Fraud Application Hardening

Heather Wighton / Director of Data Insights
Paul Ireifej / Principal Member of Technical Staff
March 10, 2022

AT&T Business

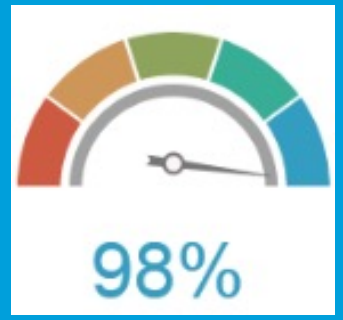
Agenda

1: Infrastructure
2: APIs
3: Tracers
4: Database
5: Messaging
6: Kafka
7: ML Models
8: Certs
9: Feeds
10: Alerting

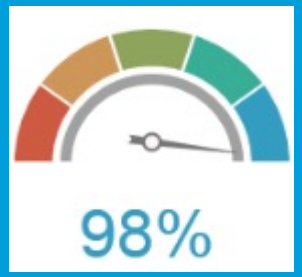
A release is like a boat. 80% of the holes plugged is not good enough.

1. Infrastructure

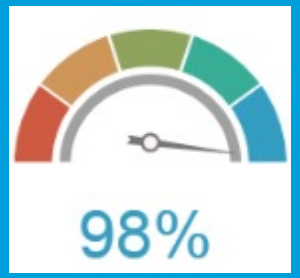
Infrastructure
Health Scorecard



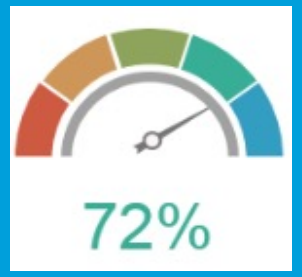
Overall Fraud Health



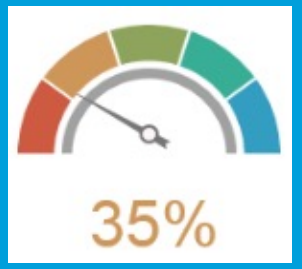
Avertack UI Health



Decision Engine Health



Internal APIs Health

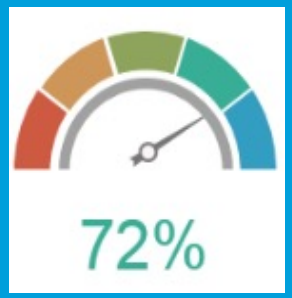


3rd Party/External APIs Health

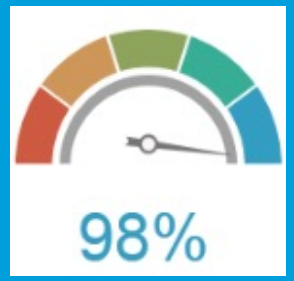
ML Models Health

MongoDB Health

Kafka Health



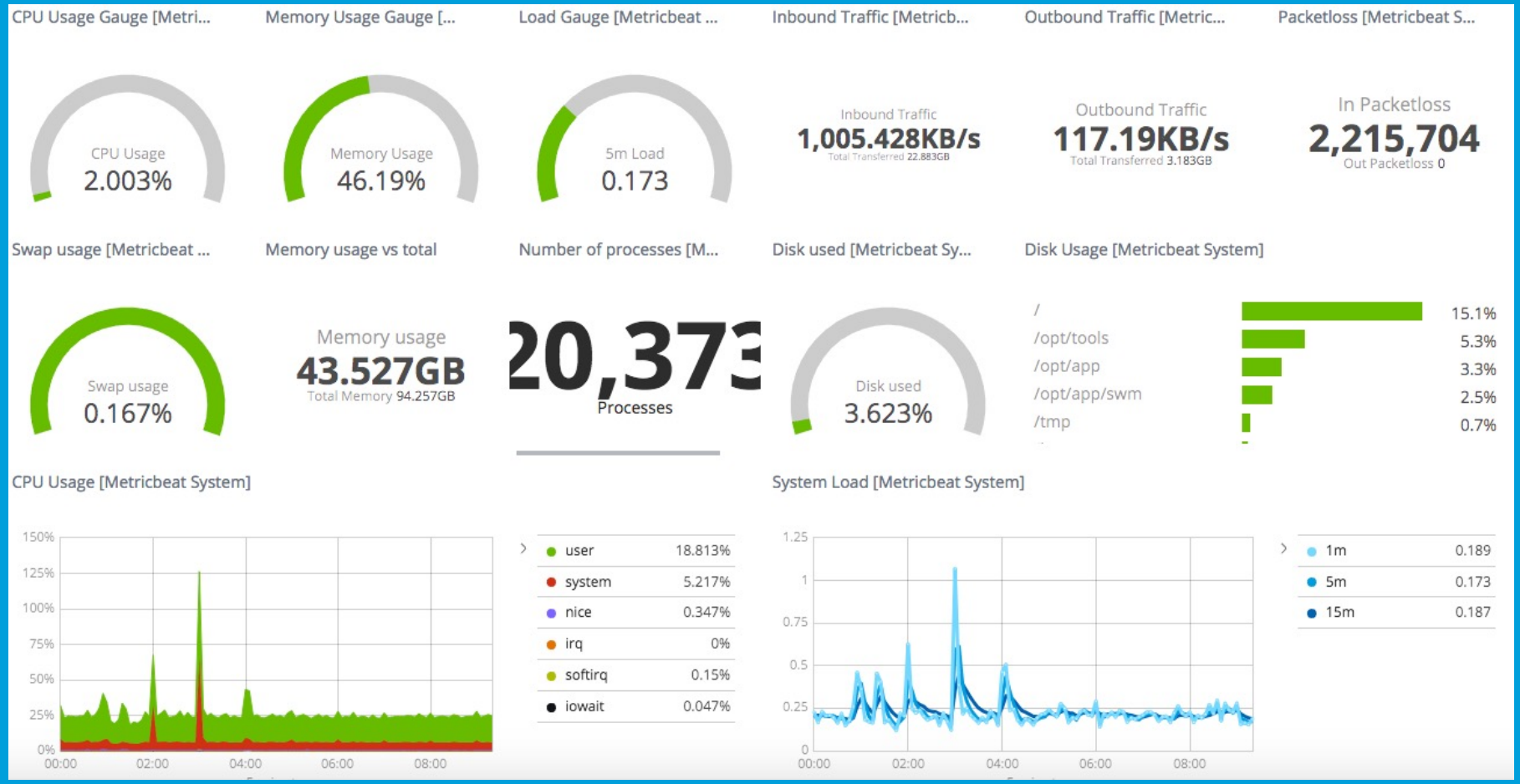
Redis Health



Infrastructure Health

Infrastructure
Health Scorecard

- Memory Usage
- Max CPI Memory Used
- Avg CPU Memory Used
- CPU Memory Promise Success
- Work Rescheduled
- Max CPU Memory Clock
- Max CPU Processor Clock
- CPU Memory Promised
- CPI Memory Available for Promise
- Max CPU Process Count



2. Internal and External APIs

Internal and External APIs

Internal

APIs exposed only to clients and developers within an organization.

Internal and External APIs

Internal

APIs exposed only to clients and developers within an organization.

External

Developers use to integrate their applications with a third-party resource, such as a public cloud service or a SaaS application

Internal and External APIs

Monitoring

Implement monitors and remediation monitoring for all business-critical flows

Internal and External APIs

Monitoring

Implement monitors and remediation monitoring for all business-critical flows

Response Time

Calling APIs, monitoring SLA and response within time (count), 200 and non-200)

Internal and External APIs

Monitoring

Implement monitors and remediation monitoring for all business-critical flows

Response Time

Calling APIs, monitoring SLA and response within time (count), 200 and non-200)

Percentage

Percentage experiencing delays , lag or non-success response

Internal and External APIs

Monitoring

Implement monitors and remediation monitoring for all business-critical flows

Response Time

Calling APIs, monitoring SLA and response within time (count), 200 and non-200)

Percentage

Percentage experiencing delays , lag or non-success response

Aggregation Windows

Ability to change the interval aggregation window by time period

Internal and External APIs

Monitoring

Implement monitors and remediation monitoring for all business-critical flows

Response Time

Calling APIs, monitoring SLA and response within time (count), 200 and non-200)

Percentage

Percentage experiencing delays , lag or non-success response

Aggregation Windows

Ability to change the interval aggregation window by time period

Statistics

Store and generate volume statistics

Internal and External APIs

Monitoring

Implement monitors and remediation monitoring for all business-critical flows

Response Time

Calling APIs, monitoring SLA and response within time (count), 200 and non-200)

Percentage

Percentage experiencing delays , lag or non-success response

Aggregation Windows

Ability to change the interval aggregation window by time period

Statistics

Store and generate volume statistics

Volume Metrics

Decision engine to monitor standard deviation of volume

3. Tracers

Tracers

What is a tracer?

- Dummy message sent over the wire / simulation to Identify connectivity between two end points.
- Create tracers for systems that our system talks to.
- External third-party systems dummy request and get response back.
- SLA how long to get message back

Tracers

What is a tracer?

- Dummy message sent over the wire / simulation to Identify connectivity between two end points.
- Create tracers for systems that our system talks to.
- External third-party systems dummy request and get response back.
- SLA how long to get message back

Portal for external connection

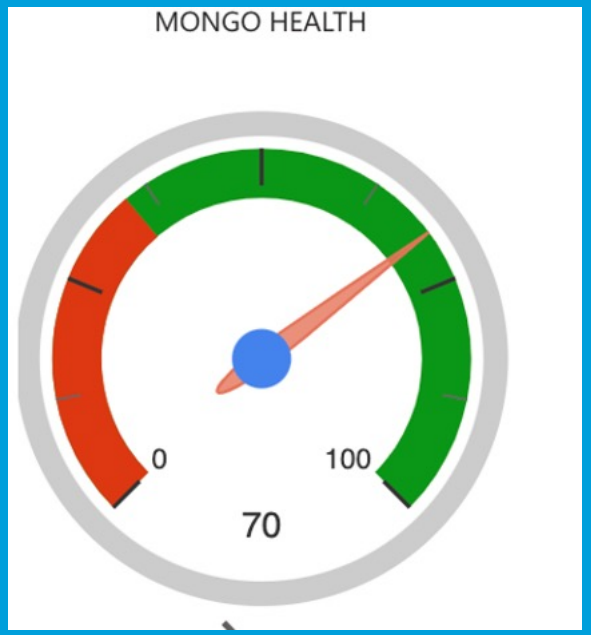
External third-party systems

- External entry point into AT&T network
- Third parties' access internal API through a portal
- Tracer used to send API as if we're an external third party

4. Database

Database (MongoDB)

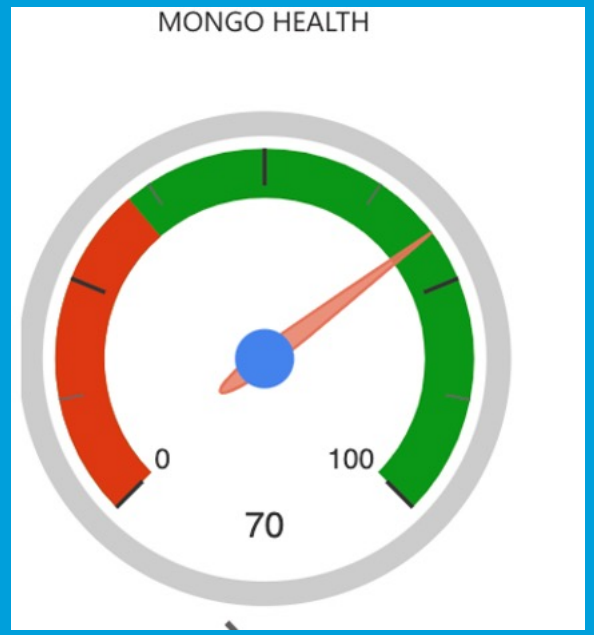
Implement monitors and remediation for MongoDB for all business-critical flows.



Disk space

Database (MongoDB)

Implement monitors and remediation for MongoDB for all business-critical flows.

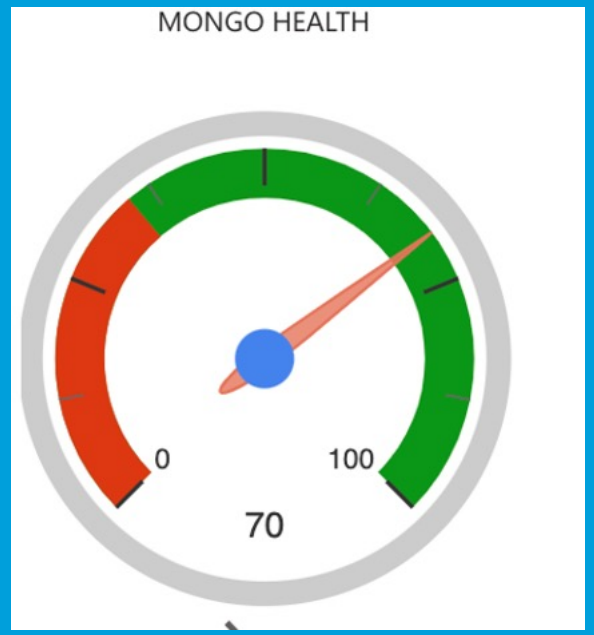


Disk space

 # connections made

Database (MongoDB)

Implement monitors and remediation for MongoDB for all business-critical flows.



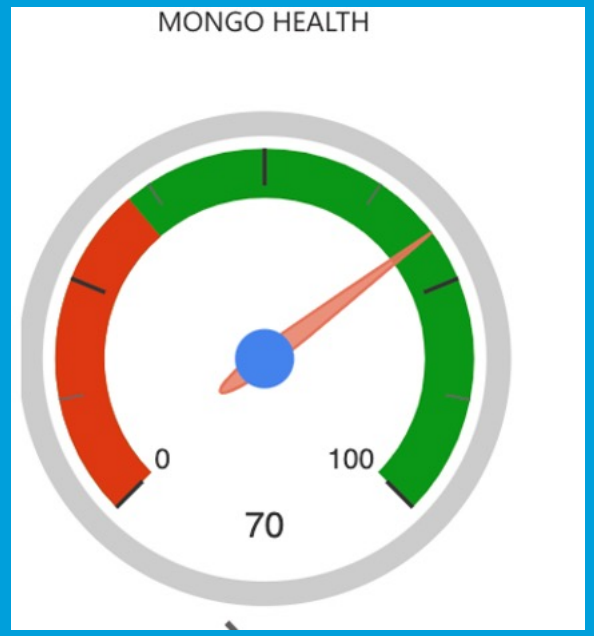
Disk space

 # connections made

 # read and writes

Database (MongoDB)

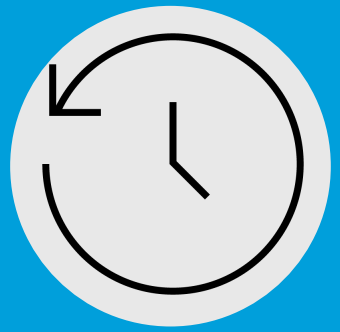
Implement monitors and remediation for MongoDB for all business-critical flows.



Disk space

 # connections made

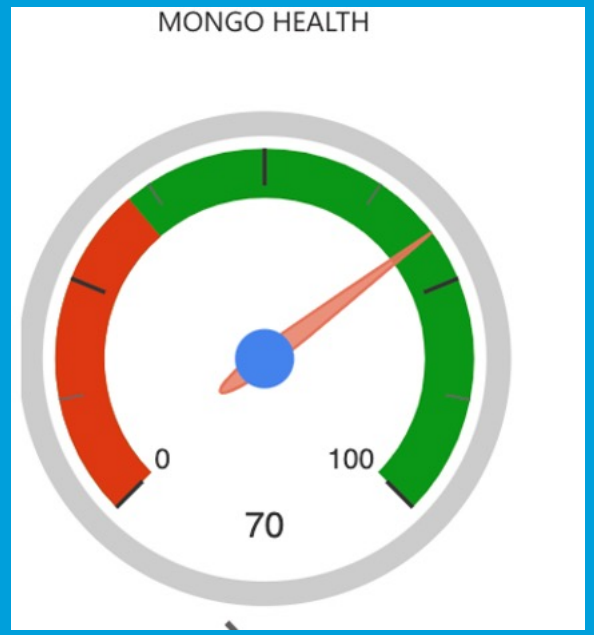
 # read and writes



Query time

Database (MongoDB)

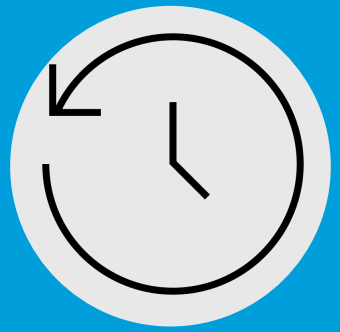
Implement monitors and remediation for MongoDB for all business-critical flows.



Disk space

 # connections made

 # read and writes



Query time

Heavy disk usage

5. Messaging System

Messaging System

Publish & Subscribe to Topics

Constantly aggregating messages published

- Configured to count on a time window
- Topic messages should never be zero
- Every 60 minutes, ensure something is published

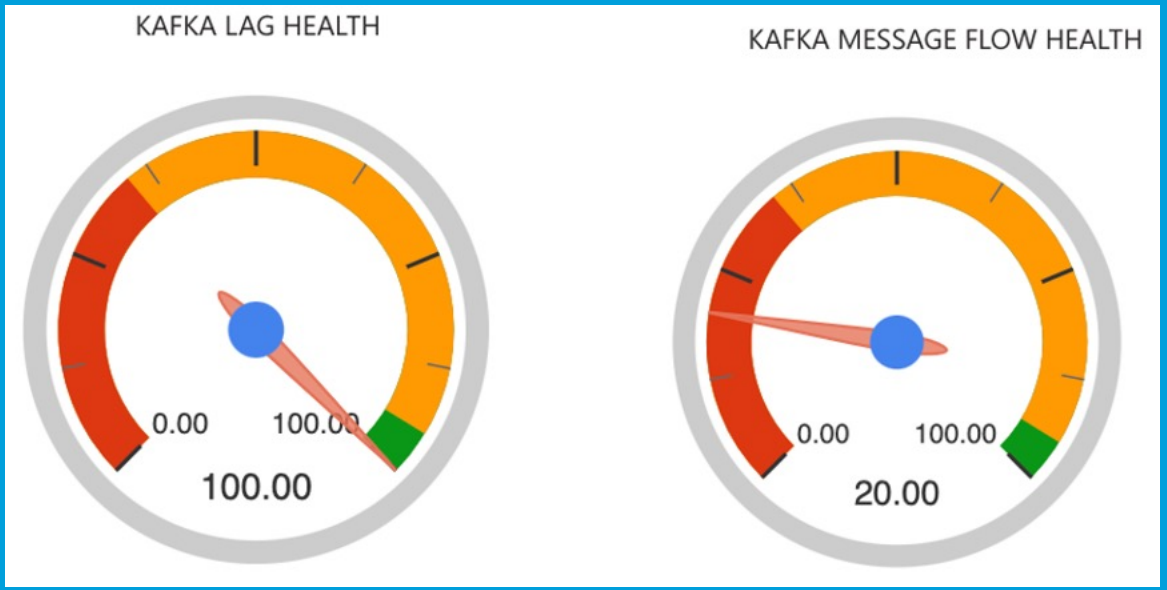
6. Kafka

Kafka

Kafka Lag Health

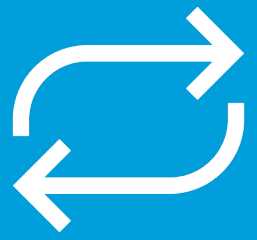
Produce & consume messages

- If lag exists, consumers are down
- Process when received
- Producer flow health



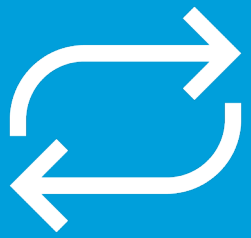
7. Machine Learning Models

Machine Learning Models
Monitoring and Maintenance

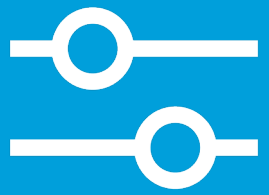


Models get stale, use a feedback loop

Machine Learning Models
Monitoring and Maintenance

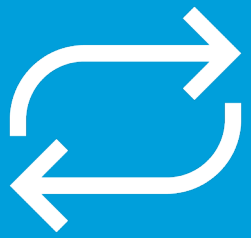


Models get stale, use a feedback loop

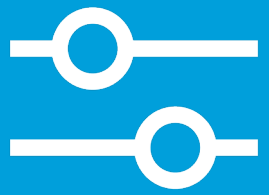


Scalability, accuracy, data & model drifting

Machine Learning Models
Monitoring and Maintenance



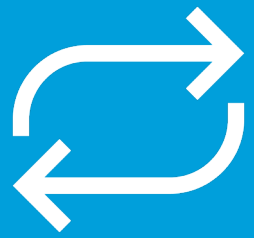
Models get stale, use a feedback loop



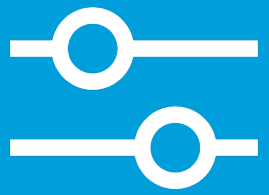
Scalability, accuracy, data & model drifting

Metrics, score, accuracy monitoring

Machine Learning Models
Monitoring and Maintenance



Models get stale, use a feedback loop

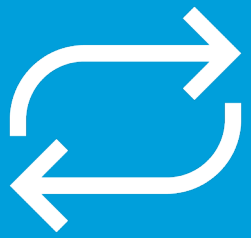


Scalability, accuracy, data & model drifting

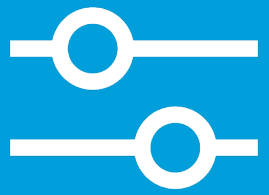
Metrics, score, accuracy monitoring

SLA for ML models

Machine Learning Models
Monitoring and Maintenance



Models get stale, use a feedback loop



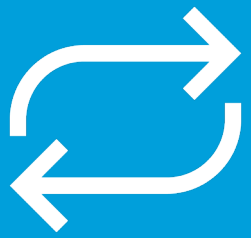
Scalability, accuracy, data & model drifting

Metrics, score, accuracy monitoring

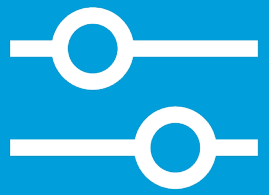
SLA for ML models

Model quality and making connections

Machine Learning Models
Monitoring and Maintenance



Models get stale, use a feedback loop



Scalability, accuracy, data & model drifting

Metrics, score, accuracy monitoring

SLA for ML models

Model quality and making connections

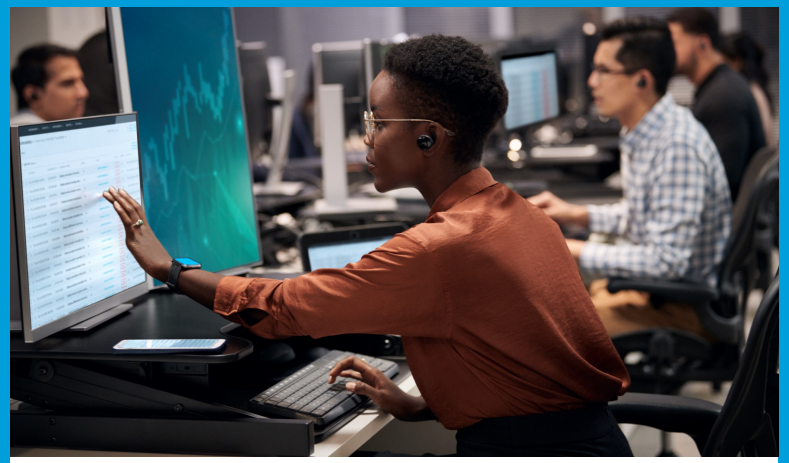
Test connection and service calls

Machine Learning Models
Tracer

Take Inventory of ML models.

Machine Learning Models
Tracer

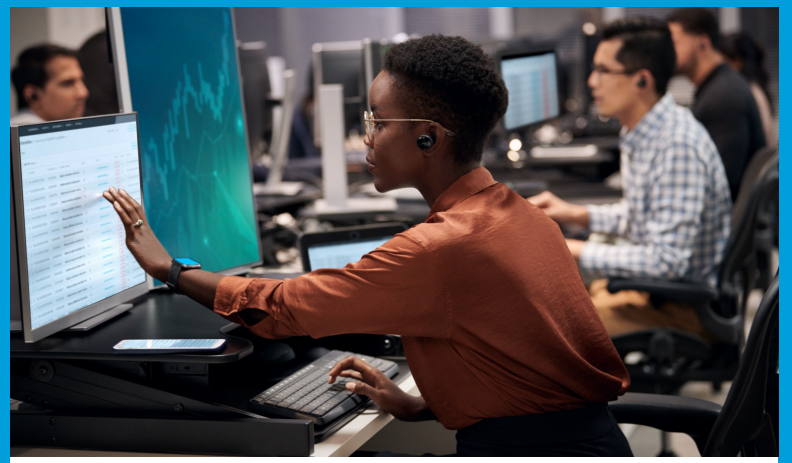
Take Inventory of ML models.



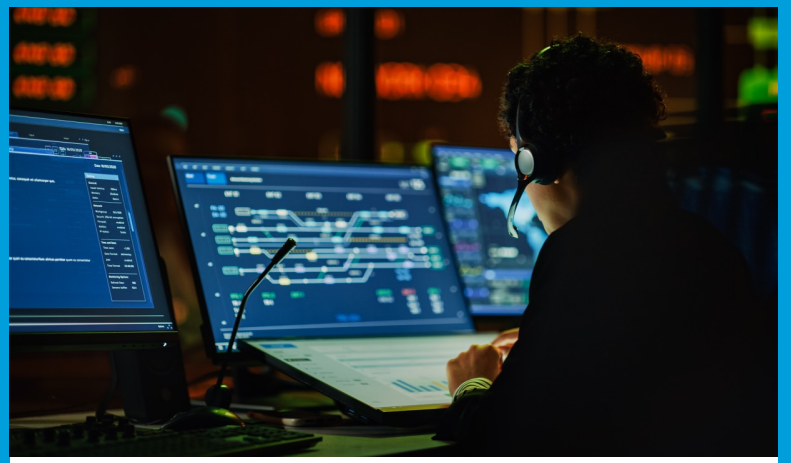
Create payload with dummy data.

Machine Learning Models
Tracer

Take Inventory of ML models.



Create payload with dummy data.



Verify results

8. Certificates

Certificates

Certificates are updated once a year. This impacts connections due to authentication.

Monitor rules for certificates

- All physical certificates on each server
- Based on physical machines, not systems
- Check is run every morning
- Certificate status, sends alert when certificate is about to expire

9. Feeds

Feeds

Record Absentee Detection

Rules run against Mongo DB collections

- Check as records are coming in
- If a feed goes away, we want to be alerted
- Application-level and case-level monitoring

10. Alerting

Alerting
Distribution of Alerts

Variety of methods (email, instant messaging, text message, phone calls, etc.)

Alerting
Distribution of Alerts

Variety of methods (email, instant messaging, text message, phone calls, etc.)

Machine Learning helps eliminate false positives

Alerting
Distribution of Alerts

Variety of methods (email, instant messaging, text message, phone calls, etc.)

Machine Learning helps eliminate false positives

Multi-escalation Engine, Production Support, Escalation Management

Alerting
Distribution of Alerts

Variety of methods (email, instant messaging, text message, phone calls, etc.)

Machine Learning helps eliminate false positives

Multi-escalation Engine, Production Support, Escalation Management

Correlating alerts across components and grouping into a single case

Alerting
Distribution of Alerts

Variety of methods (email, instant messaging, text message, phone calls, etc.)

Machine Learning helps eliminate false positives

Multi-escalation Engine, Production Support, Escalation Management

Correlating alerts across components and grouping into a single case

Greatly reduce noise

Alerting
Distribution of Alerts

Variety of methods (email, instant messaging, text message, phone calls, etc.)

Machine Learning helps eliminate false positives

Multi-escalation Engine, Production Support, Escalation Management

Correlating alerts across components and grouping into a single case

Greatly reduce noise

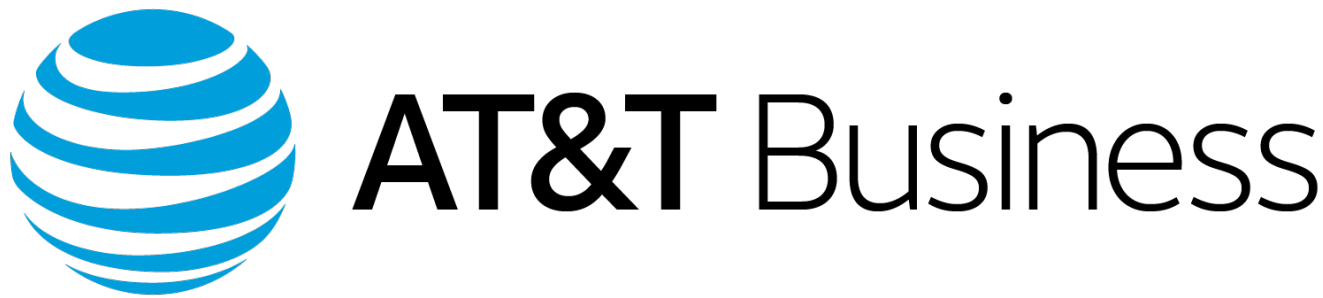
Created targeted remediation group for each business flow

Conclusion

All encapsulating monitoring and alerting tool

Fraud Application Hardening – complete protection

- Customized rules & logic
- Correlate all alerts based on unique key
- Aggregate and generate one alert


AT&T Business