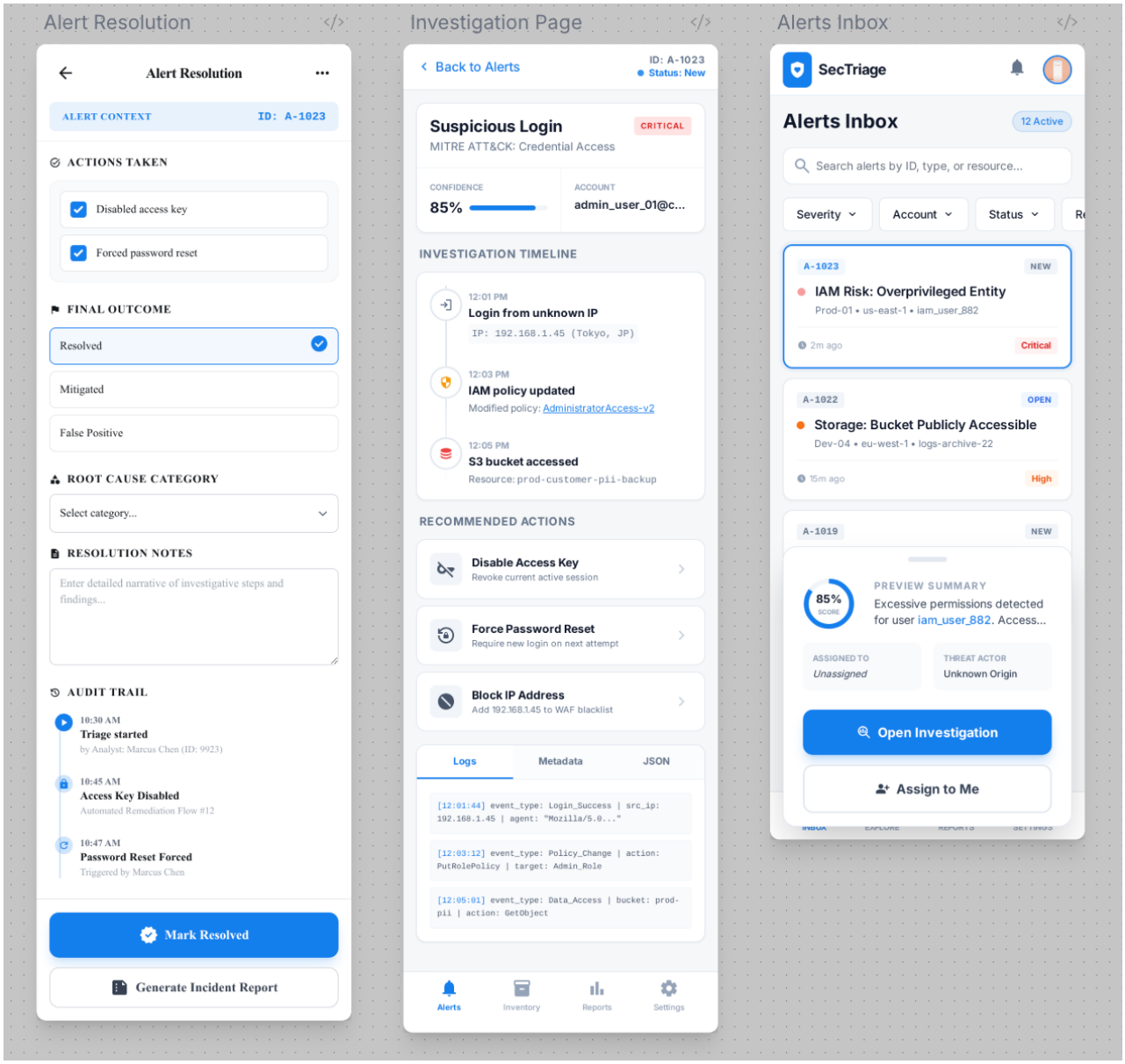
5. Compliance / Documentation Metrics

- **% alerts closed with investigation notes attached**
- **% alerts with complete audit trail (actions + evidence)**

North Star Metric

% Critical Alerts Resolved Within SLA

Because it directly shows: speed + reliability + security impact.


Alert Resolution
Alert Resolution
ALERT CONTEXT
ID: A-1023
ACTIONS TAKEN
Disabled access key
Forced password reset
FINAL OUTCOME
Resolved
Mitigated
False Positive
ROOT CAUSE CATEGORY
Select category...
RESOLUTION NOTES
Enter detailed narrative of investigative steps and findings...
AUDIT TRAIL
10:30 AM
Triage started
by Analyst: Marcus Chen (ID: 9923)
10:45 AM
Access Key Disabled
Automated Remediation Flow #12
10:47 AM
Password Reset Forced
Triggered by Marcus Chen
Mark Resolved
Generate Incident Report
Investigation Page
Back to Alerts
ID: A-1023
Status: New
Suspicious Login
CRITICAL
MITRE ATT&CK: Credential Access
CONFIDENCE
85%
ACCOUNT
admin_user_01@c...
INVESTIGATION TIMELINE
12:01 PM
Login from unknown IP
IP: 192.168.1.45 (Tokyo, JP)
12:03 PM
IAM policy updated
Modified policy: AdministratorAccess-v2
12:05 PM
S3 bucket accessed
Resource: prod-customer-pii-backup
RECOMMENDED ACTIONS
Disable Access Key
Revoke current active session
Force Password Reset
Require new login on next attempt
Block IP Address
Add 192.168.1.45 to WAF blacklist
Logs
Metadata
JSON
[12:01:44] event_type: Login_Success | src_ip: 192.168.1.45 | agent: "Mozilla/5.0..."
[12:03:12] event_type: Policy_Change | action: PutRolePolicy | target: Admin_Role
[12:05:01] event_type: Data_Access | bucket: prod-pii | action: GetObject
Alerts
Inventory
Reports
Settings
Alerts Inbox
SecTriage
Alerts Inbox
12 Active
Search alerts by ID, type, or resource...
Severity
Account
Status
A-1023
NEW
IAM Risk: Overprivileged Entity
Prod-01 • us-east-1 • iam_user_882
2m ago
Critical
A-1022
OPEN
Storage: Bucket Publicly Accessible
Dev-04 • eu-west-1 • logs-archive-22
15m ago
High
A-1019
NEW
85%
SCORE
PREVIEW SUMMARY
Excessive permissions detected for user iam_user_882. Access...
ASSIGNED TO
Unassigned
THREAT ACTOR
Unknown Origin
Open Investigation
Assign to Me