OPEN COMPLIANCE SUMMIT

Security Analytics From Use Case and User Needs to Innovation

Dr. Aparna Sundar, Senior Researcher
OpenSearch Project

December 8th 2023

OpenSearch

Agenda

WHAT ARE WE SOLVING FOR?

CORE USER AND USER NEEDS

PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER

1

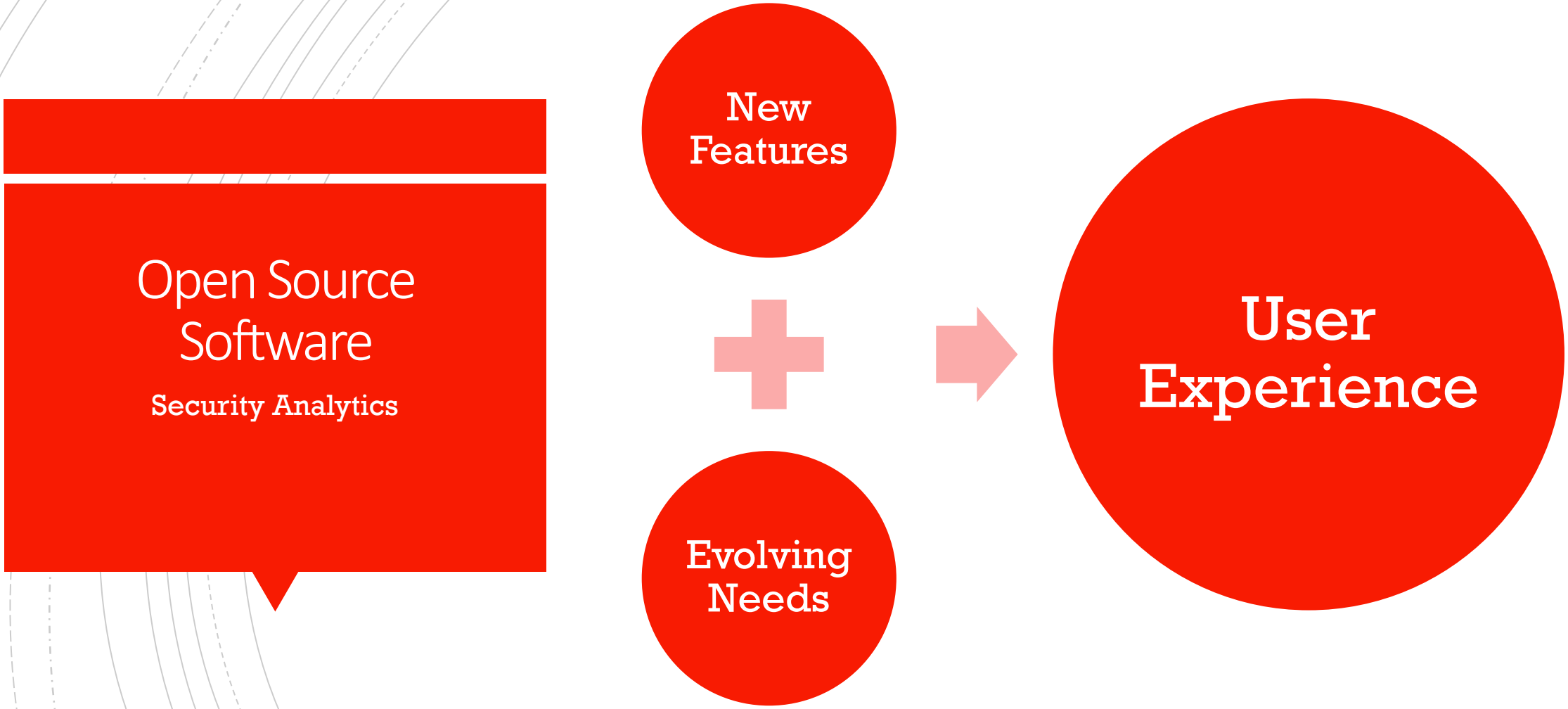
WHAT ARE WE SOLVING FOR?

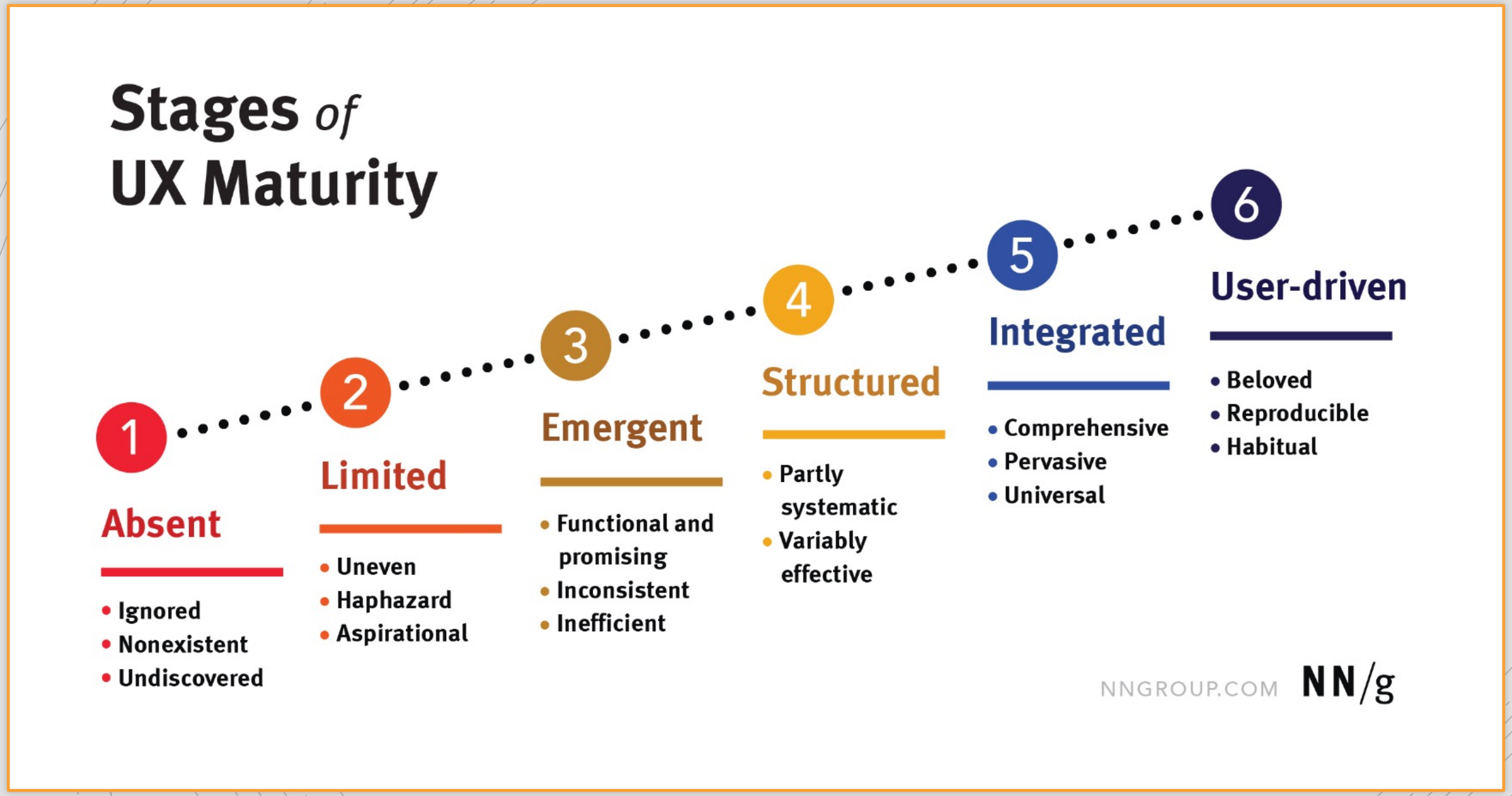
CORE USER AND USER NEEDS

PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER


Open Source Software
Security Analytics
New Features
Evolving Needs
User Experience


Stages of UX Maturity
1
Absent
• Ignored
• Nonexistent
• Undiscovered
2
Limited
• Uneven
• Haphazard
• Aspirational
3
Emergent
• Functional and promising
• Inconsistent
• Inefficient
4
Structured
• Partly systematic
• Variably effective
5
Integrated
• Comprehensive
• Pervasive
• Universal
6
User-driven
• Beloved
• Reproducible
• Habitual
NNGROUP.COM
NN/g

Future Trends in Security Analysis

1

Artificial Intelligence

AI-powered solutions will enhance threat detection and response capabilities.

2

IoT Security

Securing the increasing number of connected devices and networks.

3

Cloud Security

Addressing the unique challenges and risks associated with cloud-based infrastructure.

Some of the Design Objectives

Designing software for security analysts requires a deep understanding of their needs. By conducting user research and engaging in direct conversations, we can develop user-centric solutions.

1

Task-Oriented Approach

Focus on providing tools and functionalities that align with the specific tasks and workflows of security analysts.

2

Intuitive Interface

Create a user-friendly interface that minimizes cognitive load and enhances productivity.

3

Flexible Customization

Allow users to customize their software, adapting it to their unique preferences and requirements.

4

Responsive Design

Ensure optimal performance across various devices, enabling seamless access in both desktop and mobile environments.

2

WHAT ARE WE SOLVING FOR?

CORE USER AND USER NEEDS

PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER

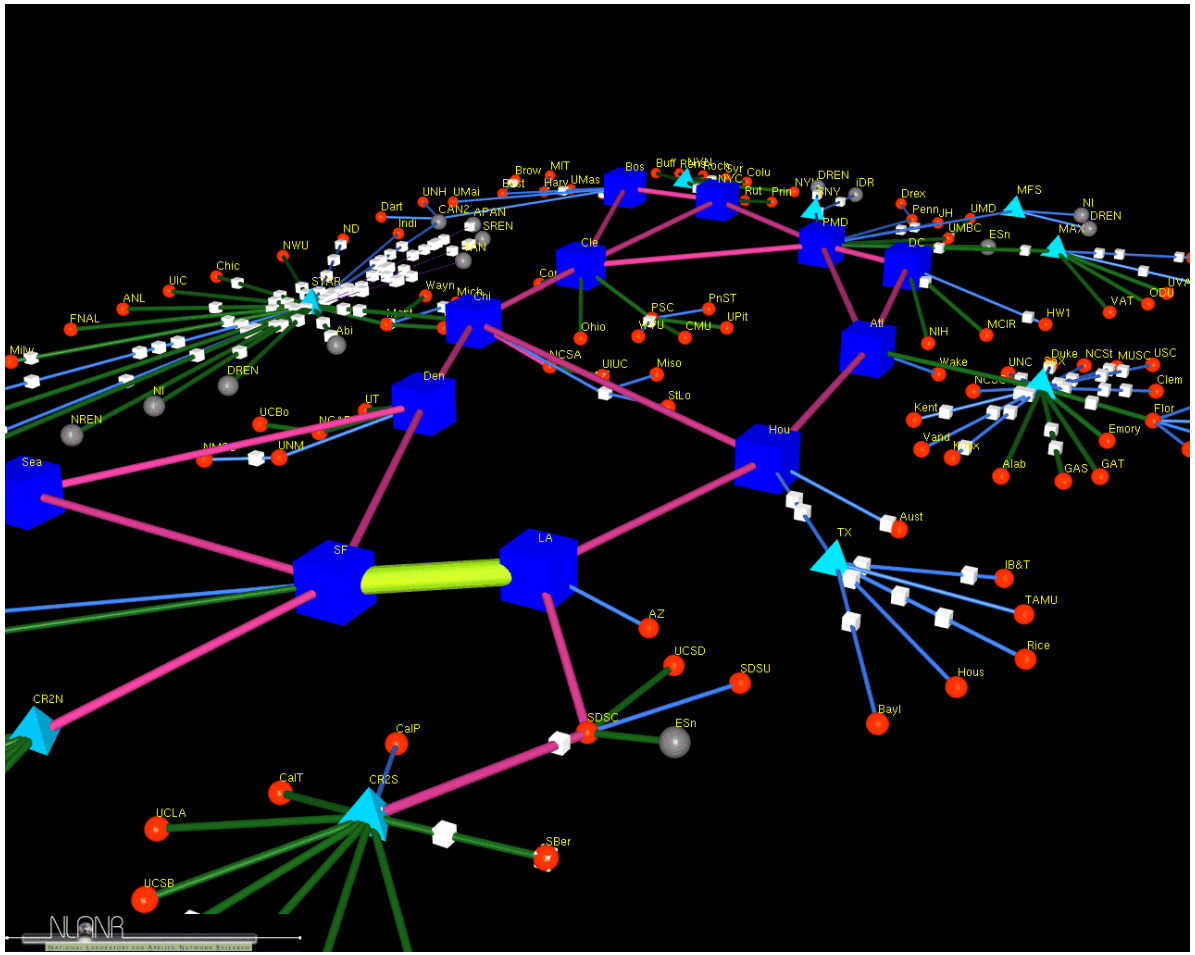
Core User

Threat Assessment

Security Architecture Design

Incident Response

Security analysts or developers are professionals who specialize in analyzing and improving the security of computer systems and networks. They play a crucial role in protecting sensitive data and preventing cyber attacks.



Software Needs

Network Traffic Analysis

Vulnerability Scanning

Security Incident Management

Security Analytics

Opportunities we find from talking to users are due to

Specialty needs

Complexity of systems

Compliance and awareness

Data Encryption

Implement robust encryption mechanisms to secure data both at rest and in transit.

User Permission Controls

Provide granular user permission settings to ensure that only authorized individuals can access sensitive data.

Compliance with Data Regulations

Adhere to data protection regulations, such as GDPR, to safeguard user privacy and maintain legal compliance.

In addition, and to enhance efficiency and productivity

Efficiency and productivity are crucial for security analysts. By incorporating intelligent features and automation, our software enables them to focus on critical tasks.

1

Automated Alert Triage

Implement intelligent algorithms to prioritize and categorize alerts, saving analysts valuable time and effort.

2

Smart Search Capabilities

Enable advanced search functionalities to quickly locate relevant information, leveraging advanced filtering options and machine learning.

3

Automated Report Generation

Streamline report creation by automating

3

WHAT ARE WE SOLVING FOR?

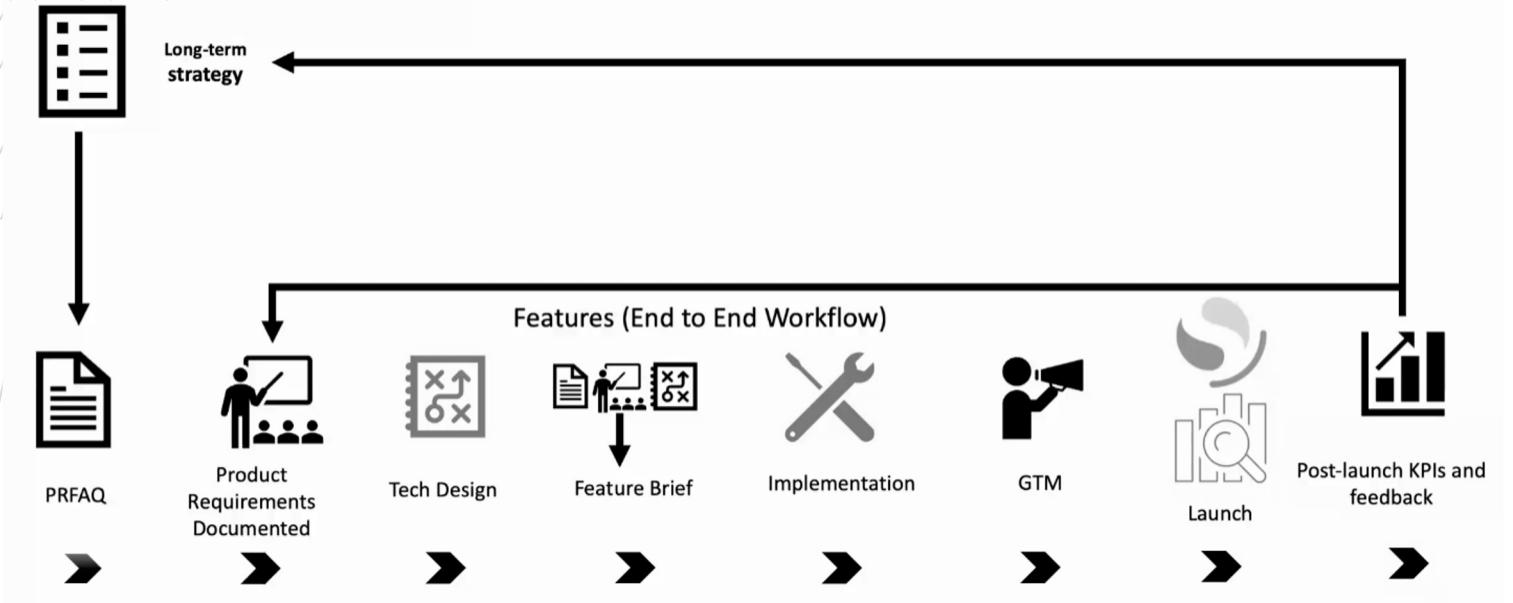
CORE USER AND USER NEEDS

PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER

Research integration with product development lifecycle

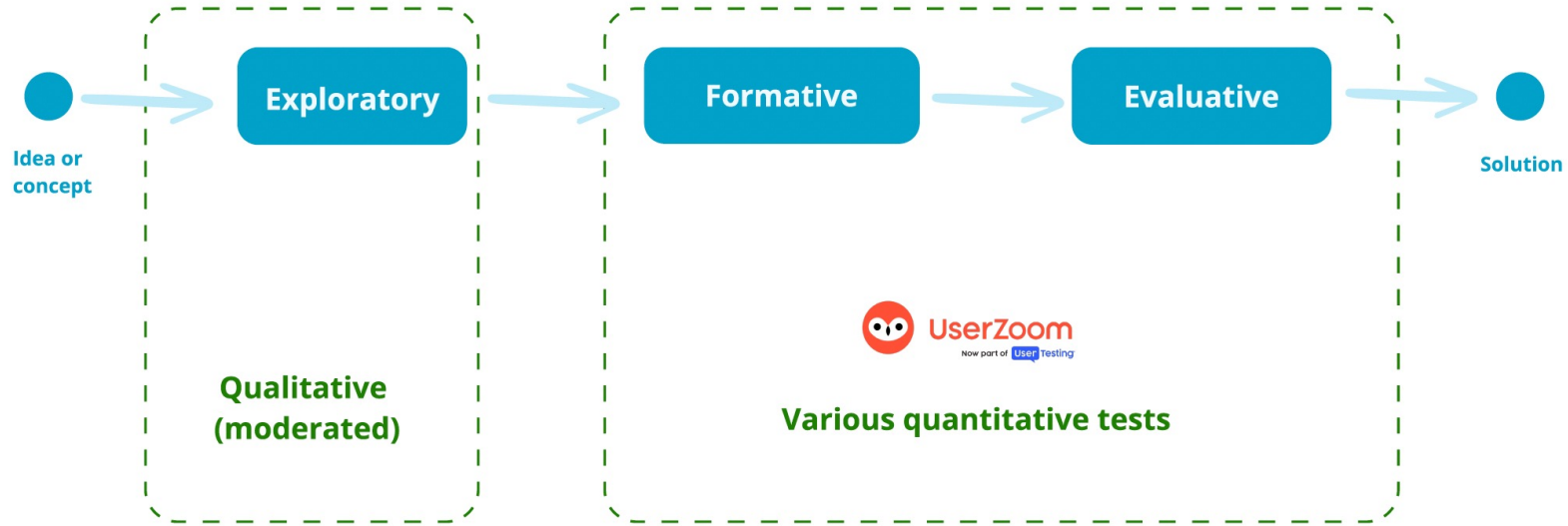


Exploratory

Formative

Evaluative

Types of User Research studies



Understanding User Needs

1

Use Cases

A list of actions or event steps defining user interactions to achieve goals.

2

Iterative Solutioning

User reflections and discussions lead to incremental innovations in security solutions.

3

Customization

Users' varying motivations may require customized log or security analytics solutions.

Research Insights

User Personas

Creating profiles of typical users to understand their needs and preferences.

Jobs to be Done

Identifying the specific tasks or problems users are trying to solve with security analytics solutions.

Strategic Reflection

Users reflecting on their experiences to drive improvements in the security solution.

4

WHAT ARE WE SOLVING FOR?

CORE USER AND USER NEEDS

PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER

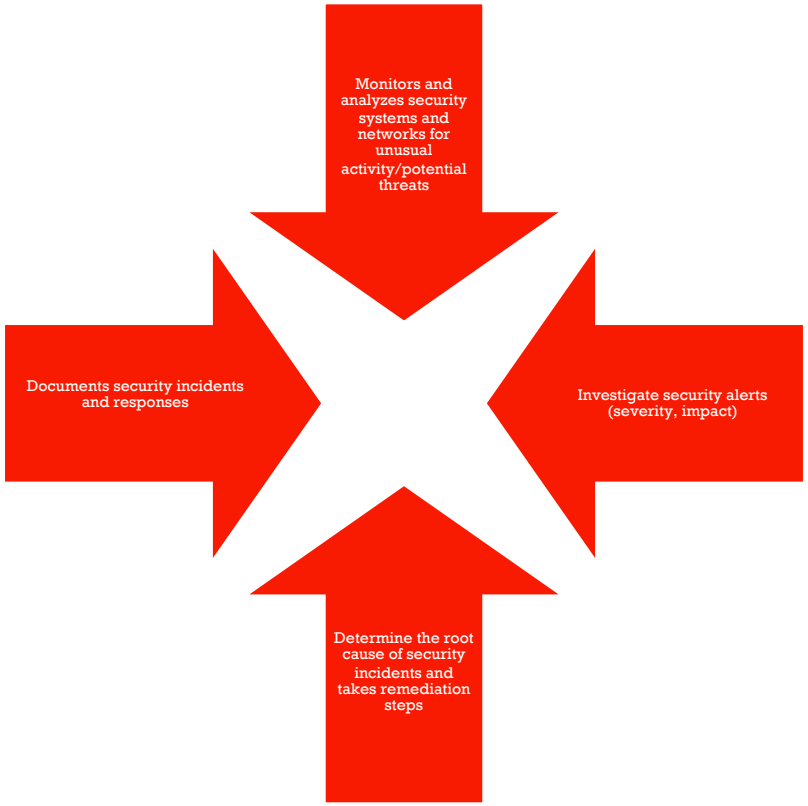
User personas

	High code	Low code
PRODUCER (SecOps)	 **1. Security Architect** Security Engineer, Data architect, Security Consultant	 **2. CISO** VP, Compliance Officer
	Data	
CONSUMER (Security Analyst)	 **3. SOC Analyst (Tier 3-4)** Incident response coordinator, Threat hunter	 **4. SOC Analyst (Tier 1-2)** Security Analyst, Triage specialist

4. SOC Analyst (Tier 1-2)

Security Analyst, Triage Specialist

Consumer | **Low Code**



Knowledge and skills:

- May be able to write a basic query
- Analyze information
- Communicate
- Stay up-to-date on the latest technology
- Code and program
- Have knowledge of JavaScript, C++, and Python

3. SOC Analyst (Tier 3-4)

Incident response coordinator, Threat hunter

Consumer **High Code**

REVIEW ALERT RESPONSES TIME

PERFORM VULNERABILITY ASSESSMENTS

PROACTIVELY LOOK FOR THREATS

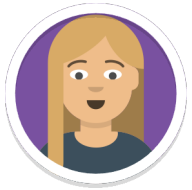
DEFINE MITIGATION STRATEGIES

SHARE DASHBOARDS

CREATE REPORTS

Knowledge and skills:

- Proficient with queries and scripting languages
- Deep domain knowledge
- Analyze information
- Manages security incidents
- Evaluates escalated security alerts
- Assesses security and other risks associated with a security incident
- Maintains an incident response plan



2. CISO

VP, Compliance Officer

Producer | **Low Code**

Facilitate legal compliance audit

Monitor PII protection policies

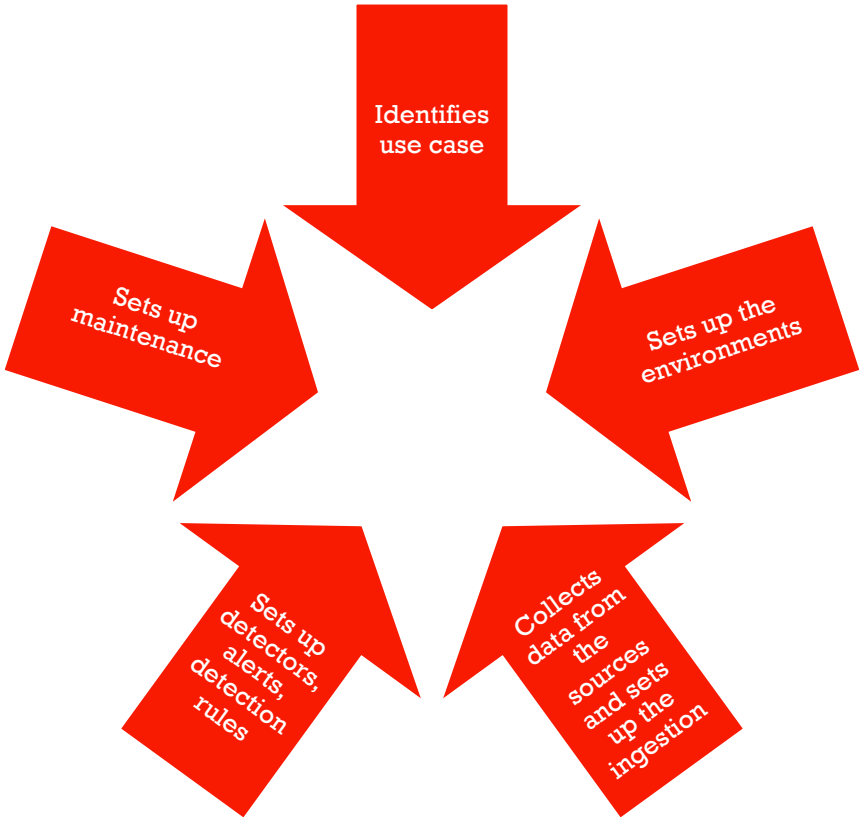
Knowledge and skills:

- Highly Technical
- More awareness of systems
- Less domain knowledge
- Developing, implementing, and enforcing security policies
- Managing security staff
- Managing the budget and capital or operating expenditure
- Developing strategy, culture, and risk profile

1. Security Architect

Security Engineer, Data architect, Security Consultant

Producer **High Code**



Knowledge and skills:

- Strong technical background
- Service and Network tooling
- Process mindset
- Data and system savvy
- Understands the nature of data, and how to connect data sources

5

WHAT ARE WE SOLVING FOR?

CORE USER AND USER NEEDS

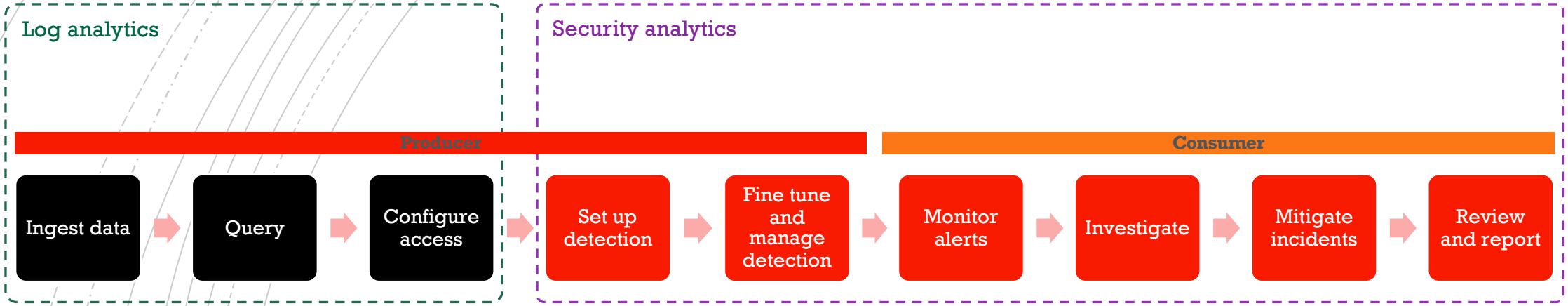
PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER

Curating User Flows

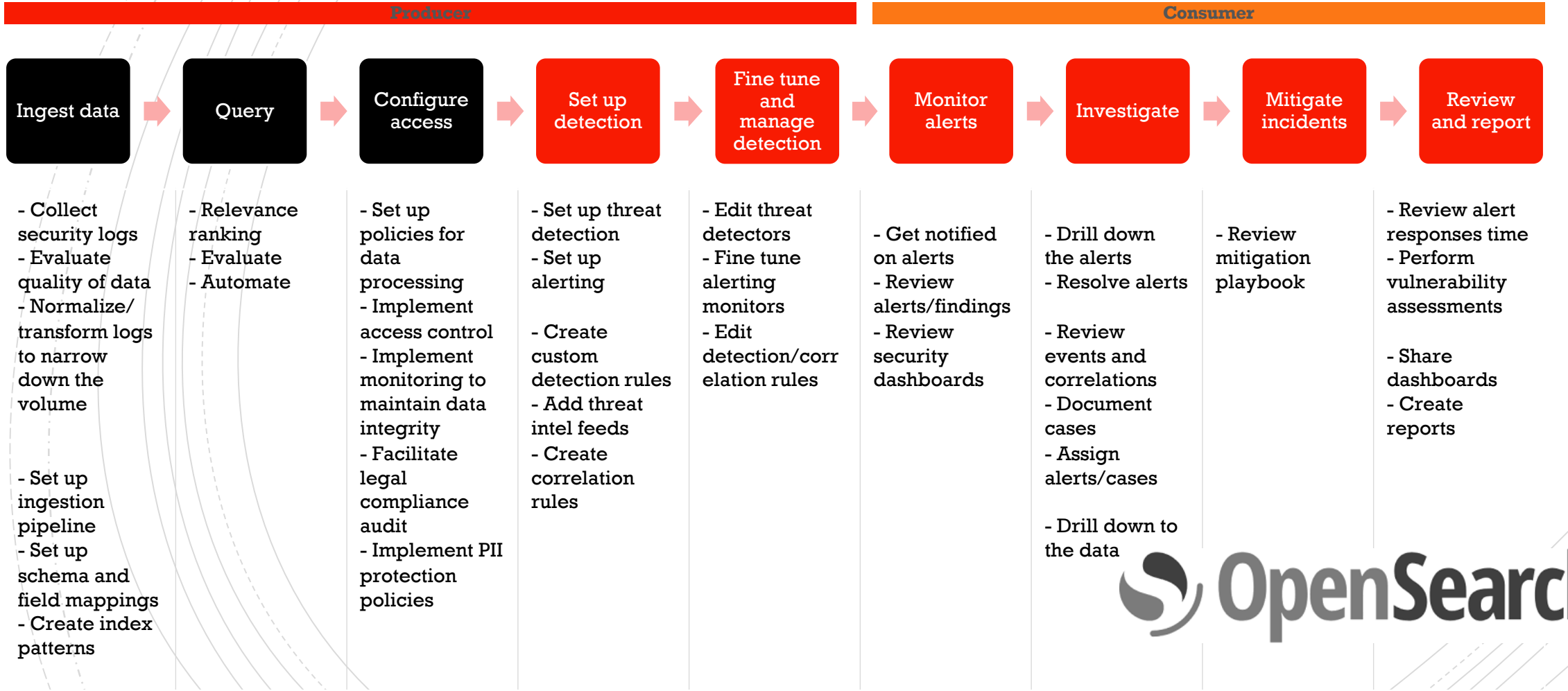
- User flows guide users through the product
- Clarify interactions
- Identifies potential pain points



User Journey

OpenSearch

User Journey



OpenSearch

Questions?

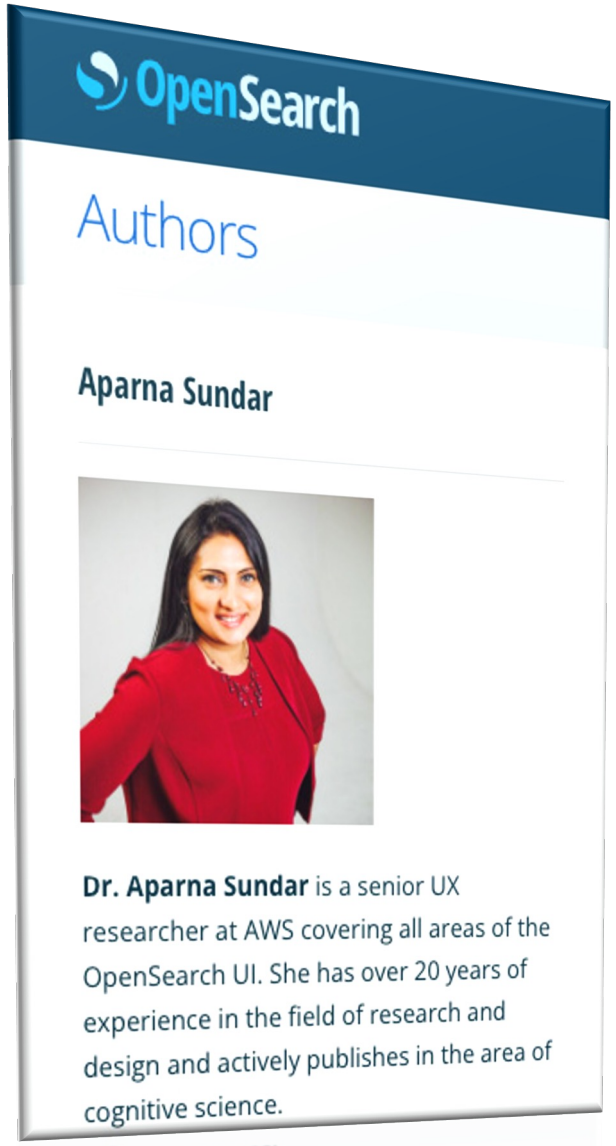
WHAT ARE WE SOLVING FOR?

CORE USER AND USER NEEDS

PROCESS OF OBTAINING USER INSIGHTS

USERS AND USER JOURNEYS

DESIGNING FOR THE USER



References

- Using community insights to create a persona framework to improve search experiences
- OpenSearch Project Q1 community survey results
- Start with Who, not Why