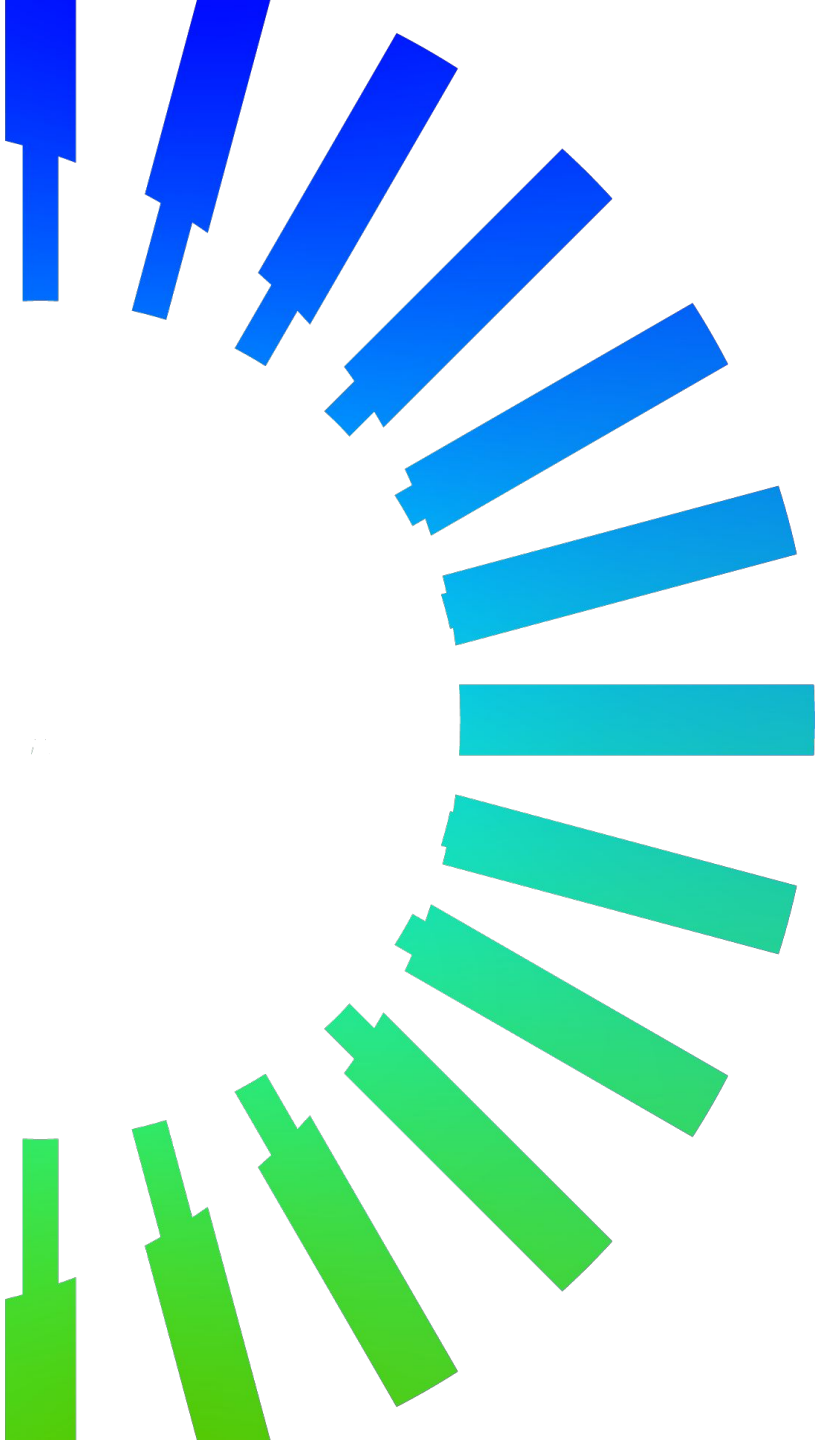


Understanding threat landscape using Threat Composer

Shilpa Nagavara
Software Architect, G-P

Ayush Modi
Sr. Data Scientist, G-P

Rakshit Chawla
Software Engineer, G-P

AWS Community Day Bengaluru, 2025.

Housekeeping

Agenda

- Why threat modelling?
- Data flow diagramming
- Usecase - Notifications
- STRIDE framework
- Usecase - Gia chatbot
- Common mitigations
- Threat composer

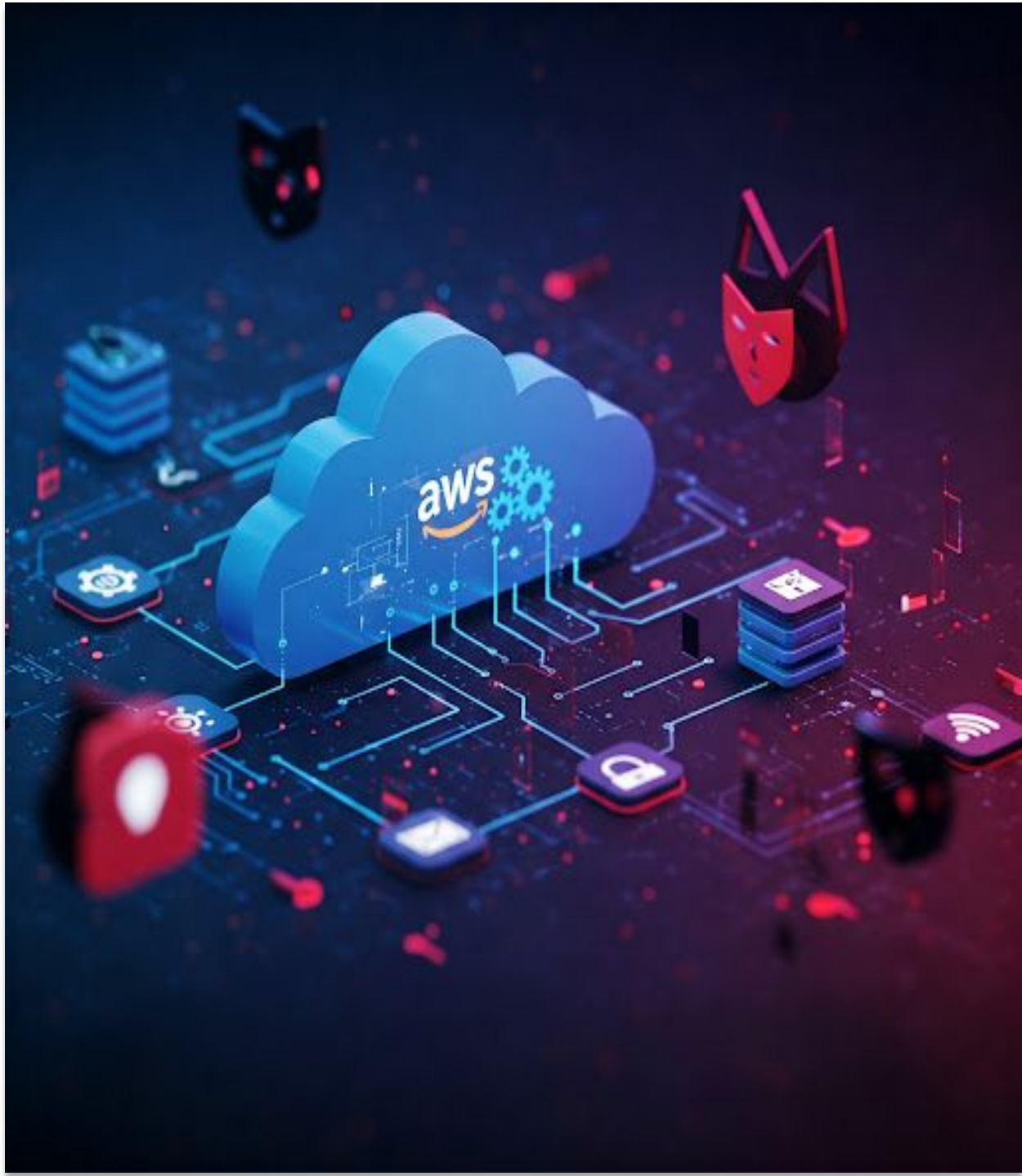
Key takeaways

- An understanding threat modeling concepts
- Identify different elements in an architecture
- Learn how to draw a data flow diagram
- Identify threats using STRIDE framework
- Learn about common mitigation techniques
- Use Threat Composer to record threats, assumptions and mitigations and generate a report

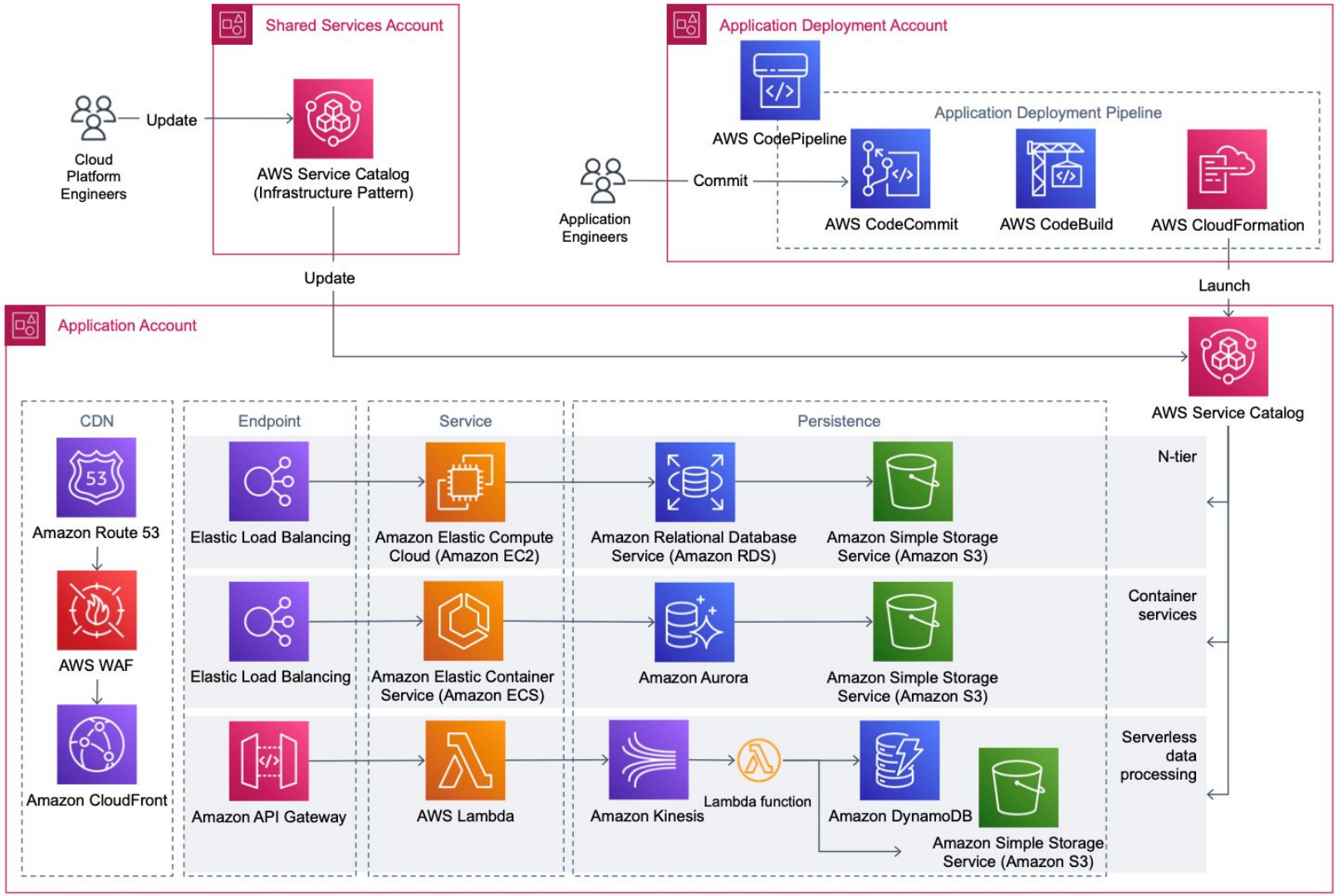
Why threat modelling?

Navigating the

Complex Cloud Landscape



The dynamic cloud threat landscape



High cost of Reactive Security

Security breach

Downtime

Financial implications

Customer and Stakeholder

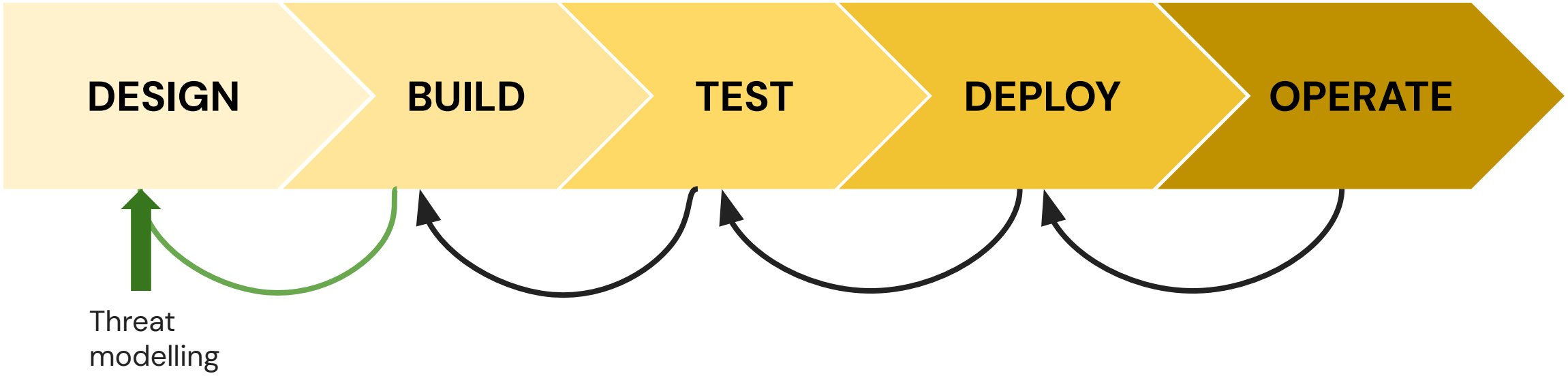
TRUST

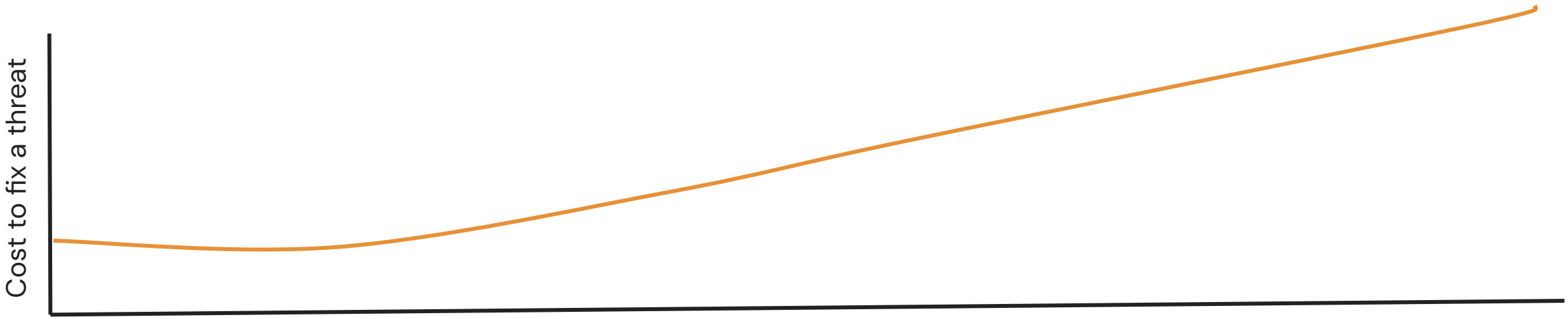
Data loss

Compliance violations

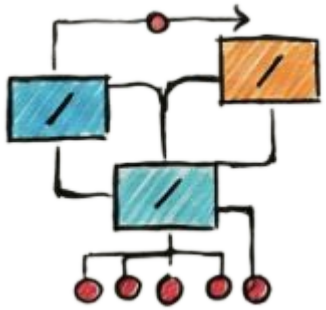
Legal hassles

Shift Left with Threat Modeling



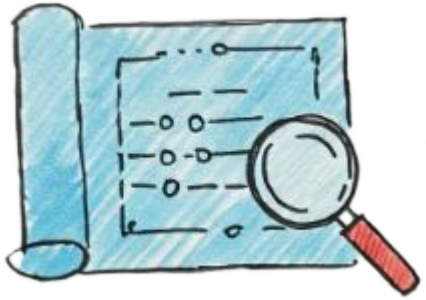


What is Threat Modeling?



DIAGRAM

Understand the system



IDENTIFY

Brainstorm threats

MITIGATE

Define controls

VALIDATE

Test controls

Software Engineer

Software Architect

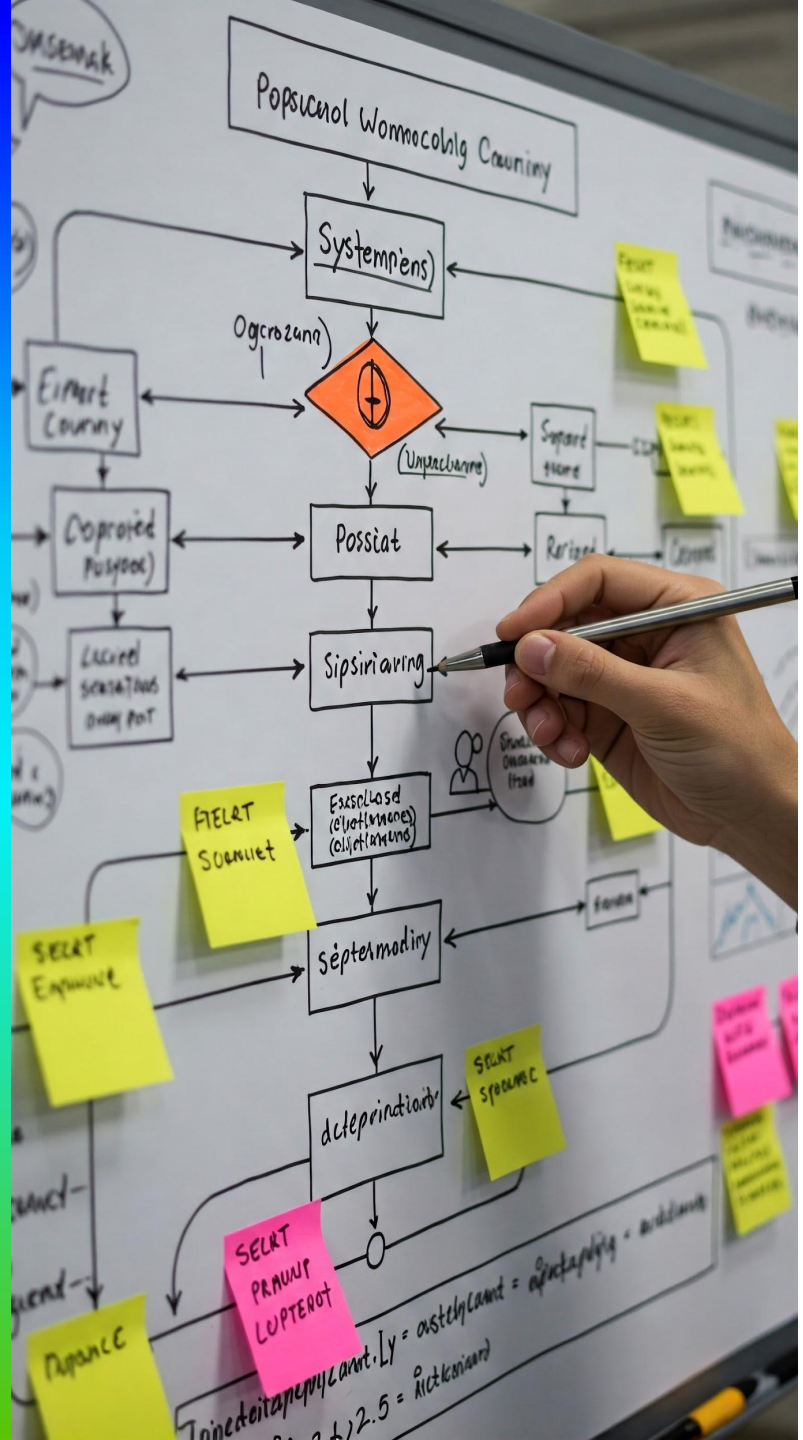
Engineering Manager

Product Manager

Cloud Engineer

Key Benefits of Threat Modeling

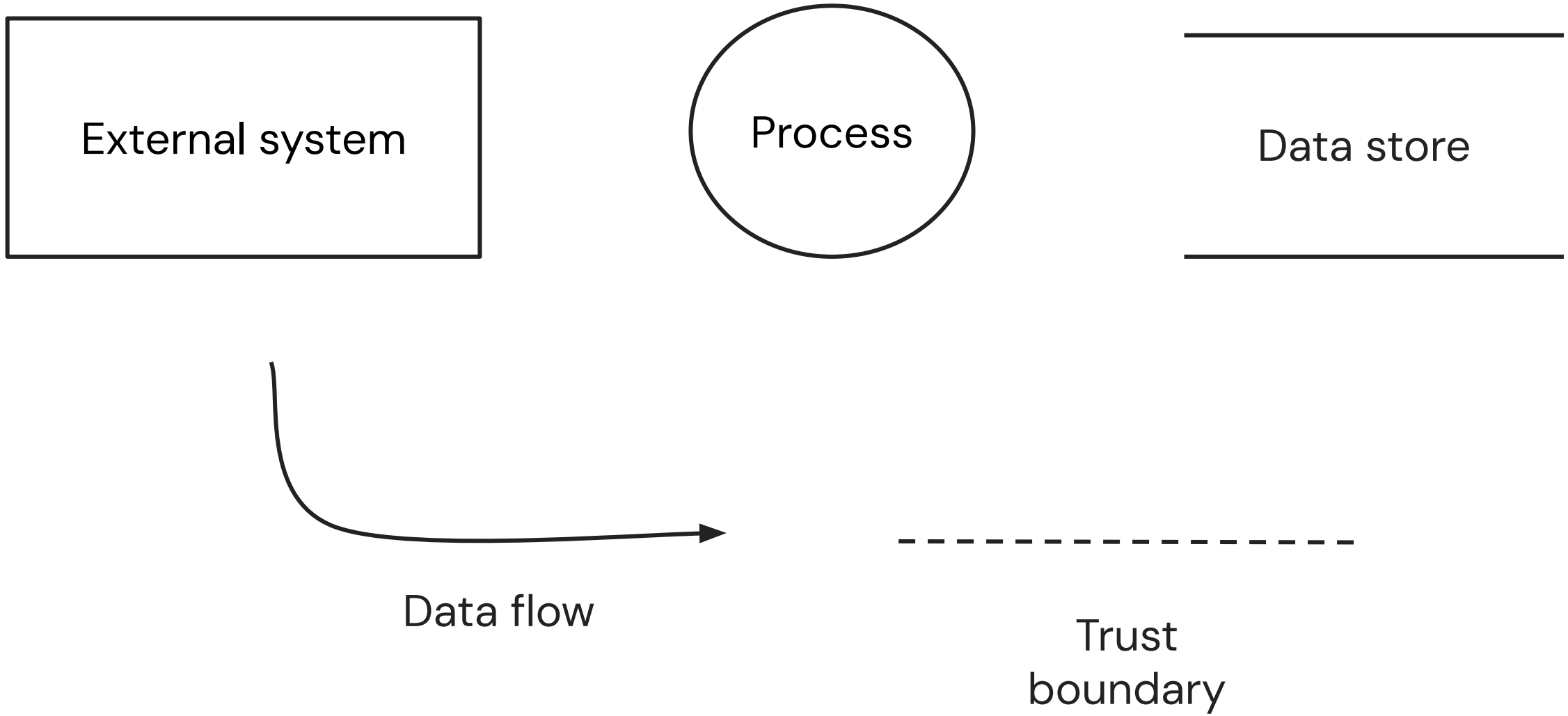
- ✓ Identifies design flaws early
- ✓ Prioritizes security efforts effectively
- ✓ Improves overall security posture
- ✓ Reduces remediation costs & time
- ✓ Enhances team collaboration
- ✓ Aids compliance & trust
- ✓ Builds security-aware culture



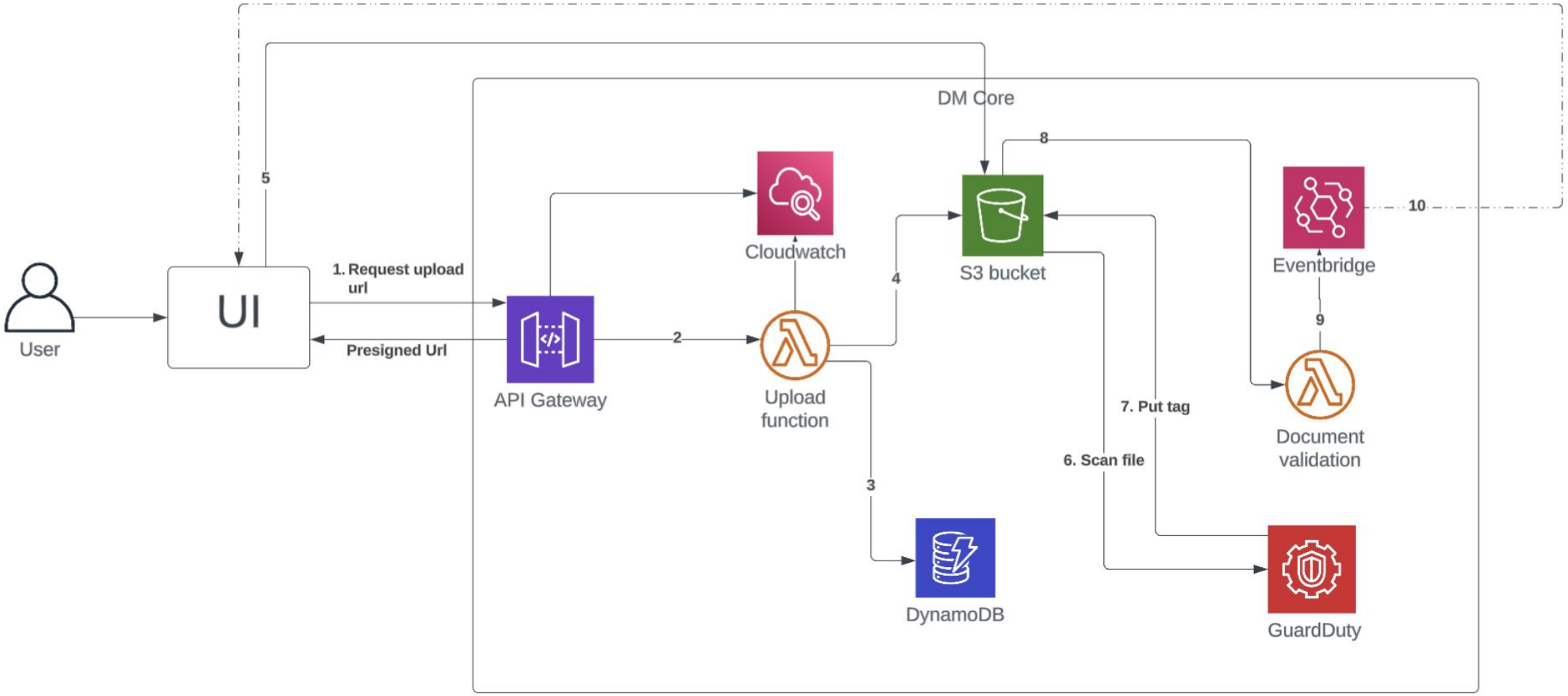
Data flow diagramming

Understanding the system

Elements


External system
Process
Data store
Data flow
Trust
boundary

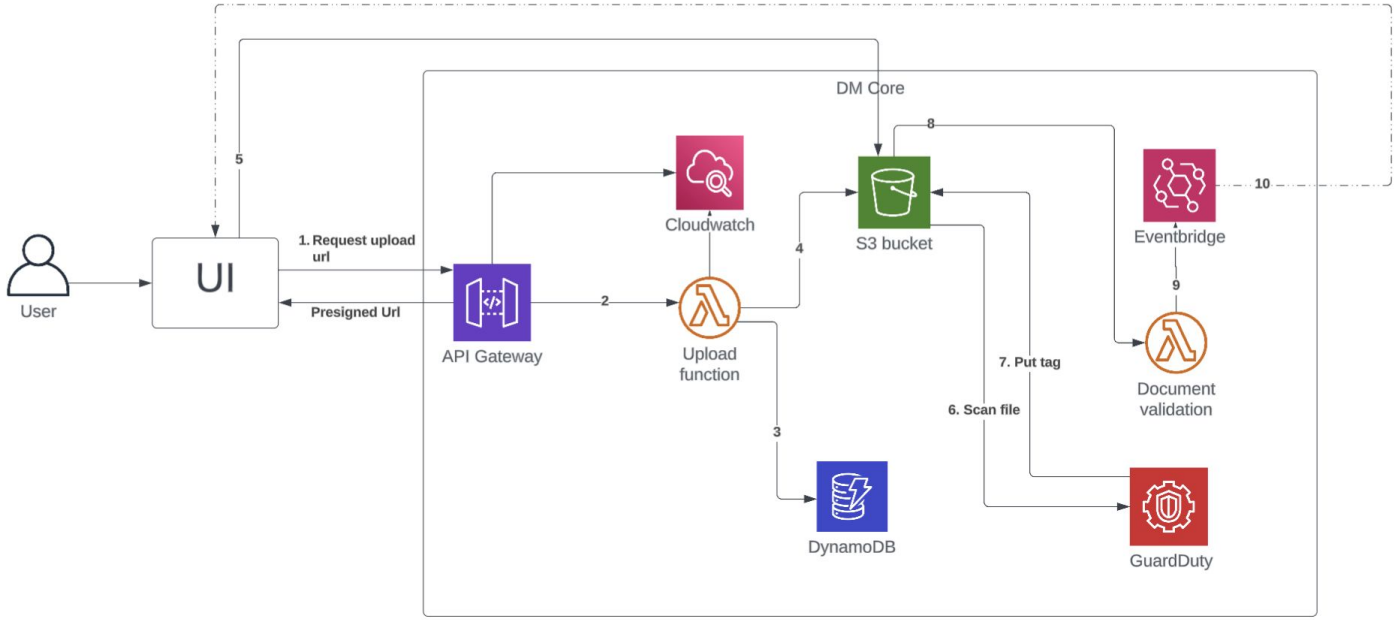
Identify the different elements



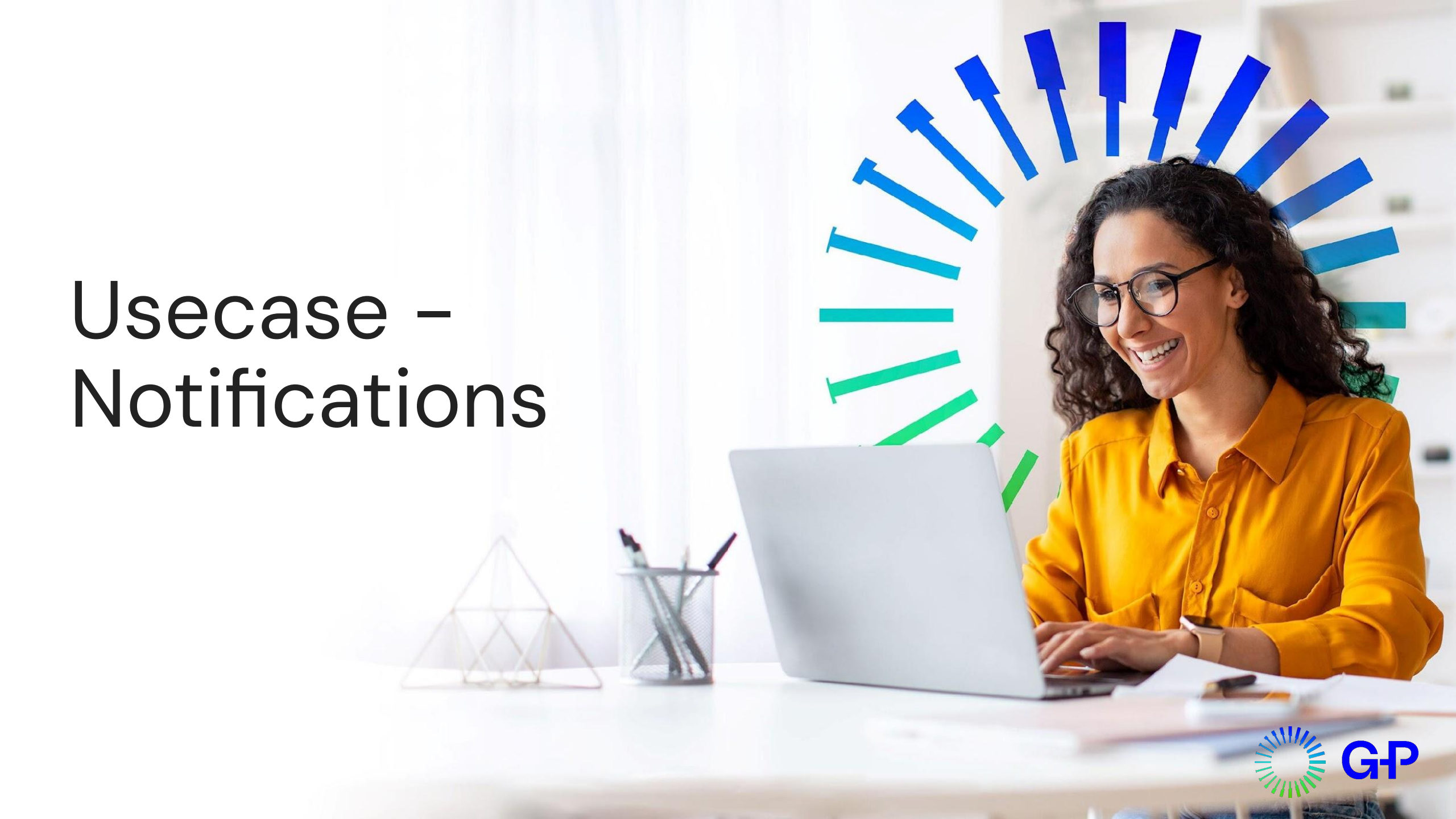
Document management system

Identify the different elements

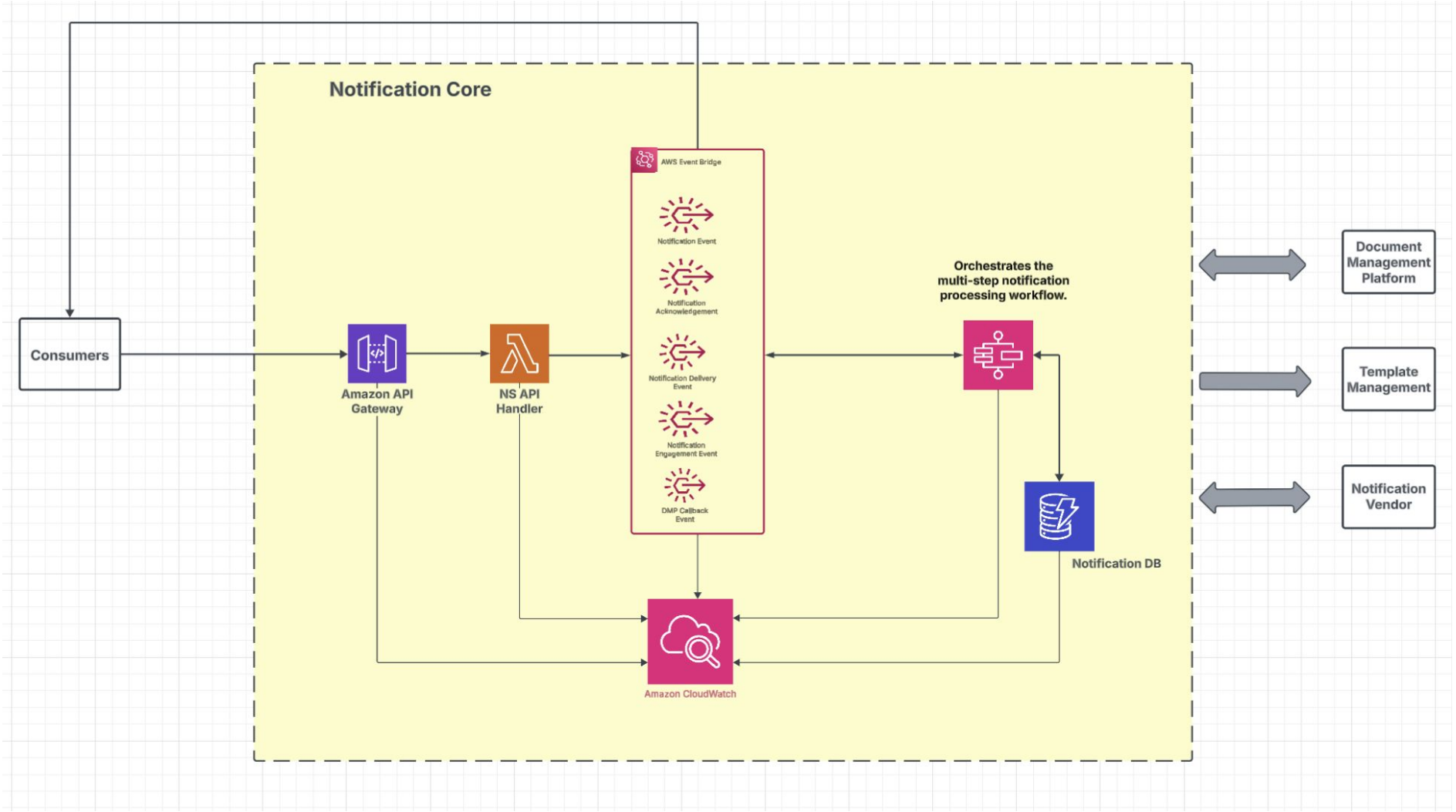
Event bridge	Process
Document validation lambda	Process
Guard Duty	Process
S3 Bucket	Data store
DynamoDB	Data store
Upload lambda	Process
Cloudwatch	Data store
API Gateway	Process
Network connections	Data flow
UI	External system
User	



Usecase – Notifications



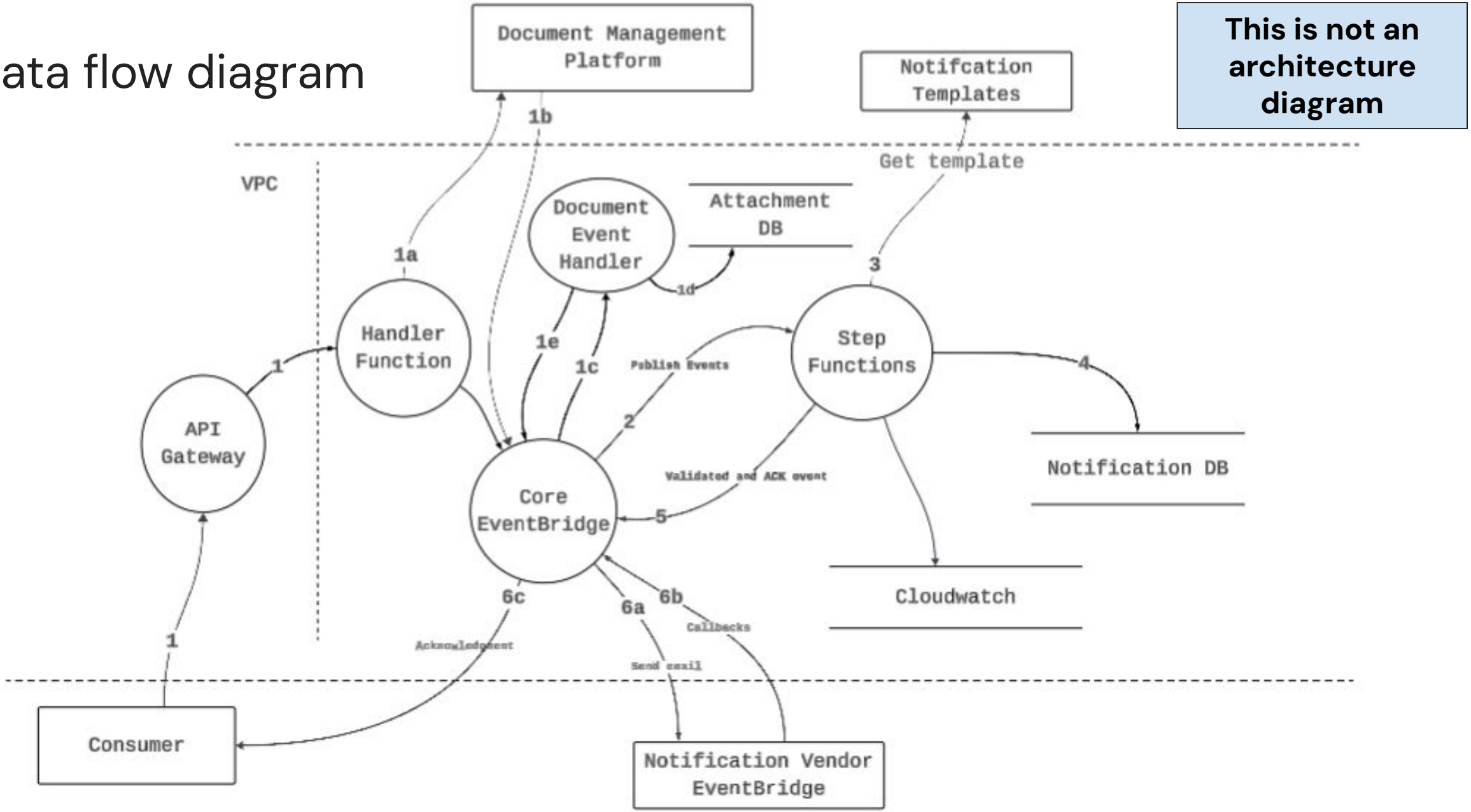
Architecture

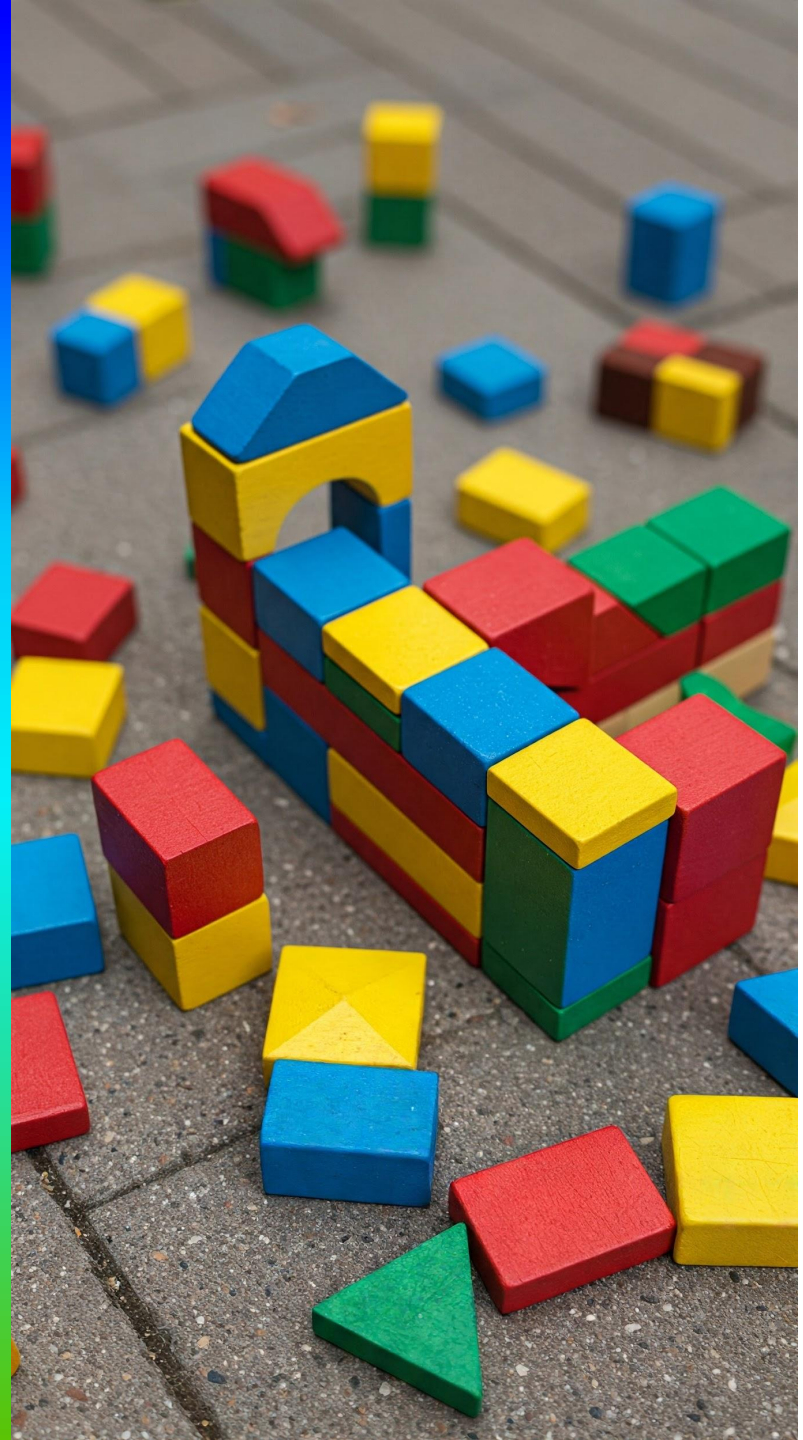


Identify the elements of data flow

Draw the data flow diagram

Data flow diagram





STRIDE

A framework for threat identification

STRIDE: Categorizing Threats Systematically

Spoofing

Impersonating something or someone else

Tampering

Modifying data or code

Repudiation

Claiming to have not performed an action

Information Disclosure

Exposing information to someone not authorized to see it

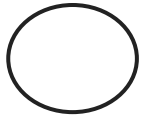
Denial of Service

Deny or degrade service to users

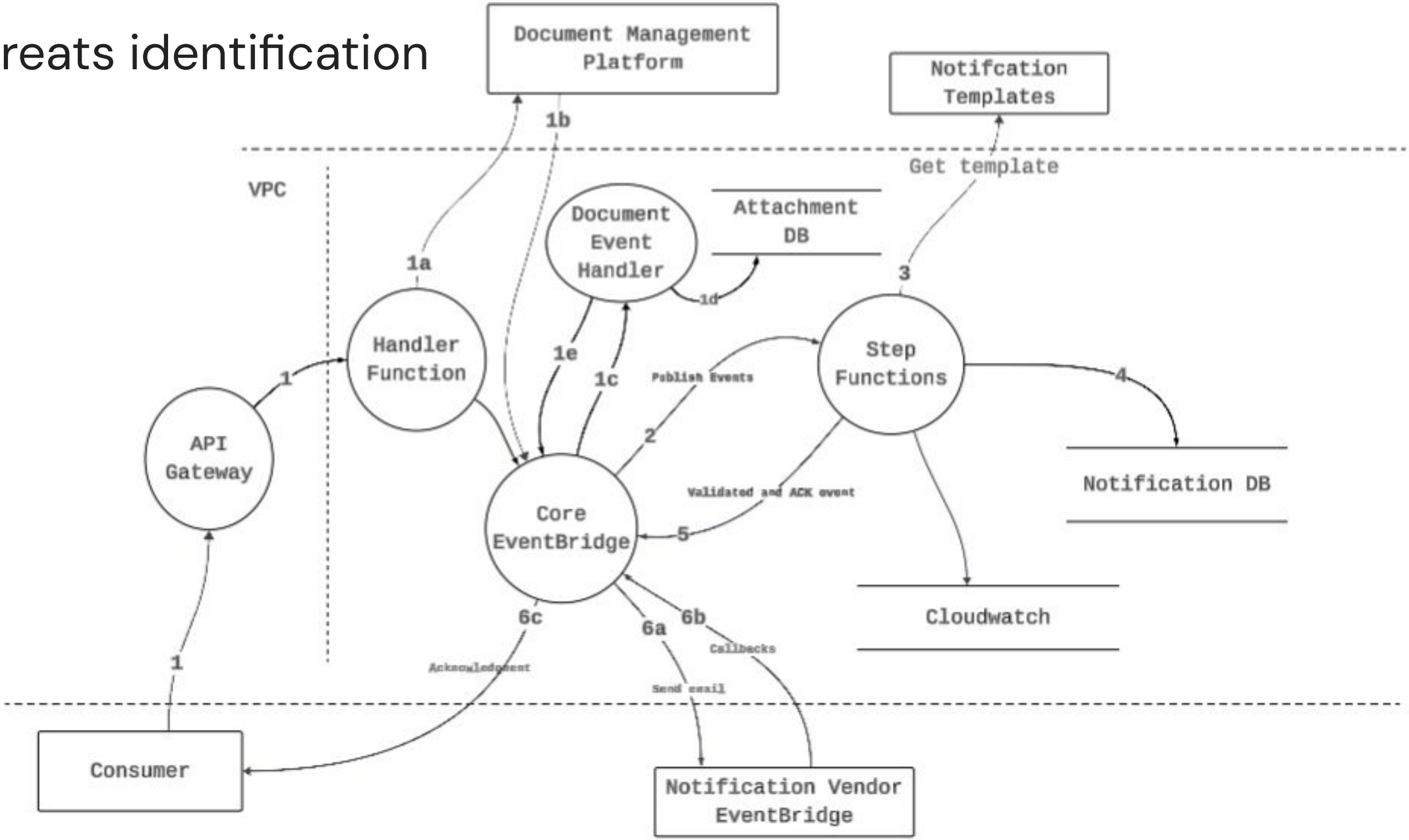
Elevation of Privilege

Gain capabilities without proper authorization

Elements and threats

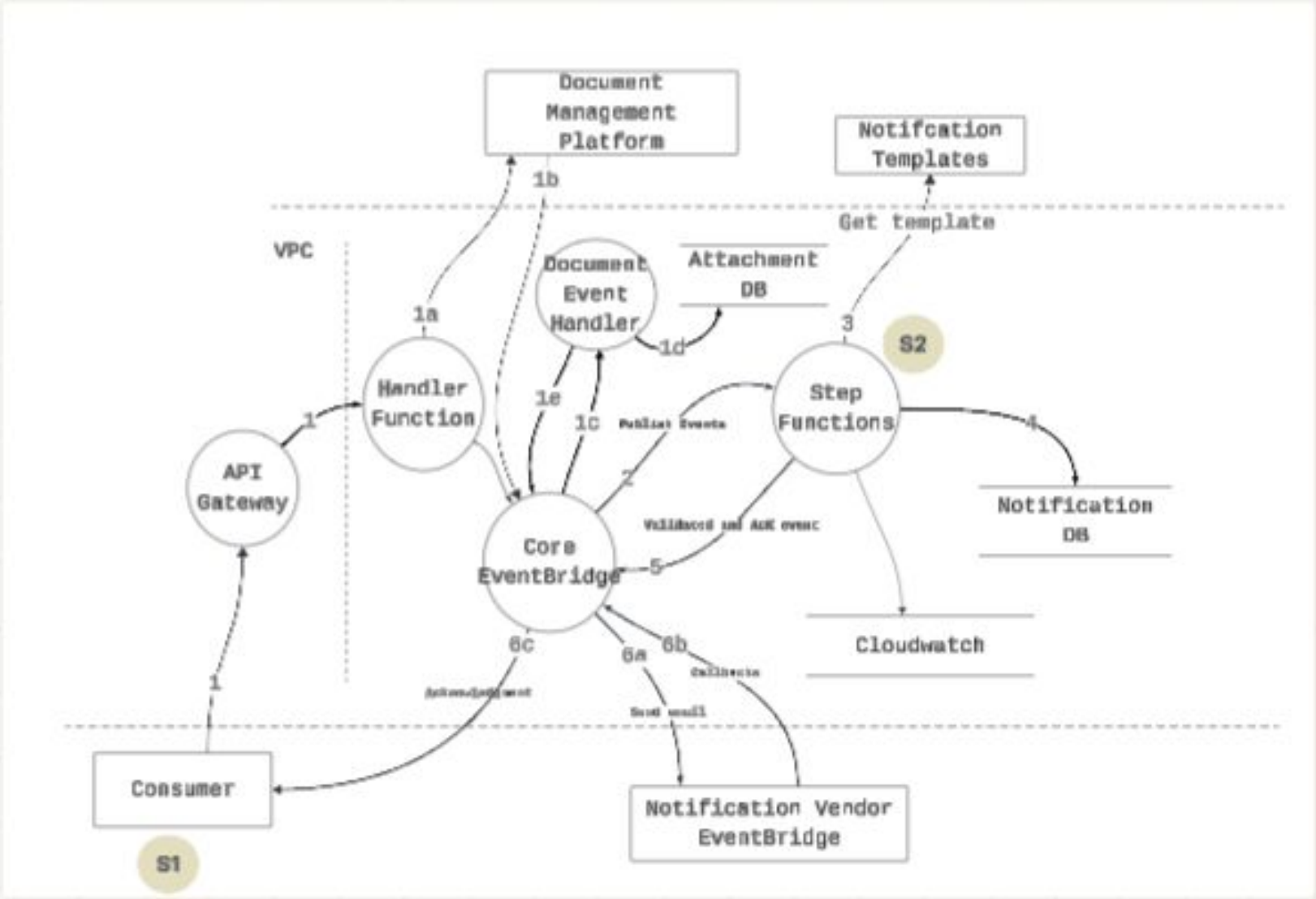
Element	S Spoofing	T Tampering	R Repudiation	I Information Disclosure	D Denial of service	E Elevation of privilege
External system 						
Process 						
Data store 						
Data flow 						
Mitigation	Authent-ication	Integrity	Non-repudiation	Confidentiality	Availability	Authorization

Threats identification



Identify the threats

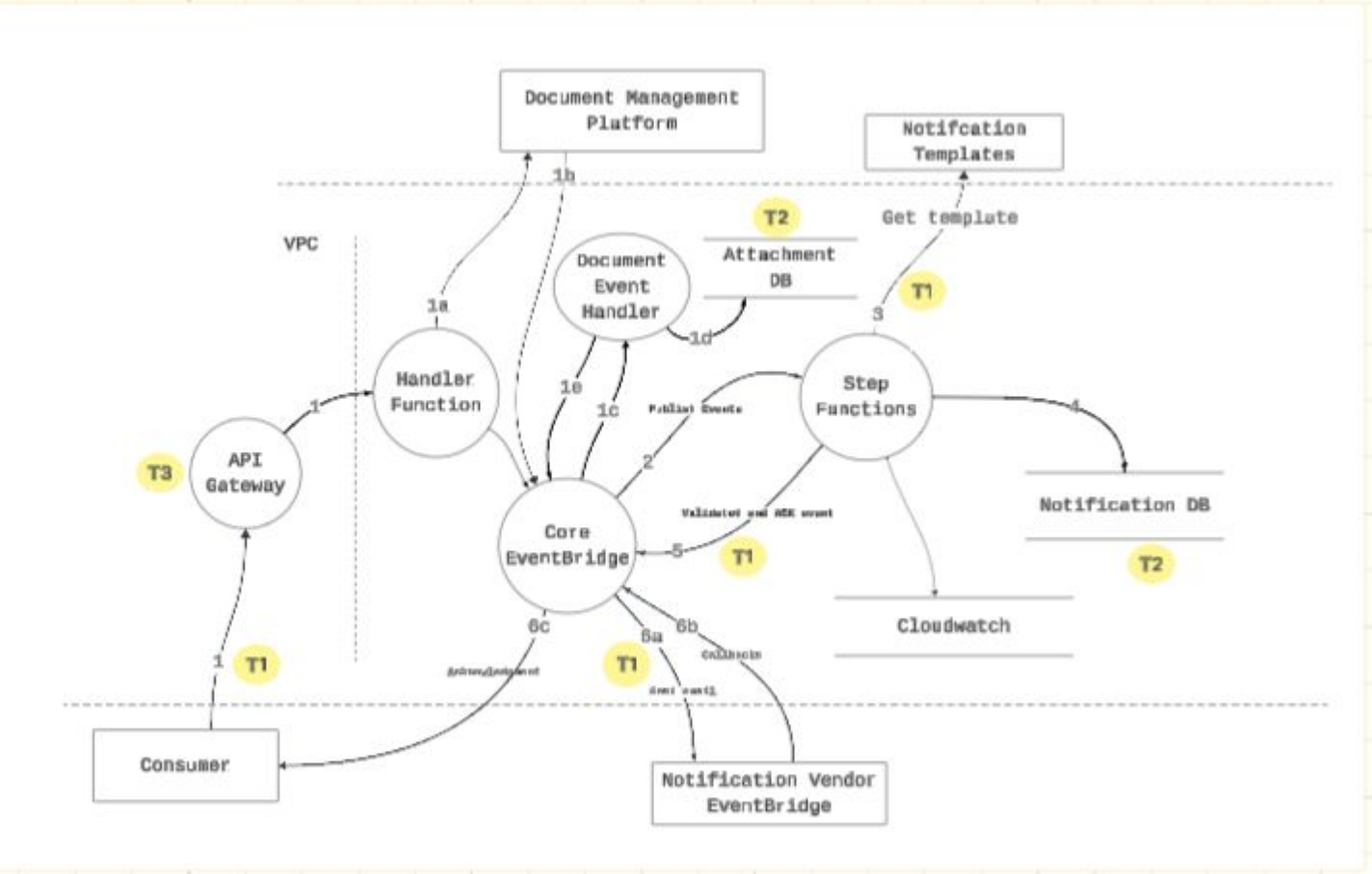
Spoofing threats



Applies to:
1. External system
2. Process

ID	Threat Description
S1	An external entity (consumer of the service) impersonates another to gain unauthorized access or deceives the system, undermining authentication
S2	A process in the step function assumes the role of another entity (for eg: document event handler) to access the Attachment DB

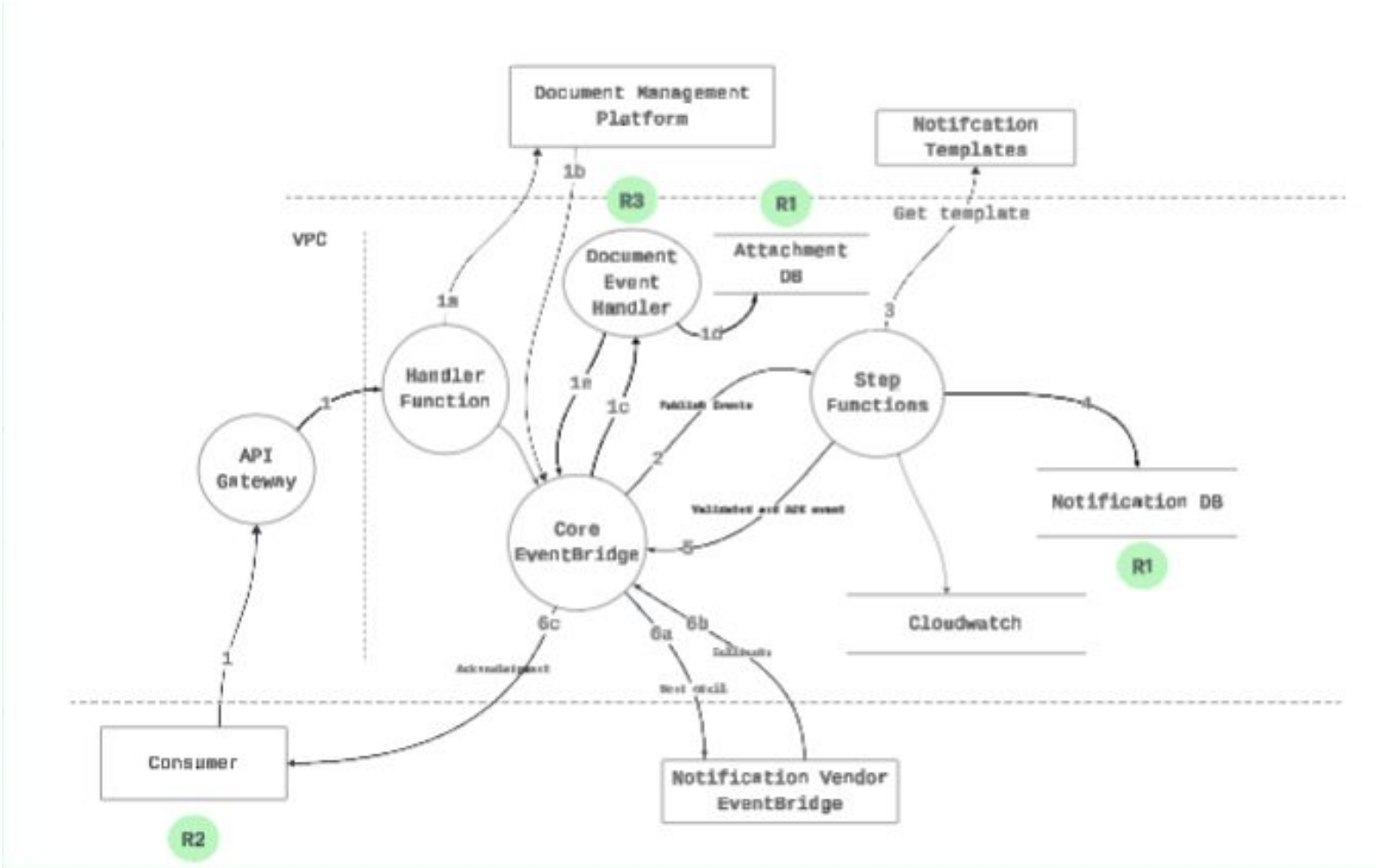
Tampering threats



Applies to:
1. Process
2. Data Store
3. Data Flow

ID	Threat Description
T1	Events/Requests in transit are tampered by malicious actors (man in the middle attack)
T2	A process in the step function assumes the role of another entity (for eg: document event handler) to access the Attachment DB
T3	The API Gateway tampers the incoming request compromising the integrity of the system and leading to unreliable and malicious operations

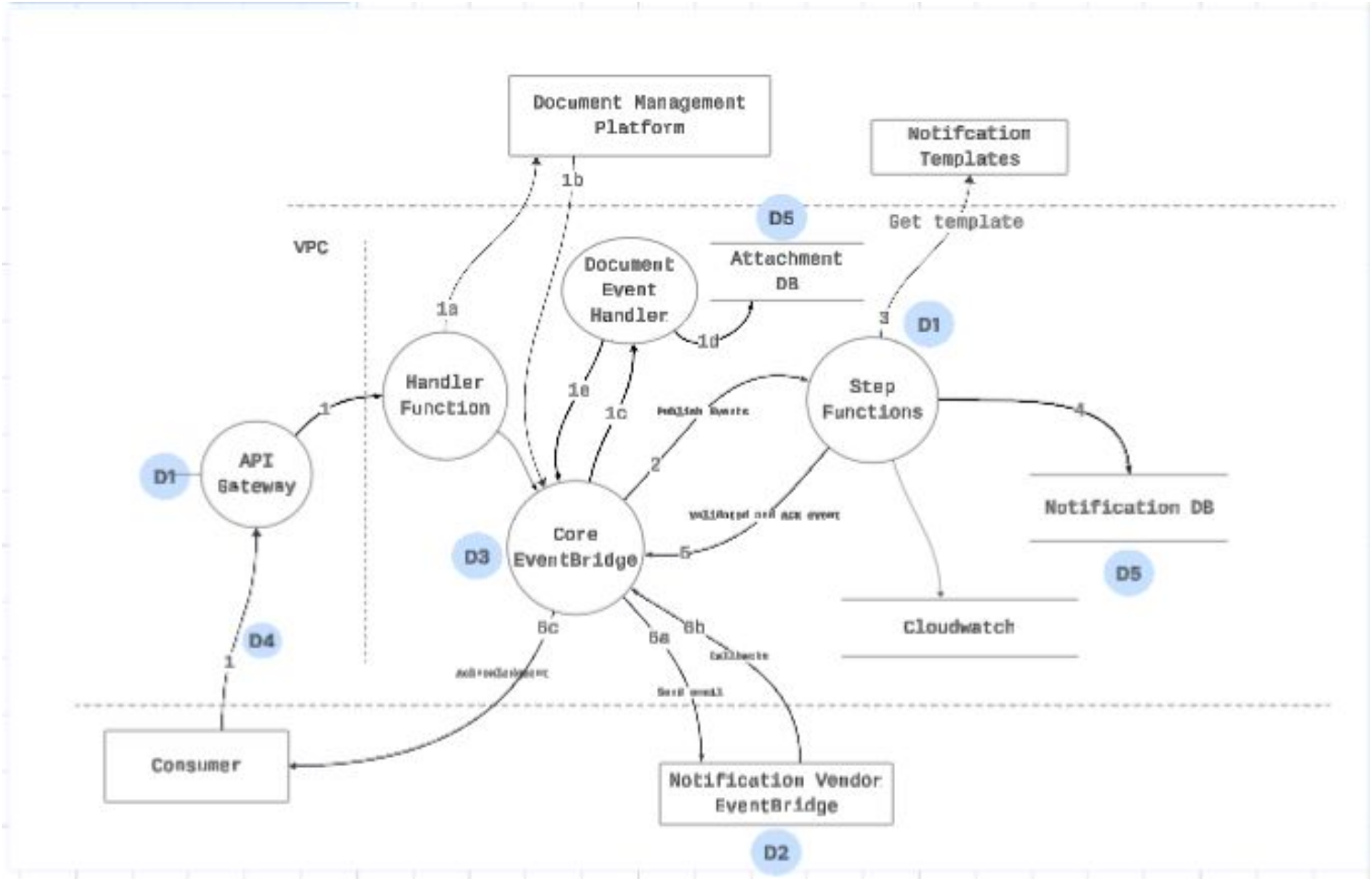
Repudiation threats



Applies to:
1. External system
2. Process
3. Data store

ID	Threat Description
R1	Operations performed in the database are untraceable
R2	An external entity performs an operation and denies doing it
R3	The document event handler process denies making an update to the attachment database

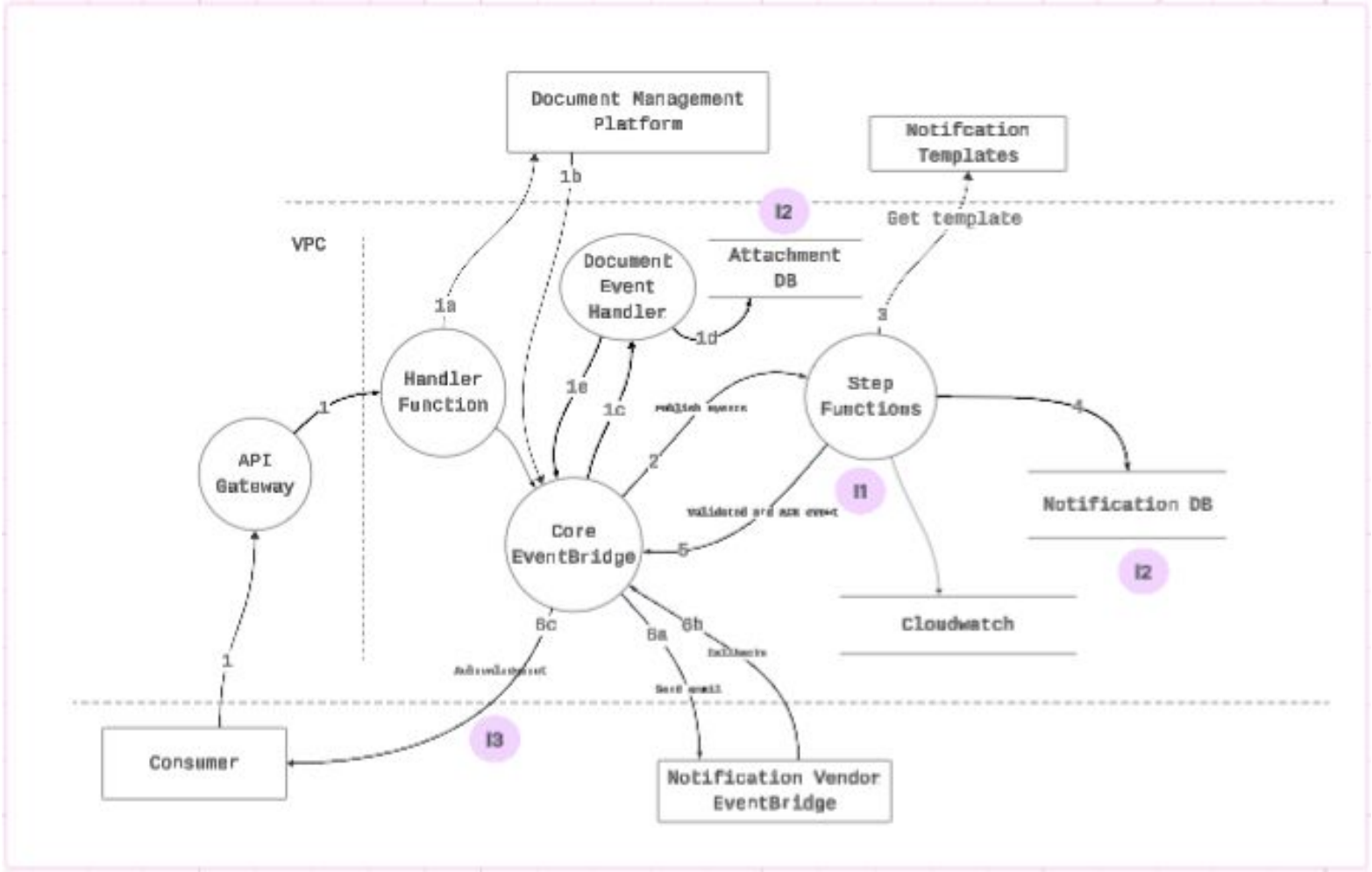
Denial of Service threats



Applies to:
1. Process
2. Data Store
3. Data Flow

ID	Threat Description
D1	API Gateway encounters a flood of requests
D2	Notification Vendor triggers events at a high velocity or triggers duplicate events causing the system's performance to degrade
D3	The document event handler process denies making an update to the attachment database
D4	Communication/network failure between the system and the consumers
D5	The database encounters requests far outnumbering its provisioned capacity or connection count

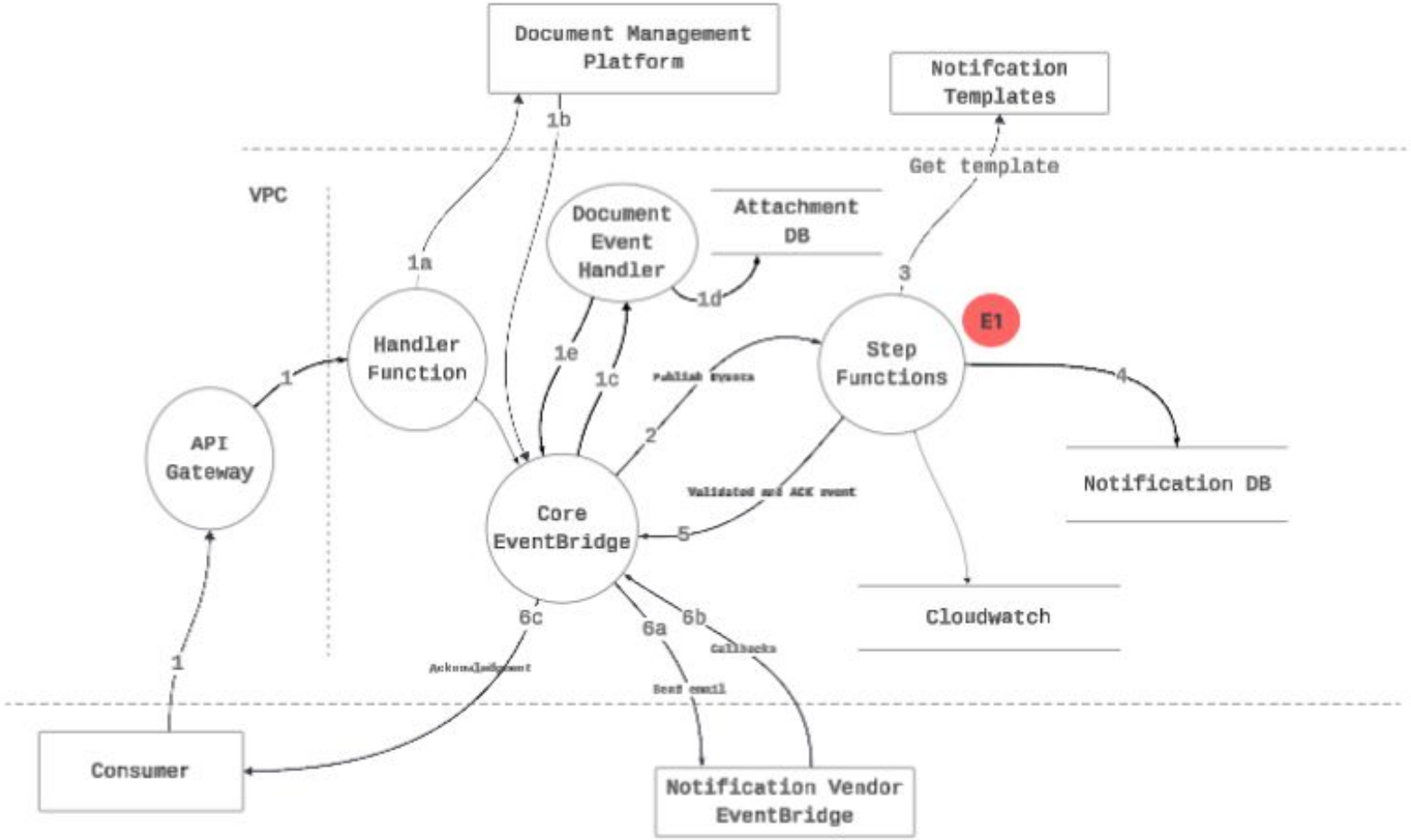
Information Disclosure threats



Applies to:
1. Process
2. Data Store
3. Data Flow

ID	Threat Description
I1	The processes in the step function unintentionally log PII data in Cloudwatch
I2	PII stored as plain text in the database
I3	The system emits events which are consumed by multiple consumers. All consumers have access to all events thus compromising confidentiality

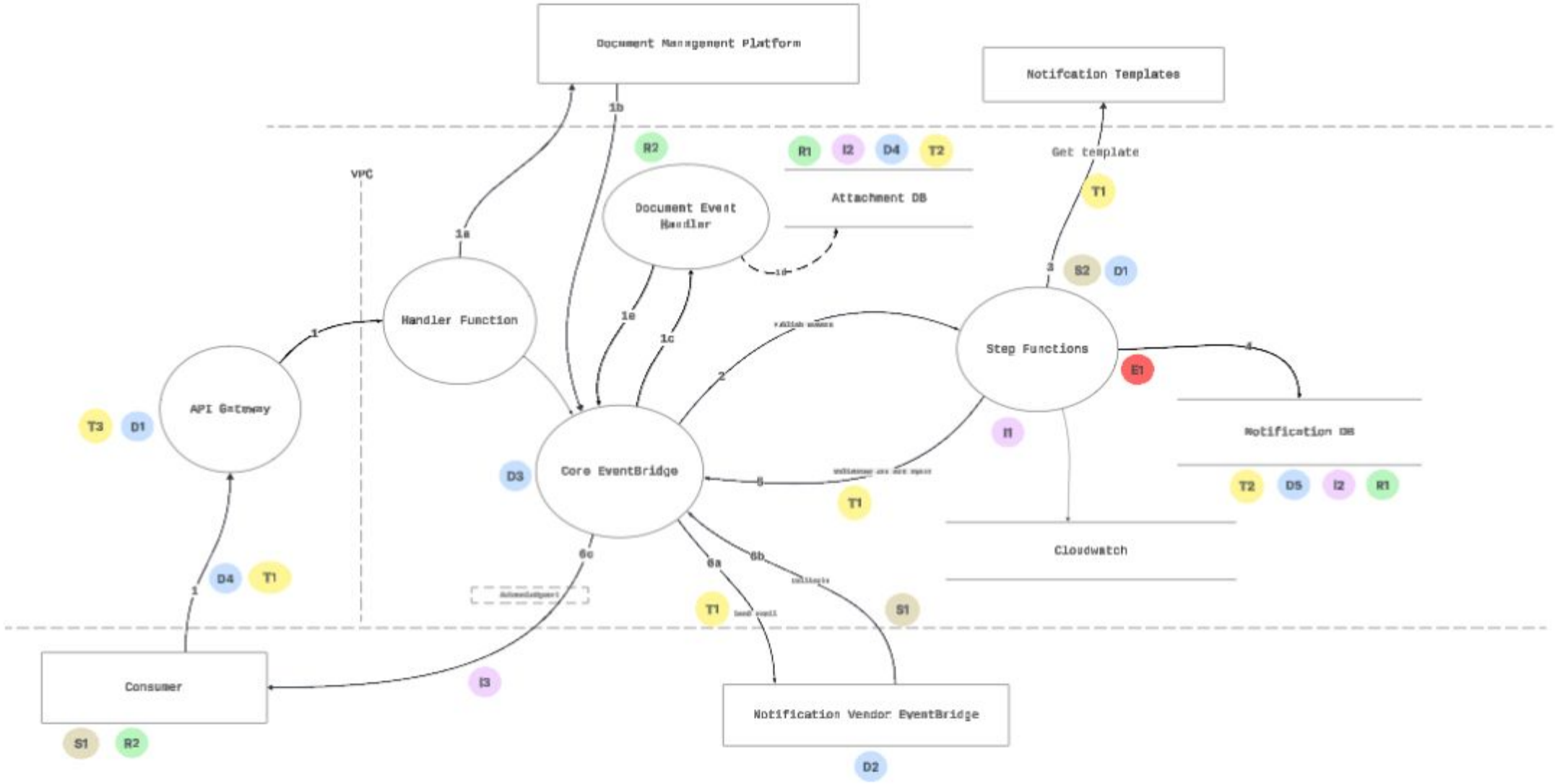
Elevation of Privilege threats



Applies to:
1. External system
2. Process

ID	Threat Description
E1	The processes in the step function that should only perform read operations on the notification database can also perform write operations

Aggregated Threats

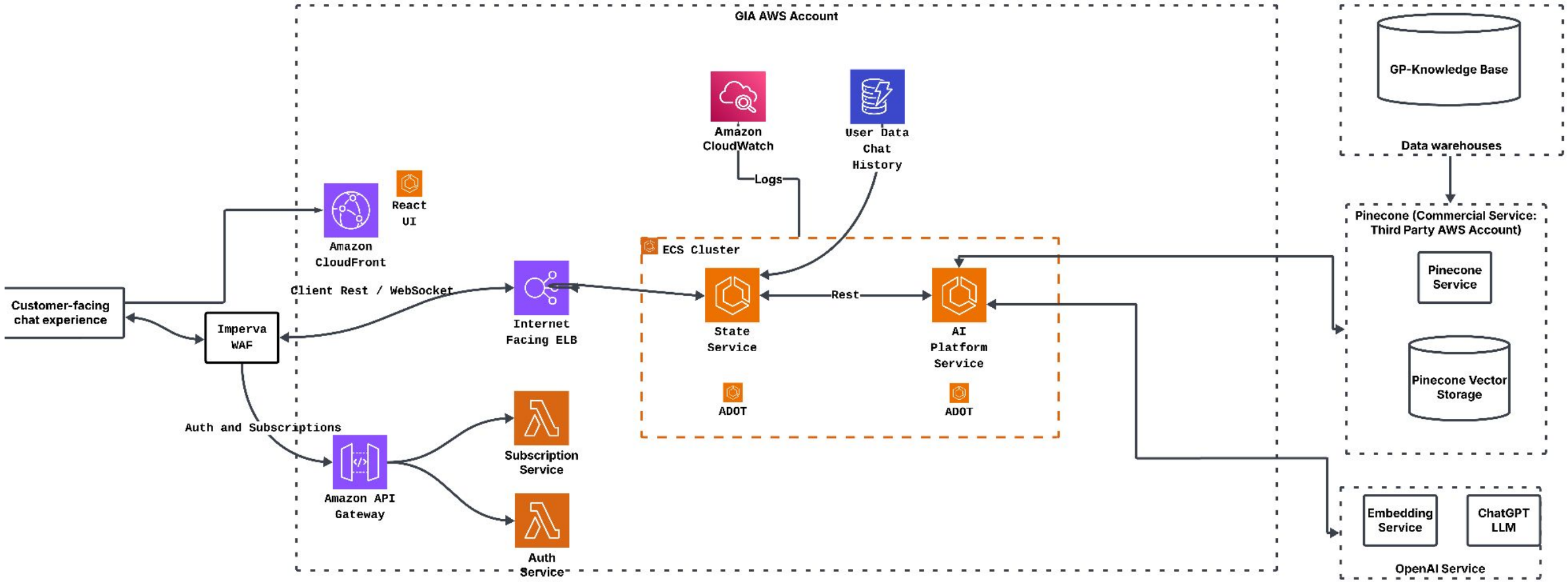


Usecase – Gia chatbot

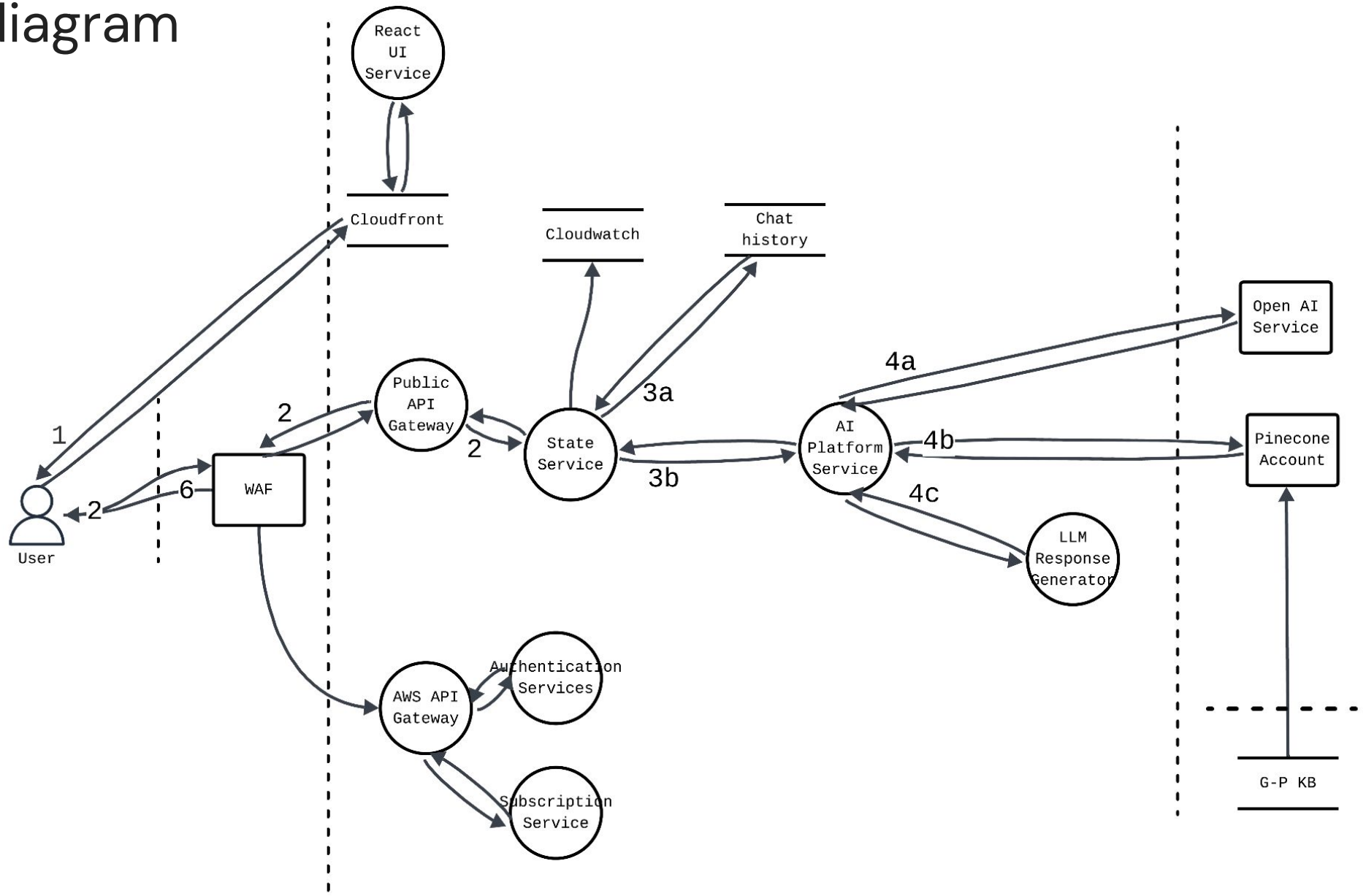
Intro

Architecture

hatbot Architecture

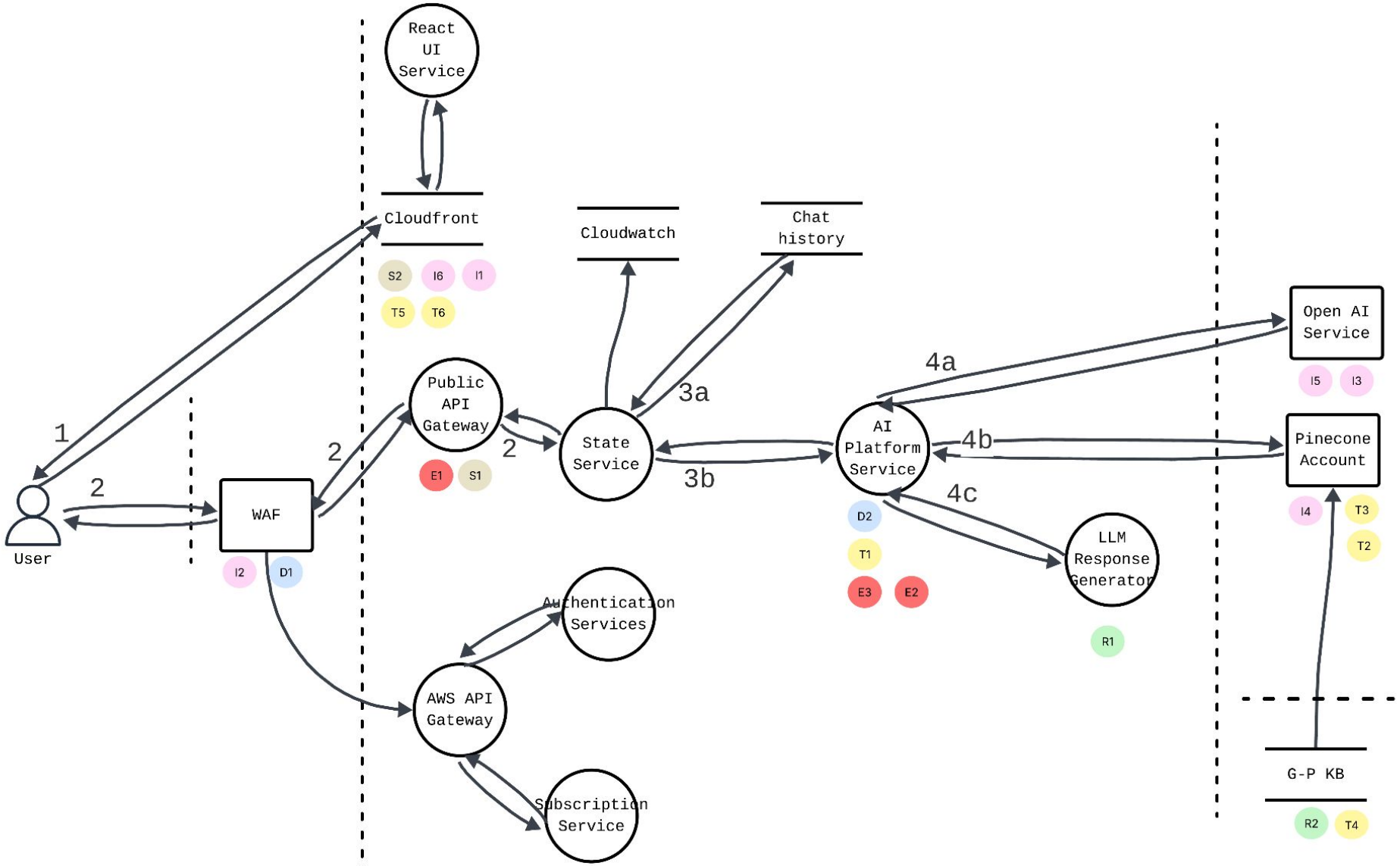


Data flow diagram



Identify the threats

Threat Modeled Data flow diagram



Common mitigations

Manage threats proactively

Common mitigations

Spoofing

Authentication

Strong authentication
- MFA
- Password policies
- Biometrics
- Hardware tokens

Identification
- Digital certificates/PKI
- Secure Session Management

Protecting secrets
- Secure Secret Management
- Principle of Least Privilege

Tampering

Integrity

Cryptographic Integrity Checks
- Hashing
- Digital Signatures

Access Control
- Authorization

Secure Communication
- TLS/SSL

Input and Output Validation

Audit Trails and Monitoring
- Immutable Logs

Repudiation

Non-repudiation

Strong Authn & Authz

Comprehensive Logging and Auditing
- Secure Audit Trails
- Centralized Log Management

Digital signatures
- Non-repudiable Protocols

Trusted third parties

Common mitigations

Information Disclosure

Confidentiality

Data Minimization & Classification

Encryption

Strict Access Controls

Secure Output and Error Handling
- Generic Error Messages
- Output Encoding
- Data masking

Secure Logging

Regular Audits & Testing
- Code Audits
- Vulnerability Scans
- Penetration Testing

Denial of Service

Availability

Scalability & Resilience
- Horizontal Scaling
- Redundancy & Failover

Traffic Management
- WAF
- Rate limiting

Resource Management
- Resource Quotas & Limits
- Connection Timeouts
- Input Validation

Caching
- CDN
- Application caching

Monitoring & Alerting

Incident Response Plan

Elevation of Privilege

Authorization

Principle of Least Privilege

Robust Authorization Checks

Secure Configuration & Patch Management
- Disable Unnecessary Features

Input Validation & Secure Coding

Privileged Access Management
- JIT Access
- Session Monitoring

Network Segmentation & Isolation

Monitoring & Alerting
- Anomaly Detection

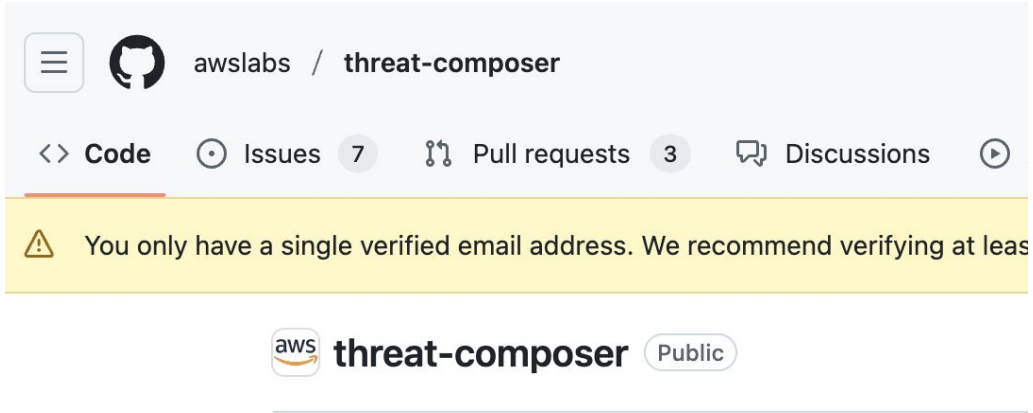
Regular Audits & Pen Testing

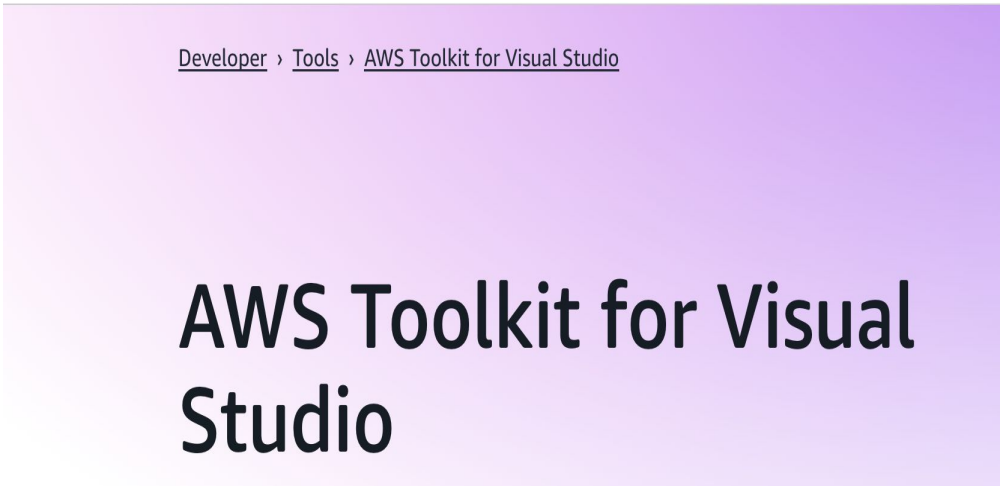
Threat composer

Threat Composer

- Tool that allows you to create, view, and edit threat models
- Describe assumptions, identify threats and mitigations, link them up together
- Features an insights dashboard to help identify areas for improvement
- Integrates with Visual Studio Code

- Application Link: AWS Threat Composer
- Documentation: Working with Threat Composer from the AWS Toolkit for VS Code





Resources

Resources

https://github.com/gp-oss/acd-blr-2025-threat-modelling/

https://lucid.app/lucidchart/02ebcb92-79ff-4daa-873a-4a8e548ef68a/view

Thank you!

Please come and say hi.

Shilpa

Ayush

Rakshit