# Submission: Business-Aware Alert Triage Workflow

## 1. Problem Statement & User Persona

### Problem Statement

Cloud security teams face a decision crisis. Modern infrastructure generates thousands of alerts daily across multiple accounts, but the data is presented as raw technical noise, stripped of business context.

A critical alert on a public S3 bucket storing payment transaction logs looks identical to a public S3 bucket in a sandbox test environment. Both show 'High Severity,' but the business impact is worlds apart. Without context, engineers waste hours context-switching between tools to find basic information, leading to alert fatigue, missed SLAs, and analyst burnout.

The core problem is not volume; it is a lack of decision intelligence.

### User Persona: Senior Cloud Security Engineer

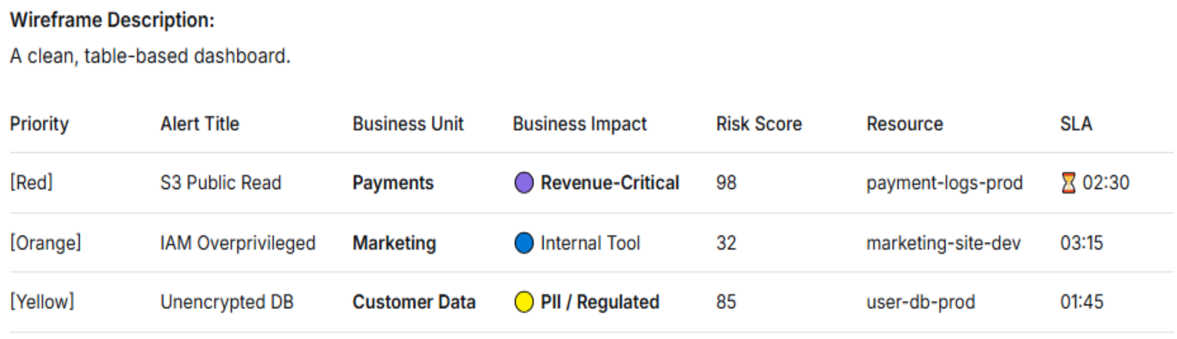
Background: 6 years experience, works in a multi-cloud enterprise (AWS/Azure) with 50+ accounts.
Goal: Triage alerts accurately and quickly to meet compliance SLAs while protecting the business.
Pain Points:
- Spends 40% of time gathering context.
- Cannot distinguish revenue-impact risks from low-stakes misconfigurations.
- Documentation is manual and tedious.

## 2. The Solution: 3-Screen Wireframe

Design Philosophy: Context over Volume.

### Screen 1: The Business-Aware Queue (The Inbox)

**Purpose**: Help prioritize based on business impact, not technical severity.



**Wireframe Description:**

A clean, table-based dashboard.

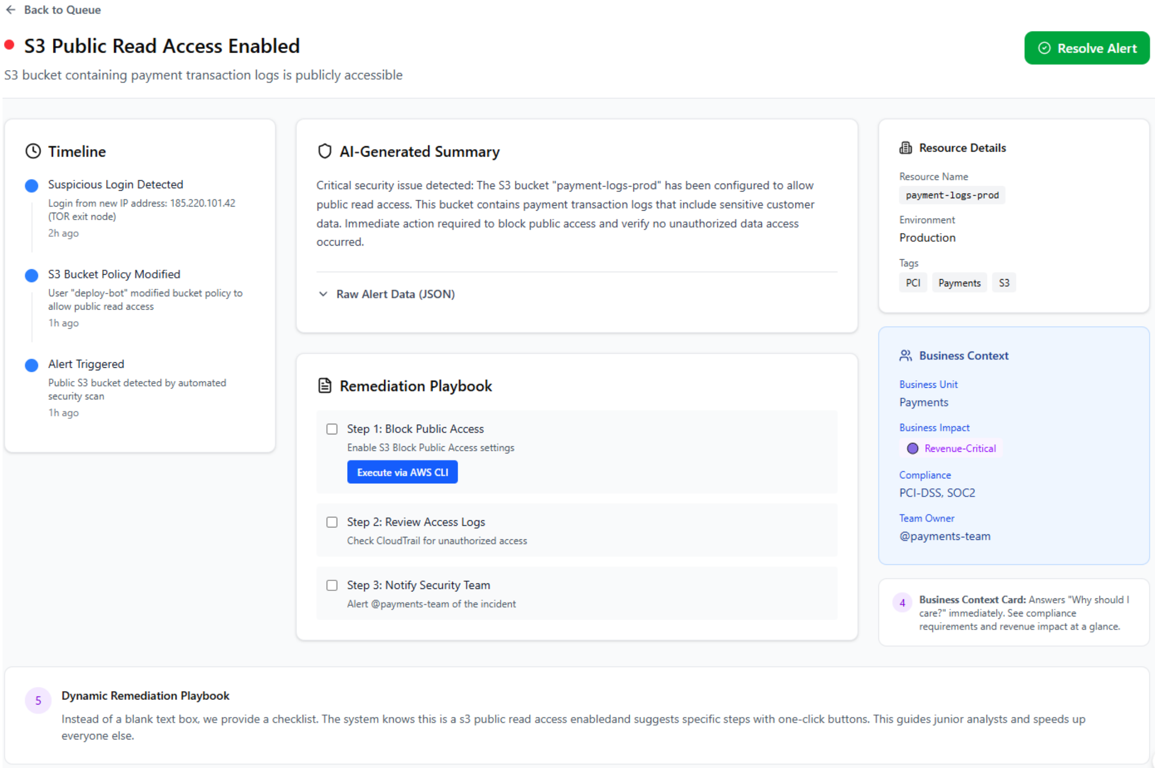
| Priority | Alert Title | Business Unit | Business Impact | Risk Score | Resource | SLA |
|---|---|---|---|---|---|---|
| [Red] | S3 Public Read | **Payments** | 🟣 **Revenue-Critical** | 98 | payment-logs-prod | ⏳ 02:30 |
| [Orange] | IAM Overprivileged | **Marketing** | 🔵 Internal Tool | 32 | marketing-site-dev | 03:15 |
| [Yellow] | Unencrypted DB | **Customer Data** | 🟡 **PII / Regulated** | 85 | user-db-prod | 01:45 |

**Key UI Elements & Annotations:**

- **Annotation 1 (The "Business Impact" Badge):** *"We replace abstract severity with concrete business context. A red badge here means 'This affects revenue.' Arjun knows immediately that the Payments alert takes priority over the Marketing alert, even if the Marketing alert was technically 'High' severity."*

- **Annotation 2 (Risk Score):** *"The score is calculated as:* Severity × Asset Criticality × Internet Exposure × Business Impact. *This ensures the queue is sorted by actual risk to the company, not just the cloud provider's severity rating."*
- **Annotation 3 (SLA Timer):** *"A visible countdown clock enforces compliance without needing to check a separate system. It adds healthy pressure to resolve business-critical issues first."*

## Screen 2: Unified Investigation Workspace



● S3 Public Read Access Enabled

S3 bucket containing payment transaction logs is publicly accessible

**Timeline**

● Suspicious Login Detected
Login from new IP address: 185.220.101.42 (TOR exit node)
2h ago

● S3 Bucket Policy Modified
User "deploy-bot" modified bucket policy to allow public read access
1h ago

● Alert Triggered
Public S3 bucket detected by automated security scan
1h ago

**AI-Generated Summary**

Critical security issue detected: The S3 bucket "payment-logs-prod" has been configured to allow public read access. This bucket contains payment transaction logs that include sensitive customer data. Immediate action required to block public access and verify no unauthorized data access occurred.

Raw Alert Data (JSON)

**Remediation Playbook**

□ Step 1: Block Public Access
Enable S3 Block Public Access settings

□ Step 2: Review Access Logs
Check CloudTrail for unauthorized access

□ Step 3: Notify Security Team
Alert @payments-team of the incident

**Resource Details**

Resource Name
`payment-logs-prod`
Environment
Production
Tags
PCI Payments S3

**Business Context**

Business Unit
Payments
Business Impact
● Revenue-Critical
Compliance
PCI-DSS, SOC2
Team Owner
@payments-team

4 **Business Context Card:** Answers "Why should I care?" immediately. See compliance requirements and revenue impact at a glance.

5 **Dynamic Remediation Playbook**
Instead of a blank text box, we provide a checklist. The system knows this is a s3 public read access enabledand suggests specific steps with one-click buttons. This guides junior analysts and speeds up everyone else.

**Purpose**: Eliminate context-switching with a three-panel layout.

**Left Panel:** Timeline of related events.
**Center Panel:** Raw logs + AI-generated summary.
**Right Panel:** Business Context Hub (Business Unit, Revenue Impact, Compliance, Owner).

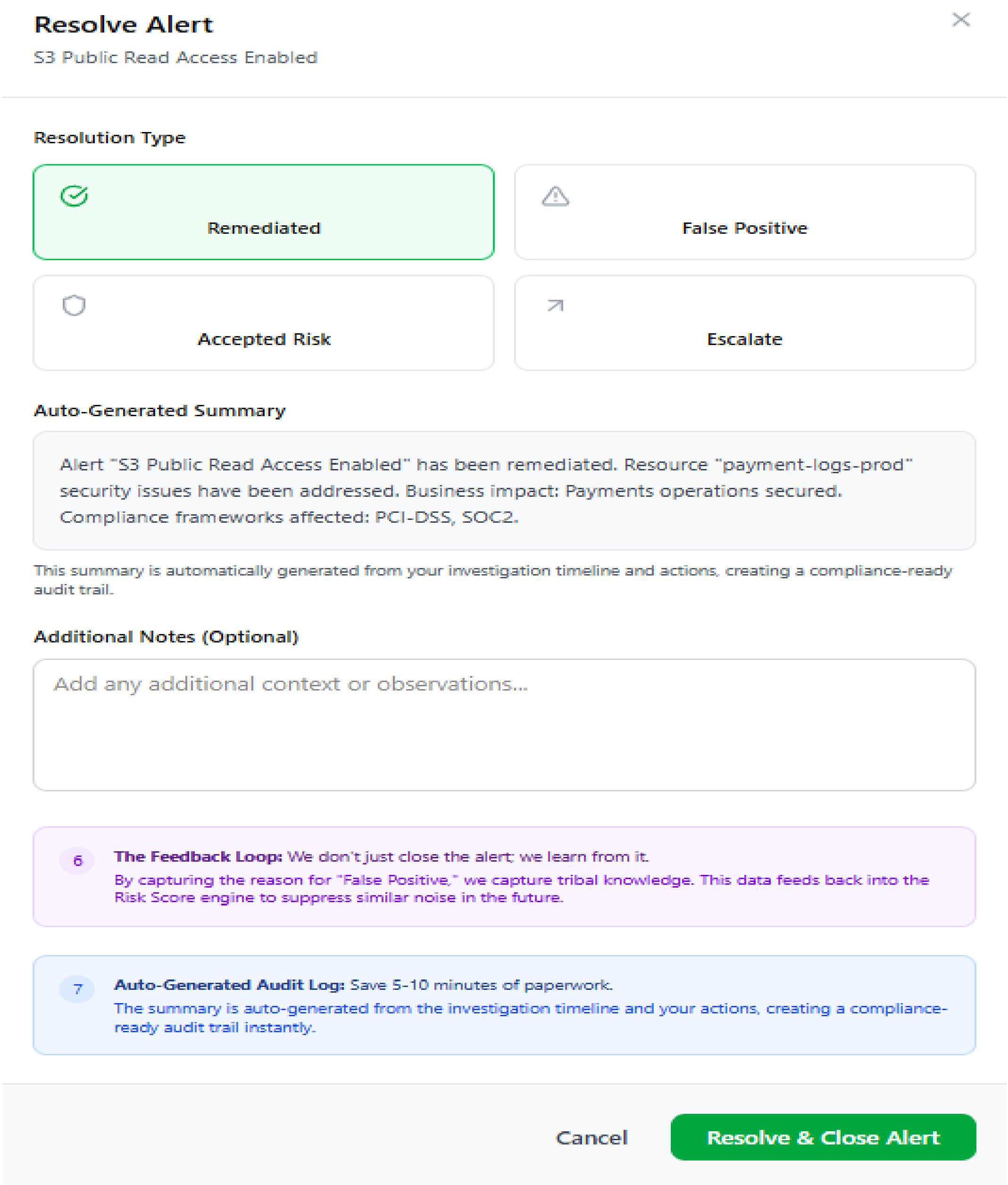
Dynamic Remediation Playbook suggests next steps with guided actions.

**Key UI Elements & Annotations:**

- **Annotation 4 (The Business Context Card):** *"This is the most important part of the screen. It answers 'Why should I care?' immediately. Arjun sees 'PCI' and 'Revenue Impact: High' and knows this alert requires immediate, careful action. He also sees the team owner, so he knows who to tag if he needs help."*
- **Annotation 5 (Dynamic Remediation Playbook):** *"Instead of a blank text box, we provide a checklist. The system knows this is a public S3 bucket and suggests 'Step 1: Block Public Access' with a one-click button. This guides junior analysts and speeds up everyone else."*

## Screen 3: The Resolution Hub

Purpose: Close alerts efficiently and capture learning.



**Resolve Alert**

S3 Public Read Access Enabled

Resolution Type

- ✓ Remediated
- ⚠ False Positive
- Accepted Risk
- ↗ Escalate

Auto-Generated Summary

Alert "S3 Public Read Access Enabled" has been remediated. Resource "payment-logs-prod" security issues have been addressed. Business impact: Payments operations secured. Compliance frameworks affected: PCI-DSS, SOC2.

This summary is automatically generated from your investigation timeline and actions, creating a compliance-ready audit trail.

Additional Notes (Optional)

Add any additional context or observations...

6 **The Feedback Loop:** We don't just close the alert; we learn from it.
By capturing the reason for "False Positive," we capture tribal knowledge. This data feeds back into the Risk Score engine to suppress similar noise in the future.

7 **Auto-Generated Audit Log:** Save 5-10 minutes of paperwork.
The summary is auto-generated from the investigation timeline and your actions, creating a compliance-ready audit trail instantly.

- Resolution Type: Remediated / False Positive / Accepted Risk / Escalate.
- Auto-Generated Summary for audit compliance.
- Feedback Loop to train risk engine and reduce noise.

**Key UI Elements & Annotations:**

- **Annotation 6 (The Feedback Loop):** *"We don't just close the alert; we learn from it. By forcing a reason for 'False Positive,' we capture tribal knowledge. This data is fed back into the Risk Score engine to suppress similar noise in the future, making the system smarter over time."*
- **Annotation 7 (Auto-Generated Audit Log):** *"We save Arjun 5-10 minutes of paperwork. The summary is auto-generated from the investigation timeline and his actions, creating a compliance-ready audit trail instantly."*

## 3. Prioritization & Success Metrics

### Feature Prioritization

prioritization based on the **RICE framework** (Reach, Impact, Confidence, Effort), focusing on the highest impact on MTTR(**Mean Time to Repair**) first.

#### Phase 1: P0 (The Foundation - Must Have)

- **Business Context Enrichment (Screen 1 & 2):** Integrating and surfacing existing cloud tags (Business Unit, Environment, Compliance) is the highest leverage feature. Without it, the rest of the workflow lacks direction.
  ***Rationale****:* High Impact, High Confidence. This directly solves the core user pain of "I don't know if this matters."
- **Unified Investigation View (Screen 2):** Combining the timeline, details, and context into one page.
  ***Rationale****:* High Impact, Medium Effort. This eliminates the 40% of time Arjun spends context-switching.

#### Phase 2: P1 (The Efficiency Layer - Should Have)

- **Dynamic Remediation Playbook (Screen 2):** Guided steps for fixing the issue.
  **Rationale***:* Medium/High Impact, Medium Effort. This standardizes responses and helps junior team members act independently.
- **False Positive Feedback Loop (Screen 3):** Capturing the reason for dismissal.
  **Rationale***:* Medium Impact (short-term), High Impact (long-term), Low Effort. It's cheap to build and pays dividends in system intelligence.

#### Phase 3: P2 (The Differentiator - Nice to Have)

- **Auto-Generated Summaries (Screen 3) & AI Anomaly Detection:** Using ML to summarize investigations and predict false positives.
  **Rationale***:* High Impact, but High Effort and Lower Confidence. This is a long-term bet for a "2.0" release once we have enough data from the Phase 1 & 2 features.

### Success Metrics

measure success across three tiers: User Adoption, User Efficiency, and Business Impact.

**1. User Efficiency Metrics (Leading Indicators)**

- **Mean Time to Triage (MTTt):** *Target: 40% reduction.*
- **Mean Time to Resolve (MTTR):** *Target: 30% reduction.* .
- **Context-Switches per Investigation:** *Target: 70% reduction.*

**2. Business Impact Metrics (Lagging Indicators)**

- **Business-Critical SLA Adherence:** *Target: 95% of alerts tagged 'Revenue-Critical' resolved within SLA.* This ensures we are protecting what matters.
- **False Positive Rate:** *Target: 20% reduction QoQ.* Measures the success of the feedback loop in training the system.
- **Analyst CSAT:** *Target: "I am confident in my triage decisions" score >4.5/5.* Measures reduction in cognitive load and burnout.

**3. Adoption Metrics**

- **Feature Adoption:** % of daily active users interacting with the Business Context filters.