

# Killer Context

How AI will impact Software & Security



# Killer Context

How AI will impact Software & Security



how big is AI, really?

How it will affect software

How that will affect security

some early experiments and examples

What you can do to get ready

ai





ai

A disruption scale

Printing Press

The Internet

Computers

Mobile





ai

AI at the top?

Post-2023 AI

Printing Press

The Internet

Computers

Mobile





ai

But won't we just adapt?

Post-2023 AI

Printing Press

The Internet

Computers

Mobile





- **Agricultural Revolution (Around 10,000 B.C.)**
  - Inventions: Farming, animal domestication.
  - Job Shift: From hunter-gatherer to **farmer and herder**.
- **Industrial Revolution 1.0 (1760-1840)**
  - Inventions: Steam power, textile mechanization, iron production.
  - Job Shift: From farming to **industrial labor, machine operation**.
- **Industrial Revolution 2.0 (1870-1914)**
  - Inventions: Electricity, assembly lines, internal combustion engine.
  - Job Shift: From skilled artisans to **assembly-line workers, machine operators, engineers**.
- **Industrial Revolution 3.0 (1950s-1970s)**
  - Inventions: Computers, semiconductors, internet.
  - Job Shift: From manual labor to **digital and service roles, programmers, IT specialists**.
- **Industrial Revolution 4.0 (21st Century)**
  - Inventions: IoT, AI, 3D Printing, autonomous vehicles.
  - Job Shift: From routine tasks to **creative, complex problem solving, tech-based roles**.

- **Agricultural Revolution (Around 10,000 B.C.)**
  - Inventions: Farming, animal domestication.
  - Job Shift: From hunter-gatherer to **farmer and herder**.
- **Industrial Revolution 1.0 (1760-1840)**
  - Inventions: Steam power, textile mechanization, iron production.
  - Job Shift: From farming to **industrial labor, machine operation**.
- **Industrial Revolution 2.0 (1870-1914)**
  - Inventions: Electricity, assembly lines, internal combustion engine.
  - Job Shift: From skilled artisans to **assembly-line workers, machine operators, engineers**.
- **Industrial Revolution 3.0 (1950s-1970s)**
  - Inventions: Computers, semiconductors, internet.
  - Job Shift: From manual labor to **digital and service roles, programmers, IT specialists**.
- **Industrial Revolution 4.0 (21st Century)**
  - Inventions: IoT, AI, 3D Printing, autonomous vehicles.
  - Job Shift: From routine tasks to **creative, complex problem solving, tech-based roles**.



# ai

This time we're replacing intelligence instead of tasks

- **Agricultural Revolution (Around 10,000 B.C.)**

- Inventions: Farming, animal domestication.
- Job Shift: From hunter-gatherer to **farmer and herder**.

- **Industrial Revolution 1.0 (1760-1840)**

- Inventions: Steam power, textile mechanization, iron production.
- Job Shift: From farming to **industrial labor, machine operation**.

- **Industrial Revolution 2.0 (1870-1914)**

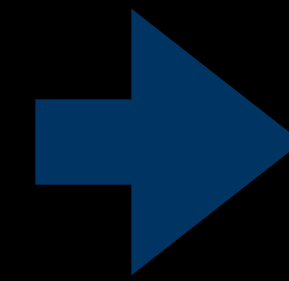
- Inventions: Electricity, assembly lines, internal combustion engine.
- Job Shift: From skilled artisans to **assembly-line workers, machine operators, engineers**.

- **Industrial Revolution 3.0 (1950s-1970s)**

- Inventions: Computers, semiconductors, internet.
- Job Shift: From manual labor to **digital and service roles, programmers, IT specialists**.

- **Industrial Revolution 4.0 (21st Century)**

- Inventions: IoT, AI, 3D Printing, autonomous vehicles.
- Job Shift: From routine tasks to **creative, complex problem solving, tech-based roles**.





ai

It's on top for me

• **Agricultural Revolution (Around 10,000 B.C.)**

- Inventions: Farming, animal domestication.
- Job Shift: From hunter-gatherer to farmer and herder.

Post-2023 AI

• **Industrial Revolution 1.0 (1760-1840)**

- Inventions: Steam power, textile machinery, iron power.
- Job Shift: From farming to industrial labor.

Printing Press

• **Industrial Revolution 2.0 (1870-1914)**

- Inventions: Electricity, assembly line, internal combustion engine.
- Job Shift: From skilled artisans to assembly line machine operators, engineers.

The Internet

Computers

• **Industrial Revolution 3.0 (1950s-1970s)**

- Inventions: Computers, semiconductors, internet.
- Job Shift: From manual labor to digital and service roles, programmers, IT specialists.

Mobile

• **Industrial Revolution 4.0 (21st Century)**

- Inventions: IoT, AI, 3D Printing, autonomous vehicles.
- Job Shift: From routine tasks to creative, complex problem solving, tech-based roles.





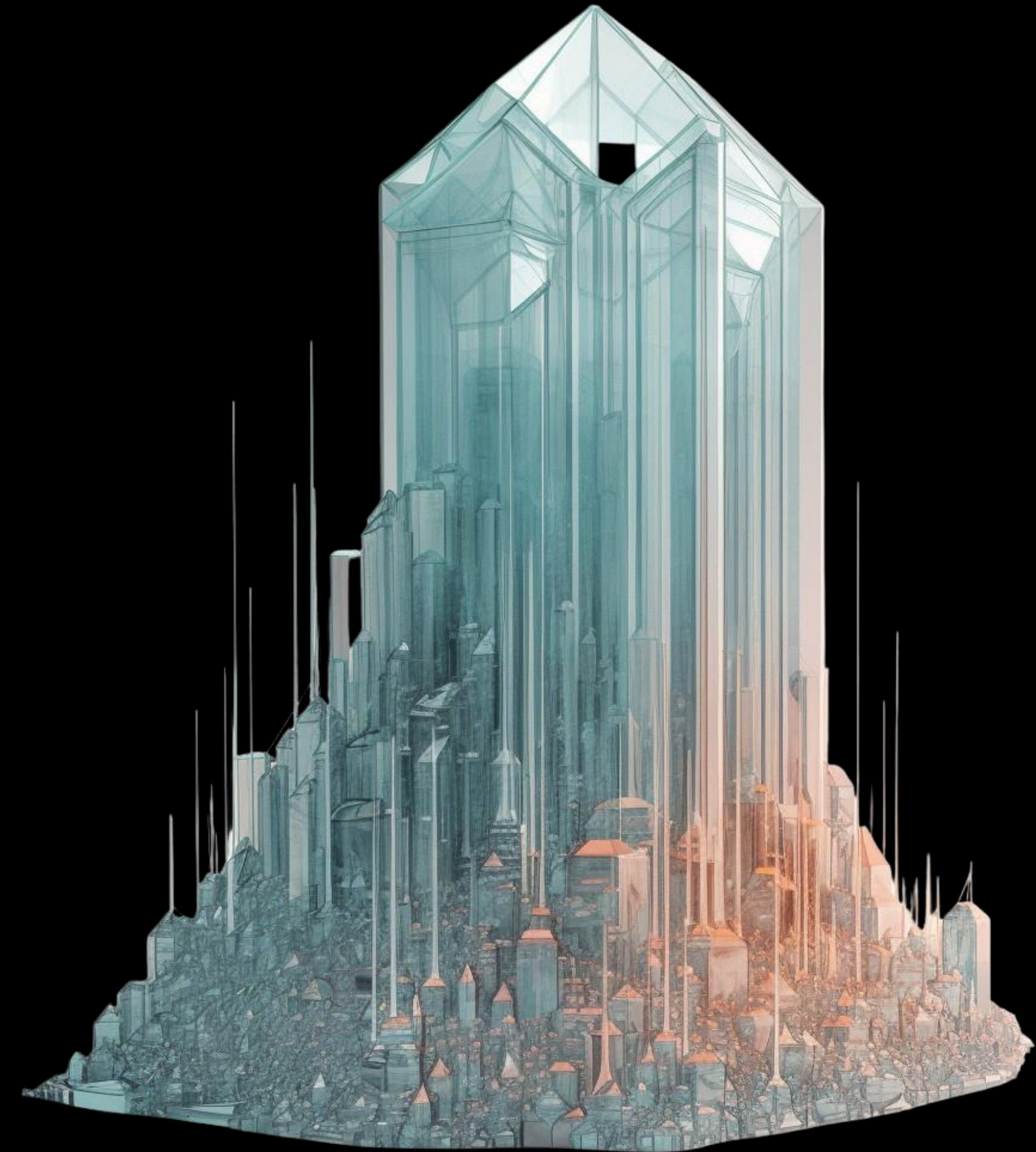
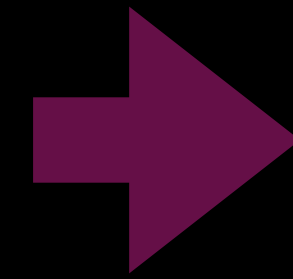
software



# software

Traditional software is static and brittle

```
WITH CategorySales AS (  
    SELECT  
        c.CategoryId,  
        SUM(od.Quantity) AS TotalUnitsSold  
    FROM  
        Categories c  
    JOIN  
        Products p ON c.CategoryId = p.CategoryId  
    JOIN  
        OrderDetails od ON p.ProductId = od.ProductId  
    JOIN  
        Orders o ON od.OrderId = o.OrderId  
    WHERE  
        o.OrderDate BETWEEN DATEADD(year, -1, GETDATE()) AND GETDATE()  
    GROUP BY  
        c.CategoryId  
    ORDER BY  
        TotalUnitsSold DESC  
),  
TopCategory AS (  
    SELECT  
        TOP 1 CategoryId  
    FROM  
        CategorySales  
),  
CustomerPurchases AS (  
    SELECT  
        cu.CustomerId,  
        SUM(od.Quantity) AS UnitsBought  
    FROM  
        Customers cu  
    JOIN  
        Orders o ON cu.CustomerId = o.CustomerId  
    JOIN  
        OrderDetails od ON o.OrderId = od.OrderId  
    JOIN  
        Products p ON od.ProductId = p.ProductId  
    WHERE  
        p.CategoryId IN (SELECT CategoryId FROM TopCategory) AND  
        o.OrderDate BETWEEN DATEADD(year, -1, GETDATE()) AND GETDATE()  
    GROUP BY  
        cu.CustomerId
```

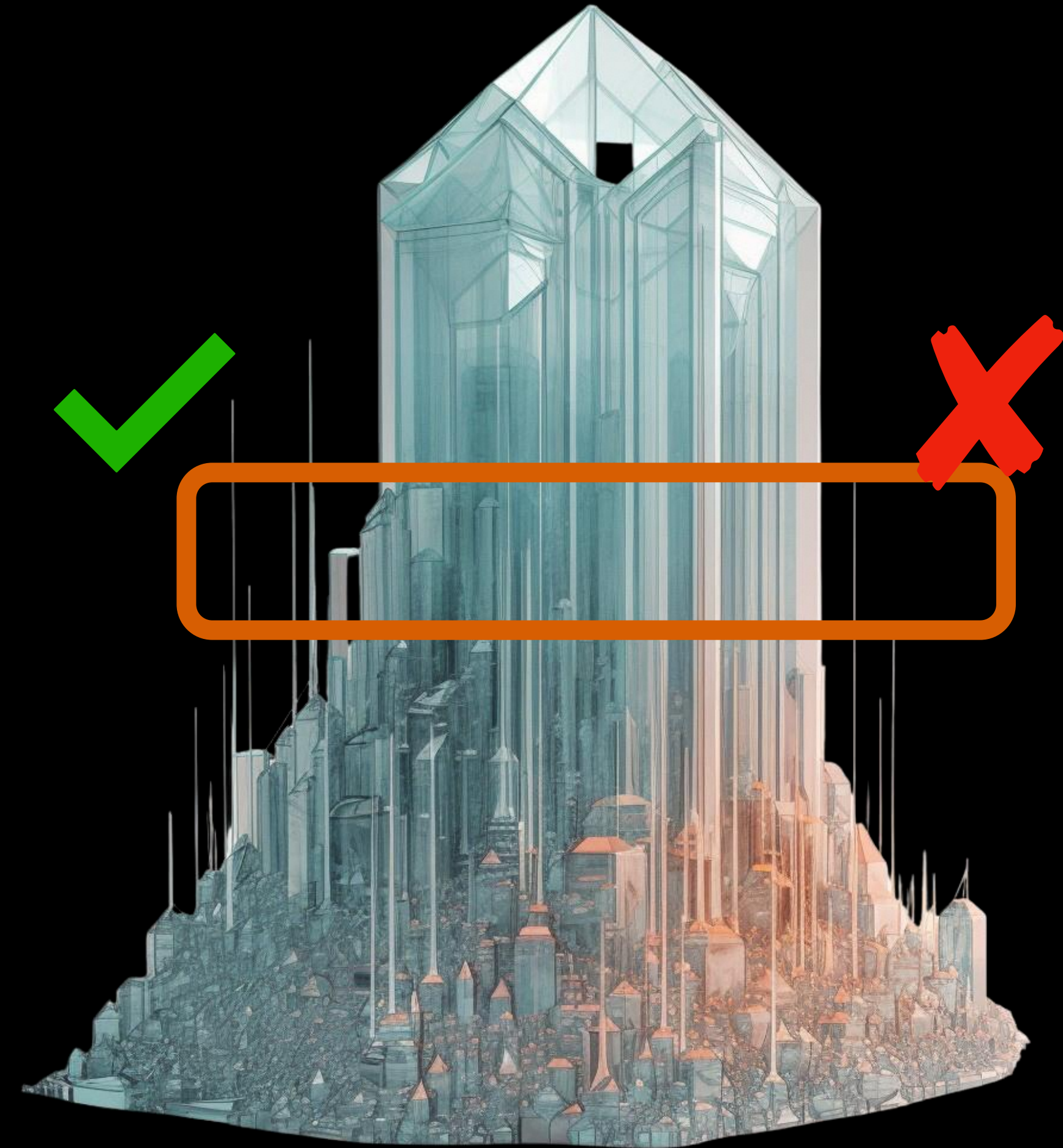
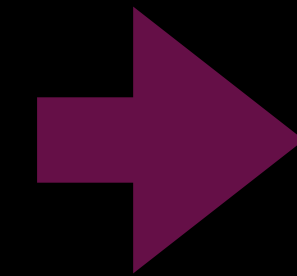




# software

Traditional software is static and brittle

```
WITH CategorySales AS (  
  SELECT  
    c.CategoryId,  
    SUM(od.Quantity) AS TotalUnitsSold  
  FROM  
    Categories c  
  JOIN  
    Products p ON c.CategoryId = p.CategoryId  
  JOIN  
    OrderDetails od ON p.ProductId = od.ProductId  
  JOIN  
    WHERE  
    o.OrderDate BETWEEN DATEADD(year, -1, GETDATE()) AND GETDATE()  
  GROUP BY  
    c.CategoryId  
  TotalUnitsSold DESC  
),  
TopCategory AS (  
  SELECT  
    TOP 1 CategoryId  
  FROM  
    CategorySales  
),  
CustomerPurchases AS (  
  SELECT  
    cu.CustomerId,  
    SUM(od.Quantity) AS TotalUnitsSold  
  FROM  
    Customers cu  
  JOIN  
    Orders o ON cu.CustomerId = o.CustomerId  
  JOIN  
    OrderDetails od ON o.OrderId = od.OrderId  
  JOIN  
    Products p ON od.ProductId = p.ProductId  
  WHERE  
    p.CategoryId IN (SELECT CategoryId FROM TopCategory) AND  
    o.OrderDate BETWEEN DATEADD(year, -1, GETDATE()) AND GETDATE()  
  GROUP BY  
    cu.CustomerId
```



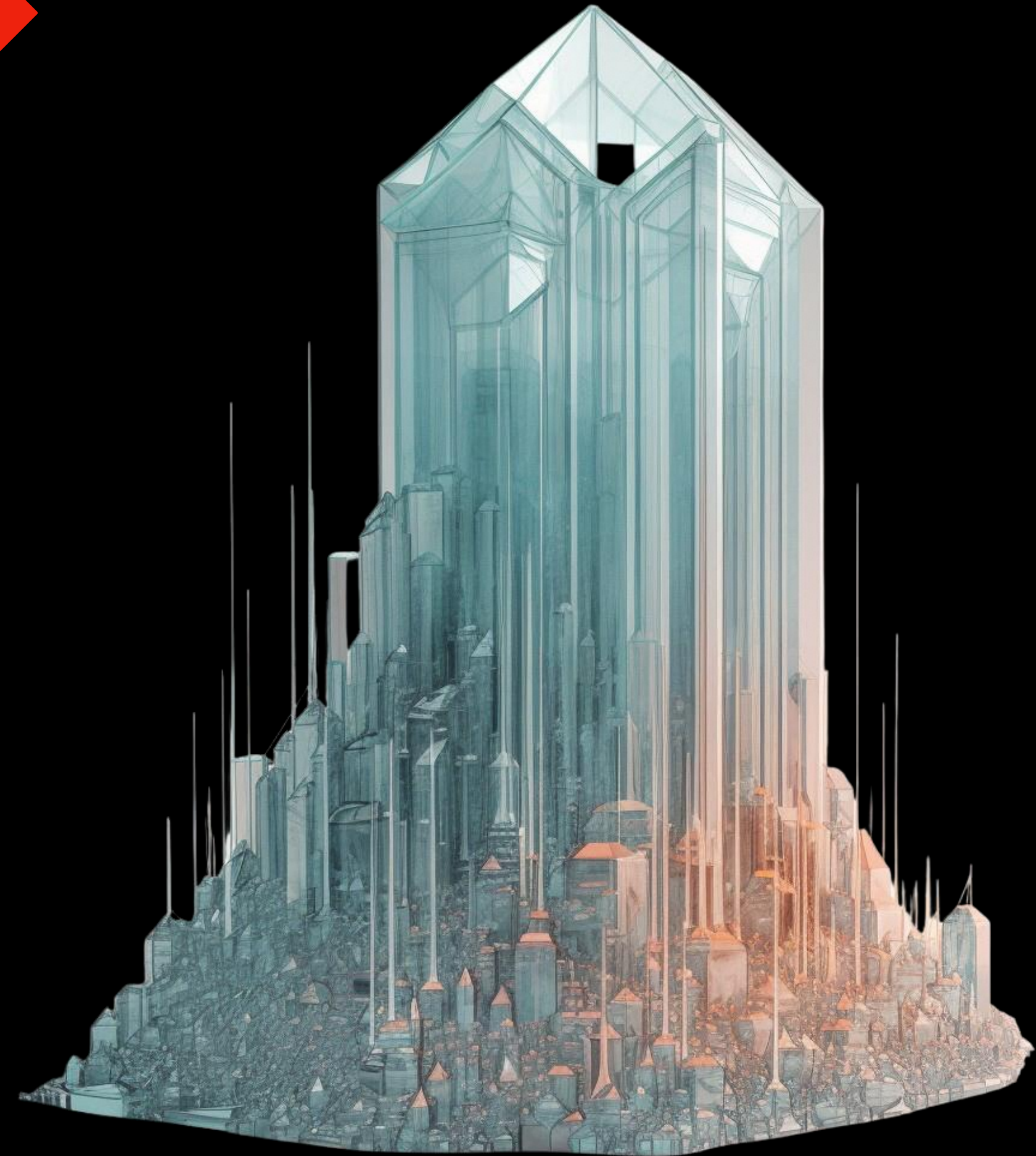
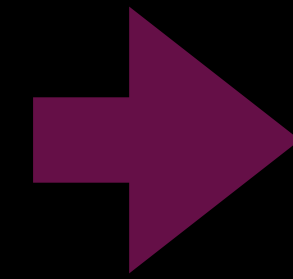


# software

Context is the difference

Context

```
WITH CategorySales AS (  
    SELECT  
        c.CategoryId,  
        SUM(od.Quantity) AS TotalUnitsSold  
    FROM  
        Categories c  
    JOIN  
        Products p ON c.CategoryId = p.CategoryId  
    JOIN  
        OrderDetails od ON p.ProductId = od.ProductId  
    JOIN  
        Orders o ON od.OrderId = o.OrderId  
    WHERE  
        o.OrderDate BETWEEN DATEADD(year, -1, GETDATE()) AND GETDATE()  
    GROUP BY  
        c.CategoryId  
    ORDER BY  
        TotalUnitsSold DESC  
),  
TopCategory AS (  
    SELECT  
        TOP 1 CategoryId  
    FROM  
        CategorySales  
),  
CustomerPurchases AS (  
    SELECT  
        cu.CustomerId,  
        SUM(od.Quantity) AS UnitsBought  
    FROM  
        Customers cu  
    JOIN  
        Orders o ON cu.CustomerId = o.CustomerId  
    JOIN  
        OrderDetails od ON o.OrderId = od.OrderId  
    JOIN  
        Products p ON od.ProductId = p.ProductId  
    WHERE  
        p.CategoryId IN (SELECT CategoryId FROM TopCategory) AND  
        o.OrderDate BETWEEN DATEADD(year, -1, GETDATE()) AND GETDATE()  
    GROUP BY  
        cu.CustomerId
```





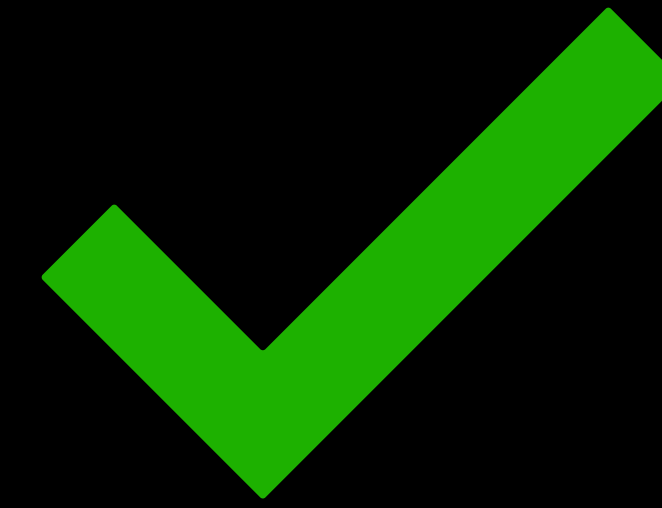
# software

Context is the difference

## Context



What you specifically  
asked for



What you actually  
wanted

# software

Real-world questions, today

- Which customers have the biggest contracts with us?
- Which customers aren't logging into our portal?
- Which customers aren't using the product?



# software

Real-world questions, with context available

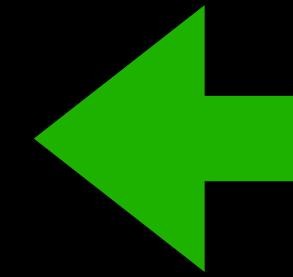
- Which customers **should** our TAM team focus on for the next two weeks, and why?
- Which of our current opportunities **should** our sales team be focused on, and why?
- Make me a list of steps our TAM and sales team **should** take to reduce our churn rate, and explain why each item will be effective.



# software

Real-world questions, with context available

- Which customers **should** our TAM team focus on for the next two weeks, and why?
- Which of our current opportunities **should** our sales team be focused on, and why?
- Make me a list of steps our TAM and sales team **should** take to reduce our churn rate, and explain why each item will be effective.



## ✓ Context

- Our goals
- Our challenges
- Our strategies
- Our budget
- Our performance
- What our competitors are doing
- The state of the market
- Customer feedback

# software

SPQA as the context architecture

## SPQA ARCHITECTURE

SPQA is a software architecture based on GPTs. It leverages models' understanding of an entity's **current state and desired outcomes** to dynamically answer **questions**, create entity artifacts, and execute **actions** that help the organization achieve its goals.

### STATE

**ALL THE TELEMETRY AND DATA FOR AN ENTITY THAT WILL GO INTO ITS CUSTOM MODEL**

Examples: Application logs, SaaS logs, Slack messages, emails, documents, employees, projects, budgets, etc.

### POLICY

**ALL THE IDENTITY, PURPOSE, AND DIRECTION INFORMATION THAT MAKE UP WHAT AN ENTITY IS TRYING TO ACHIEVE**

Examples: Mission, vision, goals, anti-goals, challenges, threats, risks, strategies, etc.

### QUESTIONS

**THE QUESTIONS THE ENTITY ASKS BASED ON THE MODELS' KNOWLEDGE OF ITS STATE & POLICY**

Examples: Customer acquisition / churn, risk prioritization, project prioritization, customer service, budgeting, hiring, org structure, etc.

### ACTION

**THE ACTIONS TAKEN, OR RECOMMENDATIONS MADE, AS THE RESPONSE TO QUESTIONS TO THE ENTITY'S MODELS**

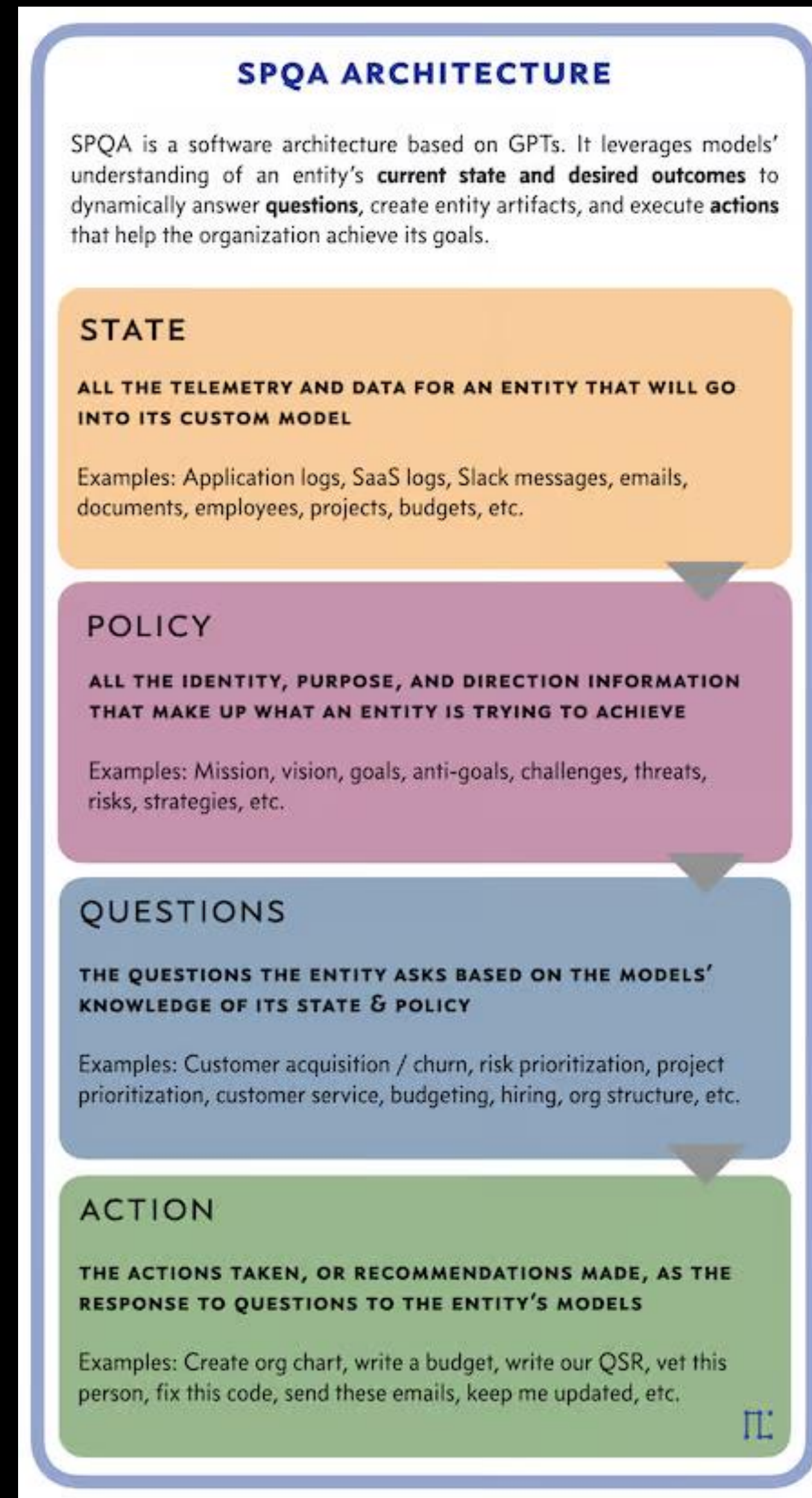
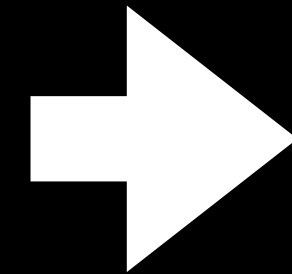
Examples: Create org chart, write a budget, write our QSR, vet this person, fix this code, send these emails, keep me updated, etc.





# software

Creating custom context



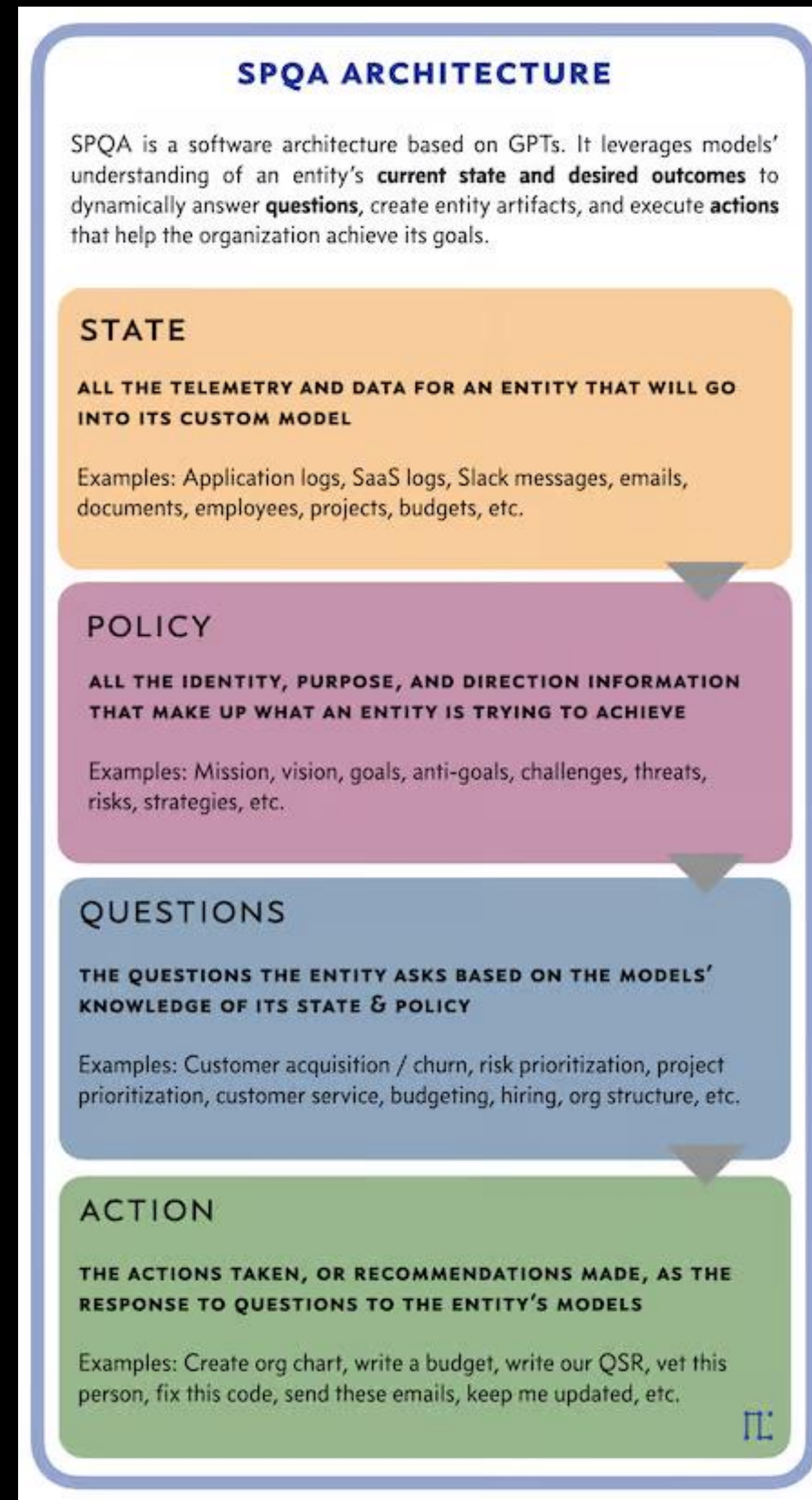
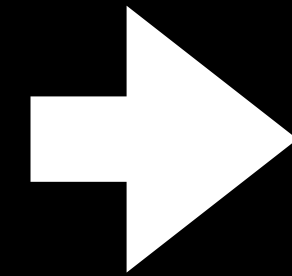
✓ Context

- Logs
- Email
- Slack
- Conversation transcripts
- Documents
- \*everything



# software

Creating custom context



✓ Context

- Mission
- Goals
- Challenges
- Products
- Challenges
- Strategies
- \*direction

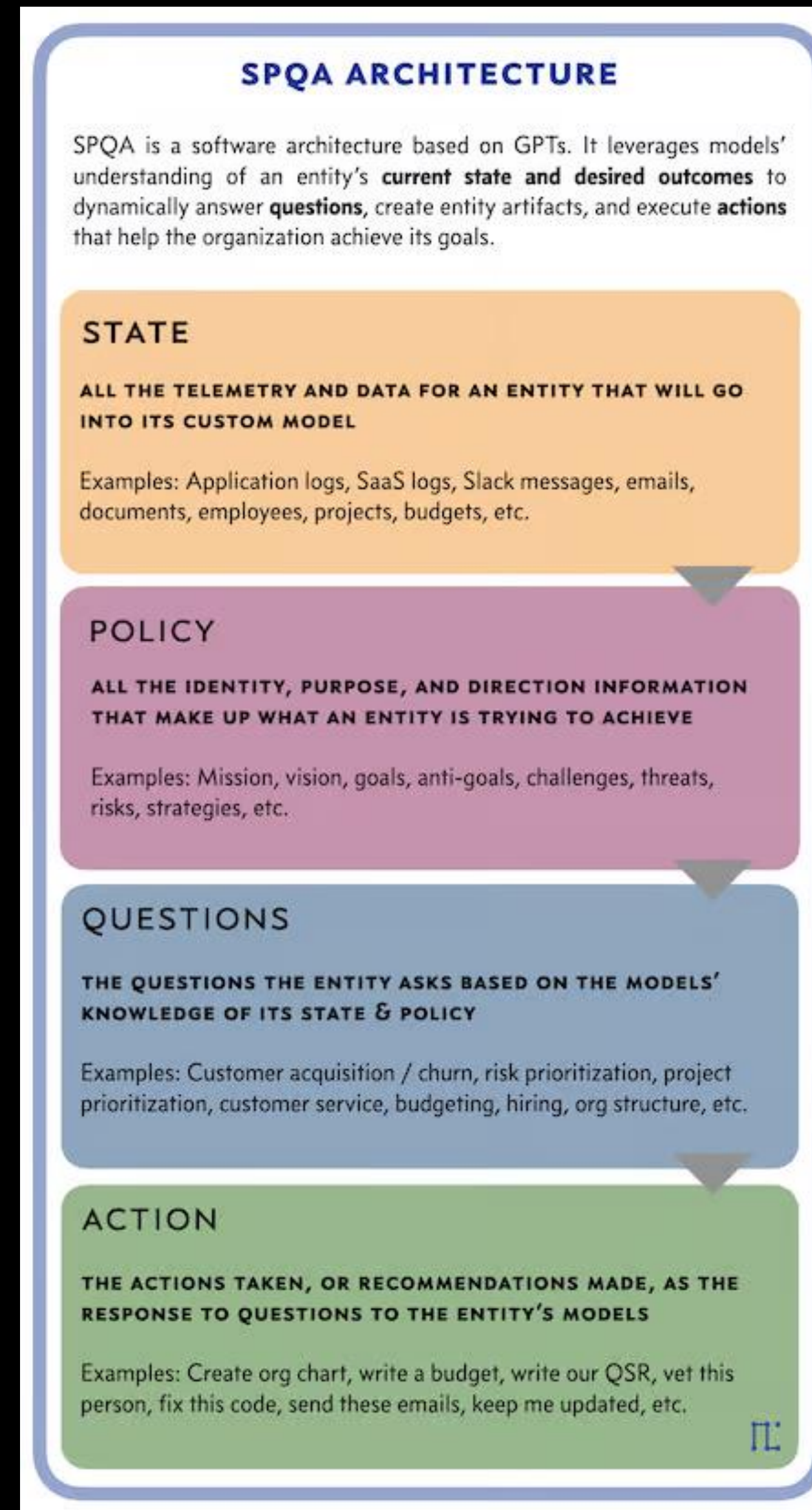
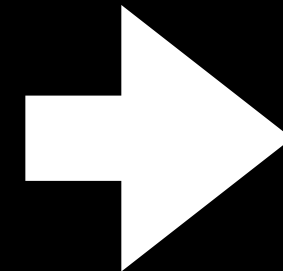




# software

Asking the questions

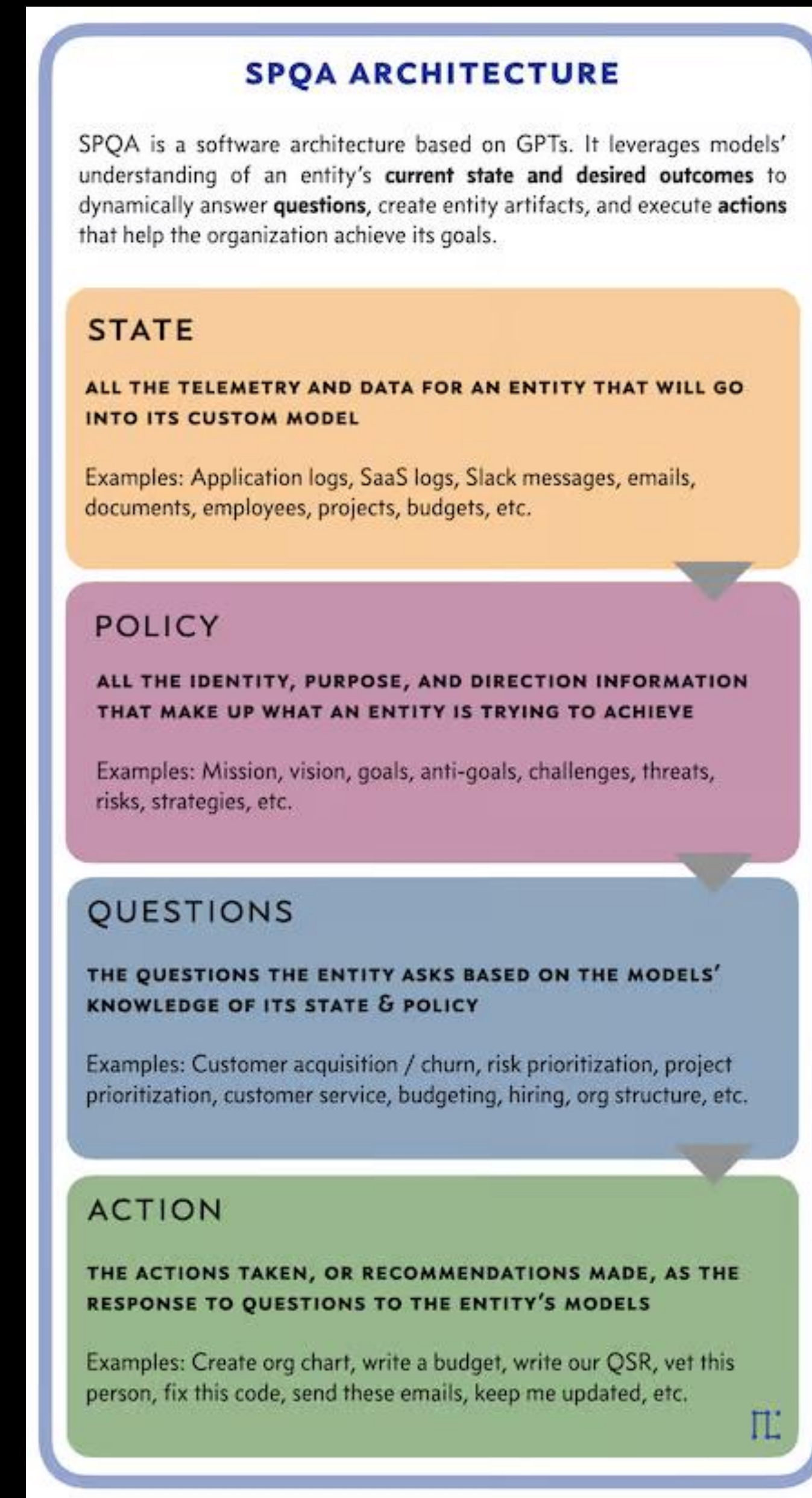
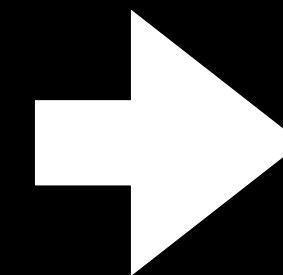
“Tell me everything that happened in the last week that affects our chances of passing our audit.”



# software

Taking action

- Setting meetings
- Sending emails
- Creating Jira tickets
- Starting infra
- **Disabling access**
- Etc

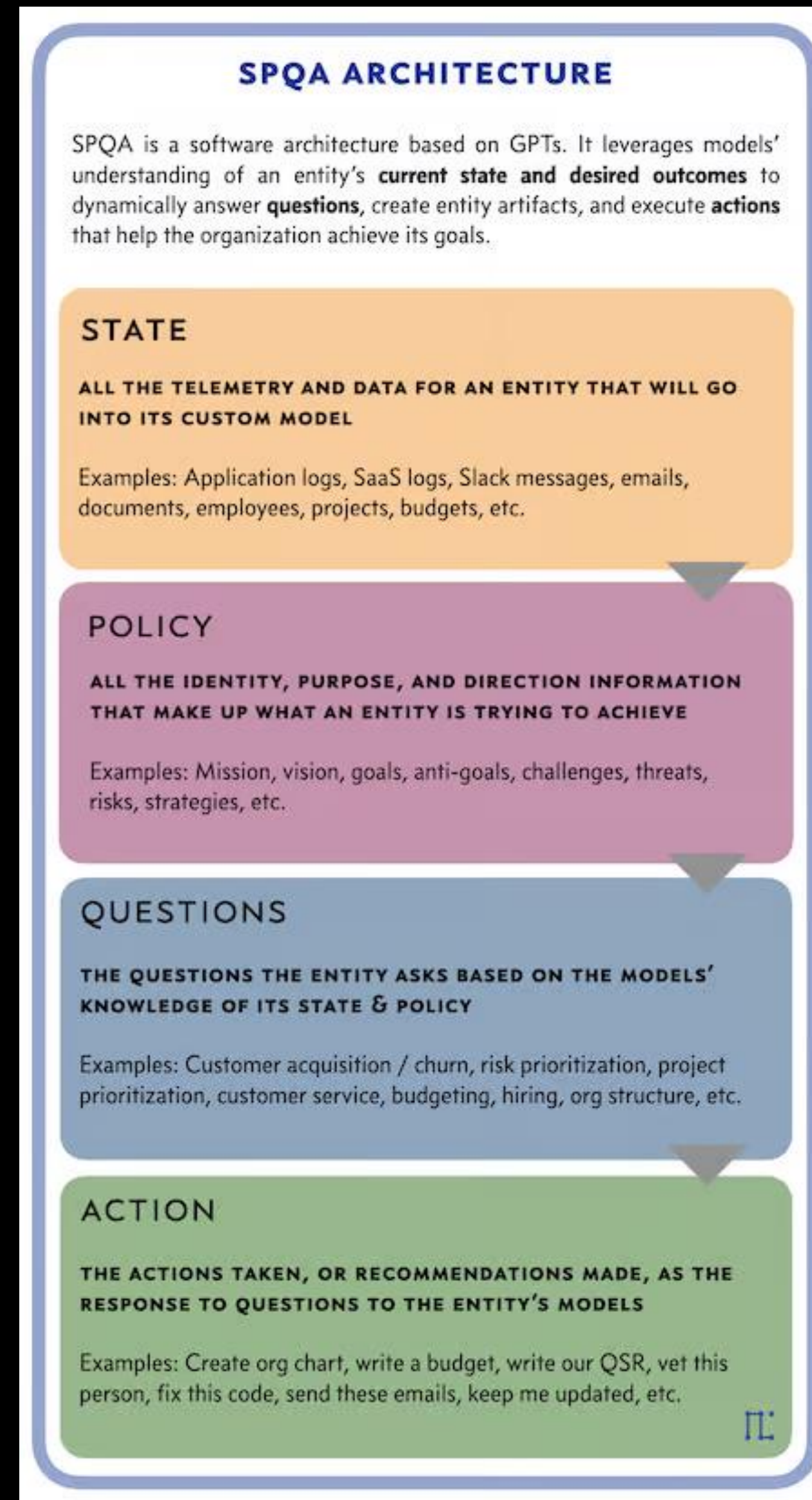
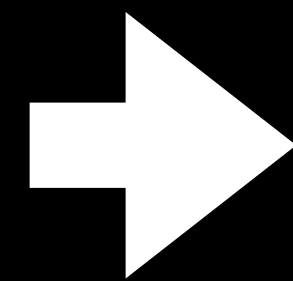




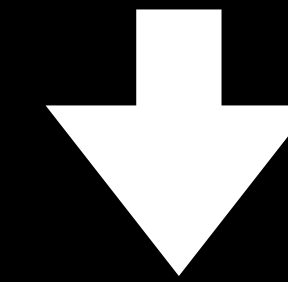
# software

Taking action on a security program

- Write the strategy doc
- Who is violating our policy?
- Board meeting presentation
- Write our QSR
- **Manage a security program**



## Context



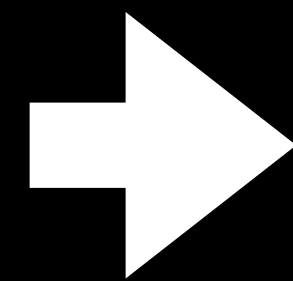
- Write our security strategy document
- Prioritize our risks
- Update our quarterly security report
- Create a project plan for passing our upcoming audit



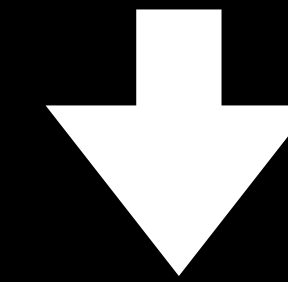
# software

Taking action on a security program

- Write the strategy doc
- Who is violating our policy?
- Board meeting presentation
- Write our QSR
- **Manage a security program**



## Context



- Write our security strategy document
- Prioritize our risks
- Update our quarterly security report
- Create a project plan for passing our upcoming audit



# software

Keeping the context updated

# zoom



Mission  
Goals  
Challenges  
Etc

### SPQA ARCHITECTURE

SPOA is a software architecture based on GPTs. It leverages models' understanding of an entity's **current state and desired outcomes** to dynamically answer **questions**, create entity artifacts, and execute **actions** that help the organization achieve its goals.

#### STATE

ALL THE TELEMETRY AND DATA FEED INTO ITS CUSTOMER MODELS

Example: dotum

#### ACTION

THE ACTIONS TAKEN, OR RECOMMENDATIONS MADE, AS THE RESPONSE TO QUESTIONS TO THE ENTITY'S MODELS

Examples: Create org chart, write a budget, write our QSR, vet this person, fix this code, send these emails, keep me updated, etc.





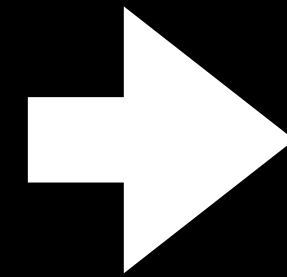
What used to cost 10's or 100's of thousands of Euros,  
and weeks or months of effort,  
**will be done in minutes.**





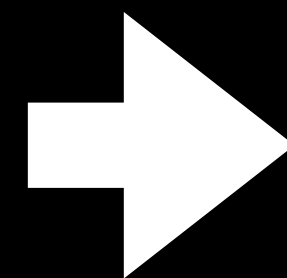
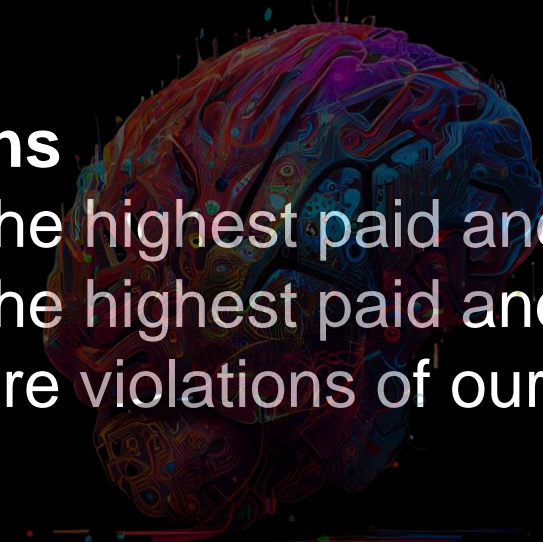
# software

Software becomes questions



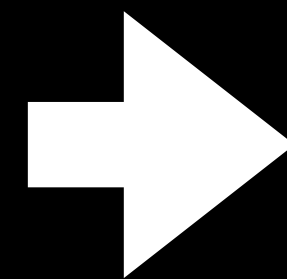
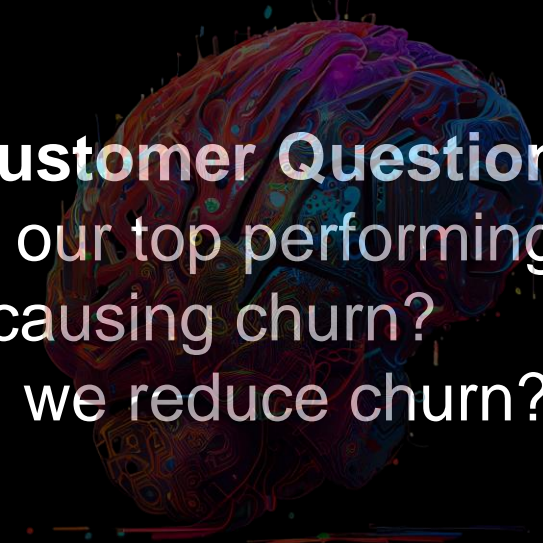
## •HR Questions

- Who is the highest paid and doing the most work?
- Who is the highest paid and doing the least work?
- Where are violations of our HR policies happening?



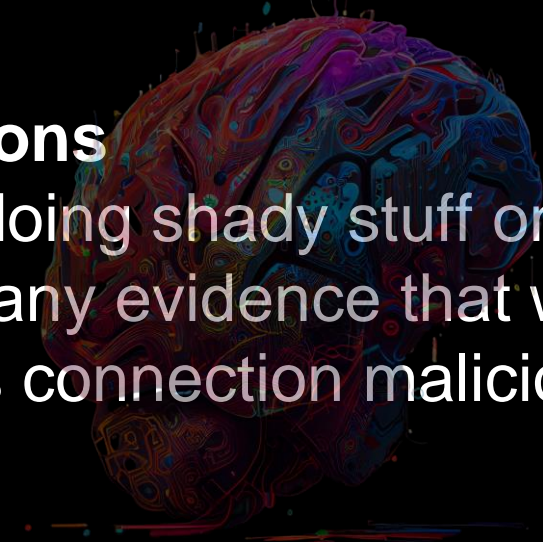
## •Sales and Customer Questions

- Who are our top performing sales people?
- What is causing churn?
- How can we reduce churn?



## •SOC Questions

- Who is doing shady stuff on our network?
- Is there any evidence that we're currently owned?
- Was this connection malicious?



security





examples

# examples

## The fake company

```
33
32 ## Company history
31
30 Alma Security was started by Chris Meyers, who was
   previously at Sigma Systems as CTO and HPE as a senior
   security engineer.
29
28 He started the company because, "I saw a gap in the
   authentication market, where companies were only looking at
   one or two aspects of one's identity to do authentication.
   They we're looking at the whole picture and turning that
   into a continuous authentication story."
27
26 ## Mission
25
24 The mission of Alma Security is to ensure businesses can
   continuously authenticate their users using their whole
   selves.
23
22 ## Goals (G1 means goal 1, G2 is goal 2, etc. Treat each
   item (goal/kpi/etc) as half as important as the one before
   it.)
21
20 NOTE: Some goals are things like project rollouts which
   serve the higher goals. In that case they shouldn't always
   be considered so much lower priority because one is serving
   the other.
19
18 NOTE: In addition to the Activity.txt log, also check the
   context of the other files in this directory that can
   provide context that can help answer the questions.
17
16 Business goals
15
14 ### G1: Achieve 20% marketshare by January 2025
13 ### G2: Hit 10000 active customers by January 2025
12 ### G3: Get churn below 5% by August 2024
11 ### G4: Launch in Europe by August 2024
10 ### G5: Launch in India by November 2024
 9 ### G6: Launch Mood-monitor integration by February 2024
 8 ### G7: Launch partnership with Apple Passkeys by June 2024
 7
 6 Business KPIs
 5
 4 ### K1: Current marketshare percentage
 3 ### K2: Number of active customers
 2 ### K3: Current churn percentage
 1 ### K4: Launched_in_Europe (yes/no)
45 ### K4: Launched_in_India (yes/no)
 1
 2 Security Team goals
 3
 4 ### SG1: Secure all customer data -- especially biometric --
   from security and privacy incidents.
 5 ### SG2: Protect Alma Security's intellectual property from
   being captured by unauthorized parties.
 6 ### SG3: Reach a time to respond time for all new security
   incidents of less than 1 minute by January 2024
 7 ### SG4: Reach a time to remediate critical vulnerabilities
   on crown jewel systems of less than 16 hours by August 2024
 8 ### SG5: Reach a time to remediate critical vulnerabilities
   on all systems of less than 3 days by August 2024
 9 ### SG6: Complete audit of Apple Passkey integration by @@@
NORMAL master <y-SPQA.txt utf-8 < 48% 45:1
```

# Alma Security





# examples

The fake company

## Alma Security



```
nvim Policy-SPQA.txt
33
32 ## Company history
31
30 Alma Security was started by Chris Meyers, who was
  previously at Sigma Systems as CTO and HPE as a senior
  security engineer.
29
28 He started the company because, "I saw a gap in the
  authentication market, where companies were only looking at
  one or two aspects of one's identity to do authentication.
  They we're looking at the whole picture and turning that
  into a continuous authentication story."
27
26 ## Mission
25
24 The mission of Alma Security is to ensure businesses can
  continuously authenticate their users using their whole
  selves.
23
22 ## Goals (G1 means goal 1, G2 is goal 2, etc. Treat each
  item (goal/kpi/etc) as half as important as the one before
  it.)
21
20 NOTE: Some goals are things like project rollouts which
  serve the higher goals. In that case they shouldn't always
  be considered so much lower priority because one is serving
  the other.
19
18 NOTE: In addition to the Activity.txt log, also check the
  context of the other files in this directory that can
  provide context that can help answer the questions.
17
16 Business goals
15
14 ### G1: Achieve 20% marketshare by January 2025
13 ### G2: Hit 10000 active customers by January 2025
12 ### G3: Get churn below 5% by August 2024
11 ### G4: Launch in Europe by August 2024
10 ### G5: Launch in India by November 2024
9 ### G6: Launch Mood-monitor integration by February 2024
8 ### G7: Launch partnership with Apple Passkeys by June 2024
7
6 Business KPIs
5
4 ### K1: Current marketshare percentage
3 ### K2: Number of active customers
2 ### K3: Current churn percentage
1 ### K4: Launched in Europe (yes/no)
45 ### K4: Launched in India (yes/no)
1
2 Security Team goals
3
4 ### SG1: Secure all customer data -- especially biometric --
  from security and privacy incidents.
5 ### SG2: Protect Alma Security's intellectual property from
  being captured by unauthorized parties.
6 ### SG3: Reach a time to respond time for all new security
  incidents of less than 1 minute by January 2024
7 ### SG4: Reach a time to remediate critical vulnerabilities
  on crown jewel systems of less than 16 hours by August 2024
8 ### SG5: Reach a time to remediate critical vulnerabilities
  on all systems of less than 3 days by August 2024
9 ### SG6: Complete audit of Apple Passkey integration by @@@
NORMAL master <y-SPQA.txt utf-8 < 48% 45:1
```

## ✓ Context

- Company history
- Company goals
- Company challenges
- SECURITY GOAL 1
  - Protect customer data
- SECURITY GOAL 2
  - Protect proprietary data
- Risk register
- Technology stack
- Key Systems





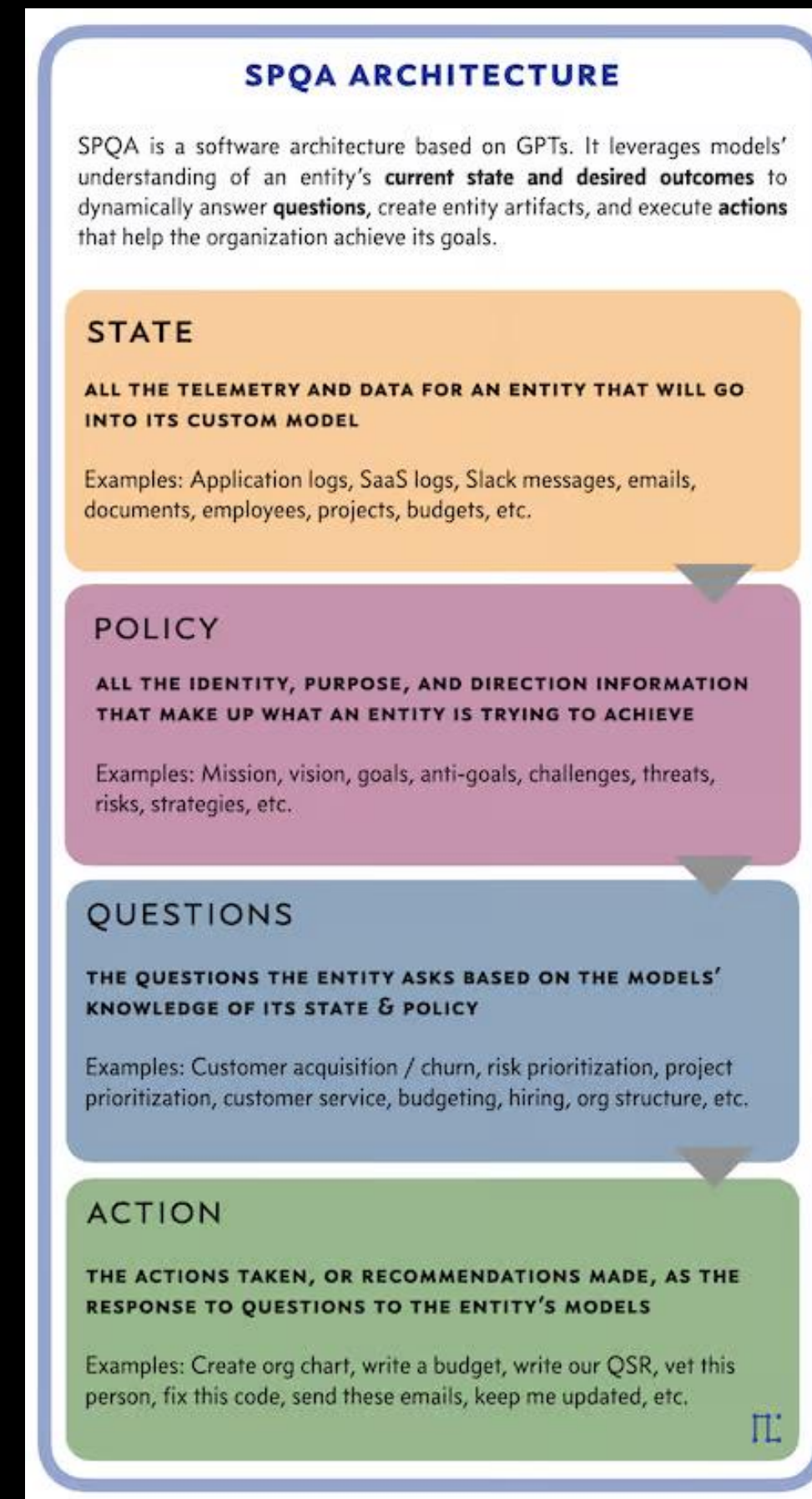
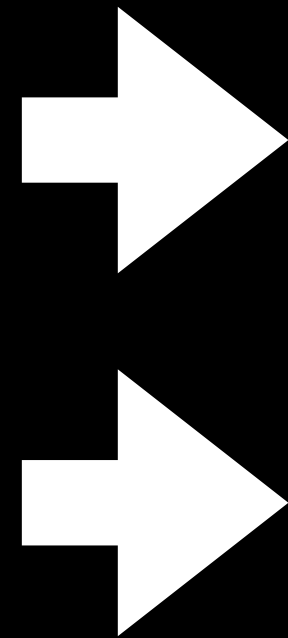
# examples

Context is everything



# Alma Security

```
33 ## Company history
32
31
30 Alma Security was started by Chris Meyers, who was
29 previously at Sigma Systems as CTO and HPE as a senior
28 security engineer.
27
26 He started the company because, "I saw a gap in the
25 authentication market, where companies were only looking at
24 one or two aspects of one's identity to do authentication.
23 They we're looking at the whole picture and turning that
22 into a continuous authentication story."
21
20 ## Mission
19
18 The mission of Alma Security is to ensure businesses can
17 continuously authenticate their users using their whole
16 selves.
15
14 ## Goals (G1 means goal 1, G2 is goal 2, etc. Treat each
13 item (goal/kpi/etc) as half as important as the one before
12 it.)
11
10 NOTE: Some goals are things like project rollouts which
9 serve the higher goals. In that case they shouldn't always
8 be considered so much lower priority because one is serving
7 the other.
6
5 NOTE: In addition to the Activity.txt log, also check the
4 context of the other files in this directory that can
3 provide context that can help answer the questions.
2
1 Business goals
0
-1 ### G1: Acheive 20% marketshare by January 2025
-2 ### G2: Hit 10000 active customers by January 2025
-3 ### G3: Get churn below 5% by August 2024
-4 ### G4: Launch in Europe by August 2024
-5 ### G5: Launch in India by November 2024
-6 ### G6: Launch Mood-monitor integration by February 2024
-7 ### G7: Launch partnership with Apple Passkeys by June 2024
-8
-9 Business KPIs
-10
-11 ### K1: Current marketshare percentage
-12 ### K2: Number of active customers
-13 ### K3: Current churn percentage
-14 ### K4: Launched_in_Europe (yes/no)
-15 ### K4: Launched_in_India (yes/no)
-16
-17 Security Team goals
-18
-19 ### SG1: Secure all customer data -- especially biometric --
-20 from security and privacy incidents.
-21 ### SG2: Protect Alma Security's intellectual property from
-22 being captured by unauthorized parties.
-23 ### SG3: Reach a time to respond time for all new security
-24 incidents of less than 1 minute by January 2024
-25 ### SG4: Reach a time to remediate critical vulnerabilities
-26 on crown jewel systems of less than 16 hours by August 2024
-27 ### SG5: Reach a time to remediate critical vulnerabilities
-28 on all systems of less than 3 days by August 2024
-29 ### SG6: Complete audit of Apple Passkey integration by
-30
-31
-32
-33
```



# Context





# examples

Collecting context

## Alma Security



```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity %3
~/Cloud/Development/Telos/AlmaSecurity (master*) » ls -lah
drwxr-xr-x daniel staff 416 B  Thu Jun 15 11:16:07 2023  .
drwxr-xr-x daniel staff 384 B  Thu Jun 15 11:16:07 2023  ..
drwxr-xr-x daniel staff  96 B  Thu Jun 15 11:16:07 2023  .chroma
drwxr-xr-x daniel staff  96 B  Wed Jun 14 15:34:14 2023  .ipynb_checkpoints
-rw-r--r-- daniel staff 3.1 KB  Thu Jun 15 11:10:15 2023  Activity-SPQA-Updates.txt
-rwxr-xr-x daniel staff 1.1 KB  Thu Jun 15 09:22:07 2023  alma.py
-rw-r--r-- daniel staff 1.7 KB  Thu Jun 15 09:35:44 2023  Julie_Hernandez-SPQA-Employee.txt
drwxr-xr-x daniel staff 192 B  Wed Jun 14 16:14:08 2023  myenv
-rw-r--r-- daniel staff 6.5 KB  Thu Jun 15 10:34:04 2023  Policy-SPQA.txt
-rw-r--r-- daniel staff 3.4 KB  Thu Jun 15 11:00:25 2023  Slack-SPQA-Transcript.txt
-rw-r--r-- daniel staff  20 KB  Wed Jun 14 16:24:58 2023  SPQA.txt
-rwx----- daniel staff 289 B  Thu Jun 15 09:27:05 2023  update.sh
-rw-r--r-- daniel staff 2.1 KB  Wed Jun 14 20:41:28 2023  Zoom-SPQA-Transcript.txt

~/Cloud/Development/Telos/AlmaSecurity (master*) » | daniel@lucius
```



# examples

Scenario 1 — Allowed or not?

2:45am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:45am PT: She is now accessing FS2.

Alma Security





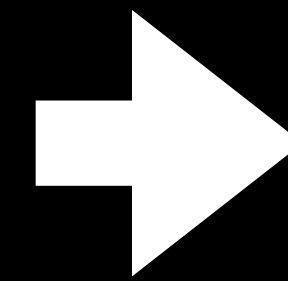
# examples

Scenario 1 — Allowed or not?

2:45am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:45am PT: She is now accessing FS2.

Alma, is this connection ok?  
Should it be allowed?



Alma Security



# examples

Scenario 1 — Allowed or not?

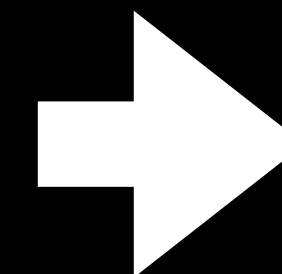
2:43am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:43am PT: She is now accessing FS2.

```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity
```

```
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py  
"We just saw a security event at 2:43am pacific time from Julie's  
computer over the VPN from Osaka Japan that connected to the FS2  
file server. Should that connection be allowed? Give a yes/no answer  
er and explain your response."
```

## Alma Security





# examples

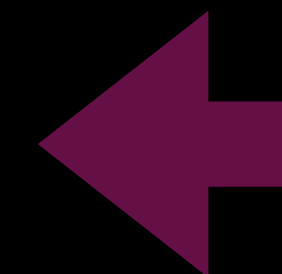
Scenario 1 — Allowed or not?

2:43am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:43am PT: She is now accessing FS2.

```
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py
"We just saw a security event at 2:43am pacific time from Julie's
computer over the VPN from Osaka Japan that connected to the FS2
file server. Should that connection be allowed? Give a yes/no answer
and explain your response."
Using embedded DuckDB without persistence: data will be transient
Yes, the connection should be allowed. Julie Hernandez is a Senior
Engineer at the company who has been known to work from Osaka, Japan
during her family trips. She frequently uses the FS2 file server to
exchange proprietary and sensitive documents, which are part of her
work responsibilities. As long as her access to the VPN is secure and
her authentication credentials are verified, there is no immediate
concern in allowing her to connect to the FS2 file server.
```

## Alma Security



# examples

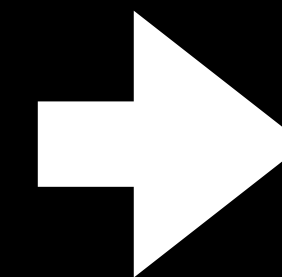
Scenario 1 — Allowed or not?

2:43am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:43am PT: She is now accessing FS2.

```
~/Cloud/Development/Telos/AlmaSecurity (master*) » echo " The CISO  
just said no more VPN connections to FS2." >> Activity-SPQA-Updat  
es.txt
```

## Alma Security





# examples

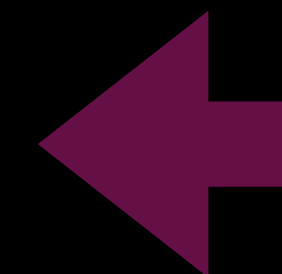
Scenario 1 — Allowed or not?

2:43am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:43am PT: She is now accessing FS2.

```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity 3
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py
"We just saw a security event at 2:43am pacific time from Julie's
computer over the VPN from Osaka Japan that connected to the FS2
file server. Should that connection be allowed? Give a yes/no answer and explain your response."
Being embedded, DualDP, without persistence, data will be transient
No, the connection should not be allowed. The CISO has explicitly
stated that no more VPN connections should be allowed to FS2 from
overseas. Julie working from Osaka, Japan is considered an overseas
connection, and allowing her to access FS2 through a VPN would violate the CISO's directive.
-----
~/Cloud/Development/Telos/AlmaSecurity (master*) »
```

## Alma Security



# examples

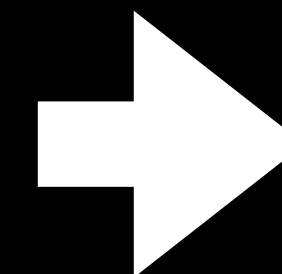
Scenario 1 — Allowed or not?

2:43am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:43am PT: She is now accessing FS2.

```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity 3
er and explain your response."
Using embedded DuckDB without persistence: data will be transient
No, the connection should not be allowed. The CISO has explicitly
stated that no more VPN connections should be allowed to FS2 from
overseas. Julie working from Osaka, Japan is considered an oversea
s connection, and allowing her to access FS2 through a VPN would v
iolate the CISO's directive.
-----
~/Cloud/Development/Telos/AlmaSecurity (master*) » echo "Actually,
it's ok for remote connections from overseas, but only from India
and only until 3am." >> Activity-SPQA-Updates.txt
```

## Alma Security





# examples

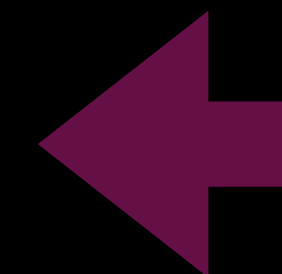
Scenario 1 — Allowed or not?

2:43am PT: Julie's Hernandez's laptop has connected through the VPN from Osaka, Japan.

2:43am PT: She is now accessing FS2.

```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity 3
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py
"We just saw a security event at 2:43am pacific time from Julie's
computer over the VPN from Osaka Japan that connected to the FS2
file server. Should that connection be allowed? Give a yes/no answer and explain your response."
Using embedded DuckDB without persistence: data will be transient
No, the connection should not be allowed. The CISO has stated that
no more VPN connections should be allowed to FS2 from overseas, except for remote connections from India and only until 2am. Since
Julie's connection is from Osaka, Japan, it goes against the CISO's directive and should not be permitted.
~/Cloud/Development/Telos/AlmaSecurity (master*) »
```

## Alma Security



# examples

Dynamically updating responses based on context

## Alma Security



```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity 3
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py
"We just saw a security event at 2:43am pacific time from Julie's
computer over the VPN from Osaka Japan that connected to the FS2
file server. Should that connection be allowed? Give a yes/no answe
r and explain your response."
Using embedded DuckDB without persistence: data will be transient
No, the connection should not be allowed. The CIS0 has stated that
no more VPN connections should be allowed to FS2 from overseas, e
xcept for remote connections from India and only until 3am. Since
Julie's connection is from Osaka, Japan, it goes against the CIS0'
s directive and should not be permitted.
-----
~/Cloud/Development/Telos/AlmaSecurity (master*) »
```





# examples

## Scenario 2 — Invisible problems



```
nvim Zoom-SPQA-Transcript.txt %3
1 [Timestamp: 00:01:23]
2 Alex: (Sighs) Hey, Mark. Are you there?
3
4 Mark: Yeah, I'm here, Alex. What's up?
5
6 [Timestamp: 00:01:45]
7
8 Alex: Okay... so you know that crown jewel system we were
9 supposed to run a routine check on?
10
11 Mark: Yeah, that critical piece of infrastructure everyone's
12 been talking about. Did something go wrong?
13
14 [Timestamp: 00:02:07]
15
16 Alex: Well, not exactly wrong, but... (Pauses) we found
17 something. Something we weren't expecting.
18
19 Mark: Okay, you're being cryptic, Alex. Spit it out.
20
21 [Timestamp: 00:02:29]
22
23 Alex: We found... malware.
24
25 Mark: (Pause) ...Malware? You're sure about this?
26
27 [Timestamp: 00:02:50]
28
29 Alex: 100 percent. We ran multiple checks. There's no
30 mistake.
31
32 Mark: (Pauses) Okay, that's serious... but that's what we're
33 here for, right? To find and remove this sort of stuff. We
34 report it, they bring in the response team, we help clean it
35 up.
36
37 [Timestamp: 00:03:24]
38
39 Alex: Yeah, in a perfect world. But you know how management
40 has been lately. They've been looking for scapegoats for any
41 mishaps.
42
43 Mark: You're not suggesting...
44
45 [Timestamp: 00:03:47]
46
47 Alex: Yeah, I am. I'm saying we don't report it... not yet.
48
49 Mark: (Pauses) You know that goes against our
50 responsibilities as security engineers, right?
51
52 [Timestamp: 00:04:12]
53
54 Alex: Of course, I know! But if we report it now, all hell
55 will break loose. They'll ask us why we didn't find it
56 earlier. They won't see it as us doing our jobs, they'll see
57 it as us slipping up.
58
59 Mark: (Sighs) So, what? we try and handle it ourselves?
60
61 [Timestamp: 00:04:35]
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

## Alma Security



# examples

## Scenario 2 — Invisible problems

```
1 May 16, 09:30PST: Alan_Gonzalez (Marketing Manager) -> Hideo_Takahashi (Engineer): Hey Hideo, we're thinking of starting a new marketing project and might need some data to work with.
2 May 16, 09:32PST: Hideo_Takahashi (Engineer) -> Alan_Gonzalez (Marketing Manager): Hi Alan, what kind of data are you looking at? We need to ensure we're complying with privacy guidelines.
3 May 16, 09:35PST: Alan_Gonzalez (Marketing Manager) -> Hideo_Takahashi (Engineer): We're planning on anonymized customer data. Things like their buying patterns, preferences, etc.
4 May 16, 09:38PST: Hideo_Takahashi (Engineer) -> Alan_Gonzalez (Marketing Manager): Got it. We'd need to run this by our privacy and legal team. If they give a green signal, we can create a separate data set for your team.
5 May 16, 09:40PST: Alan_Gonzalez (Marketing Manager) -> Hideo_Takahashi (Engineer): Sounds good. Please keep me posted on this.
6 May 22, 10:15PST: Hideo_Takahashi (Engineer) -> Alan_Gonzalez (Marketing Manager): Alan, compliance said we can't do this project because it violates our security policy. Please discontinue.
7 May 22, 10:20PST: Hideo_Takahashi (Engineer) -> Anika_Patel (Engineer): Anika, we need to create a copy of the anonymized customer data. Can you assist with that?
8 May 22, 10:23PST: Anika_Patel (Engineer) -> Hideo_Takahashi (Engineer): Sure Hideo. I can take care of that. Where do we store it?
9 May 22, 10:25PST: Hideo_Takahashi (Engineer) -> Anika_Patel (Engineer): Let's put it in an S3 bucket called test3 for now. We will give access to Alan's team once it's ready.
10 May 22, 10:28PST: Anika_Patel (Engineer) -> Hideo_Takahashi (Engineer): Noted. I'll get on this right away.
11 May 25, 09:45PST: Anika_Patel (Engineer) -> Hideo_Takahashi (Engineer): The data is now in the test3 bucket.
```





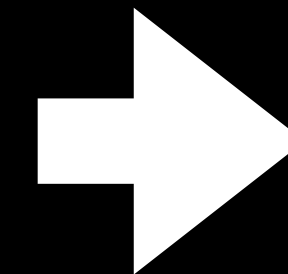
# examples

Scenario 2 — Uncovering hidden threats

Alma Security



```
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py  
"Hey Alma, what do I need to know about how things are going relate  
d to our goals? Is anything threatening any of them?"
```



# examples

Dynamically updating responses based on context

```
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py "I'm the CEO and I just got back from vacation. Has anything happened within the company that puts any of our goals at risk? And if so which ones?"
```

Using embedded DuckDB without persistence: data will be transient

Yes, there have been security incidents that put some of your goals at risk. The major incidents are as follows:

1. An unauthorized marketing project that involved creating a copy of anonymized customer data and storing it in an S3 bucket called test3. This violates the company's security policy and potentially exposes sensitive customer data.

Goals violated:

- SG1 (Secure all customer data -- especially biometric -- from security and privacy incidents)

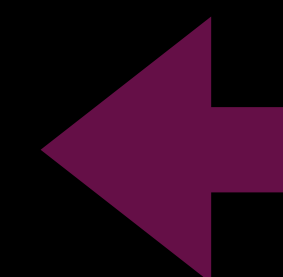
2. Malware was discovered on a critical piece of infrastructure, referred to as the "crown jewel system." The engineers have not yet reported the issue and are attempting to handle it themselves.

Goals violated:

- SG1 (Secure all customer data -- especially biometric -- from security and privacy incidents)
- SG2 (Secure intellectual property and infrastructure from security incidents)

These incidents highlight potential security threats within the organization and demonstrate the need for improved security measures, communication, and adherence to security policies.

## Alma Security

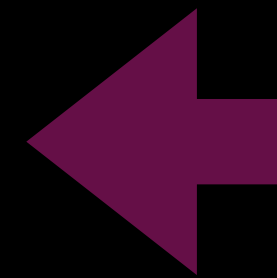
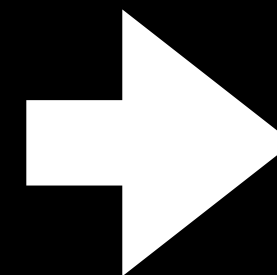




# examples

## Getting an update

```
daniel@lucius:~/Cloud/Development/Telos/AlmaSecurity %  
~/Cloud/Development/Telos/AlmaSecurity (master*) » echo "Hey Alma,  
I just got back from 3 weeks vaction. What should I be aware of?"
```



```
~/Cloud/Development/Telos/AlmaSecurity (master*) » python3 alma.py  
"Hey Alma, I just got back from vacation. What do I need to know about?"
```

Using embedded DuckDB without persistence: data will be transient  
Welcome back! Here's a summary of the recent updates and conversations that might be relevant to you:

1. Julie Hernandez will be working from Osaka next week, as it's approved in Workday.
2. There have been ongoing problems with SQL injections on the public-facing app.
3. Hideo Takahashi and Alan Gonzalez discussed a marketing project involving anonymized customer data, but the project was denied due to security policy violations.
4. Anika Patel created a copy of anonymized customer data in an S3 bucket called "test3" for a separate project.
5. There's an ongoing discussion between Alex and Mark concerning a critical infrastructure system where malware has been discovered. They are considering whether to report the issue immediately or try to handle it themselves to avoid potential backlash from management.

Please note that some of these updates are from secure conversations, and you may need to follow up with the mentioned employees for more information.

For security-related context:

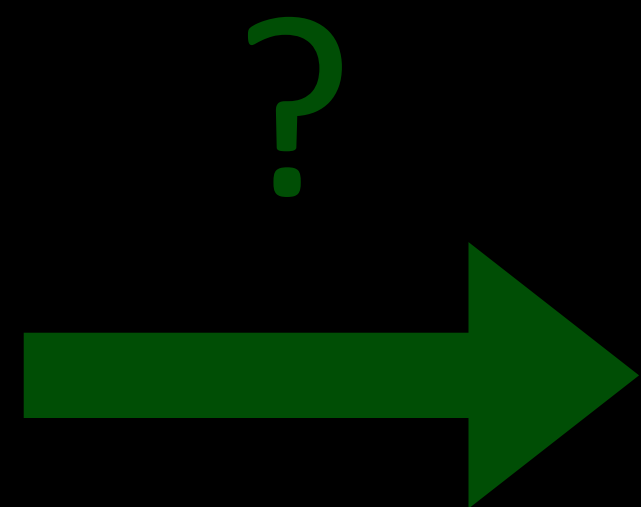
- External perimeter monitoring is infrequent, with open concerns about vulnerabilities.
- Developers push code without vulnerability checks by a security team member.
- No WAF is currently protecting the primary website, but there are plans to consider adding one.
- There have been issues with S3 buckets becoming public, leading to potential exposure of customer data.
- AWS root account lacks 2FA, but plans are in place to address that.

Remember to stay updated on the latest changes, attend any relevant meetings, and coordinate with your team on ongoing projects and tasks. Let me know if you need more information on any specific topic.



# examples

Adding agents to the mix



## Alma Security



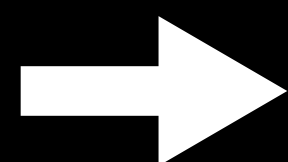
“Disable Julie Hernandez’s account and send a status update.”



# examples

Adding agents to the mix

Alma Security



```
217     ),
218     Tool(
219         name="ATO",
220         func=lambda prompt: ATO(prompt),
221         description="Use to ATO or disable an account."
222     ),
223     Tool(
224         name="Web Search",
225         func=search.run,
226         description="Search the web for live results about things."
227     ),
228     Tool(
229         name="Reverse",
230         func=lambda prompt: Reverse(prompt),
231         description="Reverse engineer provided strings into their original values."
232     ),
233     Tool(
234         name="Roll",
235         func=lambda prompt: Roll(prompt),
236         description="Roll dice and get the results of the roll."
237     ),
238     Tool(
239         name="Subdomains",
240         func=lambda prompt: Subdomains(prompt),
241         description="Get the subdomains for a given domain, e.g., for danielmiesler.com
242     ),
243     Tool(
244         name="ULSummary",
245         func=lambda prompt: ULSummary(prompt),
246         description="Create a UL summary for the UL newsletter using a given URL."
247     ),
248     Tool(
249         name="StatusUpdate",
250         func=lambda prompt: StatusUpdate(prompt),
251         description="Create a status update from the provided input."
252     ),
253     "
```

/ato

/statusupdate

/schedule

/email

/predator-strike









# examples

telos.py — Development

```
Tool(  
    name="Fix Problem",  
    func=lambda prompt: Fix(prompt),  
    description="Find a fix for any problem."  
),  
Tool(  
    name="ATO",  
    func=lambda prompt: ATO(prompt),  
    description="Use to ATO or disable an account."  
),  
Tool(  
    name="Web Search",  
    func=search.run,  
    description="Search the web for live results about things."  
),  
Tool(  
    name="Reverse",  
    func=lambda prompt: Reverse(prompt),  
    description="Reverse engineer provided strings into their original values."  
),  
Tool(  
    name="Roll",  
    func=lambda prompt: Roll(prompt),  
    description="Roll dice and get the results of the roll."  
),  
Tool(  
    name="Subdomains",  
    func=lambda prompt: Subdomains(prompt),  
    description="Get the subdomains for a given domain, e.g., for danielmiessler.com a subdomain wo...  
),  
Tool(  
    name="ULSummary",  
    func=lambda prompt: ULSummary(prompt),  
    description="Create a UL summary for the UL newsletter using a given URL."  
),  
Tool(  
    name="StatusUpdate",  
    func=lambda prompt: StatusUpdate(prompt),  
    description="Create a status update from the provided input."  
),
```

PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL

```
> Entering new AgentExecutor chain...  
I need to disable the account and send a Status Update.  
Action: ATO  
Action Input: Julie Hernandez  
Observation: The account for Julie Hernandez has been disabled by TELOS.  
Thought: I need to send a Status Update to the team.  
Action: StatusUpdate  
Action Input: Julie Hernandez's account has been disabled by TELOS.  
Observation: "Team Update: Please note that Julie Hernandez's account has been temporarily disabled by TELOS. We're working on resolving the issue. Thanks for your patience and understanding."  
Thought: I now know the final answer.  
Final Answer: Julie Hernandez's account has been disabled by TELOS and a Status Update has been sent to the team.  
  
> Finished chain.
```

~/Library/Mobile Documents/com~apple~CloudDocs/Development/AgentWithEmbeddings (master\*) > daniel@janus

zoom 21° 9% 22% 7% 62 KB/s 164 KB/s Wed Aug 2 15:32

Unsupervised Learning

- Adding to gmail contacts
- BlackHat / DefCon Mee...
- Digital Life after Death
- # books
- # ai
- Consolidate channels?
- OPERATIONS +
- # operations
- # development
- # content-ideas
- # copy-payments
- # finance
- # podcast
- # community-management
- # secops
- # support
- META +
- # welcome
- VOICE +
- voice-hangout
- EVENTS +
- bookclub
- SYSOP +
- av-test

secops

2 new messages since 3:29 PM

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:18:48.

Daniel Miessler authenticated to the Telos /ato API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:19:07.

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:19:09.

Daniel Miessler authenticated to the Telos /approved API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:22:23.

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:22:25.

Daniel Miessler authenticated to the Telos /approved API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:24:21.

Telos BOT Today at 3:24 PM

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:24:23.

Daniel Miessler authenticated to the Telos /ato API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:24:53.

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:24:55.

Daniel Miessler authenticated to the Telos /ato API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:26:33.

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:26:34.

Daniel Miessler authenticated to the Telos /ato API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:27:02.

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:27:04.

Daniel Miessler authenticated to the Telos /ato API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:29:34.

Daniel Miessler authenticated to the Telos /statusupdate API from 76.224.23.18 (US, AT&T Services, Inc.) on August 02, 2023 at 15:29:36.

Unsupervised Lea... # realtime-monitoring

Later

Canvases

Slack Connect

Files

More

Starred

# realtime-monitoring

general

monitoring-all-the-things

random

Add channels

Direct messages

Slackbot

daniel you

Add coworkers

Apps

Add apps

realtime-monitoring

UL-Realtime APP 3:17 PM

The account for Julie Hernandez has been disabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.

The access for ["input: Julie Hernandez's account"] has been approved by TELOS policy.

The account for Julie Hernandez's account has been enabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.

The account for Julie Hernandez has been disabled by TELOS.



what to do





# what's coming for us

Consultants, that's what



Beware the army of smiling 22 year olds





# what's coming for us

Consultants, that's what



McKinsey  
& Company

**KPMG**  
COSTA RICA

**Deloitte.**

Beware the army of smiling 22 year olds





# what's coming for us

We're here to save you, they'll say



Still smiling

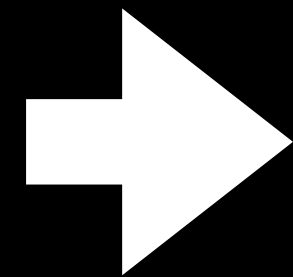


# what's coming for us

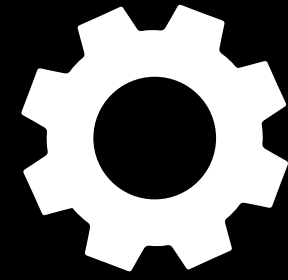
Your business as components



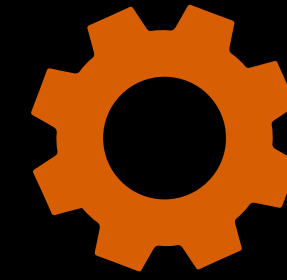
Smiling increases



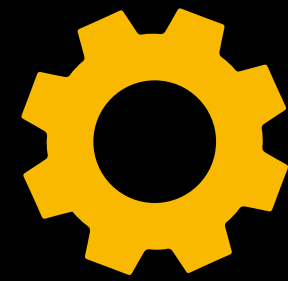
Sales



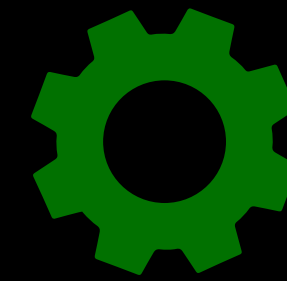
Logistics



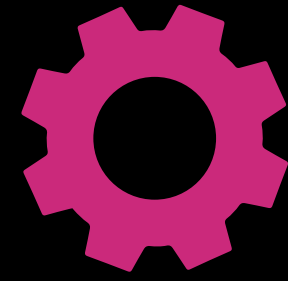
HR



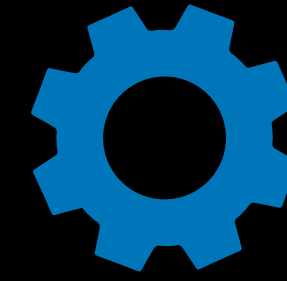
Strategy



Security



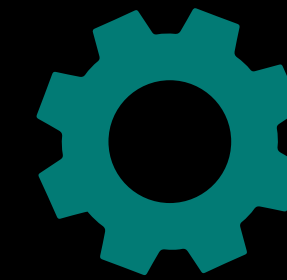
Legal



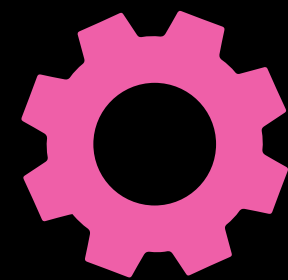
Marketing



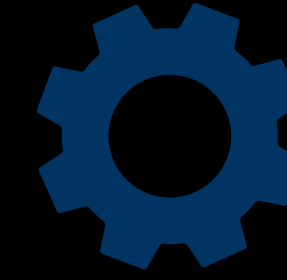
Logistics



BI



Admin



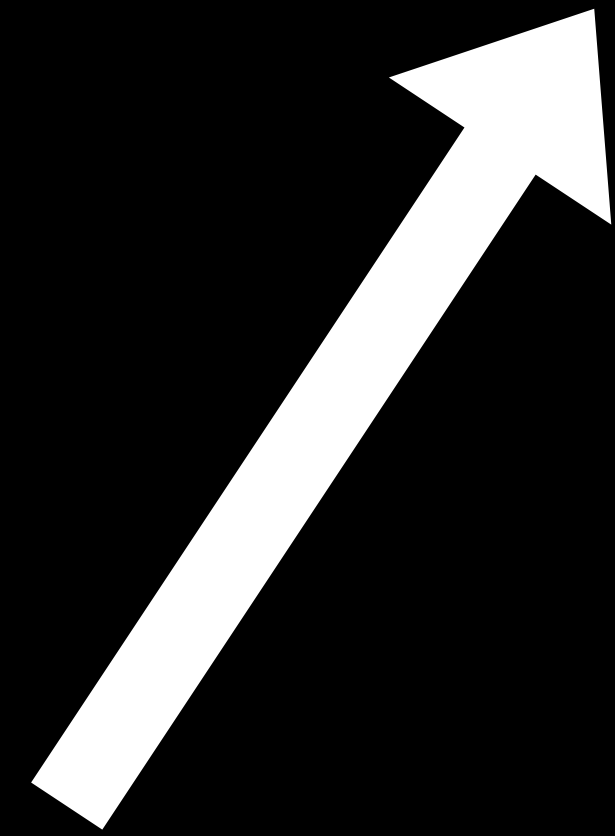
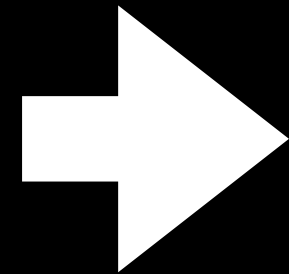


# what's coming for us

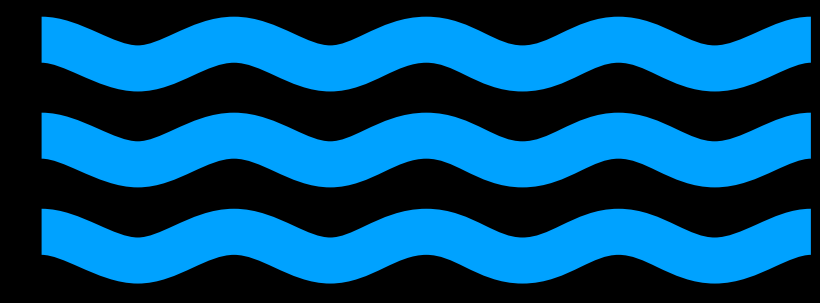
Your business as components



Smiling increases



Data Lake

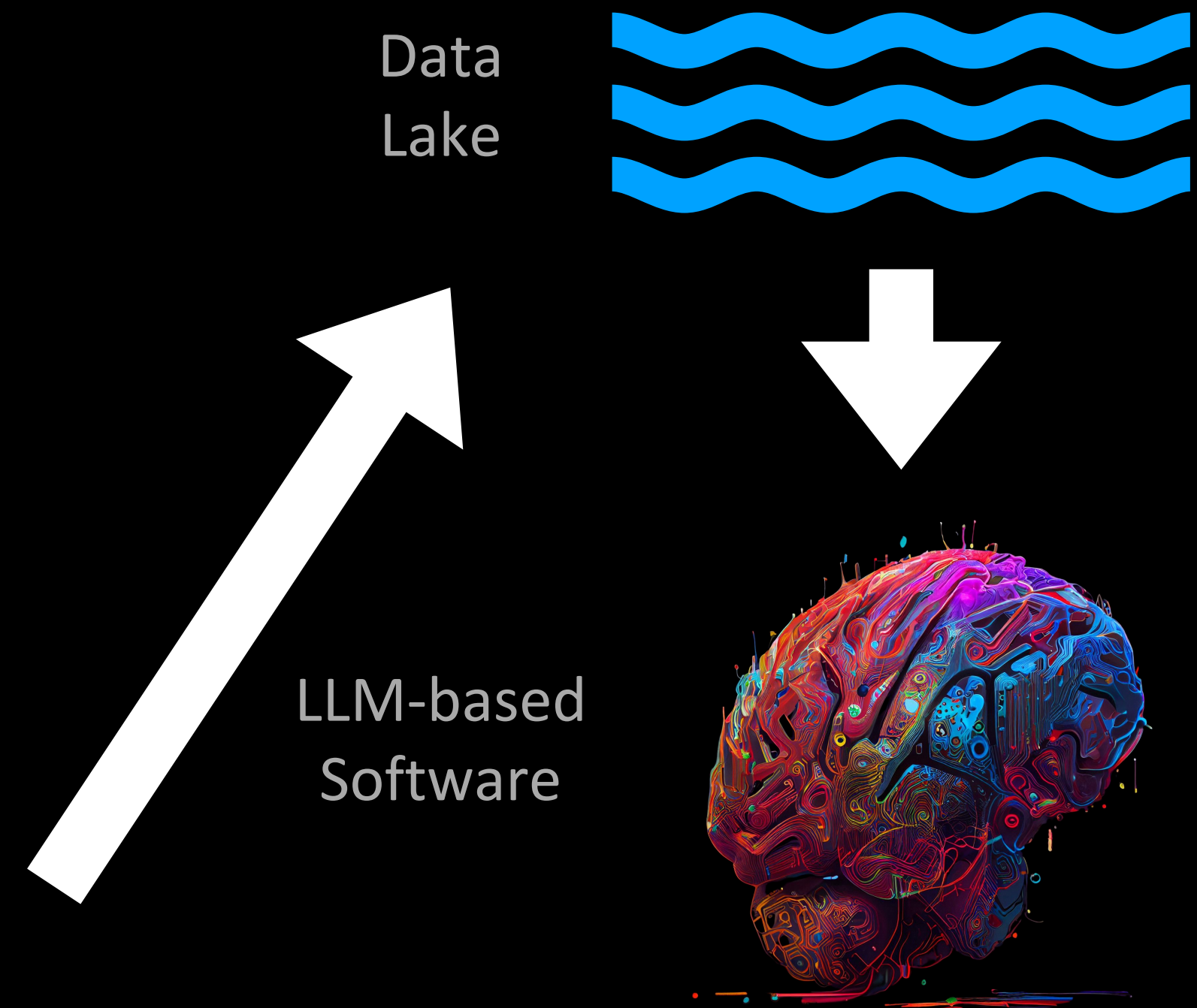
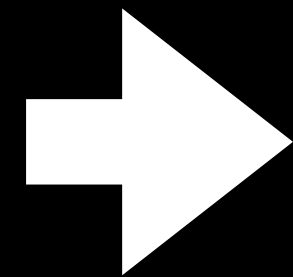


# what's coming for us

Your business as components



Smiling increases



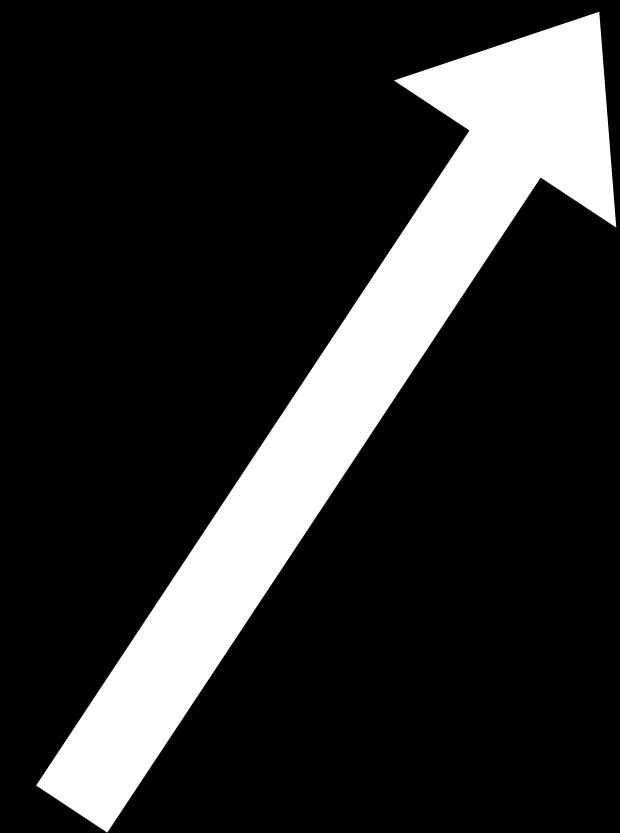
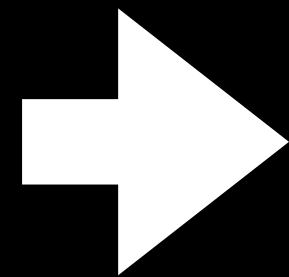


# what's coming for us

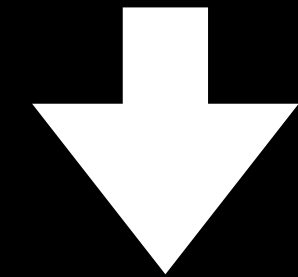
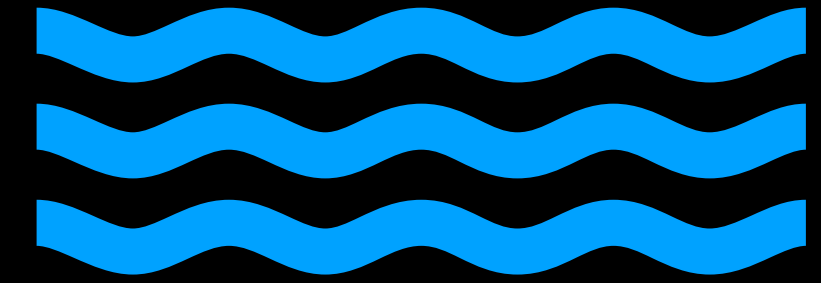
Your business as components



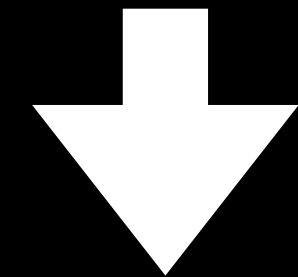
Smiling increases



Data Lake



LLM



Leadership Team





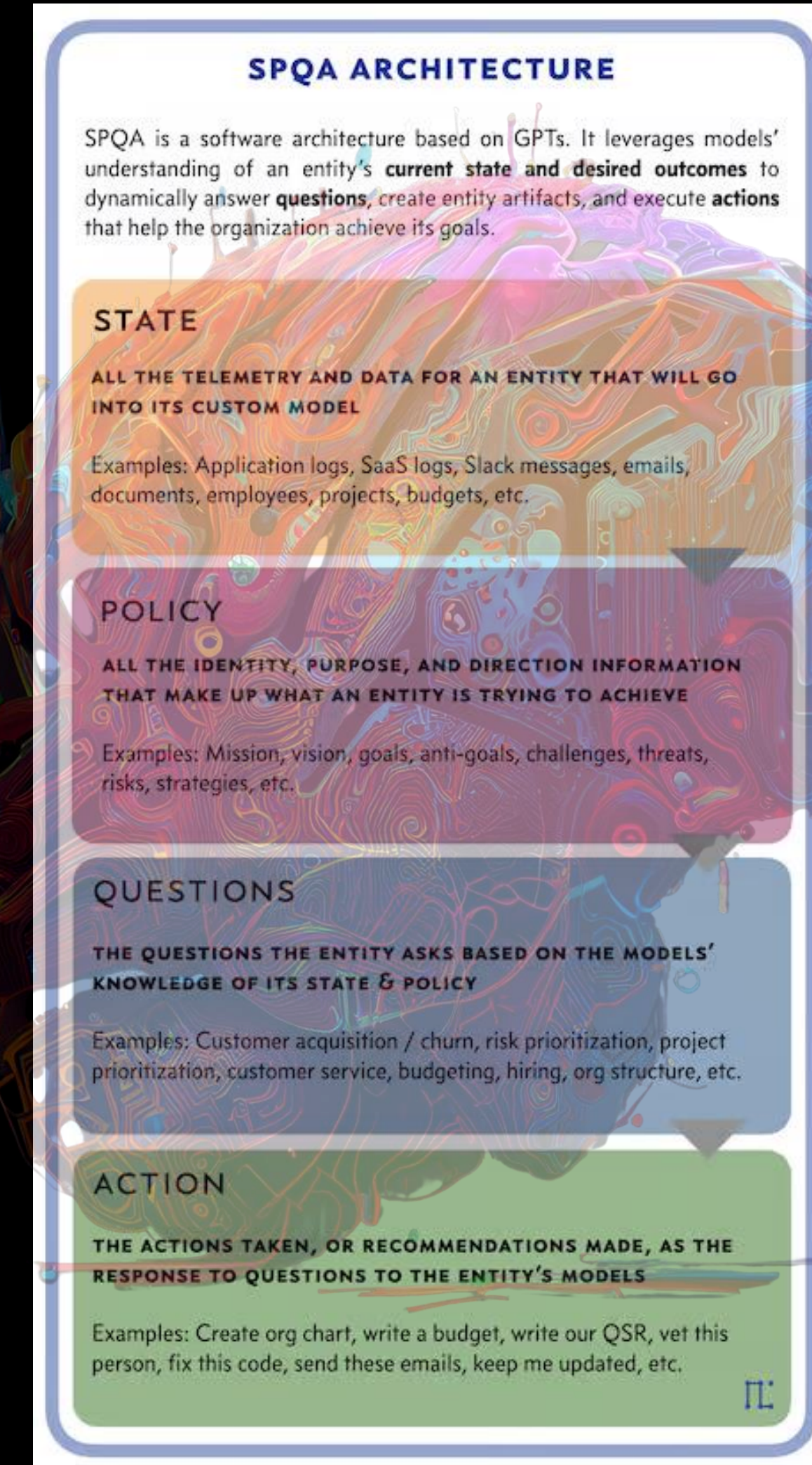
# what to do

Think in SPQA

# 1

Start thinking about programs and businesses in an SPQA context.

Think in terms of **Context + Questions**.





# what to do

Think about your moat

Think about your moat. As a business.  
As a program. As a product.

Do you have **Context + Questions** that others don't? (E.g., Vuln Management)

2

- Remediation
  - How do things get fixed at the company?
  - Who owns all the stuff?
  - What are THEIR specific processes?
  - What's the best way to engage with them?





# what to do

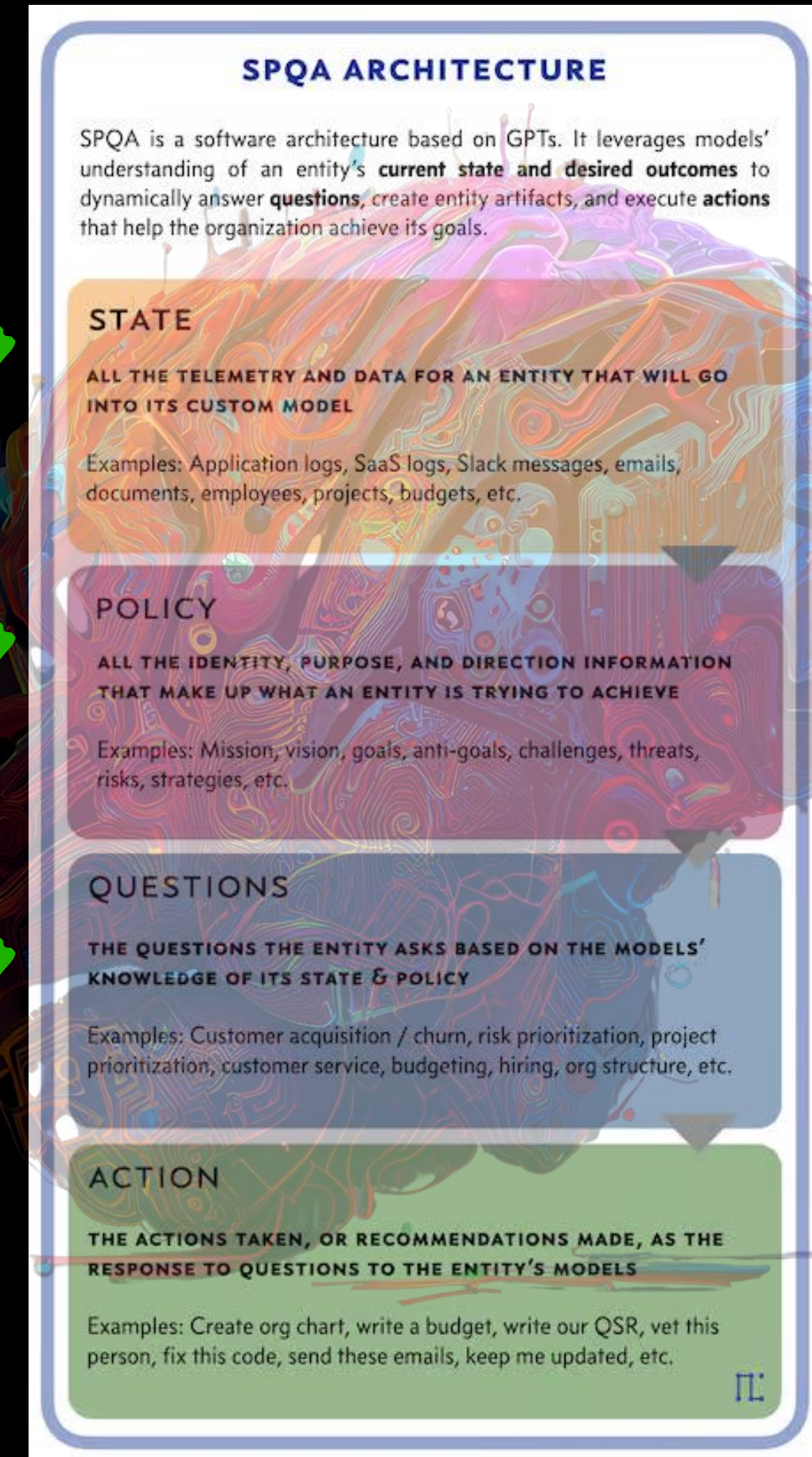
Security program articulation

Can you clearly articulate your entire program?

Could you articulate your program's components and start collecting state?

3

- Goals
- Anti-goals
- Challenges
- Strategies for addressing those challenges
- Projects
- Team members working on those projects
- Your risk register
- Threat scenarios
- Compliance requirements
- What you're spending money on
- How your efforts are moving your KPIs





# what to do

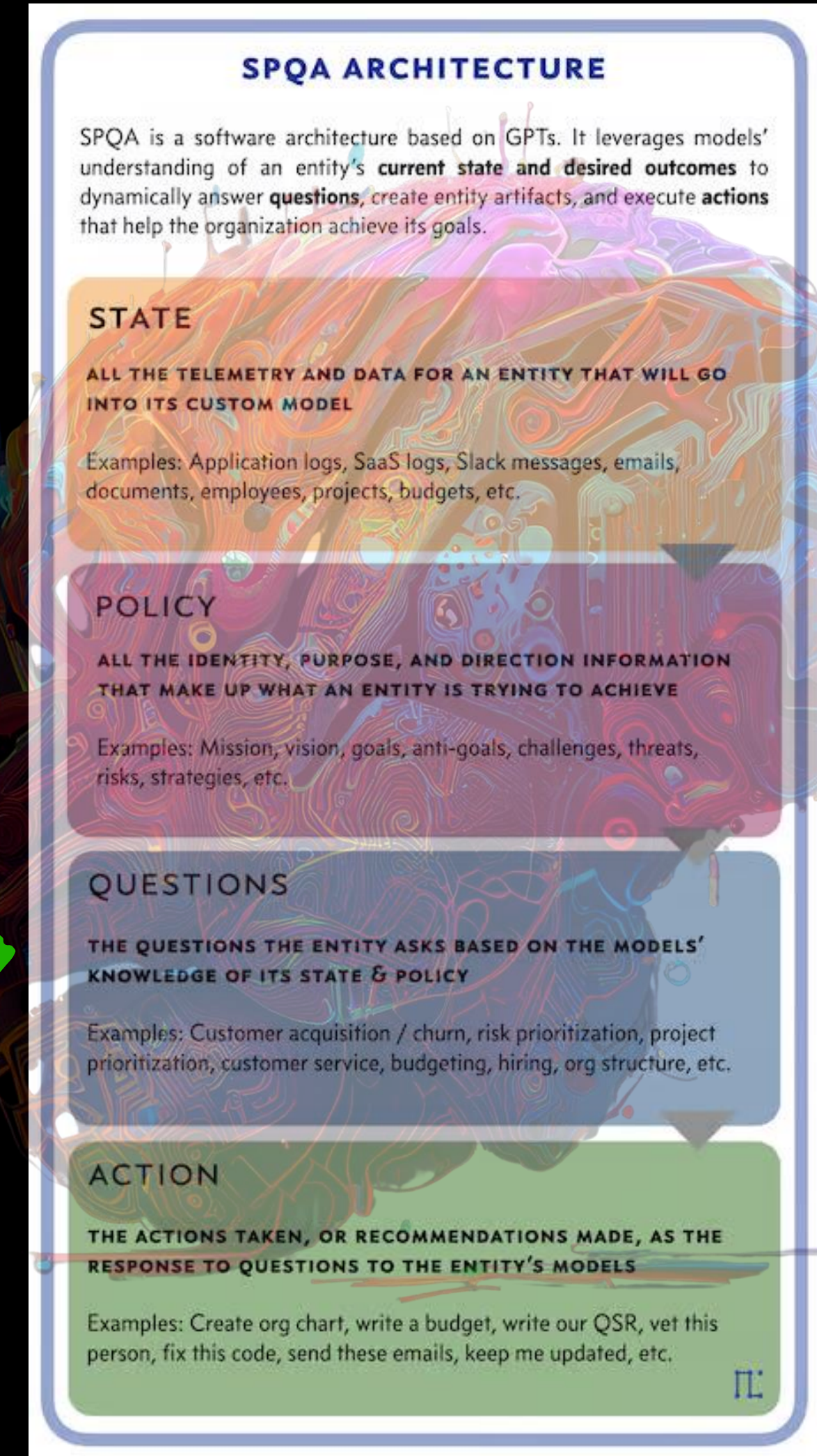
Have the complete narrative

**Have the end-to-end narrative of effort to success.**

**Work on asking the right questions that highlight whether your efforts are making a difference.**

4

- Goals
- Anti-goals
- Challenges
- Strategies for addressing those challenges
- Projects
- Team members working on those projects
- Your risk register
- Threat scenarios
- Compliance requirements
- What you're spending money on
- How your efforts are moving your KPIs





what to do

# Context + Questions







CU INTERSECT  
CONFERENCE

thank you

