

The 25th hour and beyond

Sep 10, 2025

Presented by: Identity

1 **Background**

2 **Measures taken**

3 **How Clients got affected?**

4 **Incident timeline**

5 **Incident commander role**

6 **Post incident reviews**

7 **Q&A**

Business requirement and technical implementation



Why Session Management?

Our B2B team received a request from a potential enterprise customer for **single sign-out functionality**. This required implementing session management infrastructure as a foundational component in Babbel.

• Why Session Management?

Our B2B team received a request from a potential enterprise customer for **single sign-out functionality**. This required implementing session management infrastructure as a foundational component in Babbel.

• Breaking Changes

As part of introducing sessions, we made two key changes:

1. UPDATED USER-ARN HEADER FORMAT

Old Format

```
X-Babbel-User-Arn: arn:aws:sts::<AWS_ACCOUNT_ID>:assumed-role/<ROLE_NAME>/account.uuid
```

New Format

```
X-Babbel-User-Arn: arn:aws:sts::<AWS_ACCOUNT_ID>:assumed-role/<ROLE_NAME>/account.uuid@session_id
```

2. REPLACED AUTHENTICATION TOKEN WITH SESSION TOKEN

Updated users/me endpoint to use session tokens instead of authentication tokens for enhanced session management.

Pre-release preparation and lessons learned

?

• Pre-Release Actions Taken

- Communicated breaking changes via `#developers` channel with advance notice
- Extended **staging environment testing period to 10 days** for validation
- Conducted comprehensive manual search across GitHub repositories to identify affected clients

• Pre-Release Actions Taken

- Communicated breaking changes via **#developers** channel with advance notice
- Extended **staging environment testing period to 10 days** for validation
- Conducted comprehensive manual search across GitHub repositories to identify affected clients

• Areas for Improvement

- Enhanced **communication strategy** required - single notification insufficient for broad reach
- Insufficient **observability tooling** - no systematic approach to identify client dependencies
- Missing **automated testing framework** for detecting breaking changes in staging environment

Strategic Takeaway

Implementing robust client discovery mechanisms and comprehensive automated testing pipelines is critical for safe deployment of breaking changes.

Understanding the authentication failure mechanism



Authentication Mechanism

user-arn-header is used by clients for **authenticating and verifying requests**. They extract the UUID from the user-arn-header to compare against the UUID in the request payload.

• Authentication Mechanism

user-arn-header is used by clients for **authenticating and verifying requests**. They extract the UUID from the user-arn-header to compare against the UUID in the request payload.

• What Went Wrong

Authentication **failed** because the format changed in the user-arn-header. Clients were still expecting the old format and couldn't parse the UUID correctly from the new format with the appended session ID.

Impact

Client applications could no longer extract and validate user UUIDs, causing authentication to fail across multiple services.

Chronological progression of events



Chronological progression of events

July 21, 2025 - 10:15 AM

PRODUCTION DEPLOYMENT

Identity team deployed PR to production containing changes to update user-arn header format.

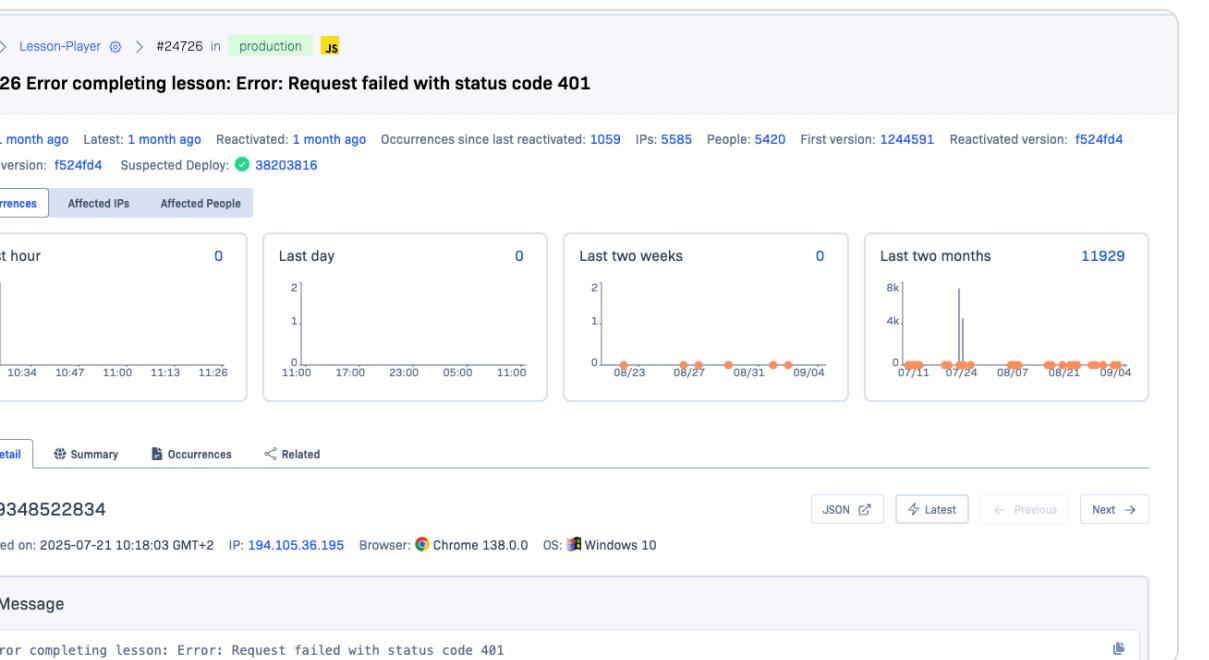
Chronological progression of events

July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

[View Rollbar Alert →](#)*Click to enlarge - Rollbar alert details*

Chronological progression of events

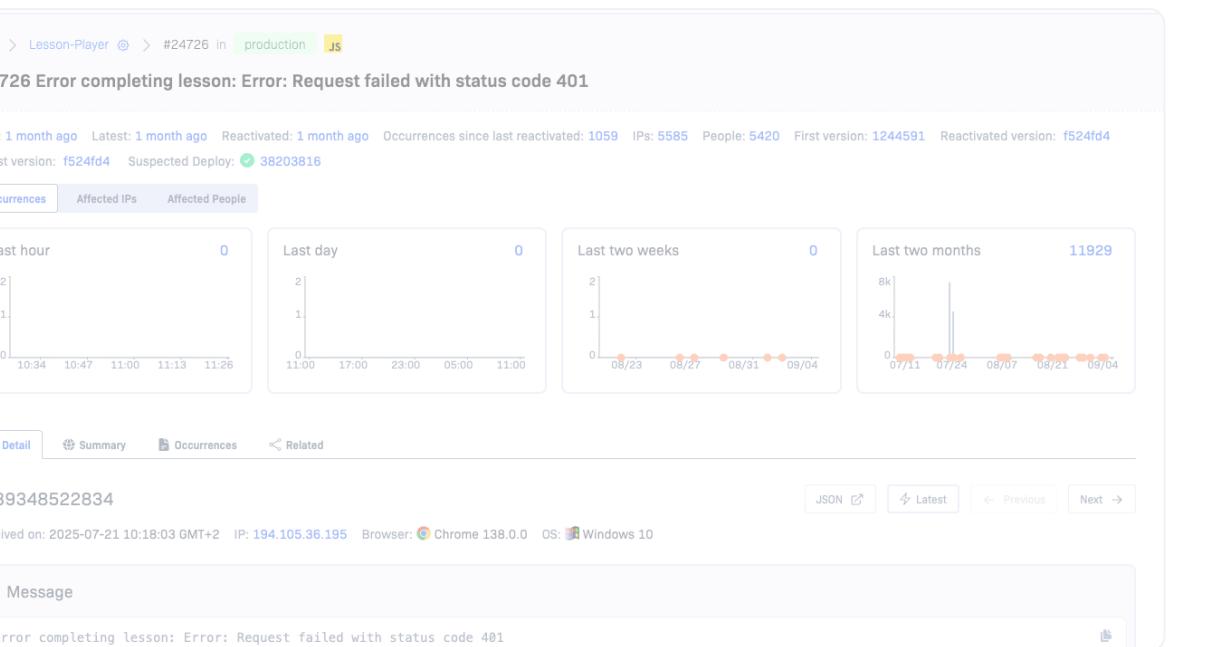
 July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

 July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

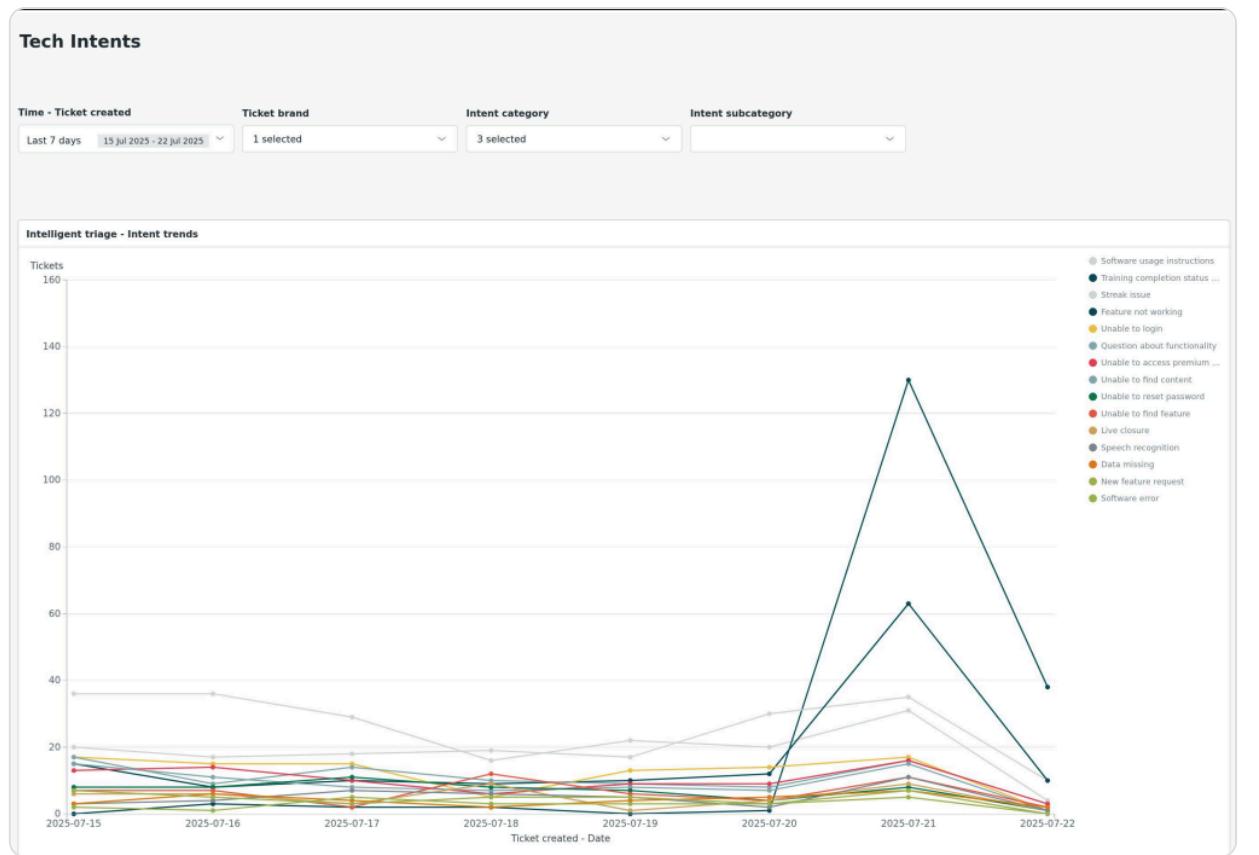
Initial error alert triggered in monitoring system.

[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

 July 21, 2025 - 5:11 PM



Click to enlarge - Support ticket spike visualization

LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

Chronological progression of events

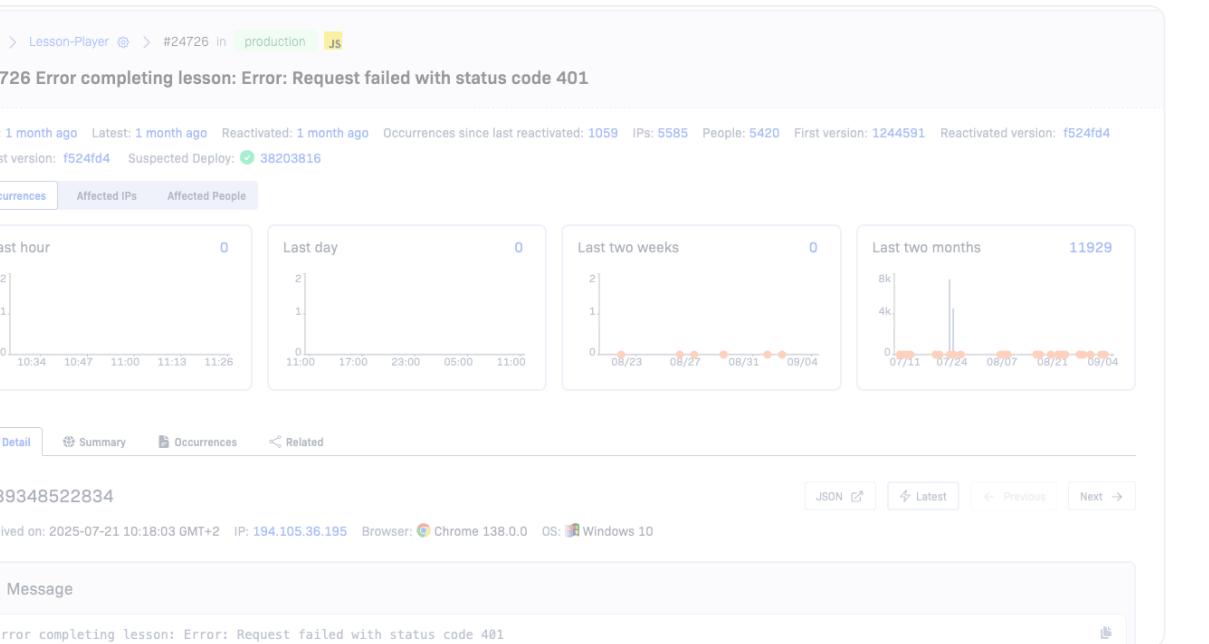
July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

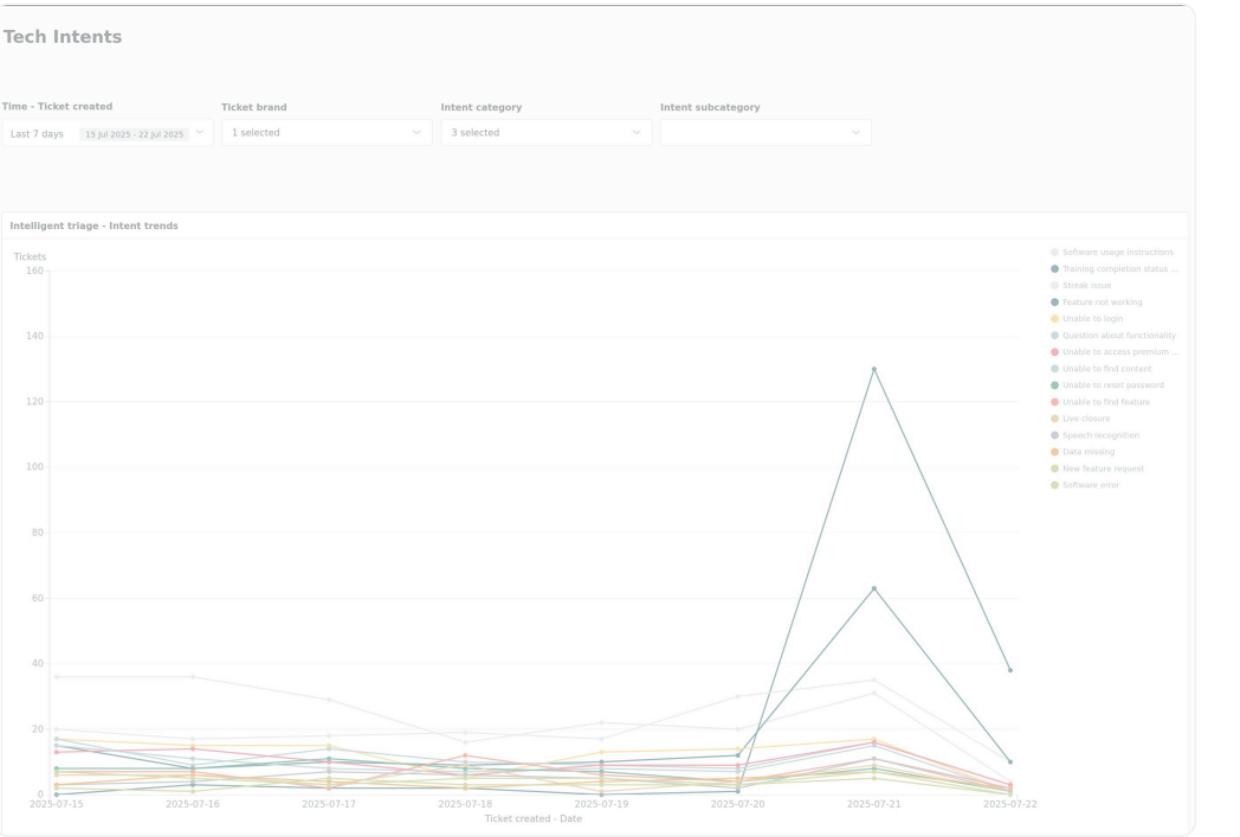
[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

July 21, 2025 - 5:11 PM

Customer Support Operations team detected issue and notified #ASK Study Core channel due to substantial increase in customer support tickets.



Click to enlarge - Support ticket spike visualization

LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

July 21, 2025 - 9:30 PM

INCIDENT TICKET CREATED

Formal incident tracking initiated.

Chronological progression of events

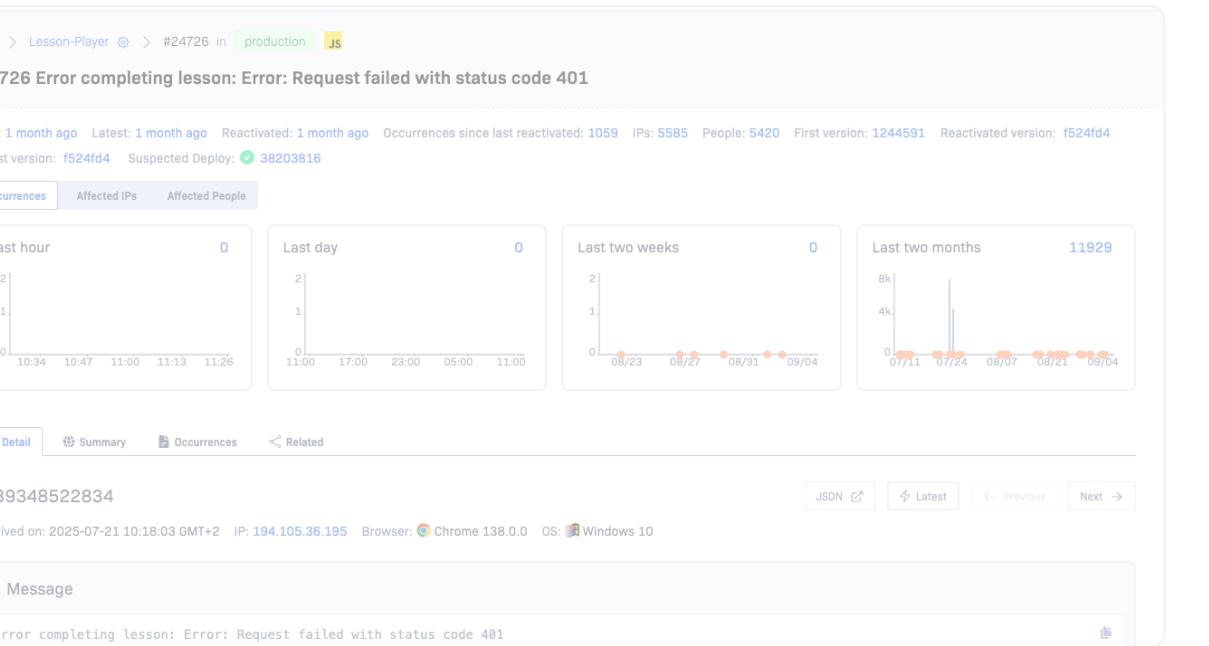
July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

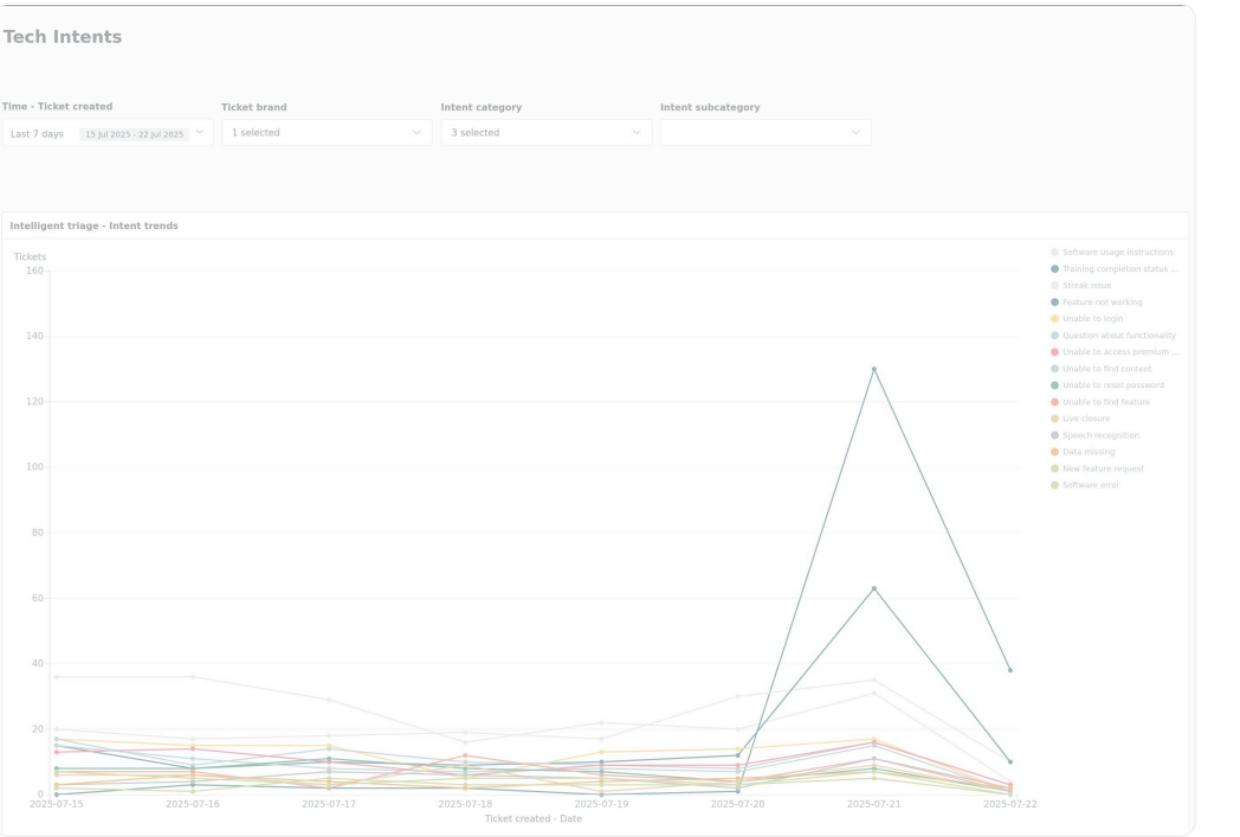
[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

July 21, 2025 - 5:11 PM

Customer Support Operations team detected issue and notified #ASK Study Core channel due to substantial increase in customer support tickets.



Click to enlarge - Support ticket spike visualization

LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

July 21, 2025 - 9:30 PM

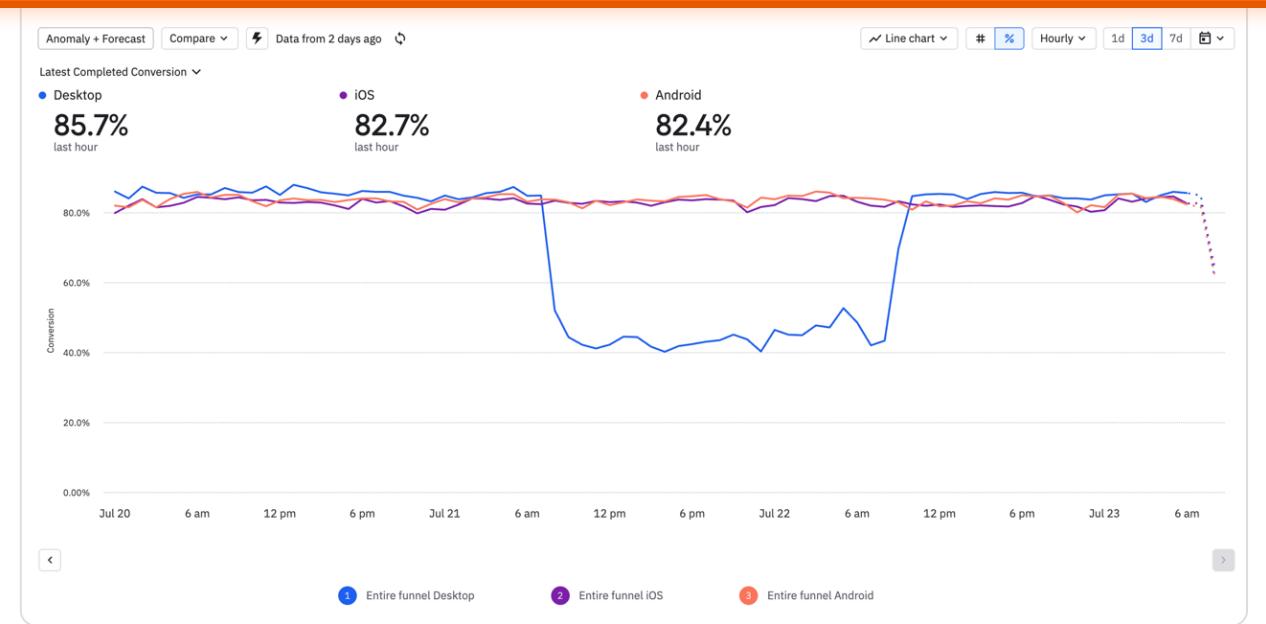
INCIDENT TICKET CREATED

Formal incident tracking initiated.

July 22, 2025 - 11:00 AM

IMPACT ANALYSIS

Drop in lesson completion rate was reported to content-platform team.



Click to enlarge - Lesson completion rate impact analysis

Chronological progression of events

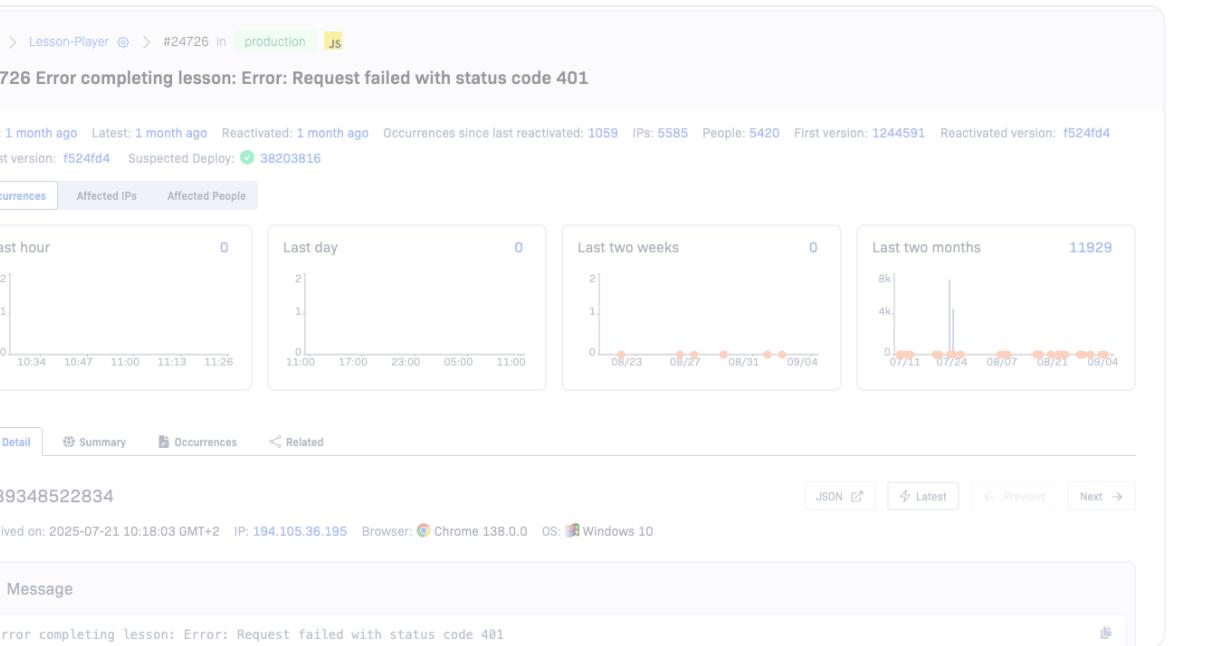
July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

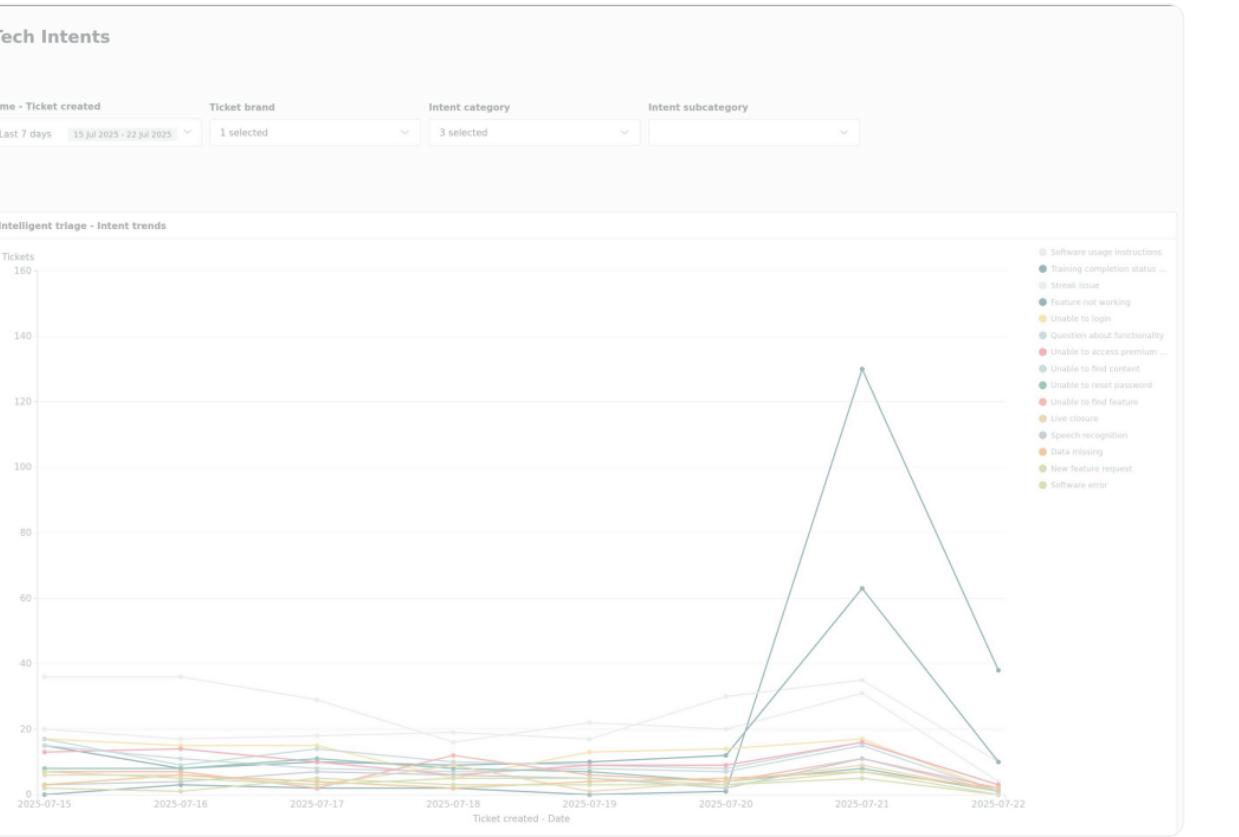
[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

July 21, 2025 - 5:11 PM

Customer Support Operations team detected issue and notified #ASK Study Core channel due to substantial increase in customer support tickets.



Click to enlarge - Support ticket spike visualization

💡 LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

July 21, 2025 - 9:30 PM

INCIDENT TICKET CREATED

Formal incident tracking initiated.

July 22, 2025 - 11:00 AM

IMPACT ANALYSIS

Drop in lesson completion rate was reported to content-platform team.



Click to enlarge - Lesson completion rate impact analysis

July 22, 2025 - 11:25 AM

EMERGENCY ROLLBACK

Redeployed older version of code in Accounts service, which fixed the issue for new requests.

⚠️ LEARNING: INCIDENT MANAGEMENT PROCESS

Instead of directly redeploying older version of a service owned by different team, it's better to inform the respective team by creating a PagerDuty incident and assigning to them. Direct rollbacks can have unintended consequences.

Chronological progression of events

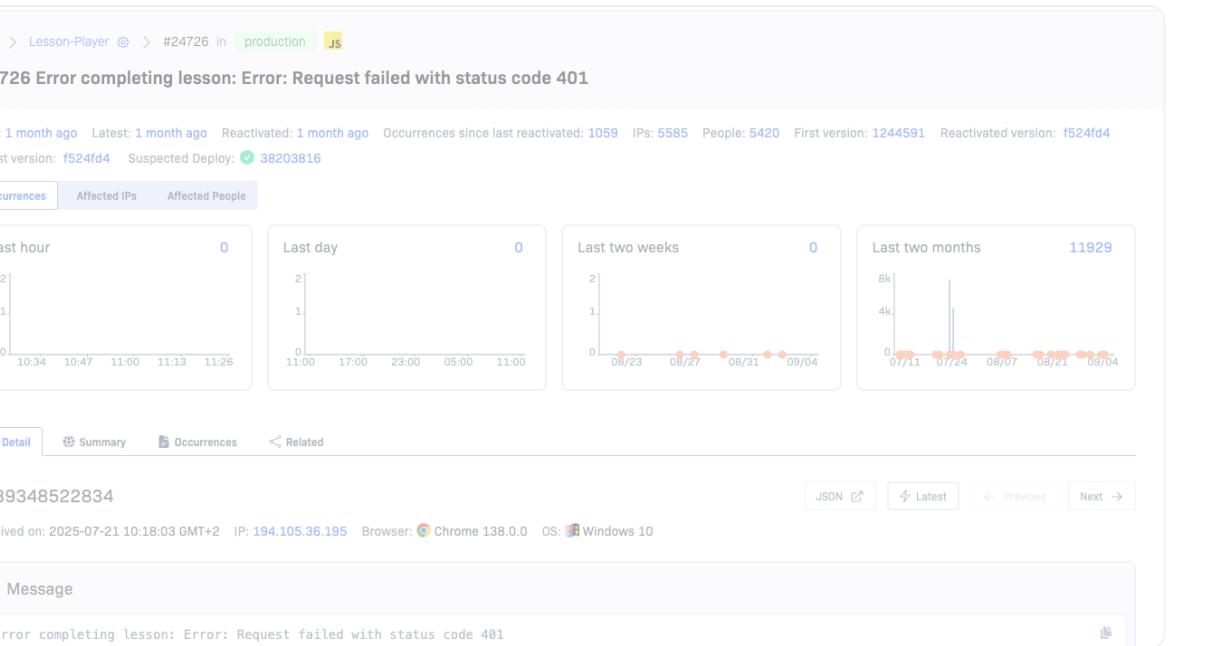
July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

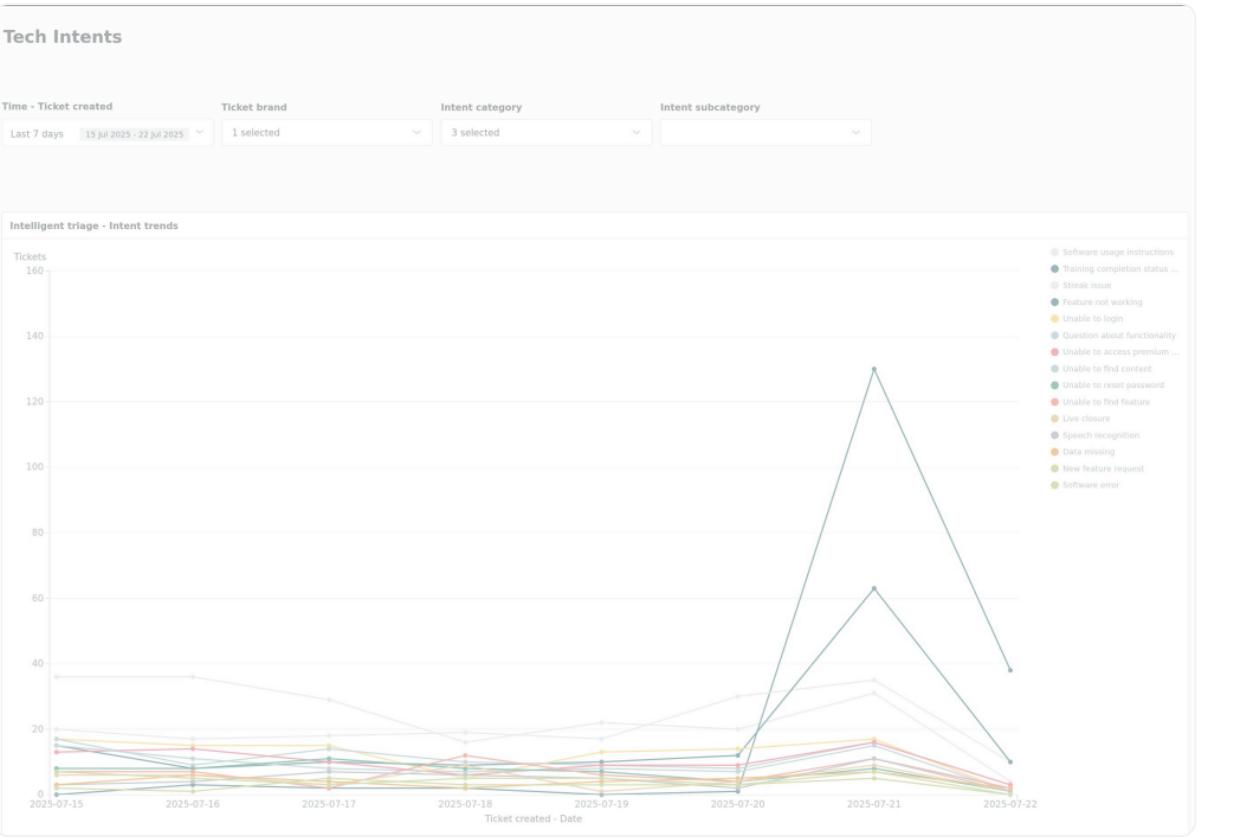
[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

July 21, 2025 - 5:11 PM

Customer Support Operations team detected issue and notified #ASK Study Core channel due to substantial increase in customer support tickets.



Click to enlarge - Support ticket spike visualization

💡 LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

July 21, 2025 - 9:30 PM

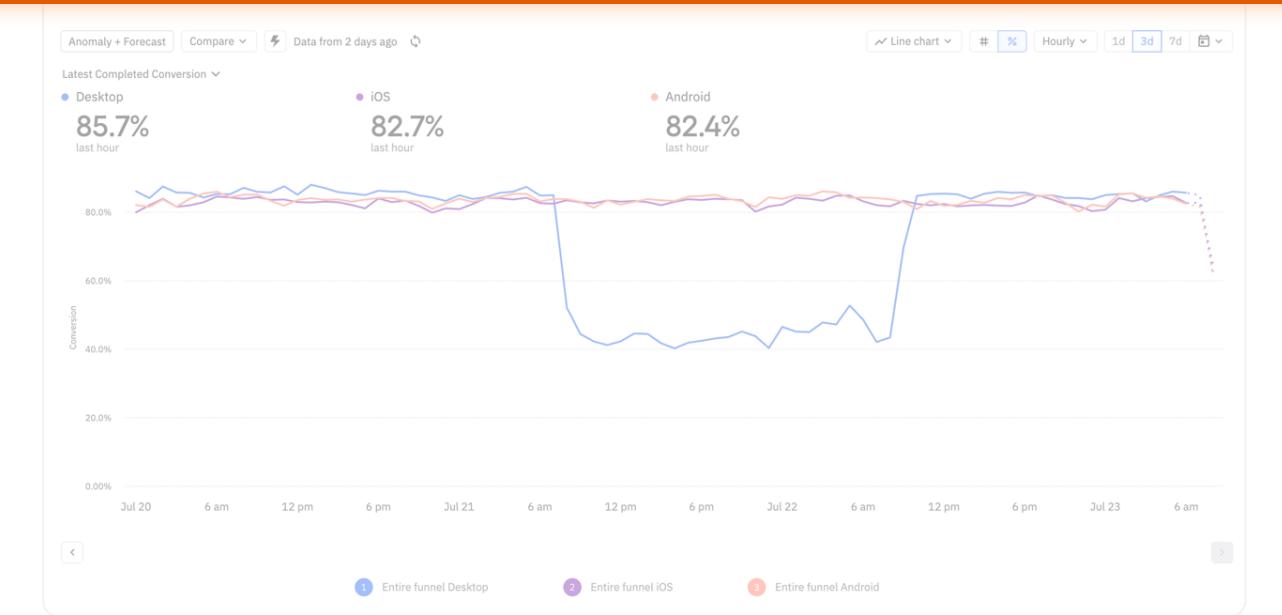
INCIDENT TICKET CREATED

Formal incident tracking initiated.

July 22, 2025 - 11:00 AM

IMPACT ANALYSIS

Drop in lesson completion rate was reported to content-platform team.



Click to enlarge - Lesson completion rate impact analysis

July 22, 2025 - 11:25 AM

EMERGENCY ROLLBACK

Redeployed older version of code in Accounts service, which fixed the issue for new requests.

⚠ LEARNING: INCIDENT MANAGEMENT PROCESS

Instead of directly redeploying older version of a service owned by different team, it's better to inform the respective team by creating a PagerDuty incident and assigning to them. Direct rollbacks can have unintended consequences.

July 22, 2025 - 12:10 PM

TEAM COLLABORATION

Identity team was notified and all stakeholders gathered in a huddle to investigate the root cause.

Chronological progression of events

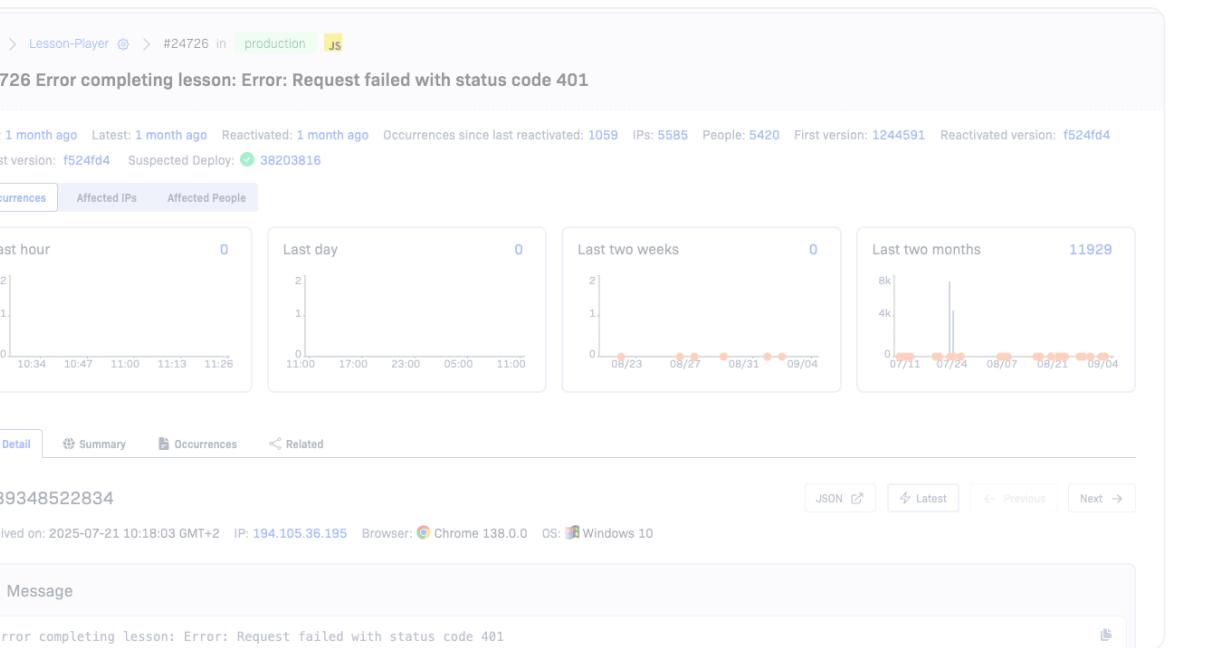
July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

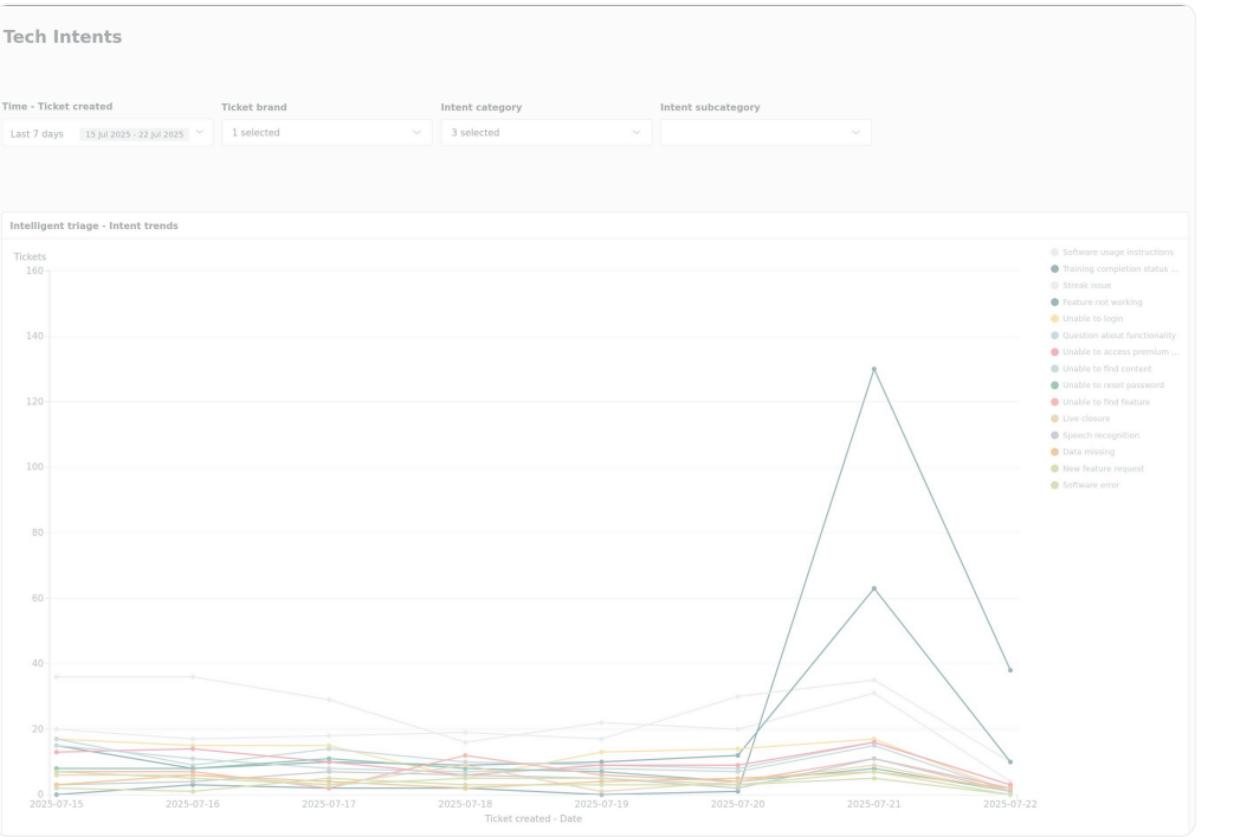
[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

July 21, 2025 - 5:11 PM

Customer Support Operations team detected issue and notified #ASK Study Core channel due to substantial increase in customer support tickets.



Click to enlarge - Support ticket spike visualization

💡 LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

July 21, 2025 - 9:30 PM

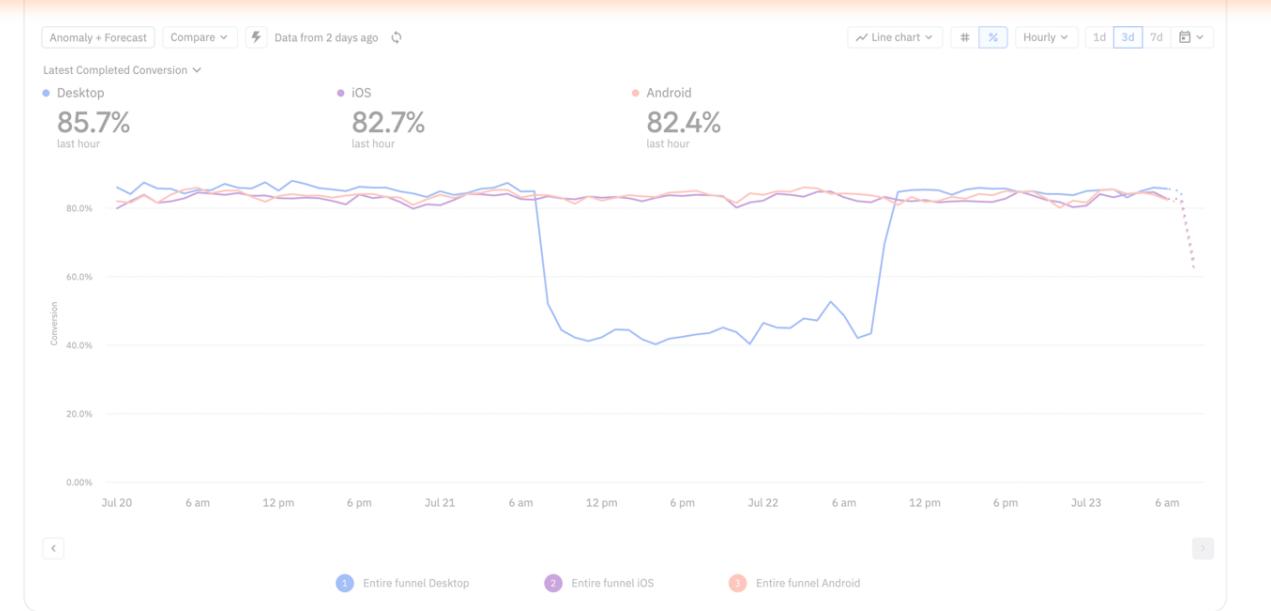
INCIDENT TICKET CREATED

Formal incident tracking initiated.

July 22, 2025 - 11:00 AM

IMPACT ANALYSIS

Drop in lesson completion rate was reported to content-platform team.



Click to enlarge - Lesson completion rate impact analysis

July 22, 2025 - 11:25 AM

EMERGENCY ROLLBACK

Redeployed older version of code in Accounts service, which fixed the issue for new requests.

⚠ LEARNING: INCIDENT MANAGEMENT PROCESS

Instead of directly redeploying older version of a service owned by different team, it's better to inform the respective team by creating a PagerDuty incident and assigning to them. Direct rollbacks can have unintended consequences.

July 22, 2025 - 12:10 PM

TEAM COLLABORATION

Identity team was notified and all stakeholders gathered in a huddle to investigate the root cause.

July 22, 2025 - 12:20 PM

ROOT CAUSE IDENTIFIED

Discovered that one of the services owned by content-platform was still using the old parsing logic for user-arn header.

Chronological progression of events

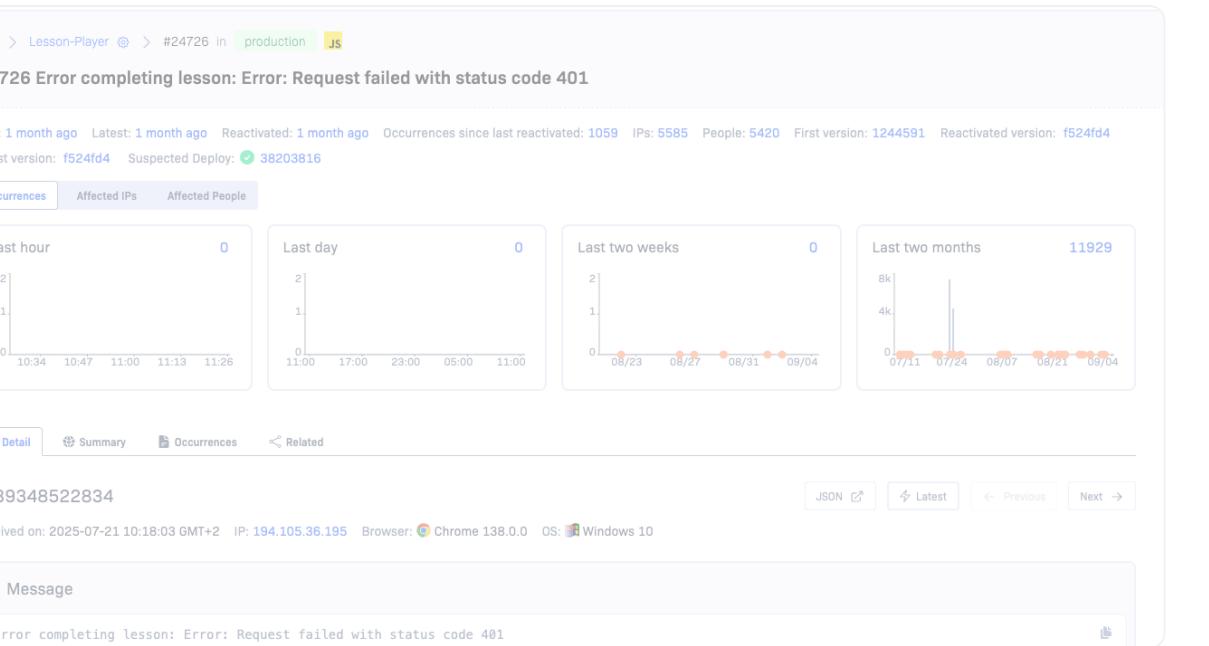
July 21, 2025 - 10:15 AM**PRODUCTION DEPLOYMENT**

Identity team deployed PR to production containing changes to update user-arn header format.

July 21, 2025 - 10:18 AM**FIRST ROLLBAR ALERT**

Initial error alert triggered in monitoring system.

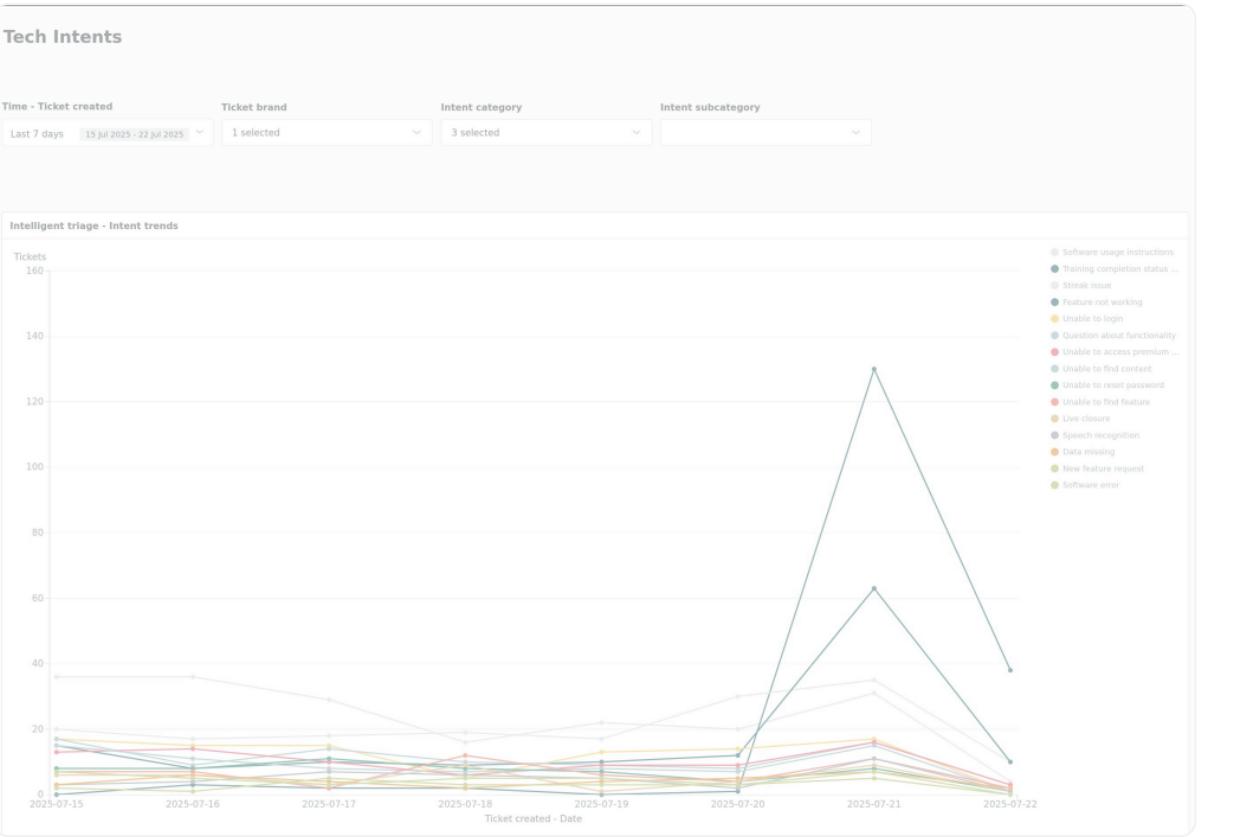
[View Rollbar Alert →](#)



Click to enlarge - Rollbar alert details

July 21, 2025 - 5:11 PM

Customer Support Operations team detected issue and notified #ASK Study Core channel due to substantial increase in customer support tickets.



Click to enlarge - Support ticket spike visualization

LEARNING: MONITORING GAP

We should have detected this from Rollbar alerts instead of relying on customer support escalation. This indicates a critical gap in our monitoring and alerting strategy.

July 21, 2025 - 9:30 PM

INCIDENT TICKET CREATED

Formal incident tracking initiated.

July 22, 2025 - 11:00 AM

IMPACT ANALYSIS

Drop in lesson completion rate was reported to content-platform team.



Click to enlarge - Lesson completion rate impact analysis

July 22, 2025 - 11:25 AM

EMERGENCY ROLLBACK

Redeployed older version of code in Accounts service, which fixed the issue for new requests.

⚠ LEARNING: INCIDENT MANAGEMENT PROCESS

Instead of directly redeploying older version of a service owned by different team, it's better to inform the respective team by creating a PagerDuty incident and assigning to them. Direct rollbacks can have unintended consequences.

July 22, 2025 - 12:10 PM

TEAM COLLABORATION

Identity team was notified and all stakeholders gathered in a huddle to investigate the root cause.

July 22, 2025 - 12:20 PM

ROOT CAUSE IDENTIFIED

Discovered that one of the services owned by content-platform was still using the old parsing logic for user-arn header.

Final fix was deployed, fully resolving the incident.

Key responsibilities during incident management

Key responsibilities during incident management

-  **Information Management**

Collect information from stakeholders and **keep the incident ticket updated** with real-time status, findings, and actions taken.

Key responsibilities during incident management

- 

Information Management

Collect information from stakeholders and **keep the incident ticket updated** with real-time status, findings, and actions taken.

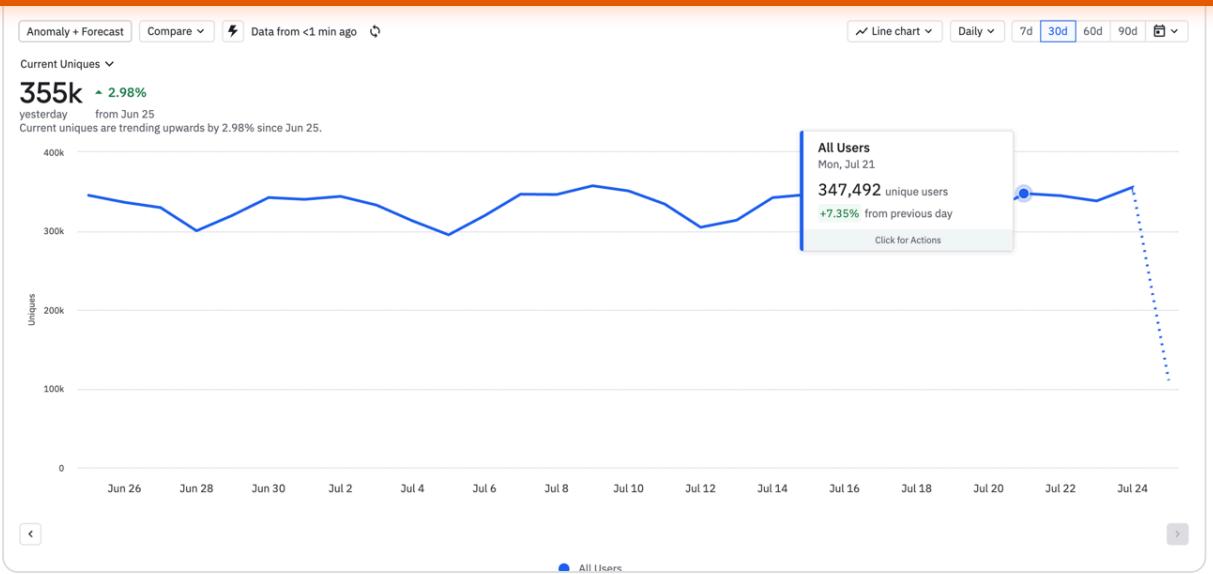
- 

Impact Calculation

Calculate the impact using the formula:

$$\text{(Affected Users / Daily Active Users)} \times 100$$

- **Affected users:** Retrieved from logs, events, or Rollbar occurrences
- **Daily active users:** Retrieved from Amplitude analytics



Click to enlarge - Impact analysis calculation

Key responsibilities during incident management

- 

Information Management

Collect information from stakeholders and **keep the incident ticket updated** with real-time status, findings, and actions taken.

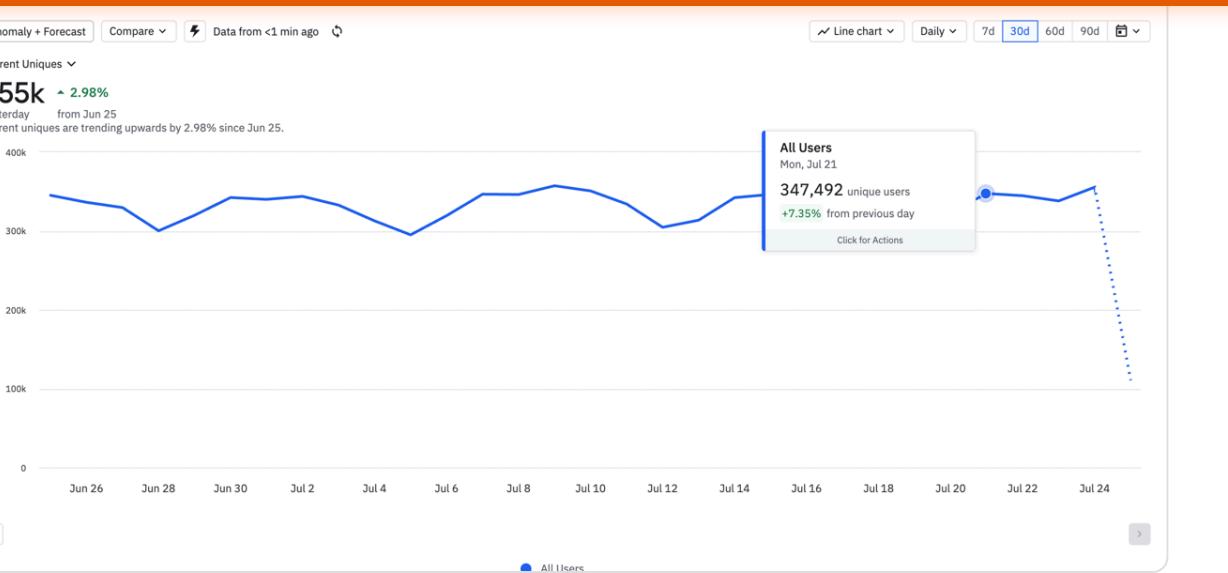
- 

Impact Calculation

Calculate the impact using the formula:

$$\text{(Affected Users / Daily Active Users)} \times 100$$

- **Affected users:** Retrieved from logs, events, or Rollbar occurrences
- **Daily active users:** Retrieved from Amplitude analytics



Click to enlarge - Impact analysis calculation

• **Post-Incident Reviews**

Schedule post-incident reviews **ASAP** with the following approach:

- Involve **all stakeholders** who were part of the incident
- If **multiple teams** are involved, conduct **multiple reviews** to ensure comprehensive coverage

Key responsibilities during incident management

- 

Information Management

Collect information from stakeholders and **keep the incident ticket updated** with real-time status, findings, and actions taken.

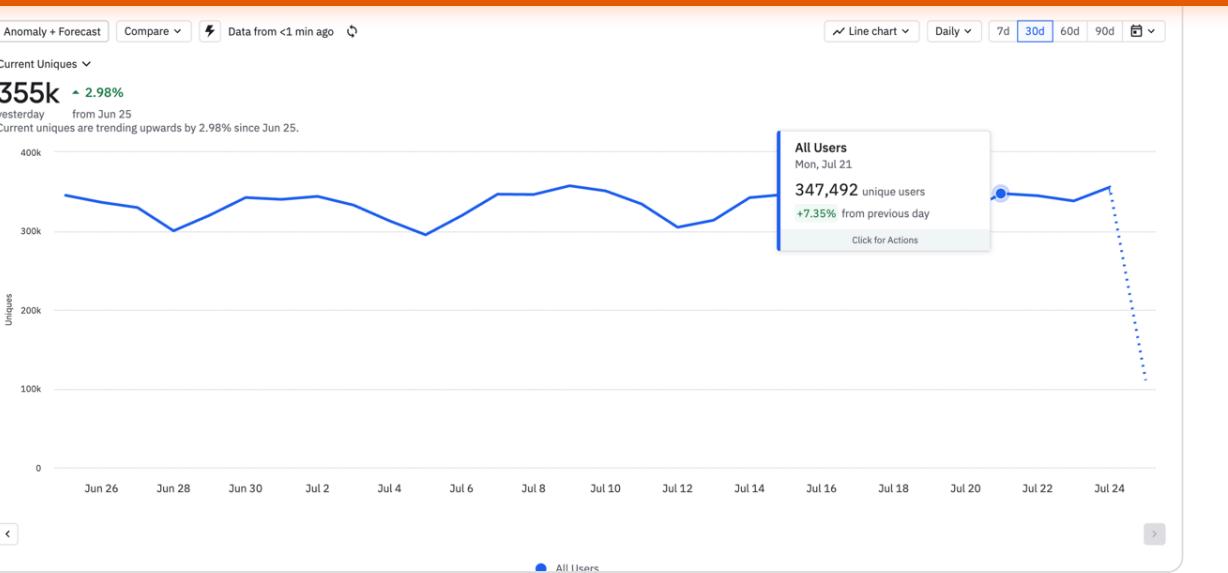
- 

Impact Calculation

Calculate the impact using the formula:

$$\text{(Affected Users / Daily Active Users)} \times 100$$

- **Affected users:** Retrieved from logs, events, or Rollbar occurrences
- **Daily active users:** Retrieved from Amplitude analytics



Click to enlarge - Impact analysis calculation

• **Post-Incident Reviews**

Schedule post-incident reviews **ASAP** with the following approach:

- Involve **all stakeholders** who were part of the incident
- If **multiple teams** are involved, conduct **multiple reviews** to ensure comprehensive coverage

• **Severity Adjustment**

Process and action item management



Create Post Incident Review

- Use the **predefined template** from Babbel's process documentation
- **Duplicate** the template and add incident-specific details

[View Template: Post-Incident Review →](#)

Template I Post-Incident Review

By Vlad Laktionov · 1 min · 102 · Add a reaction

Create new Post-Incident Review document

To create a new Post-Incident Review document, use name notation: Year > Month > Severity > Team name > Jira Incident ID
New Post-Incident Review should be labeled post-incident-review

[Meeting details and incident overview] [Incident Details] [Incident Narrative] [Lessons Learned] [Action Items]

Meeting details and incident overview

Post-incident review owner	
Incident Commander	
Incident ticket	
Incident Date	
Severity Level	SEV-1 (CRITICAL) / SEV-2 (HIGH) / SEV-3 (LOW)
Incident Executive Summary	
Post-incident review Date	
Participants	

Incident Details

Click to enlarge - Post-incident review template



Create Post Incident Review

- Use the **predefined template** from Babbel's process documentation
- **Duplicate** the template and add incident-specific details

[View Template: Post-Incident Review →](#)

Template I Post-Incident Review

By Vlad Laktionov · 1 min · 102 · Add a reaction

Create new Post-Incident Review document

To create a new Post-Incident Review document, use name notation: Year > Month > Severity > Team name > Jira Incident ID
New Post-Incident Review should be labeled post-incident-review

[Meeting details and incident overview] [Incident Details] [Incident Narrative] [Lessons Learned] [Action Items]

Meeting details and incident overview

Post-incident review owner	
Incident Commander	
Incident ticket	
Incident Date	
Severity Level	SEV-1 (CRITICAL) / SEV-2 (HIGH) / SEV-3 (LOW)
Incident Executive Summary	
Post-incident review Date	
Participants	

Incident Details

Click to enlarge - Post-incident review template

-  **Schedule Reviews Early**

Schedule reviews **as early as possible** so no context is missed while details are still fresh in everyone's memory.



Create Post Incident Review

- Use the **predefined template** from Babbel's process documentation
- **Duplicate** the template and add incident-specific details

[View Template: Post-Incident Review →](#)

Template I Post-Incident Review

By Vlad Laktionov 1 min 102 Add a reaction

Create new Post-Incident Review document

To create a new Post-Incident Review document, use name notation: Year > Month > Severity > Team name > Jira Incident ID
New Post-Incident Review should be labeled post-incident-review

[Meeting details and incident overview] [Incident Details] [Incident Narrative] [Lessons Learned] [Action Items]

Meeting details and incident overview

Post-incident review owner	
Incident Commander	
Incident ticket	
Incident Date	
Severity Level	SEV-1 (CRITICAL) / SEV-2 (HIGH) / SEV-3 (LOW)
Incident Executive Summary	
Post-incident review Date	
Participants	

Incident Details

Click to enlarge - Post-incident review template

-  **Schedule Reviews Early**

Schedule reviews **as early as possible** so no context is missed while details are still fresh in everyone's memory.

-  **Involve All Parties**

Ensure **all stakeholders** who were involved in the incident participate in the review process for complete perspective.



Create Post Incident Review

- Use the **predefined template** from Babbel's process documentation
- **Duplicate** the template and add incident-specific details

[View Template: Post-Incident Review →](#)

Template I Post-Incident Review

By Vlad Laktionov 1 min 102 Add a reaction

Create new Post-Incident Review document

To create a new Post-Incident Review document, use name notation: Year > Month > Severity > Team name > Jira Incident ID
New Post-Incident Review should be labeled post-incident-review

[Meeting details and incident overview] [Incident Details] [Incident Narrative] [Lessons Learned] [Action Items]

Meeting details and incident overview

Post-incident review owner	
Incident Commander	
Incident ticket	
Incident Date	
Severity Level	SEV-1 (CRITICAL) / SEV-2 (HIGH) / SEV-3 (LOW)
Incident Executive Summary	
Post-incident review Date	
Participants	

Incident Details

Click to enlarge - Post-incident review template

• ⏱ Schedule Reviews Early

Schedule reviews **as early as possible** so no context is missed while details are still fresh in everyone's memory.

• 📸 Involve All Parties

Ensure **all stakeholders** who were involved in the incident participate in the review process for complete perspective.

• 📝 Create JIRA Action Items

Create JIRA tickets for **all post-incident review action items** using priority-based tags:

 **p0-post-incident-review-action-item** Critical priority

 **p1-post-incident-review-action-item** High priority

 **p2-post-incident-review-action-item** Medium priority

What went well	
What went not so well	
Where we got lucky (optional)	

Action Items

Action items derived from the review findings are essential for **mitigating**, **preventing**, or **better detecting the issue**. Each action is assigned to a responsible party or team, along with specific deadlines, to ensure that progress is monitored and completed effectively. This process guarantees that lessons learned are translated into improvements, enhancing our preparedness for future incidents.

The tickets created for the identified Action Items should include the following labels as appropriate:

- `p0-post-incident-review-action-item`
- `p1-post-incident-review-action-item`
- `p2-post-incident-review-action-item`

Action Item	Type	Priority	Owner	Link (JIRA issue)
	Mitigation / Prevention / Detection	P0: STOP-THE-WORLD / P1: HIGH PRIORITY / P2: NICE-TO-HAVE		

Click to enlarge - JIRA action items with priority tags



Q&A

Questions & Discussion

Thank you for your attention

