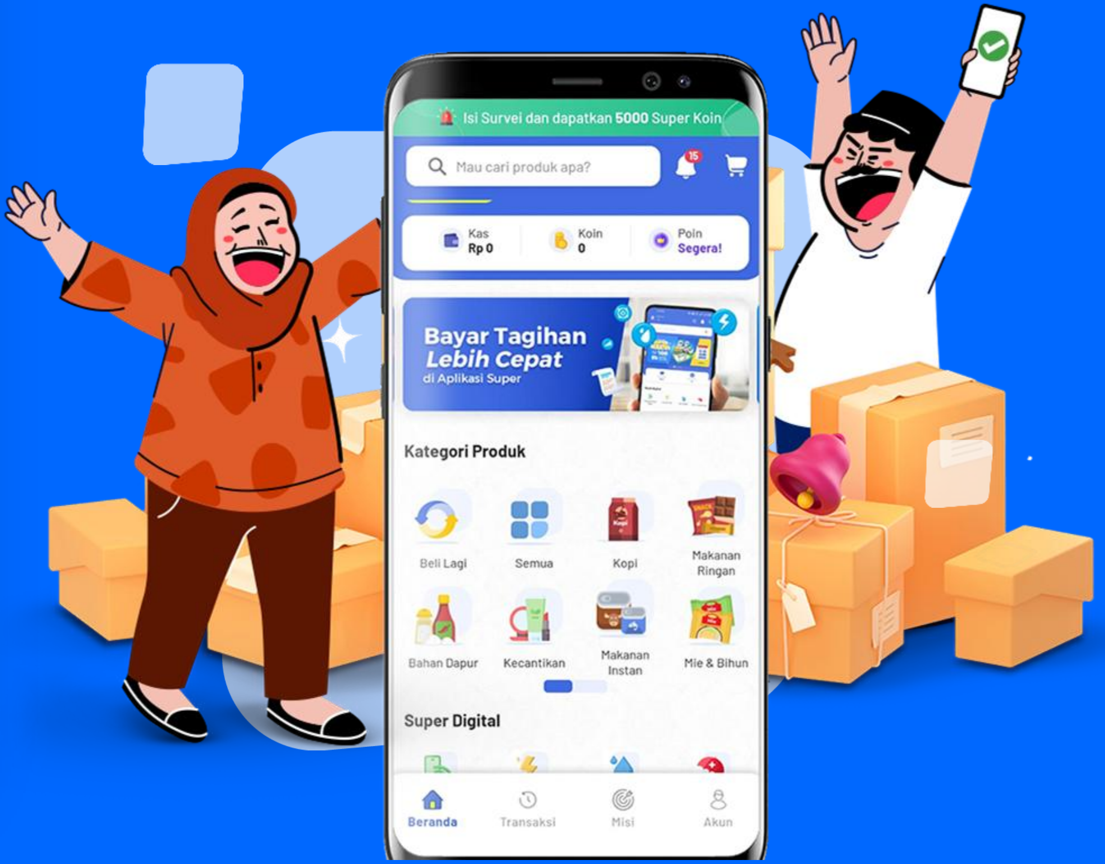
SUPERAPP

Fortifying Security, Continuously: Building Resilience in a Digital Native Company



Bayu Aji

Site Reliability Engineer - SuperApp (YC W18)

CISO Indonesia | 2025

#BeraniJadiLebih

What is SuperApp (YC W18) ?

- First social commerce platform in Indonesia
- Aims to solve economic inequality across cities for Indonesia's future economy
- An agent-led commerce that enables community leaders to become retailers within their communities.
- ISO 9001:2015 and 27001:2022 certified
- One of the top YC companies

🏆 **Ranked on LinkedIn Top Startups**

Jangkauan Distribusi SuperApp

Beroperasi di seluruh area
Jawa Timur & Makassar.

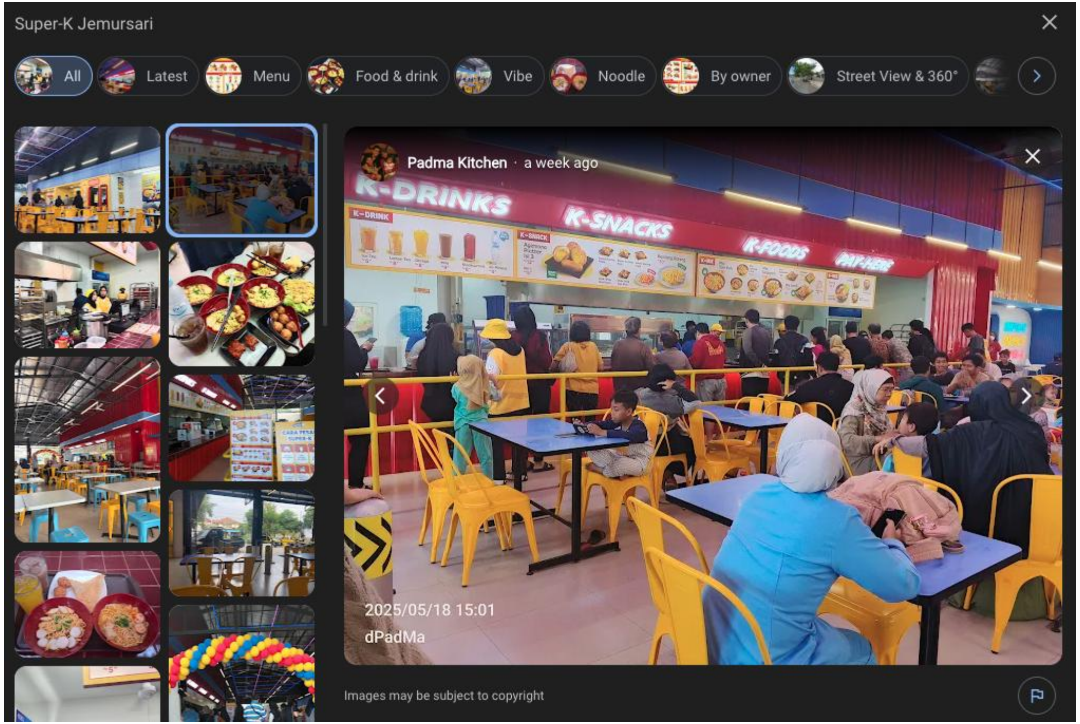
SuperApp Business Units

40k Warungs /Agents

10+ Warehouses & Logistics

40+ Principals / Brands

SuperApp Business Units



Super-K Jemursari

Images may be subject to copyright

Challenges

Growing complexity of Apps and ERP increases security risks

Fast-moving teams and limited resources challenge best practice adoption

Reactive security is no longer enough

From Reaction to Resilience: Our Security Shift

Challenge	How We're Addressing It
Growing complexity increases attack surface	We adopt a **secure-by-design** approach by embedding security reviews, IaC scanning, and secure coding into our development and architectural processes.
Limited resources vs ideal best practices	We prioritize **scalable and high-impact practices** such as IAM policy enforcement, container image scanning, and integrated controls designed to work within our delivery pace and team capacity.
Reactive model is no longer enough	We are shifting toward a more **proactive security posture** by integrating custom alerting, lightweight observability, and periodic threat assessments into our operations.

Navigating Implementation Challenges: Secure-by-Design

Requires mindset shift across engineering teams (case mengubah mindset)

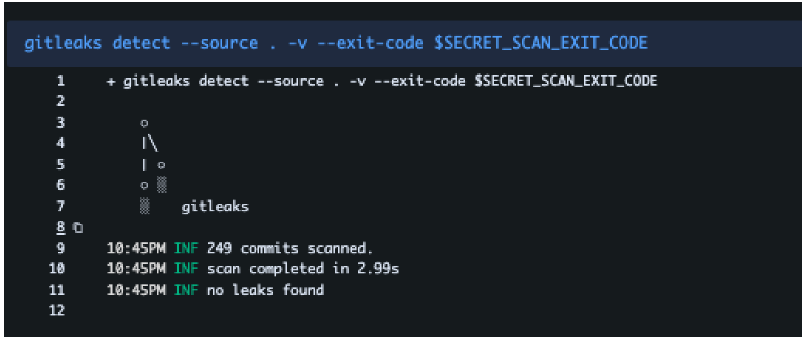
Everyone involved in the engineering process needs to change how they think about security. Instead of considering security as an afterthought or an add-on, it should be integrated into every part of the development lifecycle.

How we're addressing it:

- Training and Awareness
- Leadership Support
- Incorporating Security in Design
- Feedback Loops

Navigating Implementation Challenges: Secure-by-Design

Requires mindset shift across engineering teams (case mengubah mindset)



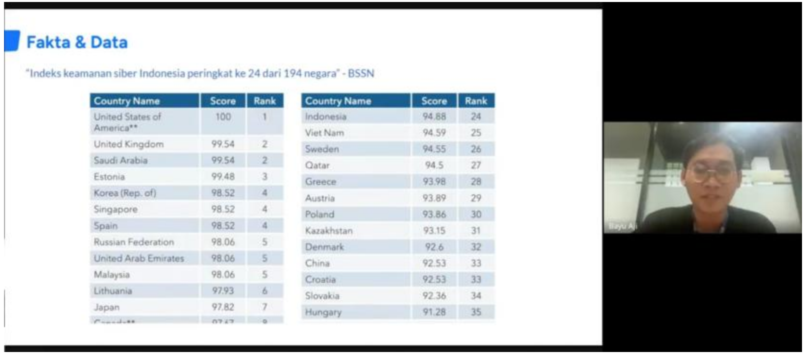
```
gitleaks detect --source . -v --exit-code $SECRET_SCAN_EXIT_CODE

+ gitleaks detect --source . -v --exit-code $SECRET_SCAN_EXIT_CODE


      ○
      │╲
      │ ○
      ○ ░
      ░    gitleaks

10:45PM INF 249 commits scanned.
10:45PM INF scan completed in 2.99s
10:45PM INF no leaks found

```



Fakta & Data

"Indeks keamanan siber Indonesia peringkat ke 24 dari 194 negara" - BSSN

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.47	8

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35

Secure-by-Design Implementation

Navigating Implementation Challenges: Secure-by-Design

Balancing between delivery speed and review depth

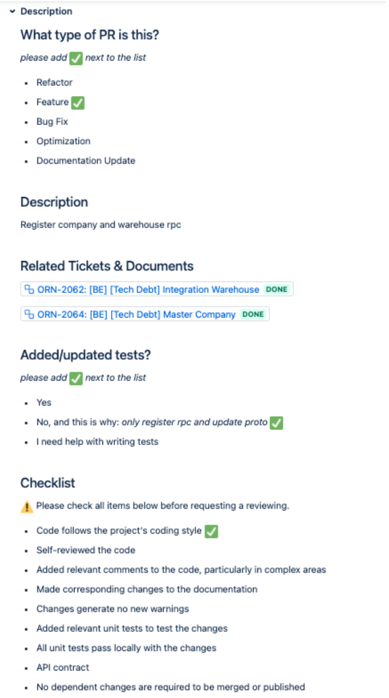
On one hand, teams often need to deliver software rapidly to meet business demands. On the other hand, skipping or rushing the review process can introduce vulnerabilities, defects, or suboptimal solutions into the system.

How we're addressing it:

- Prioritize Critical Reviews
- Automated Code Reviews
- Incremental Reviews
- Establish Clear Review Guidelines
- Iterative Development

Navigating Implementation Challenges: Secure-by-Design

Balancing between delivery speed and review depth



Description

What type of PR is this?

please add ✅ next to the list

- Refactor
- Feature ✅
- Bug Fix
- Optimization
- Documentation Update

Description

Register company and warehouse rpc

Related Tickets & Documents

ORN-2062: [BE] [Tech Debt] Integration Warehouse DONE

ORN-2064: [BE] [Tech Debt] Master Company DONE

Added/updated tests?

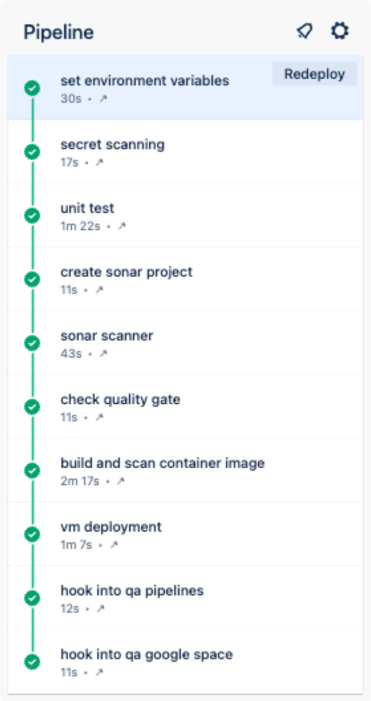
please add ✅ next to the list

- Yes
- No, and this is why: *only register rpc and update proto* ✅
- I need help with writing tests

Checklist

⚠ Please check all items below before requesting a reviewing.

- Code follows the project's coding style ✅
- Self-reviewed the code
- Added relevant comments to the code, particularly in complex areas
- Made corresponding changes to the documentation
- Changes generate no new warnings
- Added relevant unit tests to test the changes
- All unit tests pass locally with the changes
- API contract
- No dependent changes are required to be merged or published



Pipeline

- ✓ set environment variables 30s • ↗
- ✓ secret scanning 17s • ↗
- ✓ unit test 1m 22s • ↗
- ✓ create sonar project 11s • ↗
- ✓ sonar scanner 43s • ↗
- ✓ check quality gate 11s • ↗
- ✓ build and scan container image 2m 17s • ↗
- ✓ vm deployment 1m 7s • ↗
- ✓ hook into qa pipelines 12s • ↗
- ✓ hook into qa google space 11s • ↗

Secure-by-Design Implementation

Navigating Implementation Challenges: Secure-by-Design

Tooling gaps or learning curve on secure practices

Many security concepts and technologies can be complex and unfamiliar to developers, especially if they have not had much experience with secure coding or vulnerability management.

How we're addressing it:

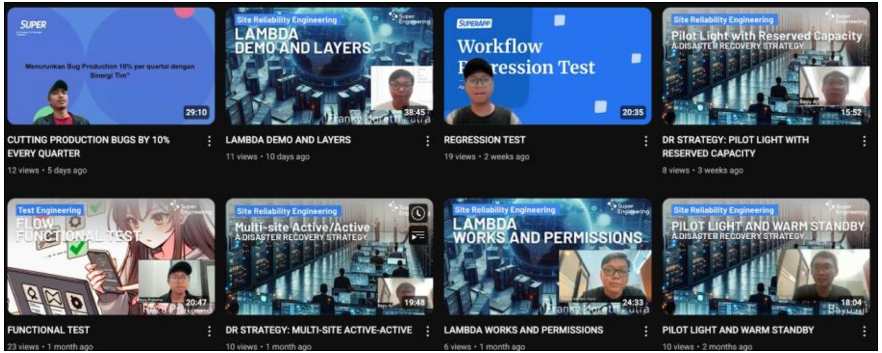
- Invest in Security Tools
- Tool Integration
- Training & Workshops
- Mentorship or Expert Support
- Document Security Best Practices
- Gradual Adoption

Navigating Implementation Challenges: Secure-by-Design

Tooling gaps or learning curve on secure practices

SUPER
TechTalk
" Product Quality: Unit Testing Practices & Automation Test "

SUPER
ngulik
One of The Most Important Thing in Building Software
By Muhammad Nafi' Furqon Diani
Rabu, 21 Mei 2025 pukul 16:00 WIB
@ Alsut Townhall
#BeraniJadiLebih


SUPER
Menurunkan Bug Production 10% per quartal dengan Sinergi Tim"
29:10
Site Reliability Engineering
LAMBDA DEMO AND LAYERS
38:45
SUPERAPP
Workflow Regression Test
20:35
Site Reliability Engineering
Pilot Light with Reserved Capacity
A DISASTER RECOVERY STRATEGY
15:52
Test Engineering
FLOW FUNCTIONAL TEST
20:47
Site Reliability Engineering
Multi-site Active/Active
A DISASTER RECOVERY STRATEGY
19:48
Site Reliability Engineering
LAMBDA WORKS AND PERMISSIONS
24:33
Site Reliability Engineering
PILOT LIGHT AND WARM STANDBY
A DISASTER RECOVERY STRATEGY
18:04

CUTTING PRODUCTION BUGS BY 10% EVERY QUARTER
12 views • 5 days ago

LAMBDA DEMO AND LAYERS
11 views • 10 days ago

REGRESSION TEST
19 views • 2 weeks ago

DR STRATEGY: PILOT LIGHT WITH RESERVED CAPACITY
8 views • 3 weeks ago

FUNCTIONAL TEST
23 views • 1 month ago

DR STRATEGY: MULTI-SITE ACTIVE-ACTIVE
10 views • 1 month ago

LAMBDA WORKS AND PERMISSIONS
6 views • 1 month ago

PILOT LIGHT AND WARM STANDBY
10 views • 2 months ago

Secure-by-Design Implementation

Navigating Implementation Challenges: Scalable and High Impact Practices

Prioritization trade-offs in constrained environments

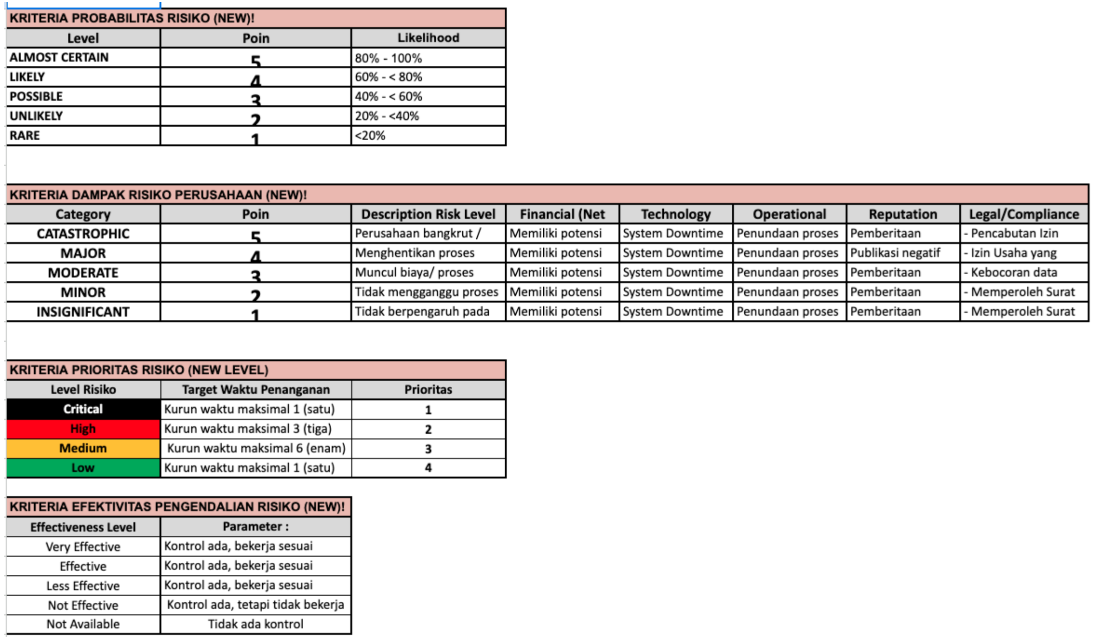
It addresses the challenge of making decisions about which security practices to prioritize when resources (such as time, money, or personnel) are limited.

How we're addressing it:

- Risk-Based Prioritization
- Focus on High-Impact, Low-Cost Practices
- Incremental Security Improvements
- Cross-Functional Collaboration
- Continuous Evaluation

Navigating Implementation Challenges: Scalable and High Impact Practices

Prioritization trade-offs in constrained environments



KRITERIA PROBABILITAS RISIKO (NEW)!

Level	Poin	Likelihood
ALMOST CERTAIN	5	80% - 100%
LIKELY	4	60% - < 80%
POSSIBLE	3	40% - < 60%
UNLIKELY	2	20% - <40%
RARE	1	<20%

KRITERIA DAMPAK RISIKO PERUSAHAAN (NEW)!

Category	Poin	Description Risk Level	Financial (Net	Technology	Operational	Reputation	Legal/Compliance
CATASTROPHIC	5	Perusahaan bangkrut /	Memiliki potensi	System Downtime	Penundaan proses	Pemberitaan	- Pencabutan Izin
MAJOR	4	Menghentikan proses	Memiliki potensi	System Downtime	Penundaan proses	Publikasi negatif	- Izin Usaha yang
MODERATE	3	Muncul biaya/ proses	Memiliki potensi	System Downtime	Penundaan proses	Pemberitaan	- Kebocoran data
MINOR	2	Tidak mengganggu proses	Memiliki potensi	System Downtime	Penundaan proses	Pemberitaan	- Memperoleh Surat
INSIGNIFICANT	1	Tidak berpengaruh pada	Memiliki potensi	System Downtime	Penundaan proses	Pemberitaan	- Memperoleh Surat

KRITERIA PRIORITAS RISIKO (NEW LEVEL)

Level Risiko	Target Waktu Penanganan	Prioritas
Critical	Kurun waktu maksimal 1 (satu)	1
High	Kurun waktu maksimal 3 (tiga)	2
Medium	Kurun waktu maksimal 6 (enam)	3
Low	Kurun waktu maksimal 1 (satu)	4

KRITERIA EFEKTIVITAS PENGENDALIAN RISIKO (NEW)!

Effectiveness Level	Parameter :
Very Effective	Kontrol ada, bekerja sesuai
Effective	Kontrol ada, bekerja sesuai
Less Effective	Kontrol ada, bekerja sesuai
Not Effective	Kontrol ada, tetapi tidak bekerja
Not Available	Tidak ada kontrol

Scalable and High Impact Practices

Navigating Implementation Challenges: Scalable and High Impact Practices

Ensuring consistency across diverse microservices or teams

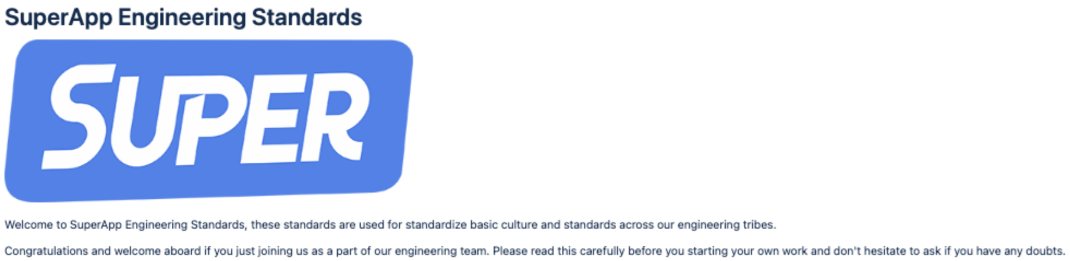
As teams work on different microservices, there’s a risk that each team might adopt its own approach to security, leading to inconsistencies. Inconsistent practices can create gaps or vulnerabilities in the system and make it harder to manage security at scale.

How we're addressing it:

- Centralized Security Policies
- Shared Security Tools and Frameworks
- Security Best Practices Templates
- Cross-Team Collaboration and Reviews

Navigating Implementation Challenges: Scalable and High Impact Practices

Ensuring consistency across diverse microservices or teams



SuperApp Engineering Standards

Welcome to SuperApp Engineering Standards, these standards are used for standardize basic culture and standards across our engineering tribes.

Congratulations and welcome aboard if you just joining us as a part of our engineering team. Please read this carefully before you starting your own work and don't hesitate to ask if you have any doubts.

Scalable and High Impact Practices

Navigating Implementation Challenges: Scalable and High Impact Practices

Operationalizing security without blocking delivery

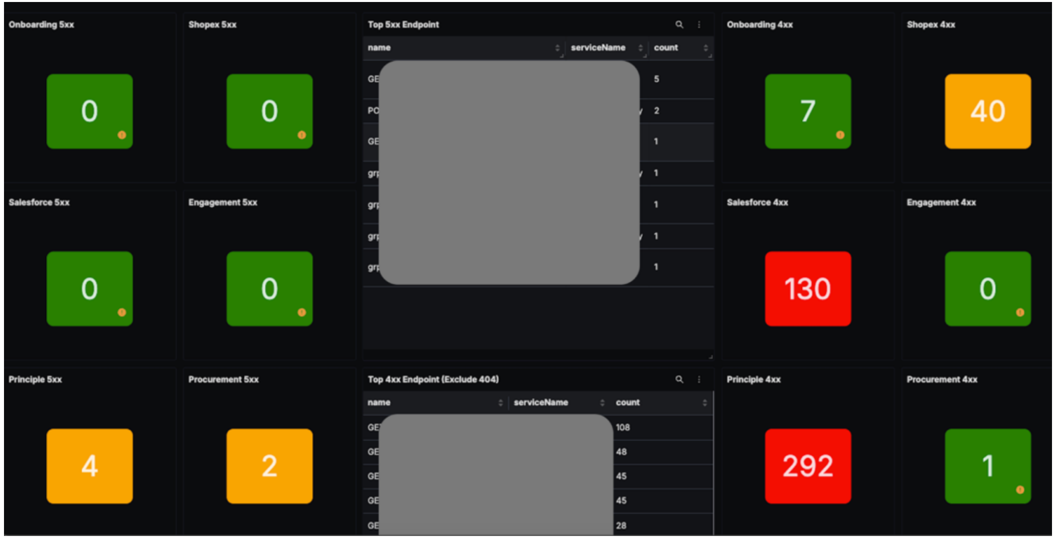
As organizations scale, integrating security into the development lifecycle is essential, but security measures should not create bottlenecks that slow down delivery times or reduce productivity.

How we're addressing it:

- Integrate Security in CI/CD Pipelines
- Shift-Left Security
- Prioritize Security Issues Based on Risk
- Feedback Loops and Continuous Improvement
- Monitor Security Impact in Real-Time

Navigating Implementation Challenges: Scalable and High Impact Practices

Operationalizing security without blocking delivery



Onboarding 5xx

0

Shopex 5xx

0

Top 5xx Endpoint

name	serviceName	count
[redacted]	[redacted]	5
[redacted]	[redacted]	2
[redacted]	[redacted]	1
[redacted]	[redacted]	1
[redacted]	[redacted]	1
[redacted]	[redacted]	1
[redacted]	[redacted]	1

Onboarding 4xx

7

Shopex 4xx

40

Salesforce 5xx

0

Engagement 5xx

0

Salesforce 4xx

130

Engagement 4xx

0

Principle 5xx

4

Procurement 5xx

2

Top 4xx Endpoint (Exclude 404)

name	serviceName	count
[redacted]	[redacted]	108
[redacted]	[redacted]	48
[redacted]	[redacted]	45
[redacted]	[redacted]	45
[redacted]	[redacted]	28

Principle 4xx

292

Procurement 4xx

1

Scalable and High Impact Practices

Navigating Implementation Challenges: Proactive Security Posture

Limited detection coverage without full SIEM/XDR

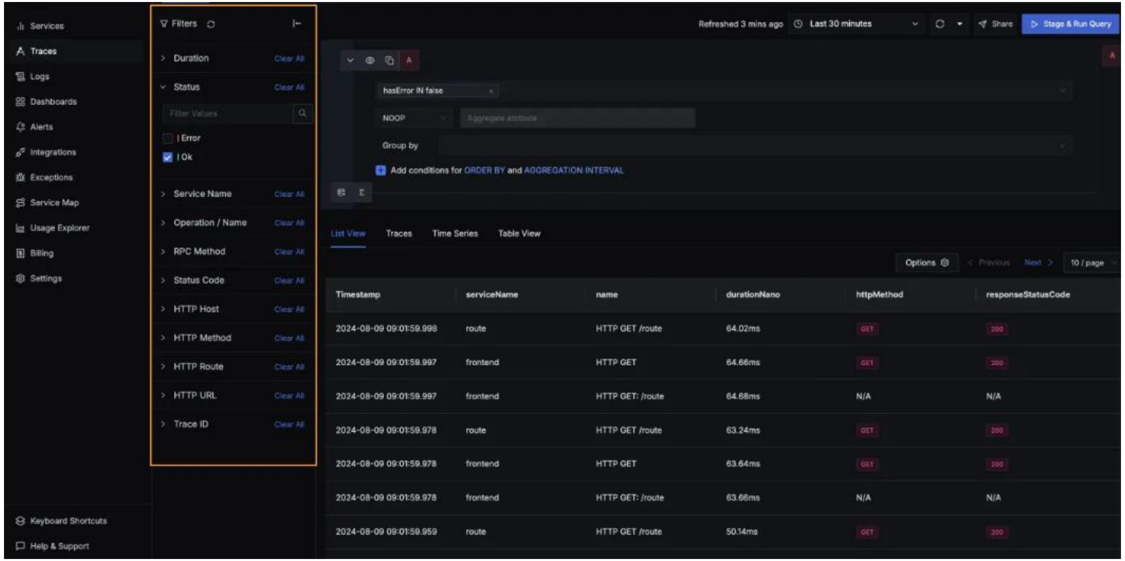
Challenge of maintaining a strong security posture when the organization does not have a complete security monitoring and detection system in place.

How we're addressing it:

- Incremental Security Monitoring
- Leverage Cloud-Native Security Tools
- Data Aggregation and Correlation
- Threat Intelligence Feeds
- Regular Vulnerability Scanning and Penetration Testing
- Hybrid Approach

Navigating Implementation Challenges: Proactive Security Posture

Limited detection coverage without full SIEM/XDR



☐ | Error
☑ | Ok

hasError IN false

NOOP

Group by

Add conditions for ORDER BY and AGGREGATION INTERVAL

Timestamp	serviceName	name	durationNano	httpMethod	responseStatusCode
2024-08-09 09:01:59.998	route	HTTP GET /route	64.02ms	GET	200
2024-08-09 09:01:59.997	frontend	HTTP GET	64.66ms	GET	200
2024-08-09 09:01:59.997	frontend	HTTP GET: /route	64.68ms	N/A	N/A
2024-08-09 09:01:59.978	route	HTTP GET /route	63.24ms	GET	200
2024-08-09 09:01:59.978	frontend	HTTP GET	63.64ms	GET	200
2024-08-09 09:01:59.978	frontend	HTTP GET: /route	63.66ms	N/A	N/A
2024-08-09 09:01:59.959	route	HTTP GET /route	50.14ms	GET	200

Proactive Security Posture

Navigating Implementation Challenges: Proactive Security Posture

Custom alerting prone to noise if not tuned well

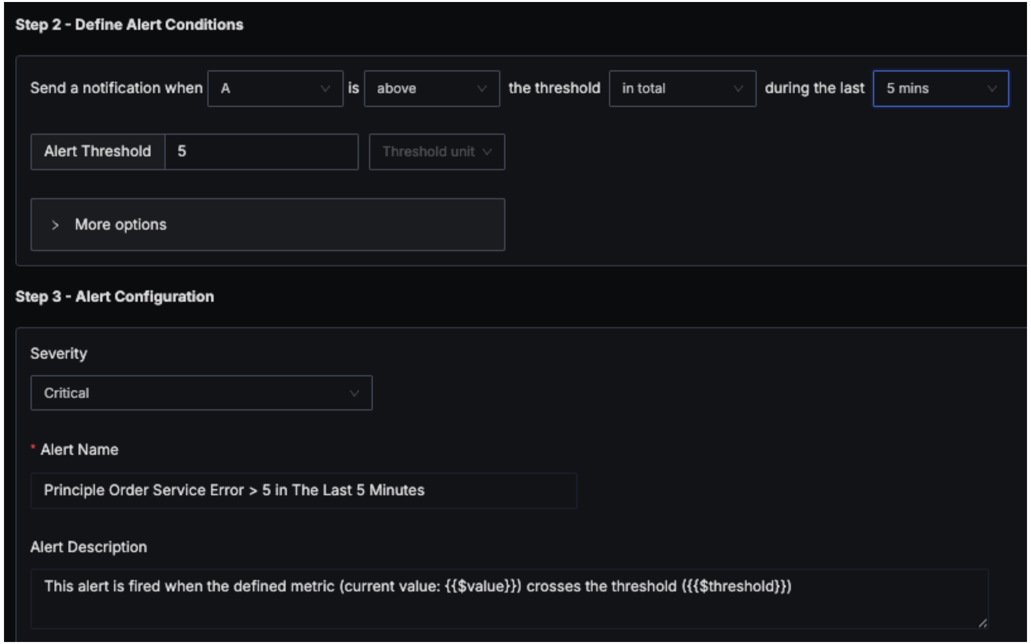
Challenge of creating an effective alerting system that can accurately notify teams of genuine threats without overwhelming them with false positives or irrelevant notifications.

How we're addressing it:

- Refining Alert Criteria
- Prioritization and Severity Levels
- False Positive Management
- Threshold Adjustments Based on Context
- Regular Review of Alerts

Navigating Implementation Challenges: Proactive Security Posture

Custom alerting prone to noise if not tuned well



Step 2 - Define Alert Conditions

Send a notification when A is above the threshold in total during the last 5 mins

Alert Threshold: 5

Threshold unit

Step 3 - Alert Configuration

Severity: Critical

* Alert Name: Principle Order Service Error > 5 in The Last 5 Minutes

Alert Description: This alert is fired when the defined metric (current value: {{$value}}) crosses the threshold ({{$threshold}})

Proactive Security Posture

Navigating Implementation Challenges: Proactive Security Posture

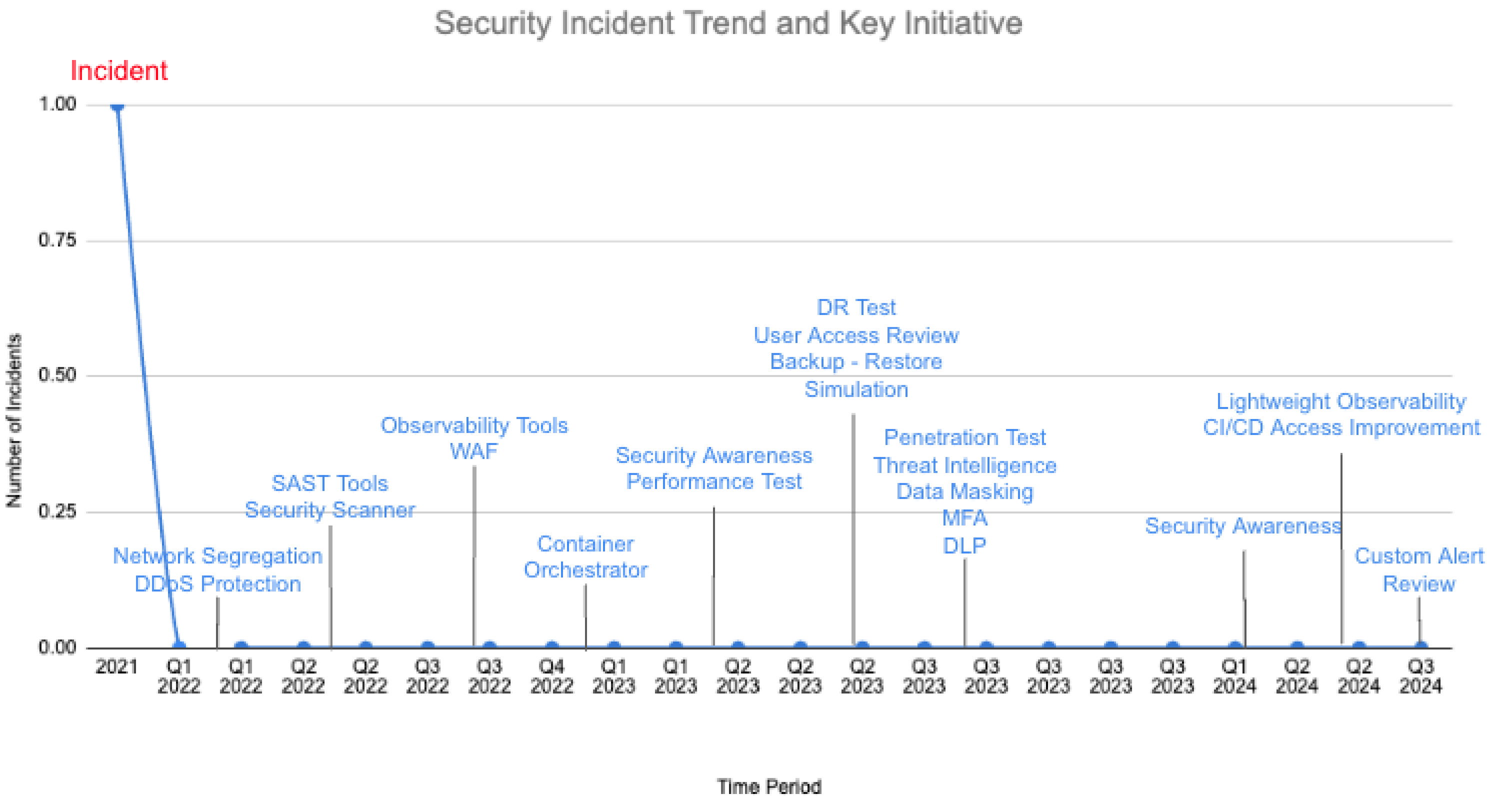
Difficult to measure ROI (Return of Investment) of proactive effort upfront

Challenge of quantifying the value of proactive security efforts before they yield measurable results.

How we're addressing it:

- Track Metrics that Indicate Prevention
- Cost Avoidance Calculation
- Incident Impact Reduction
- Case Studies and Historical Data
- Executive Communication

Key Initiatives and Their Impact on Incidents Over Time



The Business Impact

Increased system availability to **99.99%**

Deployment time improved by 8.5%, accelerating the delivery of key features

Customer trust reflects our **4.4/5 rating.**

2% of annual revenue saved through proactive cybersecurity investments and risk mitigation efforts.

Lessons Learned and Future Plans

What We’ve Learned	Where We’re Heading
Continuous security > reactive fixes	Mature observability & alert tuning
Pragmatic approach works	CI/CD & infra-level integration
Culture matters	Security education across roles
Early wins are hard to measure	From control-heavy to impact-driven

SUPERAPP

Thank You

Terima Kasih