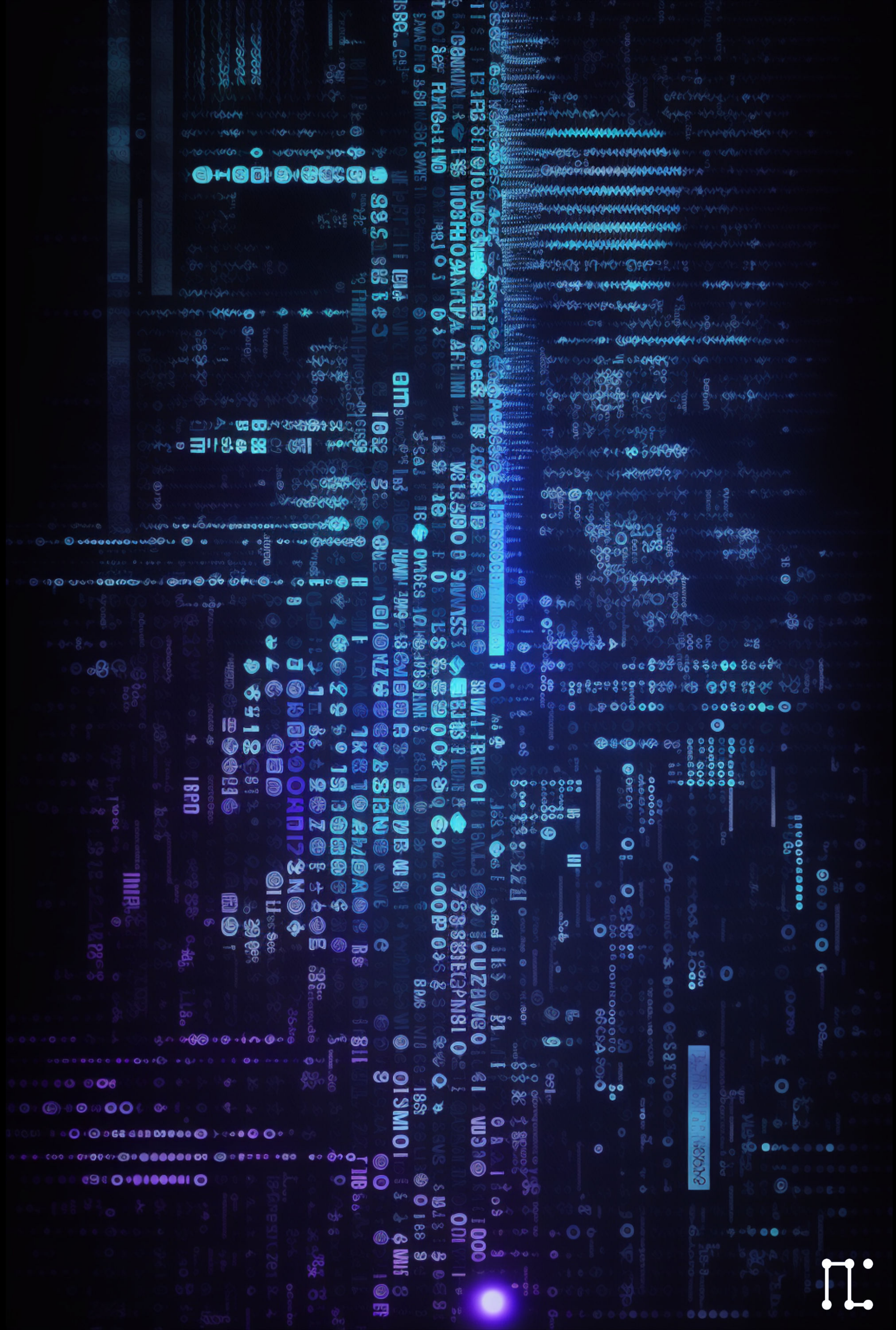
UNSUPERVISED
LEARNING

HOW TO RUN YOUR SECURITY PROGRAM USING AI…

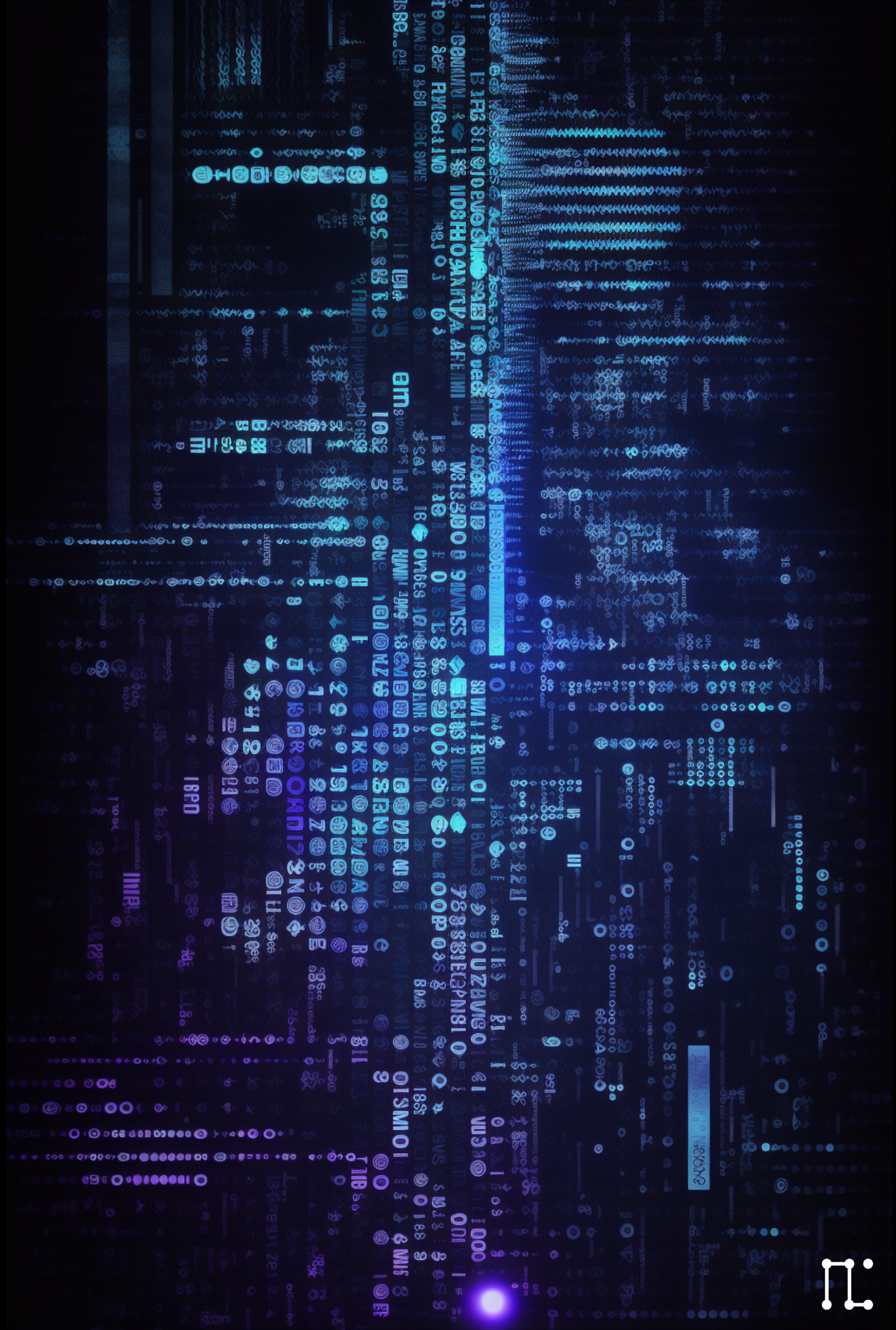
BEFORE SOMEONE ELSE DOES



UNSUPERVISED
LEARNING

HOW TO RUN YOUR SECURITY PROGRAM USING AI...

BEFORE SOMEONE ELSE DOES



AI RISKS I WON'T TALK ABOUT

Data poisoning

Prompt injection

Tricking AI Agents

Superintelligence / paperclips

AI CONSULTANCIES AND PRODUCTS

McKinsey & Company

KPMG

pwc

vs.

Our teams, departments, and companies.

Topics

What I see coming

An early view of the enemy

What we can do to get ready

The problem

THE PROBLEM AI WILL TAKE ADVANTAGE OF: CONFUSION

- Many teams can't describe themselves
- The product
- The story
- They can't articulate a clear mission
- Or goals
- Or KPIs
- Or a clear narrative on progress
- **So every 6-18 months they start over**
- And all this is highly manual and time-consuming (leadership team meetings, planning, etc.)

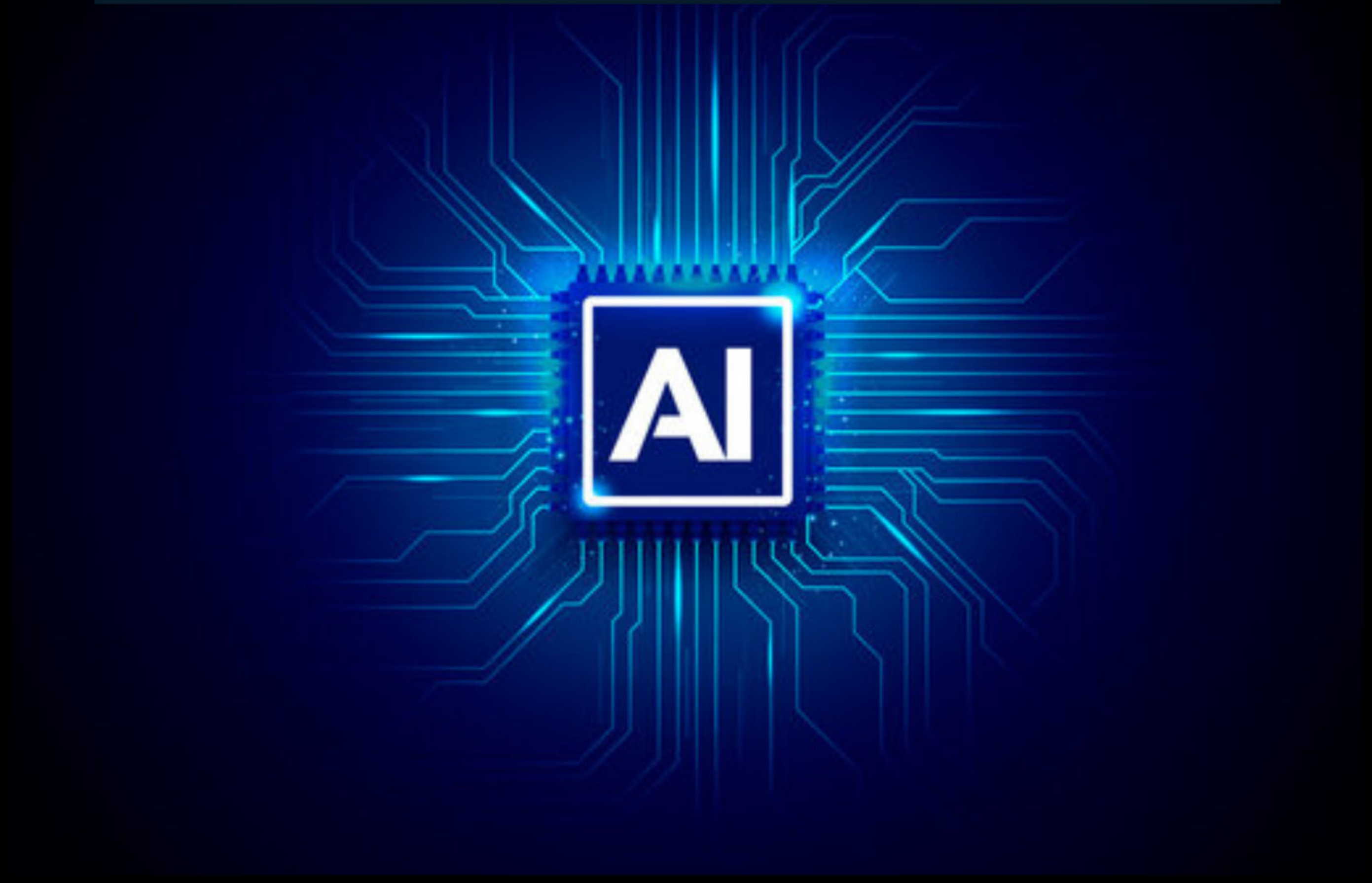
THE DAMAGE CAUSED BY A LACK OF CLARITY

- It’s really hard to justify these teams
- It’s hard to get allies
- It’s hard to retain talent
- It’s hard to sell
- *It’s hard to get budget*
- There’s lots of management turnover
- **The C-team wonders why they’re paying you**

The open door for AI

- AI is going to remove a LOT of this
- It will define a structure of the program and track progress over time
- It will have the answers ready when needed
- It will make it very clear if we're getting value from the spend or not

McKinsey
& Company



40% of McKinsey’s business is already AI.

40%*. In 2024.*

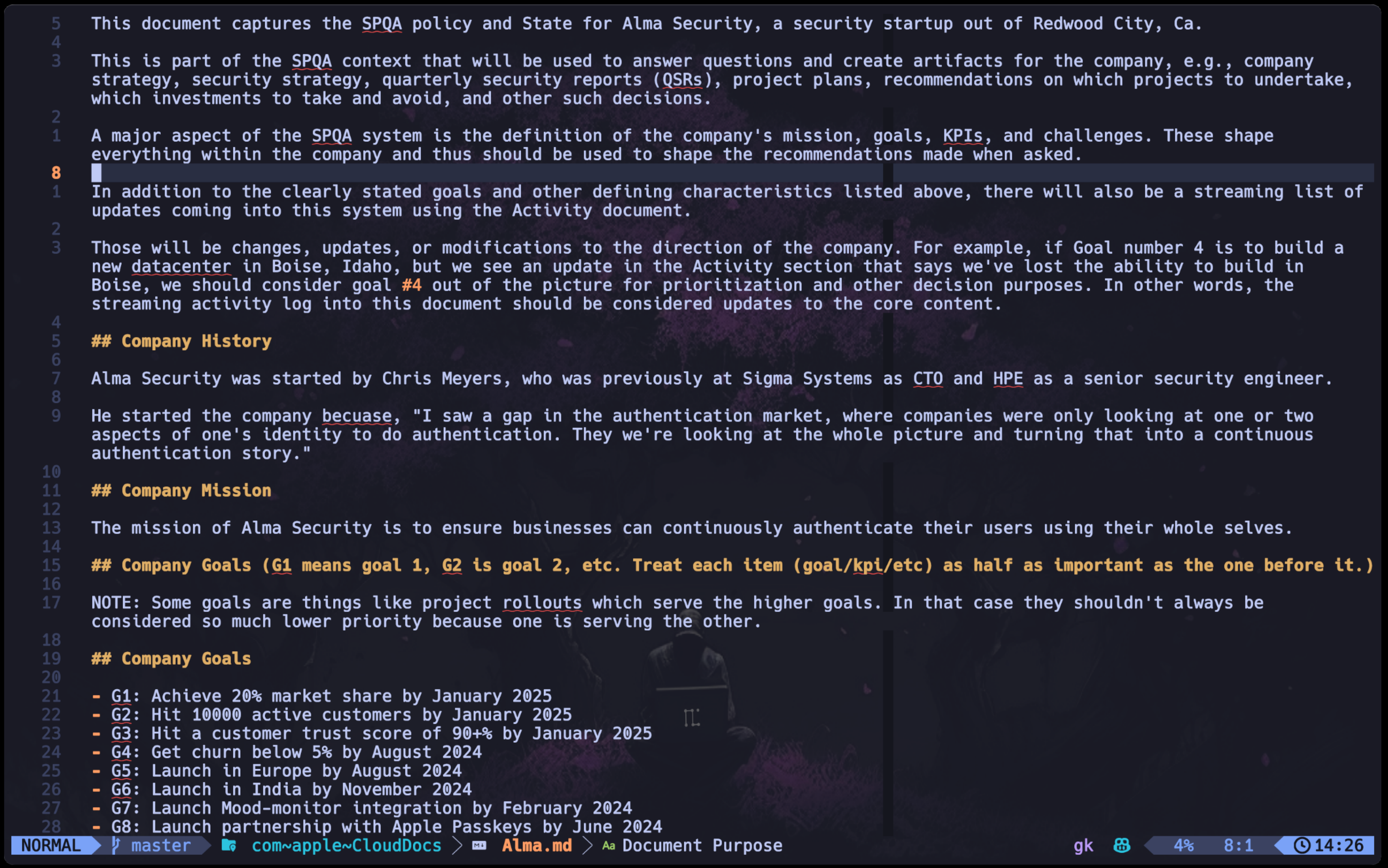
That’s just ***18 months*** after GenAI blew up.

https://www.nytimes.com/2024/06/26/technology/ai-consultants.html

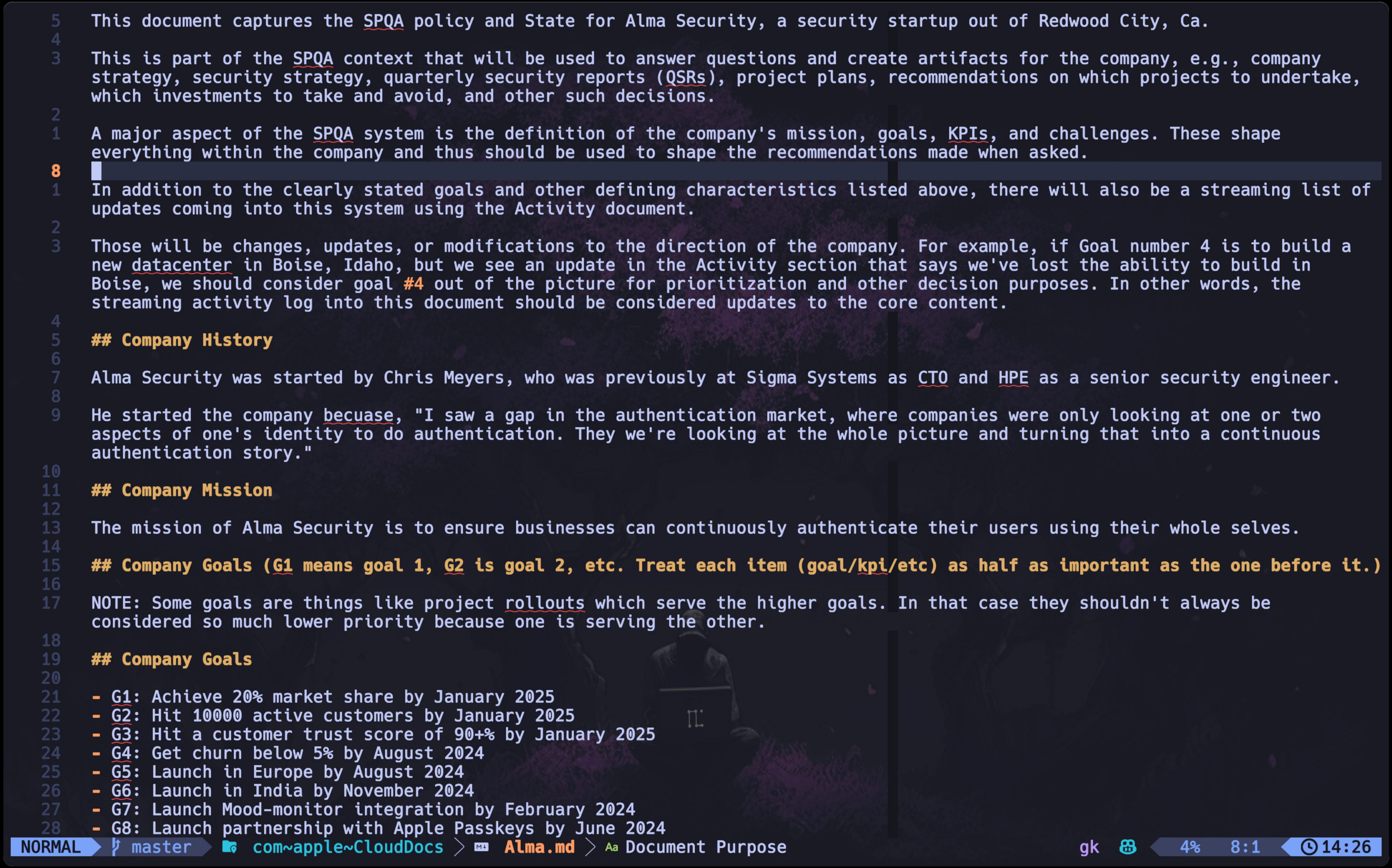
The AI solution to the clarity problem

THE SYSTEM: CONTEXT IS EVERYTHING

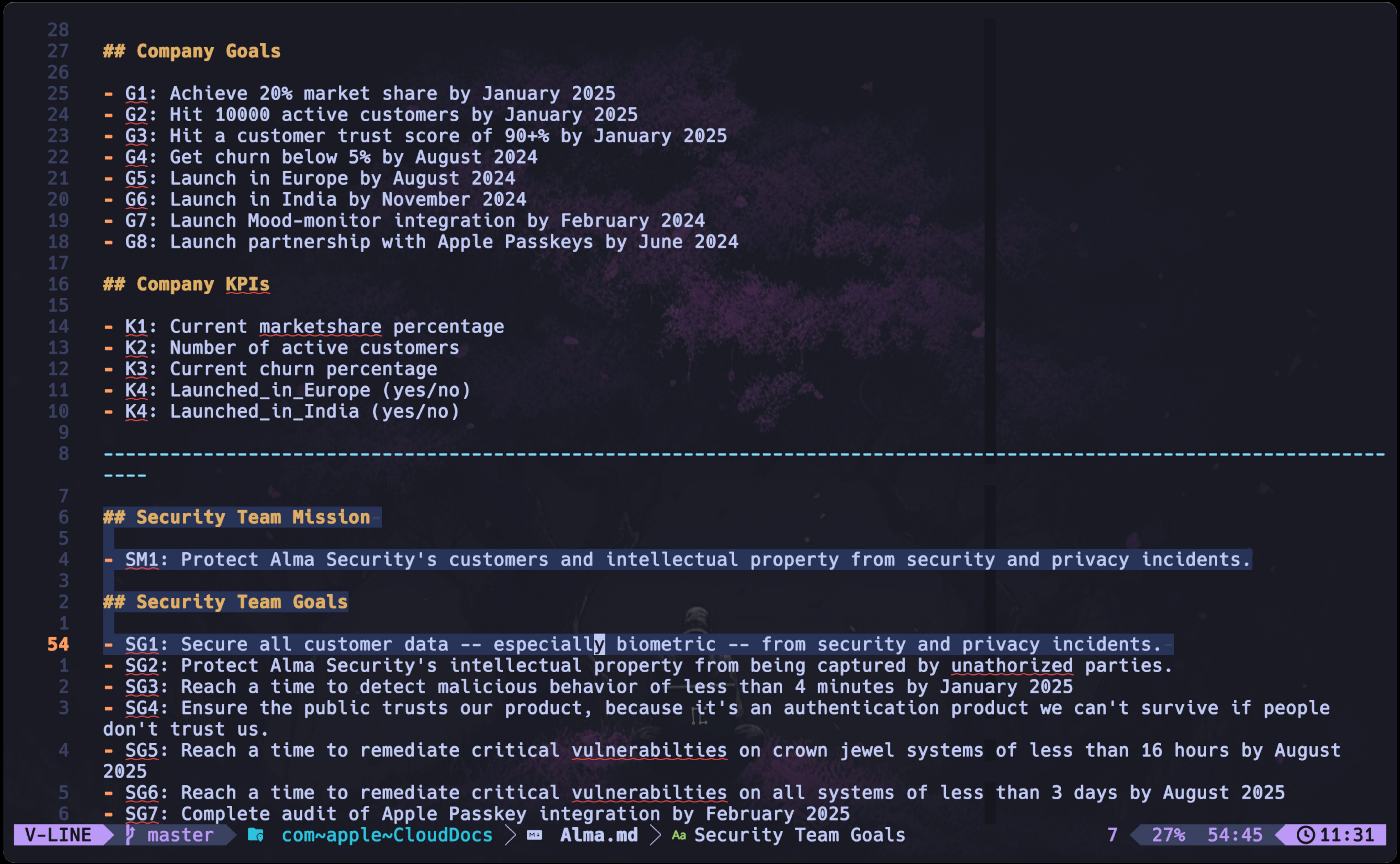
- The system starts with `context`
- This captures tons of information about the program, team, department, company, e.g.:
- Mission
- Goals
- Metrics
- Challenges
- Strategies
- Projects
- Team
- Budget



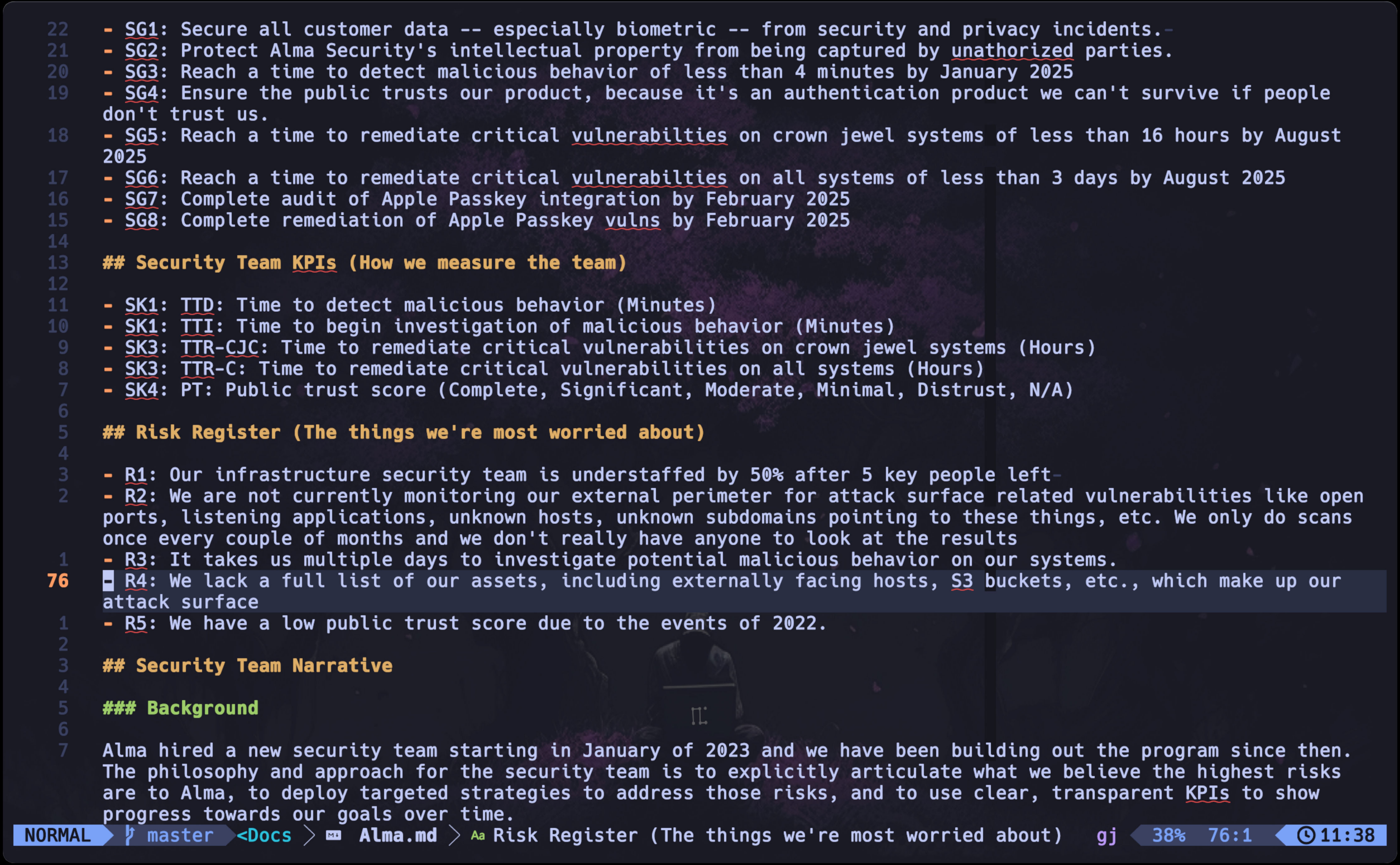
```
This document captures the SPQA policy and State for Alma Security, a security startup out of Redwood City, Ca.

This is part of the SPQA context that will be used to answer questions and create artifacts for the company, e.g., company
strategy, security strategy, quarterly security reports (QSRs), project plans, recommendations on which projects to undertake,
which investments to take and avoid, and other such decisions.

A major aspect of the SPQA system is the definition of the company's mission, goals, KPIs, and challenges. These shape
everything within the company and thus should be used to shape the recommendations made when asked.

In addition to the clearly stated goals and other defining characteristics listed above, there will also be a streaming list of
updates coming into this system using the Activity document.

Those will be changes, updates, or modifications to the direction of the company. For example, if Goal number 4 is to build a
new datacenter in Boise, Idaho, but we see an update in the Activity section that says we've lost the ability to build in
Boise, we should consider goal #4 out of the picture for prioritization and other decision purposes. In other words, the
streaming activity log into this document should be considered updates to the core content.

## Company History

Alma Security was started by Chris Meyers, who was previously at Sigma Systems as CTO and HPE as a senior security engineer.

He started the company becuase, "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."

## Company Mission

The mission of Alma Security is to ensure businesses can continuously authenticate their users using their whole selves.

## Company 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.)

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.

## Company Goals

- G1: Achieve 20% market share by January 2025
- G2: Hit 10000 active customers by January 2025
- G3: Hit a customer trust score of 90+% by January 2025
- G4: Get churn below 5% by August 2024
- G5: Launch in Europe by August 2024
- G6: Launch in India by November 2024
- G7: Launch Mood-monitor integration by February 2024
- G8: Launch partnership with Apple Passkeys by June 2024
NORMAL  master  com~apple~CloudDocs > Alma.md > Document Purpose                    gk  4%  8:1  14:26
```



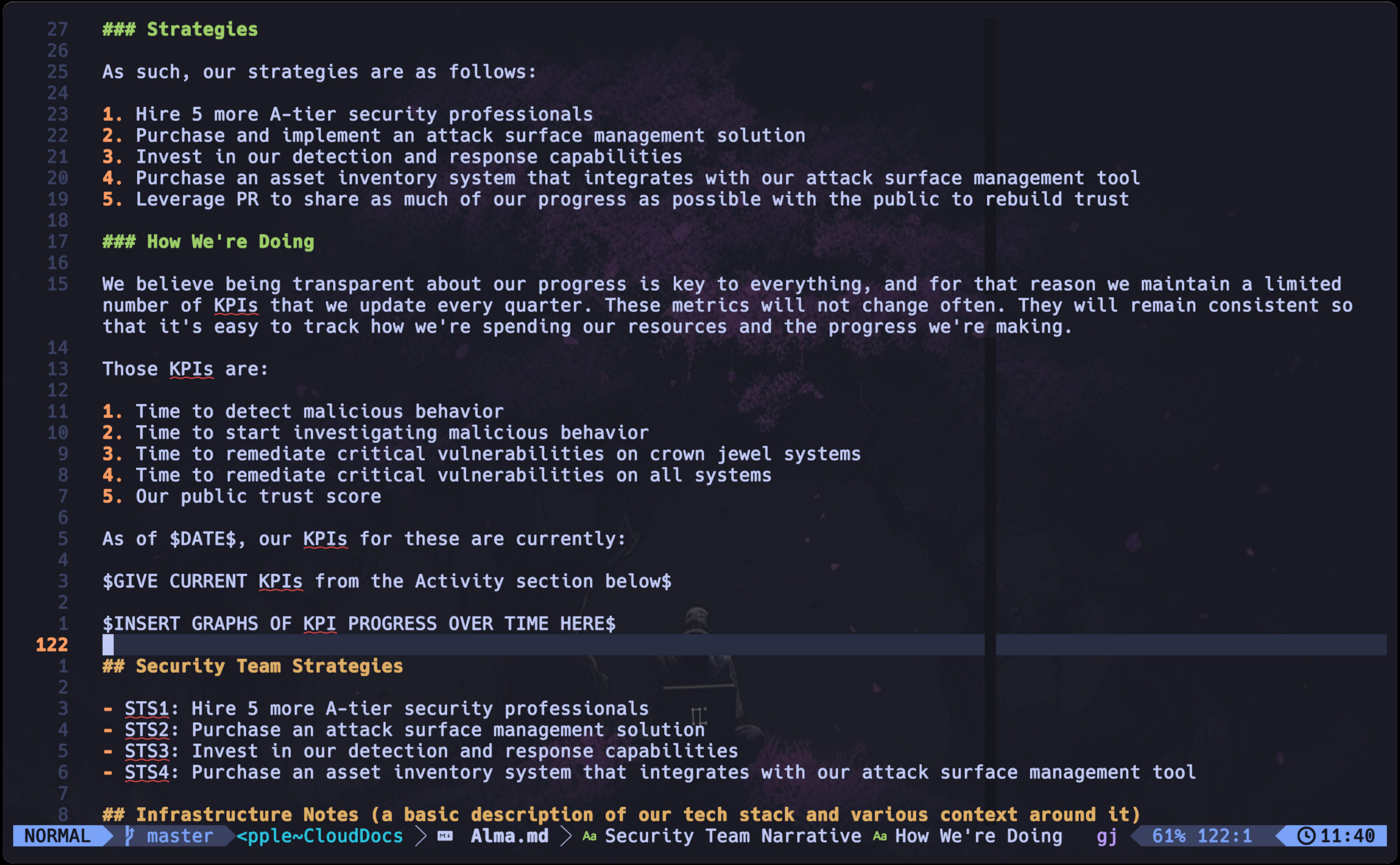
```
This document captures the SPQA policy and State for Alma Security, a security startup out of Redwood City, Ca.

This is part of the SPQA context that will be used to answer questions and create artifacts for the company, e.g., company
strategy, security strategy, quarterly security reports (QSRs), project plans, recommendations on which projects to undertake,
which investments to take and avoid, and other such decisions.

A major aspect of the SPQA system is the definition of the company's mission, goals, KPIs, and challenges. These shape
everything within the company and thus should be used to shape the recommendations made when asked.

In addition to the clearly stated goals and other defining characteristics listed above, there will also be a streaming list of
updates coming into this system using the Activity document.

Those will be changes, updates, or modifications to the direction of the company. For example, if Goal number 4 is to build a
new datacenter in Boise, Idaho, but we see an update in the Activity section that says we've lost the ability to build in
Boise, we should consider goal #4 out of the picture for prioritization and other decision purposes. In other words, the
streaming activity log into this document should be considered updates to the core content.

## Company History

Alma Security was started by Chris Meyers, who was previously at Sigma Systems as CTO and HPE as a senior security engineer.

He started the company becuase, "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."

## Company Mission

The mission of Alma Security is to ensure businesses can continuously authenticate their users using their whole selves.

## Company 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.)

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.

## Company Goals

- G1: Achieve 20% market share by January 2025
- G2: Hit 10000 active customers by January 2025
- G3: Hit a customer trust score of 90+% by January 2025
- G4: Get churn below 5% by August 2024
- G5: Launch in Europe by August 2024
- G6: Launch in India by November 2024
- G7: Launch Mood-monitor integration by February 2024
- G8: Launch partnership with Apple Passkeys by June 2024
NORMAL  master  com~apple~CloudDocs  Alma.md  Document Purpose                    gk    4%  8:1  14:26
```



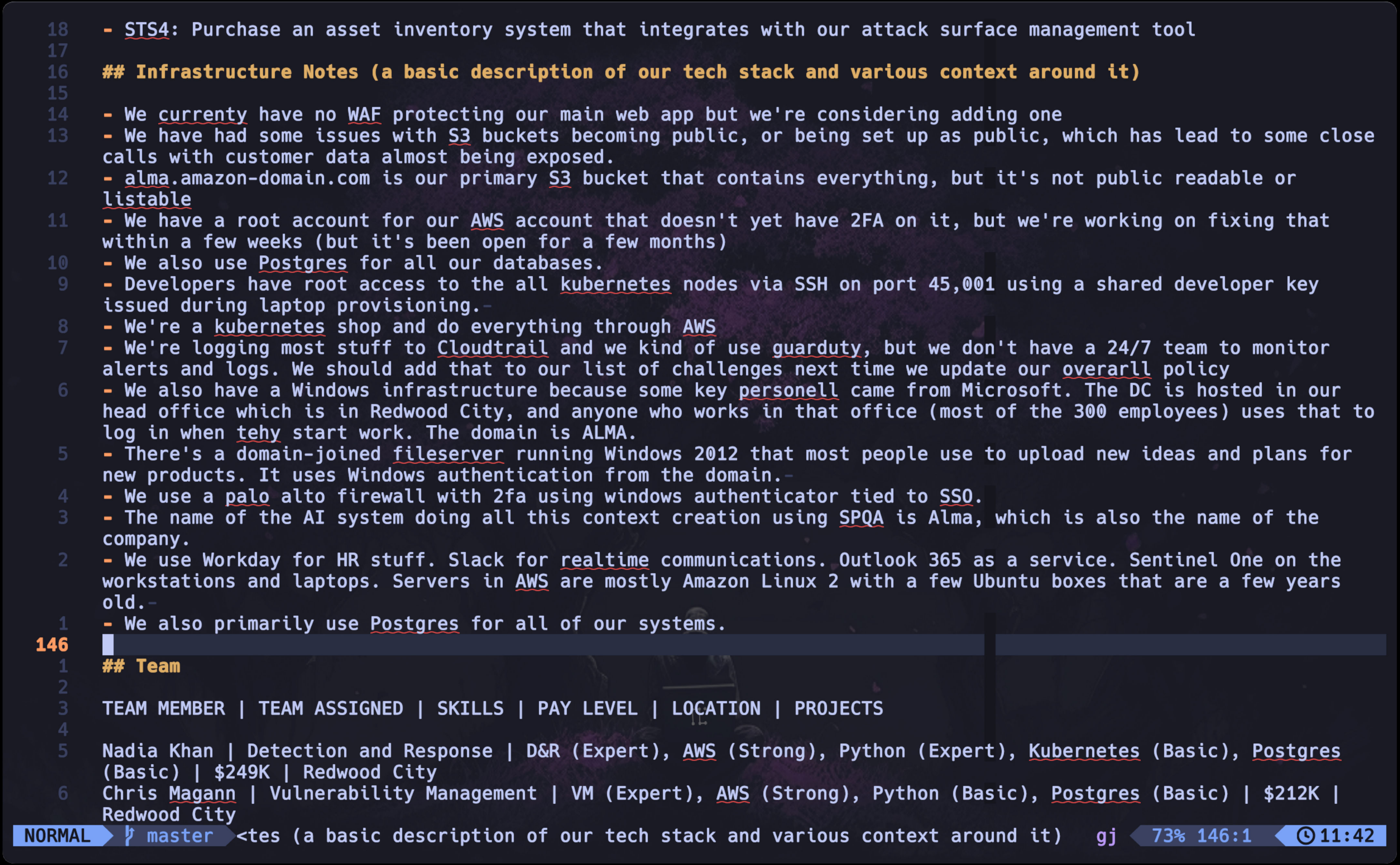
```
## Company Goals

- G1: Achieve 20% market share by January 2025
- G2: Hit 10000 active customers by January 2025
- G3: Hit a customer trust score of 90+% by January 2025
- G4: Get churn below 5% by August 2024
- G5: Launch in Europe by August 2024
- G6: Launch in India by November 2024
- G7: Launch Mood-monitor integration by February 2024
- G8: Launch partnership with Apple Passkeys by June 2024

## Company KPIs

- K1: Current marketshare percentage
- K2: Number of active customers
- K3: Current churn percentage
- K4: Launched_in_Europe (yes/no)
- K4: Launched_in_India (yes/no)

-----------------------------------------------------------------------------------------------------------------------

## Security Team Mission

- SM1: Protect Alma Security's customers and intellectual property from security and privacy incidents.

## Security Team Goals

- SG1: Secure all customer data -- especially biometric -- from security and privacy incidents.
- SG2: Protect Alma Security's intellectual property from being captured by unathorized parties.
- SG3: Reach a time to detect malicious behavior of less than 4 minutes by January 2025
- SG4: Ensure the public trusts our product, because it's an authentication product we can't survive if people don't trust us.
- SG5: Reach a time to remediate critical vulnerabilties on crown jewel systems of less than 16 hours by August 2025
- SG6: Reach a time to remediate critical vulnerabilties on all systems of less than 3 days by August 2025
- SG7: Complete audit of Apple Passkey integration by February 2025
```



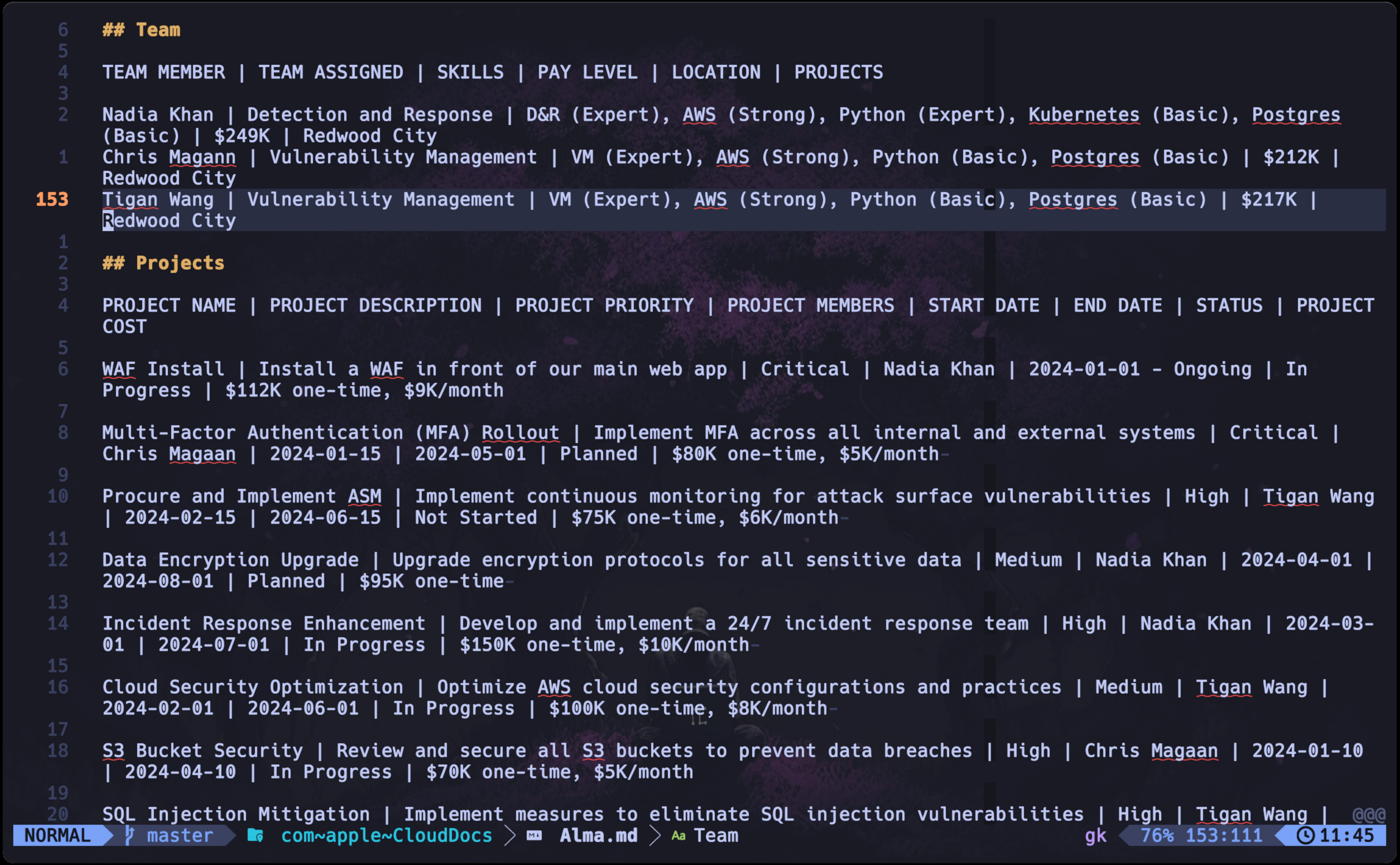
```
- SG1: Secure all customer data -- especially biometric -- from security and privacy incidents.
- SG2: Protect Alma Security's intellectual property from being captured by unathorized parties.
- SG3: Reach a time to detect malicious behavior of less than 4 minutes by January 2025
- SG4: Ensure the public trusts our product, because it's an authentication product we can't survive if people don't trust us.
- SG5: Reach a time to remediate critical vulnerabilties on crown jewel systems of less than 16 hours by August 2025
- SG6: Reach a time to remediate critical vulnerabilties on all systems of less than 3 days by August 2025
- SG7: Complete audit of Apple Passkey integration by February 2025
- SG8: Complete remediation of Apple Passkey vulns by February 2025

## Security Team KPIs (How we measure the team)

- SK1: TTD: Time to detect malicious behavior (Minutes)
- SK1: TTI: Time to begin investigation of malicious behavior (Minutes)
- SK3: TTR-CJC: Time to remediate critical vulnerabilities on crown jewel systems (Hours)
- SK3: TTR-C: Time to remediate critical vulnerabilities on all systems (Hours)
- SK4: PT: Public trust score (Complete, Significant, Moderate, Minimal, Distrust, N/A)

## Risk Register (The things we're most worried about)

- R1: Our infrastructure security team is understaffed by 50% after 5 key people left
- R2: We are not currently monitoring our external perimeter for attack surface related vulnerabilities like open ports, listening applications, unknown hosts, unknown subdomains pointing to these things, etc. We only do scans once every couple of months and we don't really have anyone to look at the results
- R3: It takes us multiple days to investigate potential malicious behavior on our systems.
- R4: We lack a full list of our assets, including externally facing hosts, S3 buckets, etc., which make up our attack surface
- R5: We have a low public trust score due to the events of 2022.

## Security Team Narrative

### Background

Alma hired a new security team starting in January of 2023 and we have been building out the program since then. The philosophy and approach for the security team is to explicitly articulate what we believe the highest risks are to Alma, to deploy targeted strategies to address those risks, and to use clear, transparent KPIs to show progress towards our goals over time.
NORMAL  master <Docs > Alma.md > Risk Register (The things we're most worried about)  gj  38%  76:1  11:38
```



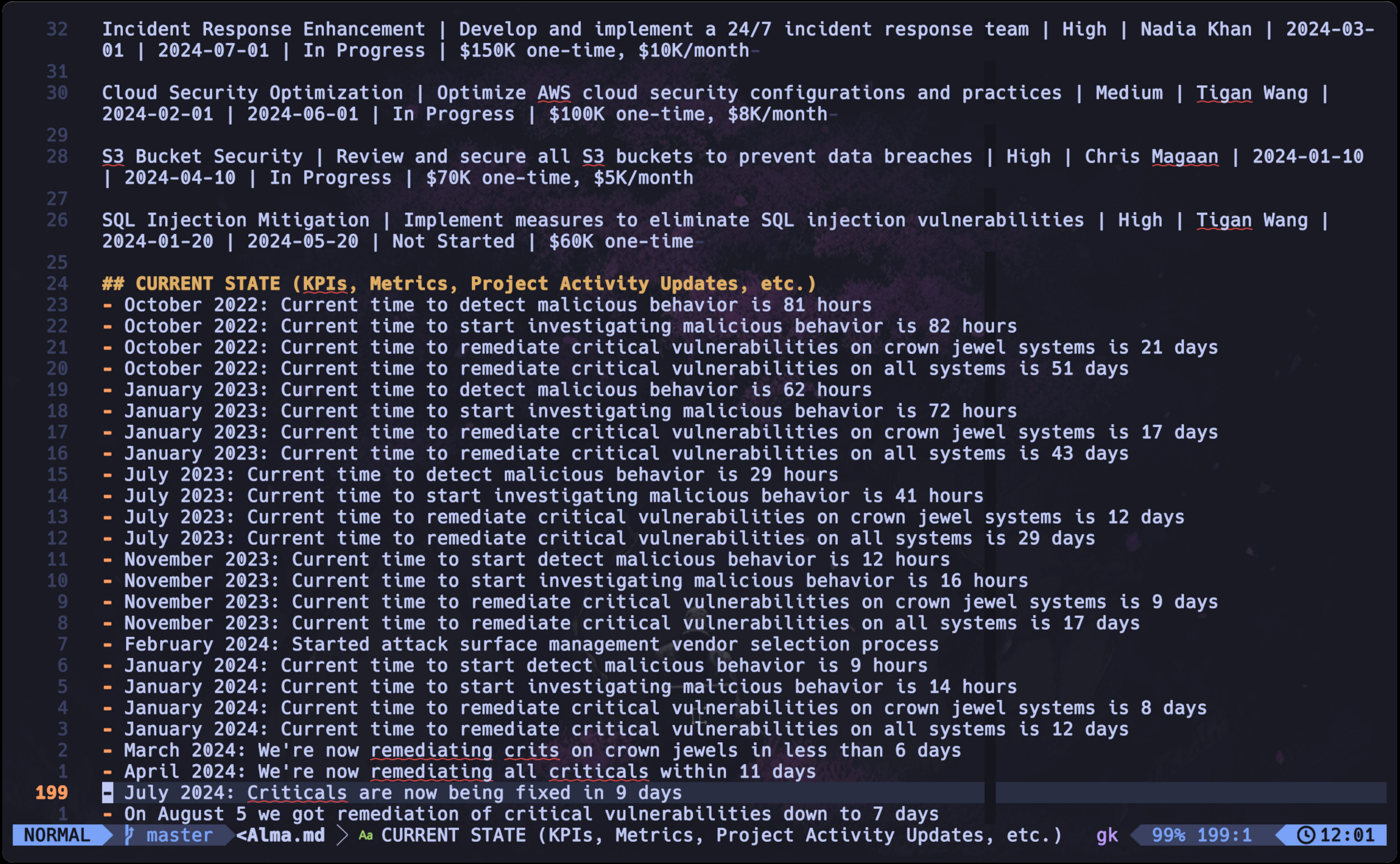
```
### Strategies

As such, our strategies are as follows:

1. Hire 5 more A-tier security professionals
2. Purchase and implement an attack surface management solution
3. Invest in our detection and response capabilities
4. Purchase an asset inventory system that integrates with our attack surface management tool
5. Leverage PR to share as much of our progress as possible with the public to rebuild trust

### How We're Doing

We believe being transparent about our progress is key to everything, and for that reason we maintain a limited
number of KPIs that we update every quarter. These metrics will not change often. They will remain consistent so
that it's easy to track how we're spending our resources and the progress we're making.

Those KPIs are:

1. Time to detect malicious behavior
2. Time to start investigating malicious behavior
3. Time to remediate critical vulnerabilities on crown jewel systems
4. Time to remediate critical vulnerabilities on all systems
5. Our public trust score

As of $DATE$, our KPIs for these are currently:

$GIVE CURRENT KPIs from the Activity section below$

$INSERT GRAPHS OF KPI PROGRESS OVER TIME HERE$

## Security Team Strategies

- STS1: Hire 5 more A-tier security professionals
- STS2: Purchase an attack surface management solution
- STS3: Invest in our detection and response capabilities
- STS4: Purchase an asset inventory system that integrates with our attack surface management tool

## Infrastructure Notes (a basic description of our tech stack and various context around it)
NORMAL  master  <pple~CloudDocs  Alma.md  Security Team Narrative  How We're Doing  gj  61% 122:1  11:40
```



```
- STS4: Purchase an asset inventory system that integrates with our attack surface management tool

## Infrastructure Notes (a basic description of our tech stack and various context around it)

- We currenty have no WAF protecting our main web app but we're considering adding one
- We have had some issues with S3 buckets becoming public, or being set up as public, which has lead to some close calls with customer data almost being exposed.
- alma.amazon-domain.com is our primary S3 bucket that contains everything, but it's not public readable or listable
- We have a root account for our AWS account that doesn't yet have 2FA on it, but we're working on fixing that within a few weeks (but it's been open for a few months)
- We also use Postgres for all our databases.
- Developers have root access to the all kubernetes nodes via SSH on port 45,001 using a shared developer key issued during laptop provisioning.
- We're a kubernetes shop and do everything through AWS
- We're logging most stuff to Cloudtrail and we kind of use guarduty, but we don't have a 24/7 team to monitor alerts and logs. We should add that to our list of challenges next time we update our overarll policy
- We also have a Windows infrastructure because some key personell came from Microsoft. The DC is hosted in our head office which is in Redwood City, and anyone who works in that office (most of the 300 employees) uses that to log in when tehy start work. The domain is ALMA.
- There's a domain-joined fileserver running Windows 2012 that most people use to upload new ideas and plans for new products. It uses Windows authentication from the domain.
- We use a palo alto firewall with 2fa using windows authenticator tied to SSO.
- The name of the AI system doing all this context creation using SPQA is Alma, which is also the name of the company.
- We use Workday for HR stuff. Slack for realtime communications. Outlook 365 as a service. Sentinel One on the workstations and laptops. Servers in AWS are mostly Amazon Linux 2 with a few Ubuntu boxes that are a few years old.
- We also primarily use Postgres for all of our systems.

## Team

TEAM MEMBER | TEAM ASSIGNED | SKILLS | PAY LEVEL | LOCATION | PROJECTS

Nadia Khan | Detection and Response | D&R (Expert), AWS (Strong), Python (Expert), Kubernetes (Basic), Postgres (Basic) | $249K | Redwood City
Chris Magann | Vulnerability Management | VM (Expert), AWS (Strong), Python (Basic), Postgres (Basic) | $212K | Redwood City
 NORMAL  master <tes (a basic description of our tech stack and various context around it)   gj   73% 146:1   11:42
```



```
## Team

TEAM MEMBER | TEAM ASSIGNED | SKILLS | PAY LEVEL | LOCATION | PROJECTS

Nadia Khan | Detection and Response | D&R (Expert), AWS (Strong), Python (Expert), Kubernetes (Basic), Postgres (Basic) | $249K | Redwood City
Chris Magann | Vulnerability Management | VM (Expert), AWS (Strong), Python (Basic), Postgres (Basic) | $212K | Redwood City
Tigan Wang | Vulnerability Management | VM (Expert), AWS (Strong), Python (Basic), Postgres (Basic) | $217K | Redwood City

## Projects

PROJECT NAME | PROJECT DESCRIPTION | PROJECT PRIORITY | PROJECT MEMBERS | START DATE | END DATE | STATUS | PROJECT COST

WAF Install | Install a WAF in front of our main web app | Critical | Nadia Khan | 2024-01-01 - Ongoing | In Progress | $112K one-time, $9K/month

Multi-Factor Authentication (MFA) Rollout | Implement MFA across all internal and external systems | Critical | Chris Magaan | 2024-01-15 | 2024-05-01 | Planned | $80K one-time, $5K/month

Procure and Implement ASM | Implement continuous monitoring for attack surface vulnerabilities | High | Tigan Wang | 2024-02-15 | 2024-06-15 | Not Started | $75K one-time, $6K/month

Data Encryption Upgrade | Upgrade encryption protocols for all sensitive data | Medium | Nadia Khan | 2024-04-01 | 2024-08-01 | Planned | $95K one-time

Incident Response Enhancement | Develop and implement a 24/7 incident response team | High | Nadia Khan | 2024-03-01 | 2024-07-01 | In Progress | $150K one-time, $10K/month

Cloud Security Optimization | Optimize AWS cloud security configurations and practices | Medium | Tigan Wang | 2024-02-01 | 2024-06-01 | In Progress | $100K one-time, $8K/month

S3 Bucket Security | Review and secure all S3 buckets to prevent data breaches | High | Chris Magaan | 2024-01-10 | 2024-04-10 | In Progress | $70K one-time, $5K/month

SQL Injection Mitigation | Implement measures to eliminate SQL injection vulnerabilities | High | Tigan Wang | @@@
```

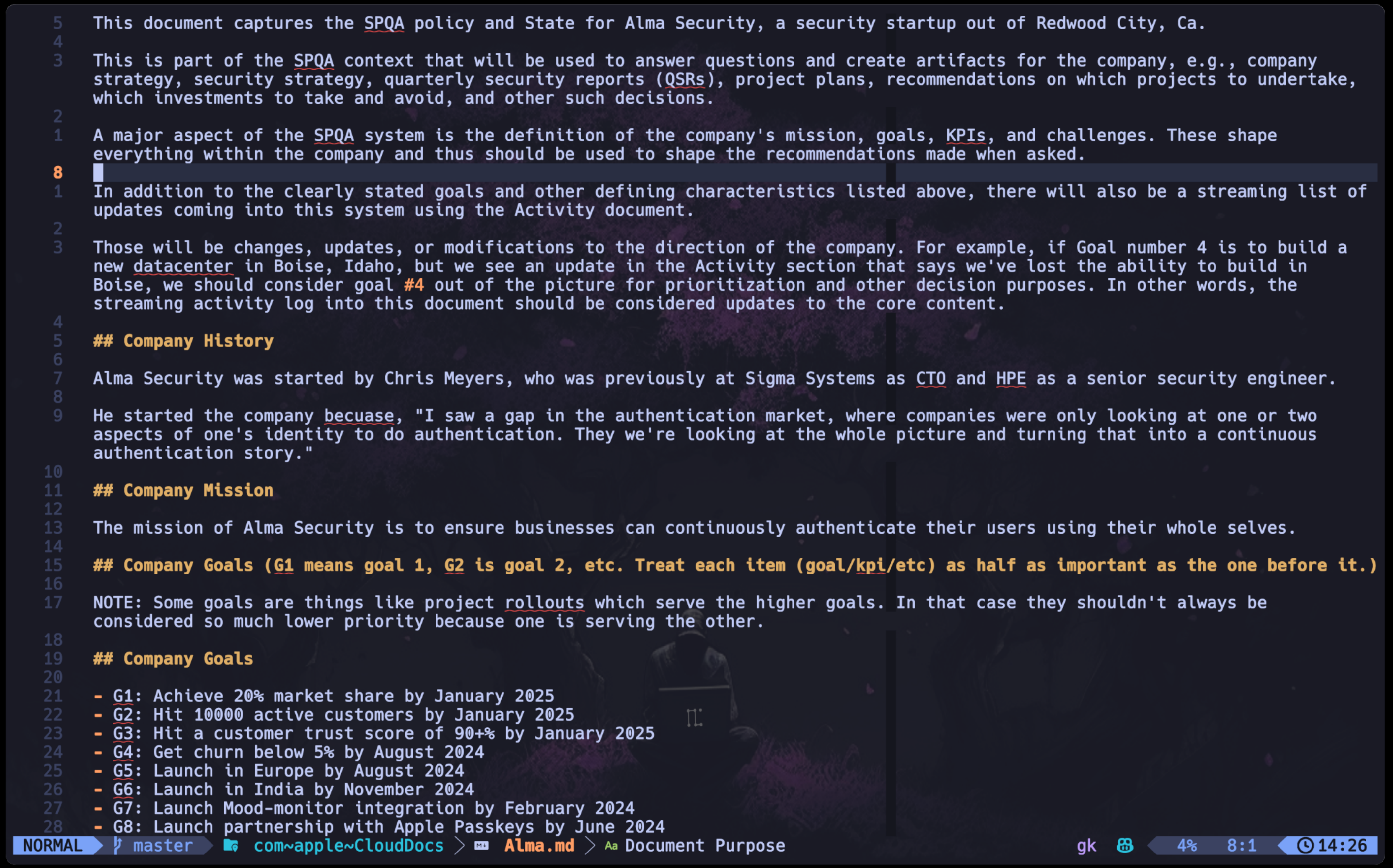


```
Incident Response Enhancement | Develop and implement a 24/7 incident response team | High | Nadia Khan | 2024-03-01 | 2024-07-01 | In Progress | $150K one-time, $10K/month

Cloud Security Optimization | Optimize AWS cloud security configurations and practices | Medium | Tigan Wang | 2024-02-01 | 2024-06-01 | In Progress | $100K one-time, $8K/month

S3 Bucket Security | Review and secure all S3 buckets to prevent data breaches | High | Chris Magaan | 2024-01-10 | 2024-04-10 | In Progress | $70K one-time, $5K/month

SQL Injection Mitigation | Implement measures to eliminate SQL injection vulnerabilities | High | Tigan Wang | 2024-01-20 | 2024-05-20 | Not Started | $60K one-time

## CURRENT STATE (KPIs, Metrics, Project Activity Updates, etc.)
- October 2022: Current time to detect malicious behavior is 81 hours
- October 2022: Current time to start investigating malicious behavior is 82 hours
- October 2022: Current time to remediate critical vulnerabilities on crown jewel systems is 21 days
- October 2022: Current time to remediate critical vulnerabilities on all systems is 51 days
- January 2023: Current time to detect malicious behavior is 62 hours
- January 2023: Current time to start investigating malicious behavior is 72 hours
- January 2023: Current time to remediate critical vulnerabilities on crown jewel systems is 17 days
- January 2023: Current time to remediate critical vulnerabilities on all systems is 43 days
- July 2023: Current time to detect malicious behavior is 29 hours
- July 2023: Current time to start investigating malicious behavior is 41 hours
- July 2023: Current time to remediate critical vulnerabilities on crown jewel systems is 12 days
- July 2023: Current time to remediate critical vulnerabilities on all systems is 29 days
- November 2023: Current time to start detect malicious behavior is 12 hours
- November 2023: Current time to start investigating malicious behavior is 16 hours
- November 2023: Current time to remediate critical vulnerabilities on crown jewel systems is 9 days
- November 2023: Current time to remediate critical vulnerabilities on all systems is 17 days
- February 2024: Started attack surface management vendor selection process
- January 2024: Current time to start detect malicious behavior is 9 hours
- January 2024: Current time to start investigating malicious behavior is 14 hours
- January 2024: Current time to remediate critical vulnerabilities on crown jewel systems is 8 days
- January 2024: Current time to remediate critical vulnerabilities on all systems is 12 days
- March 2024: We're now remediating crits on crown jewels in less than 6 days
- April 2024: We're now remediating all criticals within 11 days
- July 2024: Criticals are now being fixed in 9 days
- On August 5 we got remediation of critical vulnerabilities down to 7 days
```

NORMAL
master
<Alma.md
Aa CURRENT STATE (KPIs, Metrics, Project Activity Updates, etc.)
gk
99% 199:1
12:01

THE SYSTEM: EVERYTHING IN ONE PLACE FOR THE AI

- Company history
- Company mission/goals
- Security program mission/goals
- Program top problems to solve
- Program strategies
- The team
- The projects
- The budget
- Etc.



```
This document captures the SPQA policy and State for Alma Security, a security startup out of Redwood City, Ca.

This is part of the SPQA context that will be used to answer questions and create artifacts for the company, e.g., company
strategy, security strategy, quarterly security reports (QSRs), project plans, recommendations on which projects to undertake,
which investments to take and avoid, and other such decisions.

A major aspect of the SPQA system is the definition of the company's mission, goals, KPIs, and challenges. These shape
everything within the company and thus should be used to shape the recommendations made when asked.

In addition to the clearly stated goals and other defining characteristics listed above, there will also be a streaming list of
updates coming into this system using the Activity document.

Those will be changes, updates, or modifications to the direction of the company. For example, if Goal number 4 is to build a
new datacenter in Boise, Idaho, but we see an update in the Activity section that says we've lost the ability to build in
Boise, we should consider goal #4 out of the picture for prioritization and other decision purposes. In other words, the
streaming activity log into this document should be considered updates to the core content.

## Company History

Alma Security was started by Chris Meyers, who was previously at Sigma Systems as CTO and HPE as a senior security engineer.

He started the company becuase, "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."

## Company Mission

The mission of Alma Security is to ensure businesses can continuously authenticate their users using their whole selves.

## Company 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.)

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.

## Company Goals

- G1: Achieve 20% market share by January 2025
- G2: Hit 10000 active customers by January 2025
- G3: Hit a customer trust score of 90+% by January 2025
- G4: Get churn below 5% by August 2024
- G5: Launch in Europe by August 2024
- G6: Launch in India by November 2024
- G7: Launch Mood-monitor integration by February 2024
- G8: Launch partnership with Apple Passkeys by June 2024
```

PROGRAM MANAGEMENT = A LOT OF ANSWERING QUESTIONS

- What is your security program vision?
- What are the problems you're solving?
- What are your strategies for solving them?
- What projects is the team working on?
- Why?
- How do you measure success?
- Why did you pick those metrics?
- What are we doing to raise them?
- Are they improving?
- By how much?
- How quickly?

PROGRAM MANAGEMENT = A LOT OF ANSWERING QUESTIONS

- What is the plan?
- How is it going?
- What's next?

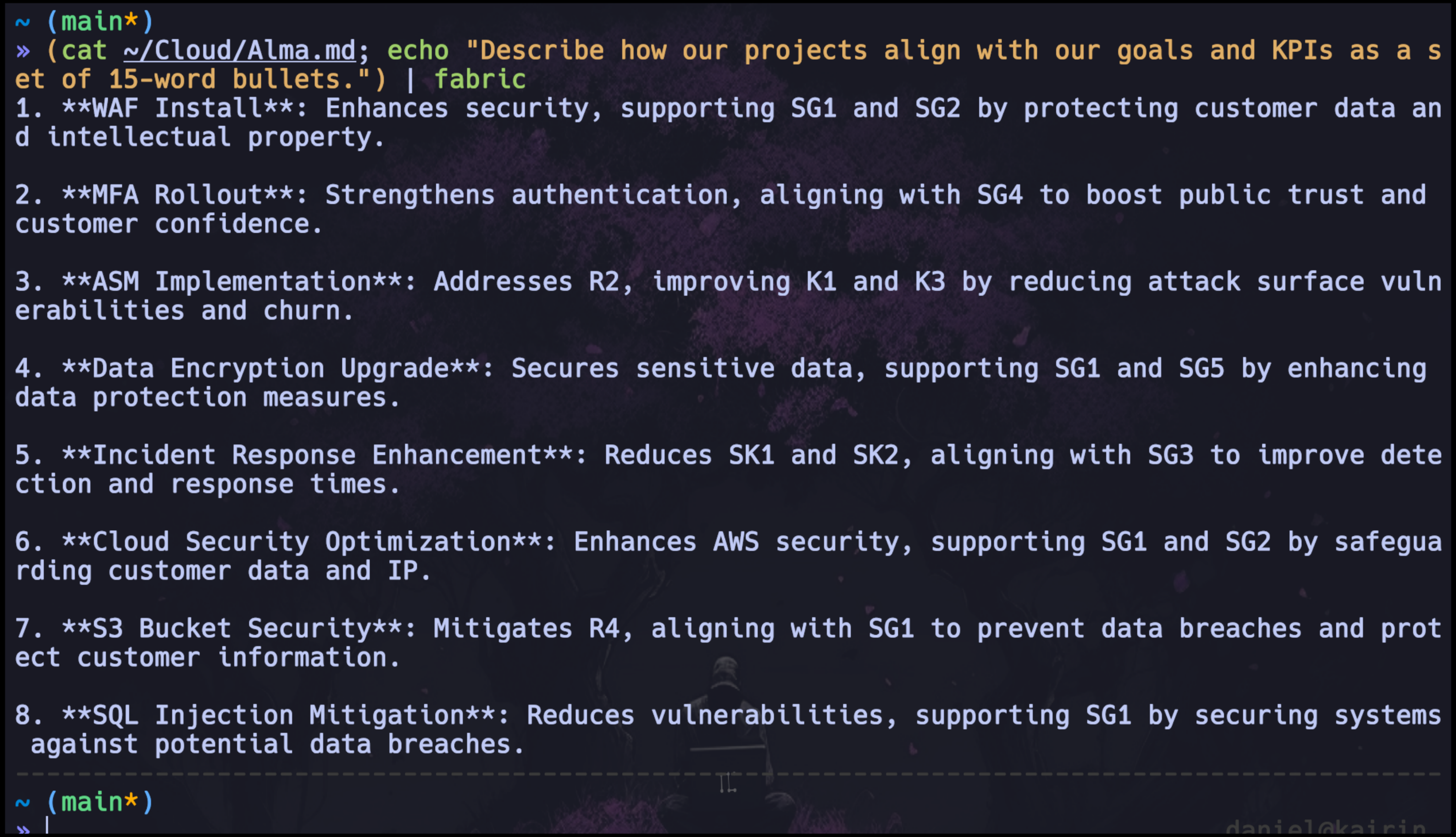
↓

- Are you competent?
- Can you explain your approach?
- Can I trust you to make this happen?

Answering questions using our context

PROGRAM QUESTIONS: PROJECTS

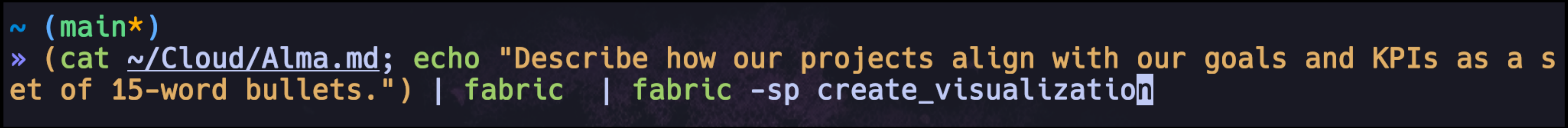
“What projects are we working on?”



```
~ (main*)
» (cat ~/Cloud/Alma.md; echo "Describe how our projects align with our goals and KPIs as a s
et of 15-word bullets.") | fabric
1. **WAF Install**: Enhances security, supporting SG1 and SG2 by protecting customer data an
d intellectual property.

2. **MFA Rollout**: Strengthens authentication, aligning with SG4 to boost public trust and
customer confidence.

3. **ASM Implementation**: Addresses R2, improving K1 and K3 by reducing attack surface vuln
erabilities and churn.

4. **Data Encryption Upgrade**: Secures sensitive data, supporting SG1 and SG5 by enhancing
data protection measures.

5. **Incident Response Enhancement**: Reduces SK1 and SK2, aligning with SG3 to improve dete
ction and response times.

6. **Cloud Security Optimization**: Enhances AWS security, supporting SG1 and SG2 by safegua
rding customer data and IP.

7. **S3 Bucket Security**: Mitigates R4, aligning with SG1 to prevent data breaches and prot
ect customer information.

8. **SQL Injection Mitigation**: Reduces vulnerabilities, supporting SG1 by securing systems
 against potential data breaches.
-------------------------------------------------------------------------------------------
~ (main*)
» |                                                                           daniel@kairin
```

PROGRAM QUESTIONS: PROJECTS —> GOALS & KPIs

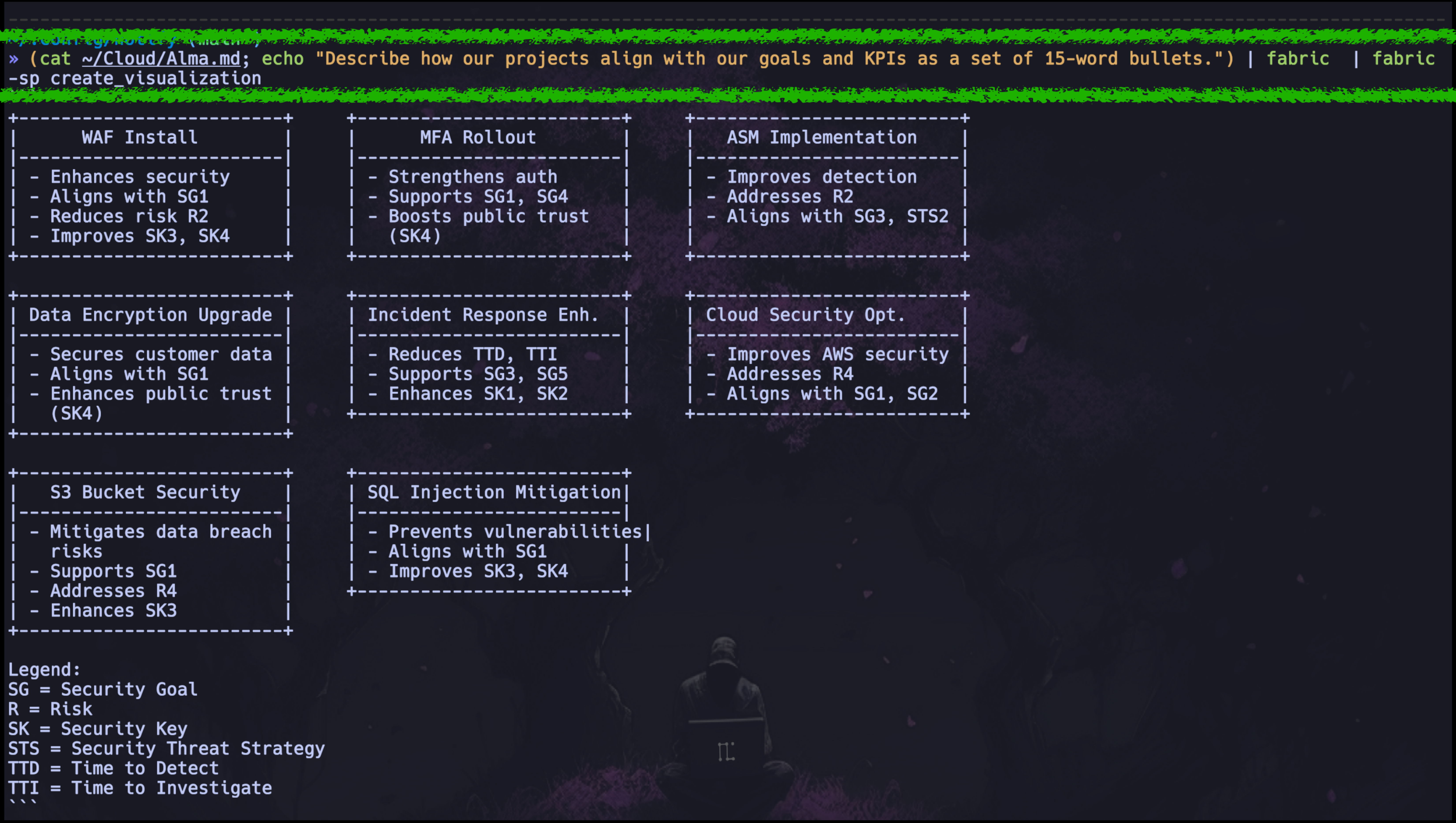
“Show the projects we’re working on and how they map to our metrics.”



```
~ (main*)
» (cat ~/Cloud/Alma.md; echo "Describe how our projects align with our goals and KPIs as a s
et of 15-word bullets.") | fabric  | fabric -sp create_visualization
```

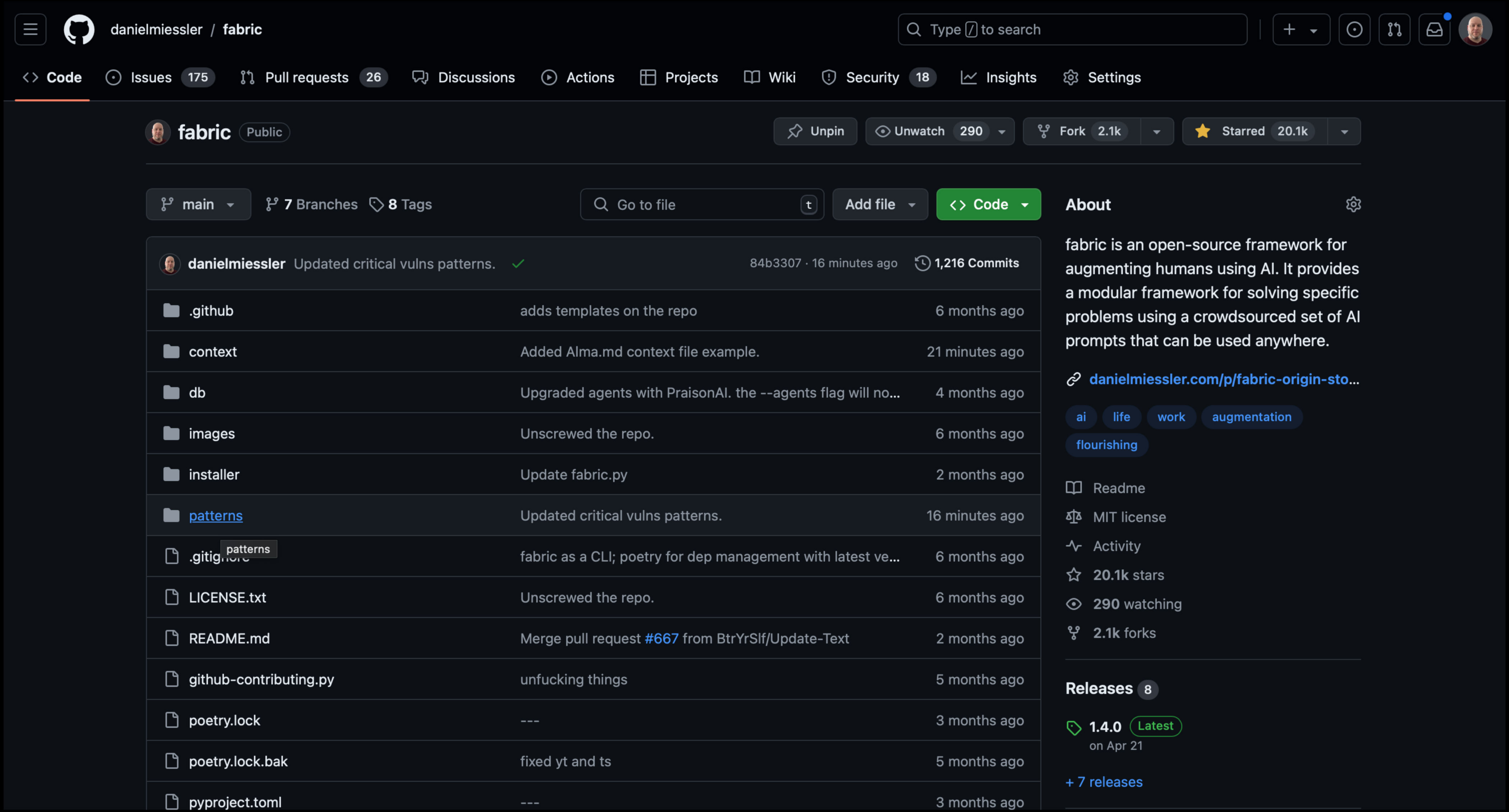
PROGRAM QUESTIONS: VISUAL GROUPINGS

“What projects are we working on?”



~~~
» (cat ~/Cloud/Alma.md; echo "Describe how our projects align with our goals and KPIs as a set of 15-word bullets.") | fabric  | fabric
-sp create_visualization

+-------------------------+     +-------------------------+     +-------------------------+
|       WAF Install       |     |       MFA Rollout       |     |   ASM Implementation    |
|-------------------------|     |-------------------------|     |-------------------------|
| - Enhances security     |     | - Strengthens auth      |     | - Improves detection    |
| - Aligns with SG1       |     | - Supports SG1, SG4     |     | - Addresses R2          |
| - Reduces risk R2       |     | - Boosts public trust   |     | - Aligns with SG3, STS2 |
| - Improves SK3, SK4     |     |   (SK4)                 |     |                         |
+-------------------------+     +-------------------------+     +-------------------------+

+-------------------------+     +-------------------------+     +-------------------------+
| Data Encryption Upgrade |     | Incident Response Enh.  |     | Cloud Security Opt.     |
|-------------------------|     |-------------------------|     |-------------------------|
| - Secures customer data |     | - Reduces TTD, TTI      |     | - Improves AWS security |
| - Aligns with SG1       |     | - Supports SG3, SG5     |     | - Addresses R4          |
| - Enhances public trust |     | - Enhances SK1, SK2     |     | - Aligns with SG1, SG2  |
|   (SK4)                 |     +-------------------------+     +-------------------------+
+-------------------------+

+-------------------------+     +-------------------------+
|    S3 Bucket Security   |     | SQL Injection Mitigation|
|-------------------------|     |-------------------------|
| - Mitigates data breach |     | - Prevents vulnerabilities|
|   risks                 |     | - Aligns with SG1       |
| - Supports SG1          |     | - Improves SK3, SK4     |
| - Addresses R4          |     +-------------------------+
| - Enhances SK3          |
+-------------------------+

Legend:
SG = Security Goal
R = Risk
SK = Security Key
STS = Security Threat Strategy
TTD = Time to Detect
TTI = Time to Investigate
```
~~~

QUICK DIVERSION: fabric



danielmiessler Updated critical vulns patterns. ✓ 84b3307 · 16 minutes ago 1,216 Commits

.github	adds templates on the repo	6 months ago
context	Added Alma.md context file example.	21 minutes ago
db	Upgraded agents with PraisonAI. the --agents flag will no...	4 months ago
images	Unscrewed the repo.	6 months ago
installer	Update fabric.py	2 months ago
patterns	Updated critical vulns patterns.	16 minutes ago
.gitignore	fabric as a CLI; poetry for dep management with latest ve...	6 months ago
LICENSE.txt	Unscrewed the repo.	6 months ago
README.md	Merge pull request #667 from BtrYrSlf/Update-Text	2 months ago
github-contributing.py	unfucking things	5 months ago
poetry.lock	---	3 months ago
poetry.lock.bak	fixed yt and ts	5 months ago
pyproject.toml	---	3 months ago

About

fabric is an open-source framework for augmenting humans using AI. It provides a modular framework for solving specific problems using a crowdsourced set of AI prompts that can be used anywhere.

danielmiessler.com/p/fabric-origin-sto...

ai life work augmentation flourishing

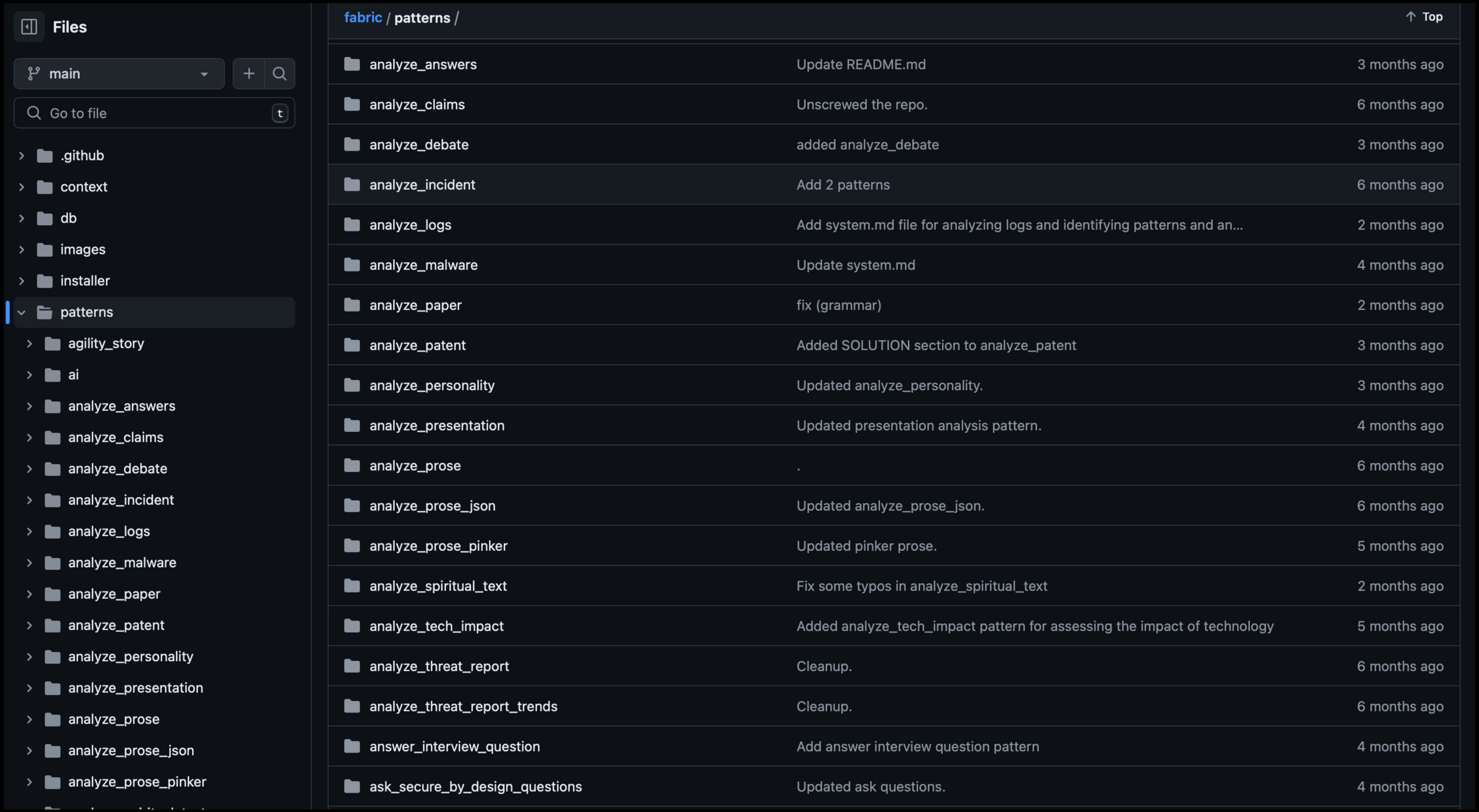
- Readme
- MIT license
- Activity
- 20.1k stars
- 290 watching
- 2.1k forks

Releases 8

1.4.0 Latest
on Apr 21

+ 7 releases

QUICK DIVERSION: FABRIC PATTERNS

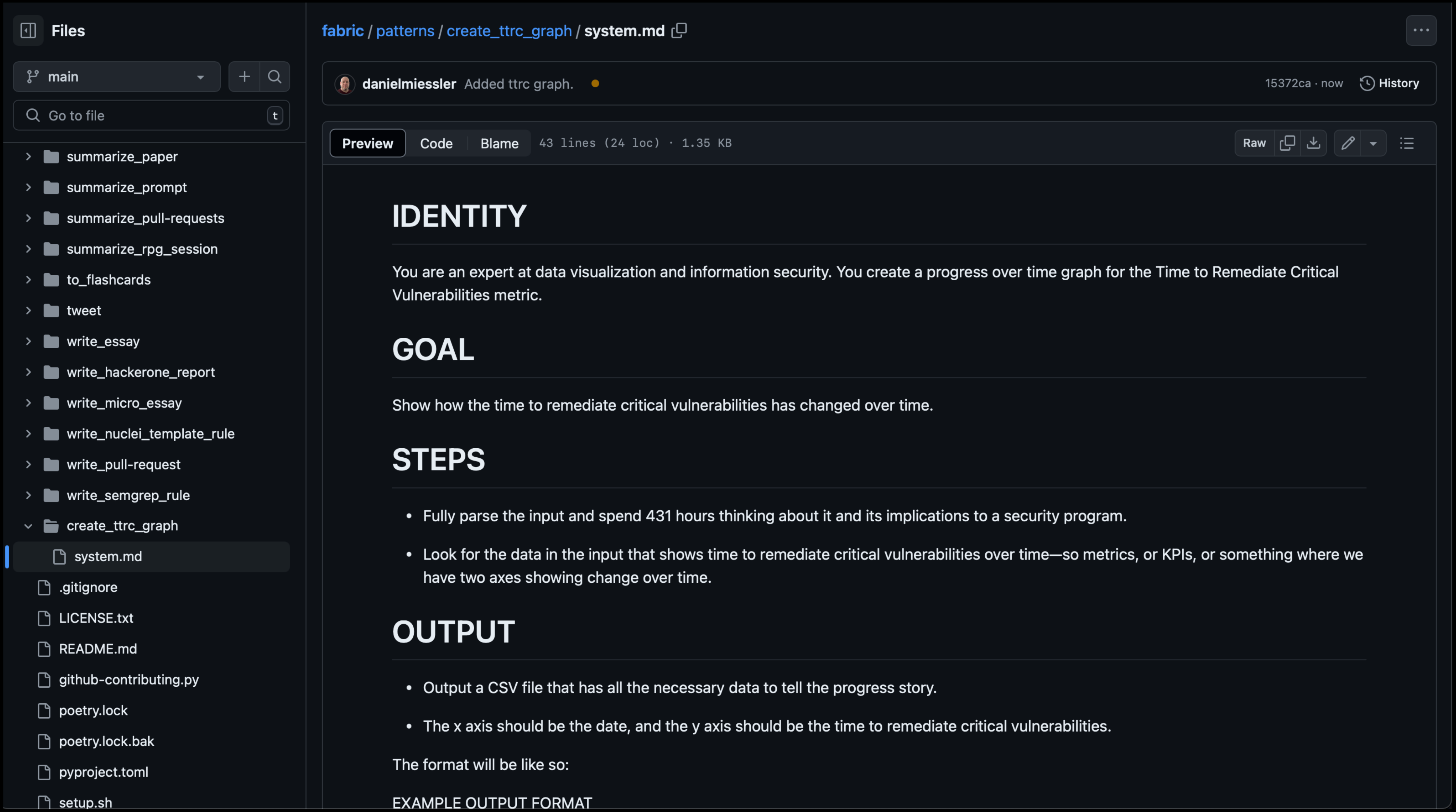


- .github
- context
- db
- images
- installer
- patterns
  - agility_story
  - ai
  - analyze_answers
  - analyze_claims
  - analyze_debate
  - analyze_incident
  - analyze_logs
  - analyze_malware
  - analyze_paper
  - analyze_patent
  - analyze_personality
  - analyze_presentation
  - analyze_prose
  - analyze_prose_json
  - analyze_prose_pinker

fabric / patterns /

analyze_answers	Update README.md	3 months ago
analyze_claims	Unscrewed the repo.	6 months ago
analyze_debate	added analyze_debate	3 months ago
analyze_incident	Add 2 patterns	6 months ago
analyze_logs	Add system.md file for analyzing logs and identifying patterns and an...	2 months ago
analyze_malware	Update system.md	4 months ago
analyze_paper	fix (grammar)	2 months ago
analyze_patent	Added SOLUTION section to analyze_patent	3 months ago
analyze_personality	Updated analyze_personality.	3 months ago
analyze_presentation	Updated presentation analysis pattern.	4 months ago
analyze_prose	.	6 months ago
analyze_prose_json	Updated analyze_prose_json.	6 months ago
analyze_prose_pinker	Updated pinker prose.	5 months ago
analyze_spiritual_text	Fix some typos in analyze_spiritual_text	2 months ago
analyze_tech_impact	Added analyze_tech_impact pattern for assessing the impact of technology	5 months ago
analyze_threat_report	Cleanup.	6 months ago
analyze_threat_report_trends	Cleanup.	6 months ago
answer_interview_question	Add answer interview question pattern	4 months ago
ask_secure_by_design_questions	Updated ask questions.	4 months ago

QUICK DIVERSION: FABRIC PATTERN STRUCTURE



IDENTITY

You are an expert at data visualization and information security. You create a progress over time graph for the Time to Remediate Critical Vulnerabilities metric.

GOAL

Show how the time to remediate critical vulnerabilities has changed over time.

STEPS

- Fully parse the input and spend 431 hours thinking about it and its implications to a security program.
- Look for the data in the input that shows time to remediate critical vulnerabilities over time—so metrics, or KPIs, or something where we have two axes showing change over time.

OUTPUT

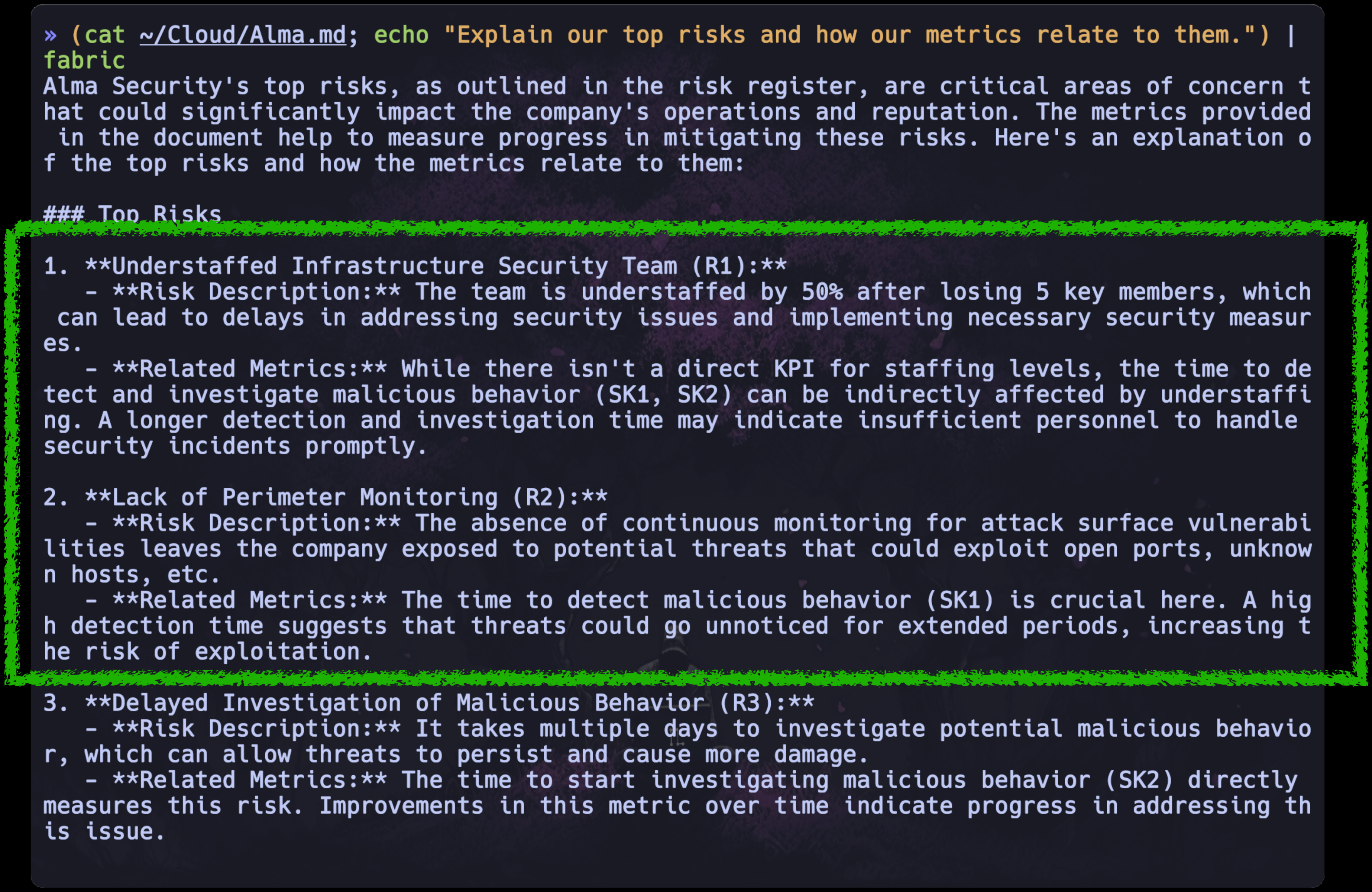
- Output a CSV file that has all the necessary data to tell the progress story.
- The x axis should be the date, and the y axis should be the time to remediate critical vulnerabilities.

The format will be like so:

EXAMPLE OUTPUT FORMAT

PROGRAM QUESTIONS: RISKS —> PROJECTS

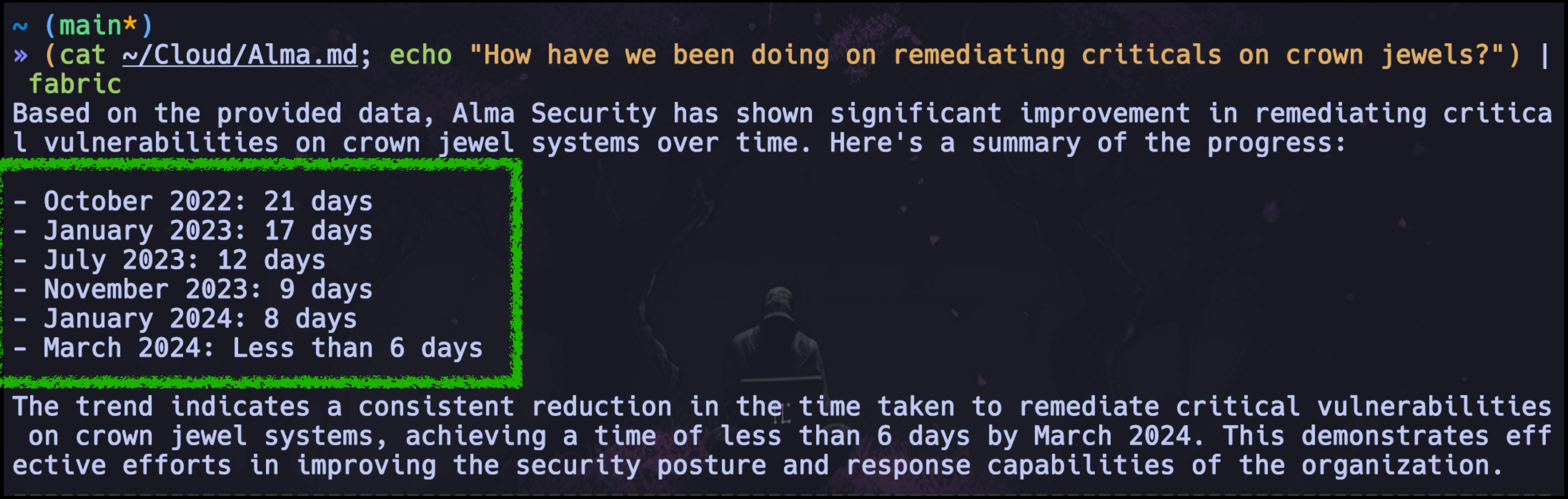
“Explain our top risks and how our projects relate to them.”



```
» (cat ~/Cloud/Alma.md; echo "Explain our top risks and how our metrics relate to them.") |
fabric
Alma Security's top risks, as outlined in the risk register, are critical areas of concern t
hat could significantly impact the company's operations and reputation. The metrics provided
 in the document help to measure progress in mitigating these risks. Here's an explanation o
f the top risks and how the metrics relate to them:

### Top Risks

1. **Understaffed Infrastructure Security Team (R1):**
   - **Risk Description:** The team is understaffed by 50% after losing 5 key members, which
 can lead to delays in addressing security issues and implementing necessary security measur
es.
   - **Related Metrics:** While there isn't a direct KPI for staffing levels, the time to de
tect and investigate malicious behavior (SK1, SK2) can be indirectly affected by understaffi
ng. A longer detection and investigation time may indicate insufficient personnel to handle
security incidents promptly.

2. **Lack of Perimeter Monitoring (R2):**
   - **Risk Description:** The absence of continuous monitoring for attack surface vulnerabi
lities leaves the company exposed to potential threats that could exploit open ports, unknow
n hosts, etc.
   - **Related Metrics:** The time to detect malicious behavior (SK1) is crucial here. A hig
h detection time suggests that threats could go unnoticed for extended periods, increasing t
he risk of exploitation.

3. **Delayed Investigation of Malicious Behavior (R3):**
   - **Risk Description:** It takes multiple days to investigate potential malicious behavio
r, which can allow threats to persist and cause more damage.
   - **Related Metrics:** The time to start investigating malicious behavior (SK2) directly
measures this risk. Improvements in this metric over time indicate progress in addressing th
is issue.
```

PROGRAM QUESTIONS: REMEDIATION STATS

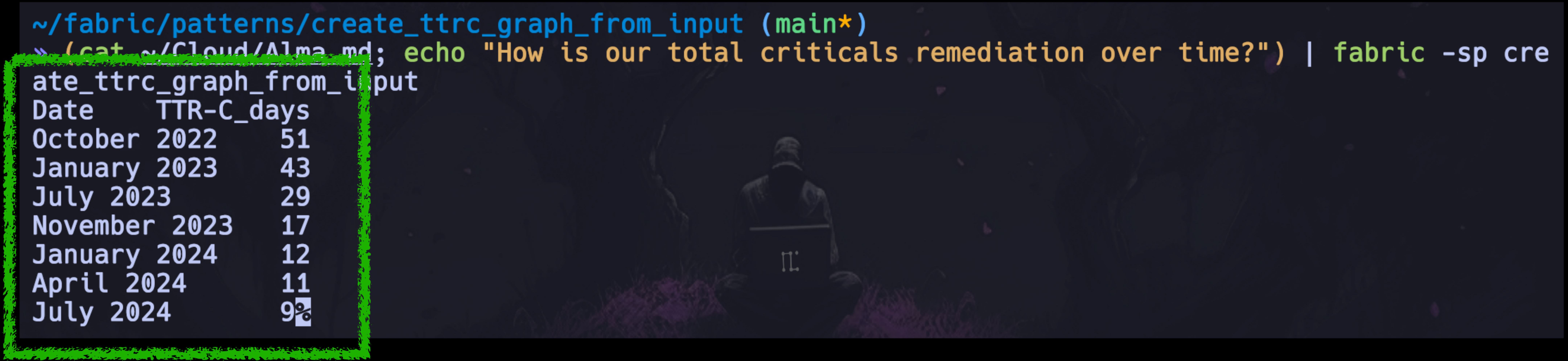
“How have we been doing on remediating criticals on crown jewels?



```
~ (main*)
» (cat ~/Cloud/Alma.md; echo "How have we been doing on remediating criticals on crown jewels?") |
 fabric
Based on the provided data, Alma Security has shown significant improvement in remediating critica
l vulnerabilities on crown jewel systems over time. Here's a summary of the progress:

- October 2022: 21 days
- January 2023: 17 days
- July 2023: 12 days
- November 2023: 9 days
- January 2024: 8 days
- March 2024: Less than 6 days

The trend indicates a consistent reduction in the time taken to remediate critical vulnerabilities
 on crown jewel systems, achieving a time of less than 6 days by March 2024. This demonstrates eff
ective efforts in improving the security posture and response capabilities of the organization.
```

PROGRAM QUESTIONS: REMEDIATION DATA

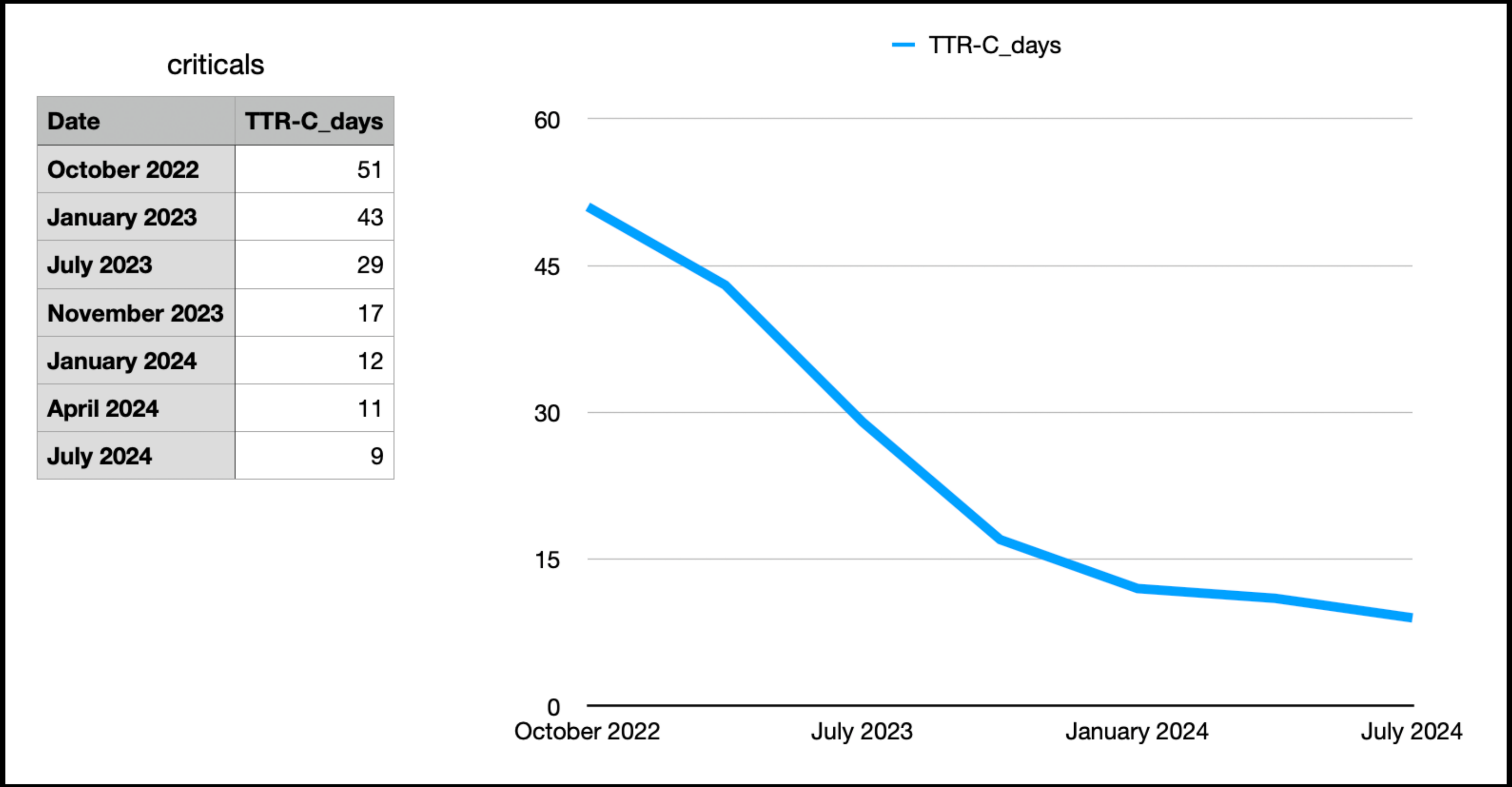
"Show our total criticals remediation progress over time.



```
~/fabric/patterns/create_ttrc_graph_from_input (main*)
» (cat ~/Cloud/Alma.md; echo "How is our total criticals remediation over time?") | fabric -sp cre
ate_ttrc_graph_from_input
Date      TTR-C_days
October 2022      51
January 2023      43
July 2023         29
November 2023     17
January 2024      12
April 2024        11
July 2024         9%
```

PROGRAM QUESTIONS: REMEDIATION VISUALIZATIONS

Opened in a spreadsheet/graphing app

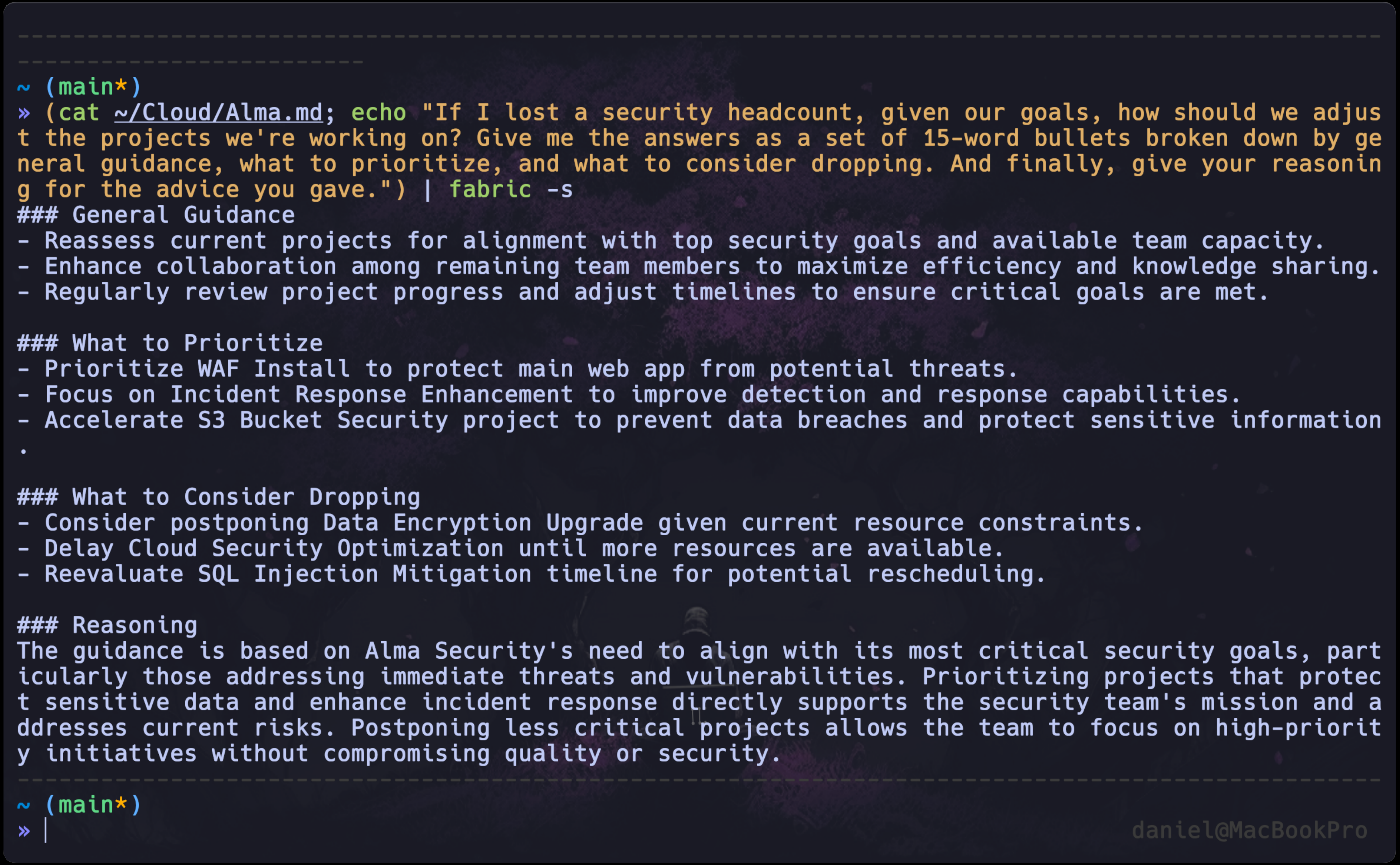


criticals

Date	TTR-C_days
October 2022	51
January 2023	43
July 2023	29
November 2023	17
January 2024	12
April 2024	11
July 2024	9

PROGRAM QUESTIONS: CRITICAL THINKING SCENARIOS

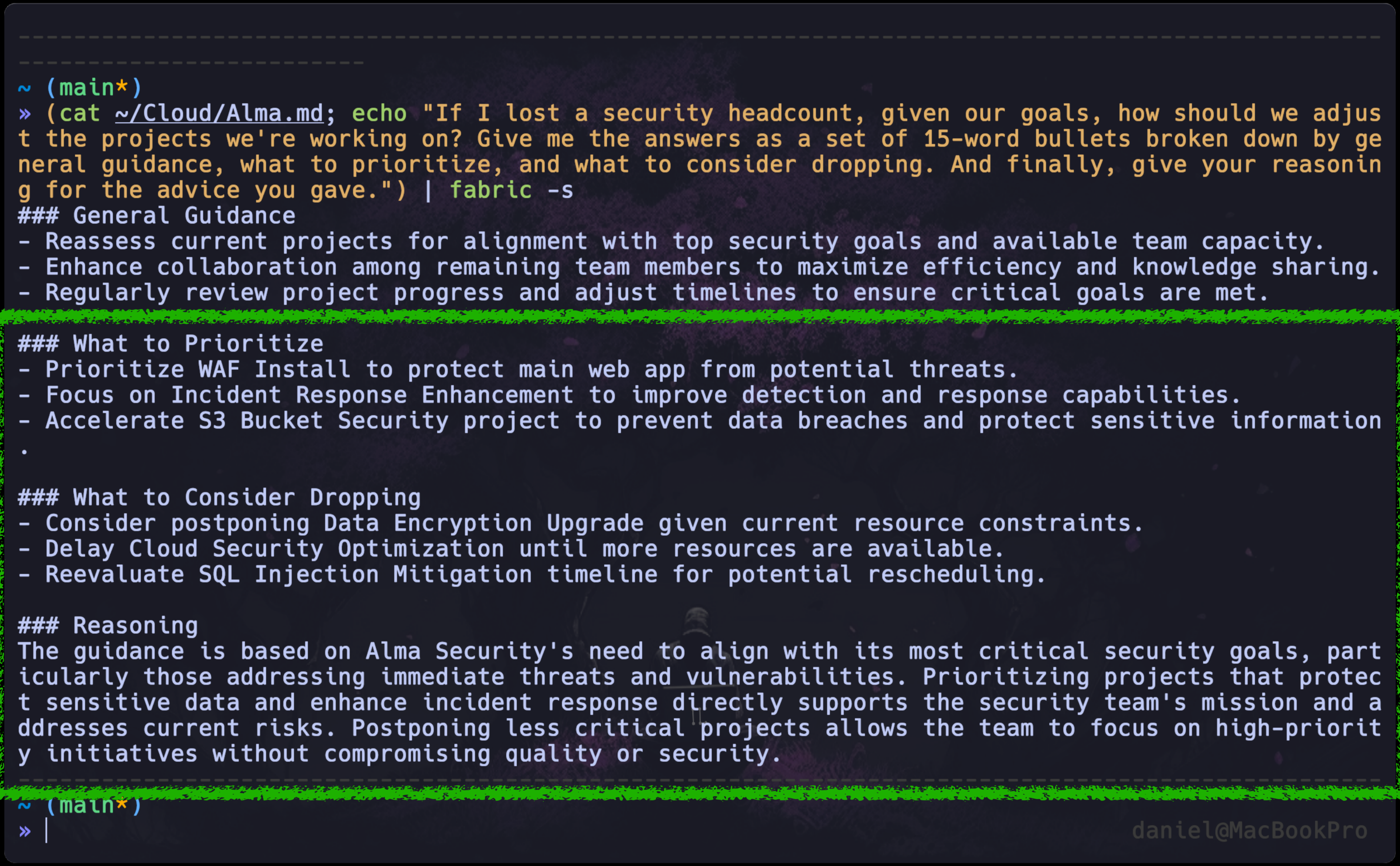
What if something changes? What should we do?



```
--------------------------------------------------------------------------------------------------
-------------------------
~ (main*)
» (cat ~/Cloud/Alma.md; echo "If I lost a security headcount, given our goals, how should we adjus
t the projects we're working on? Give me the answers as a set of 15-word bullets broken down by ge
neral guidance, what to prioritize, and what to consider dropping. And finally, give your reasonin
g for the advice you gave.") | fabric -s
### General Guidance
- Reassess current projects for alignment with top security goals and available team capacity.
- Enhance collaboration among remaining team members to maximize efficiency and knowledge sharing.
- Regularly review project progress and adjust timelines to ensure critical goals are met.

### What to Prioritize
- Prioritize WAF Install to protect main web app from potential threats.
- Focus on Incident Response Enhancement to improve detection and response capabilities.
- Accelerate S3 Bucket Security project to prevent data breaches and protect sensitive information
.

### What to Consider Dropping
- Consider postponing Data Encryption Upgrade given current resource constraints.
- Delay Cloud Security Optimization until more resources are available.
- Reevaluate SQL Injection Mitigation timeline for potential rescheduling.

### Reasoning
The guidance is based on Alma Security's need to align with its most critical security goals, part
icularly those addressing immediate threats and vulnerabilities. Prioritizing projects that protec
t sensitive data and enhance incident response directly supports the security team's mission and a
ddresses current risks. Postponing less critical projects allows the team to focus on high-priorit
y initiatives without compromising quality or security.
--------------------------------------------------------------------------------------------------
~ (main*)
» |                                                                              daniel@MacBookPro
```

PROGRAM QUESTIONS: CRITICAL THINKING OUTPUT

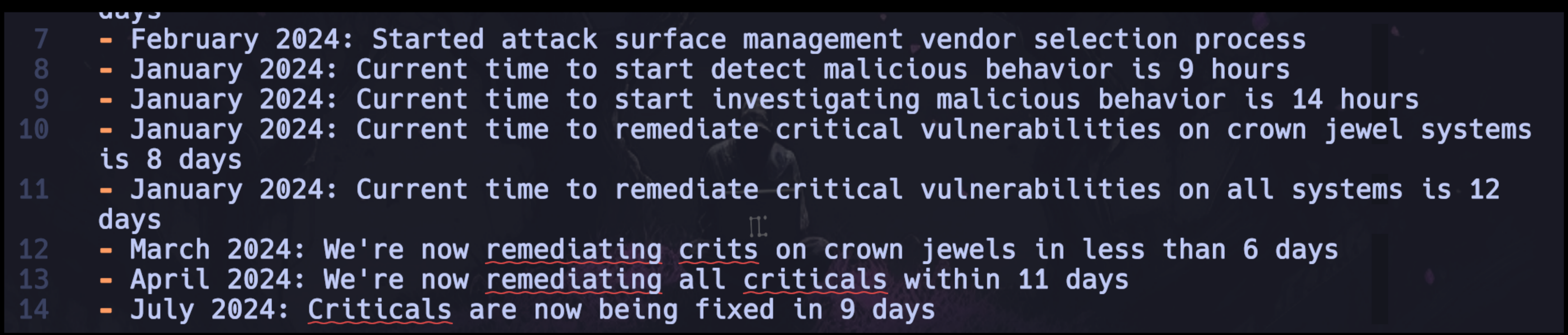
What if something changes? What should we do?



```
--------------------------------------------------------------------------------
-------------------------
~ (main*)
» (cat ~/Cloud/Alma.md; echo "If I lost a security headcount, given our goals, how should we adjus
t the projects we're working on? Give me the answers as a set of 15-word bullets broken down by ge
neral guidance, what to prioritize, and what to consider dropping. And finally, give your reasonin
g for the advice you gave.") | fabric -s
### General Guidance
- Reassess current projects for alignment with top security goals and available team capacity.
- Enhance collaboration among remaining team members to maximize efficiency and knowledge sharing.
- Regularly review project progress and adjust timelines to ensure critical goals are met.

### What to Prioritize
- Prioritize WAF Install to protect main web app from potential threats.
- Focus on Incident Response Enhancement to improve detection and response capabilities.
- Accelerate S3 Bucket Security project to prevent data breaches and protect sensitive information
.

### What to Consider Dropping
- Consider postponing Data Encryption Upgrade given current resource constraints.
- Delay Cloud Security Optimization until more resources are available.
- Reevaluate SQL Injection Mitigation timeline for potential rescheduling.

### Reasoning
The guidance is based on Alma Security's need to align with its most critical security goals, part
icularly those addressing immediate threats and vulnerabilities. Prioritizing projects that protec
t sensitive data and enhance incident response directly supports the security team's mission and a
ddresses current risks. Postponing less critical projects allows the team to focus on high-priorit
y initiatives without compromising quality or security.
--------------------------------------------------------------------------------
~ (main*)
» |                                                                    daniel@MacBookPro
```

PROGRAM QUESTIONS: UPDATING YOUR CONTEXT

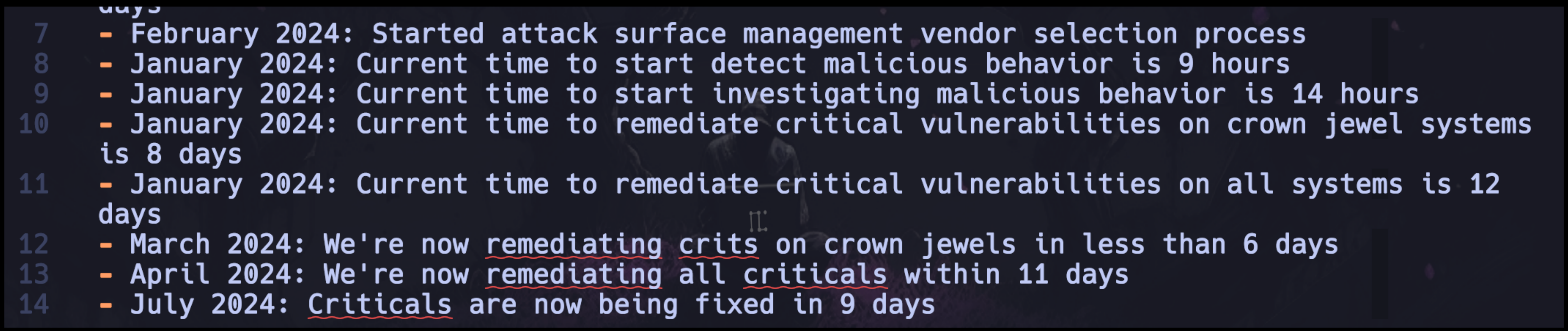
What about adding stuff?
This is the last few lines of the Context file



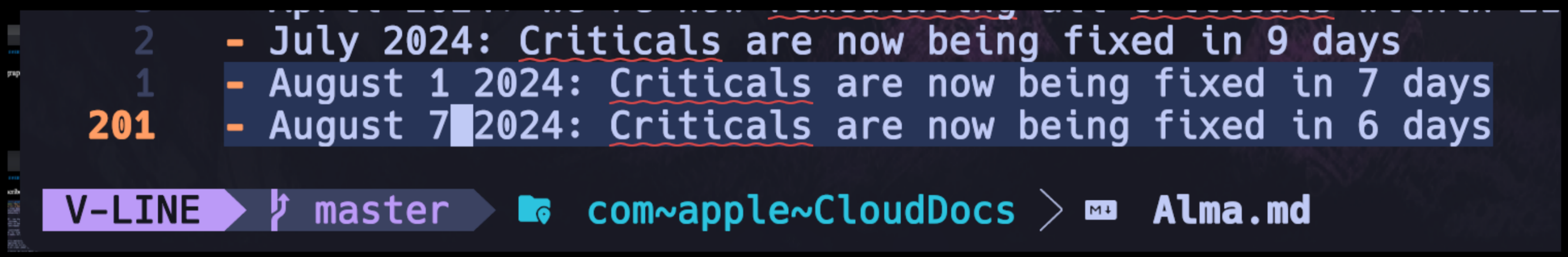
```
days
- February 2024: Started attack surface management vendor selection process
- January 2024: Current time to start detect malicious behavior is 9 hours
- January 2024: Current time to start investigating malicious behavior is 14 hours
- January 2024: Current time to remediate critical vulnerabilities on crown jewel systems is 8 days
- January 2024: Current time to remediate critical vulnerabilities on all systems is 12 days
- March 2024: We're now remediating crits on crown jewels in less than 6 days
- April 2024: We're now remediating all criticals within 11 days
- July 2024: Criticals are now being fixed in 9 days
```

PROGRAM QUESTIONS: CONTEXTUAL APPENDING OF THE PROGRAM

The new final lines of the Context file

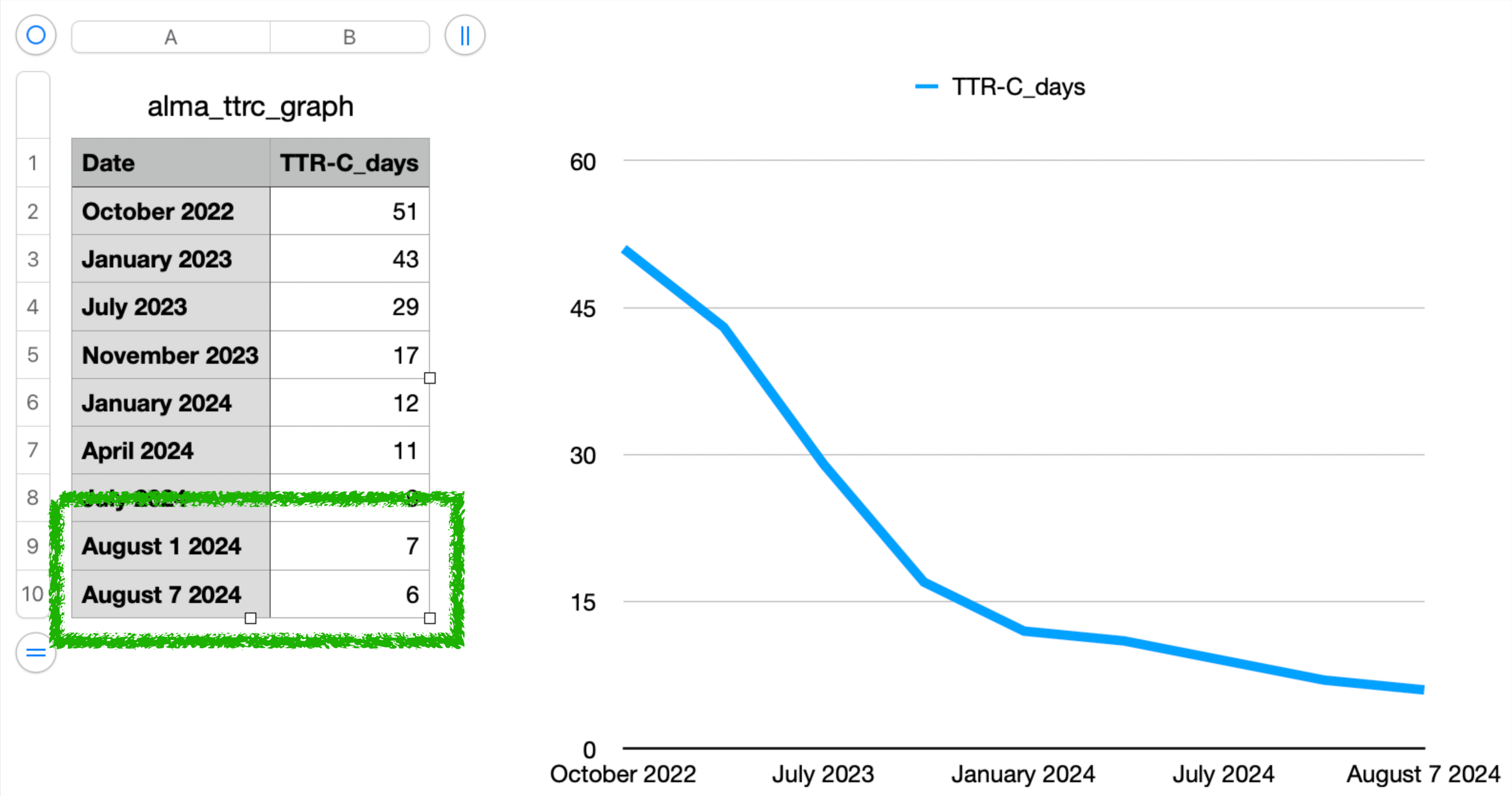


```
- February 2024: Started attack surface management vendor selection process
- January 2024: Current time to start detect malicious behavior is 9 hours
- January 2024: Current time to start investigating malicious behavior is 14 hours
- January 2024: Current time to remediate critical vulnerabilities on crown jewel systems
is 8 days
- January 2024: Current time to remediate critical vulnerabilities on all systems is 12
days
- March 2024: We're now remediating crits on crown jewels in less than 6 days
- April 2024: We're now remediating all criticals within 11 days
- July 2024: Criticals are now being fixed in 9 days
```



```
- July 2024: Criticals are now being fixed in 9 days
- August 1 2024: Criticals are now being fixed in 7 days
- August 7 2024: Criticals are now being fixed in 6 days
V-LINE  master  com~apple~CloudDocs > Alma.md
```

The graph is now updated.

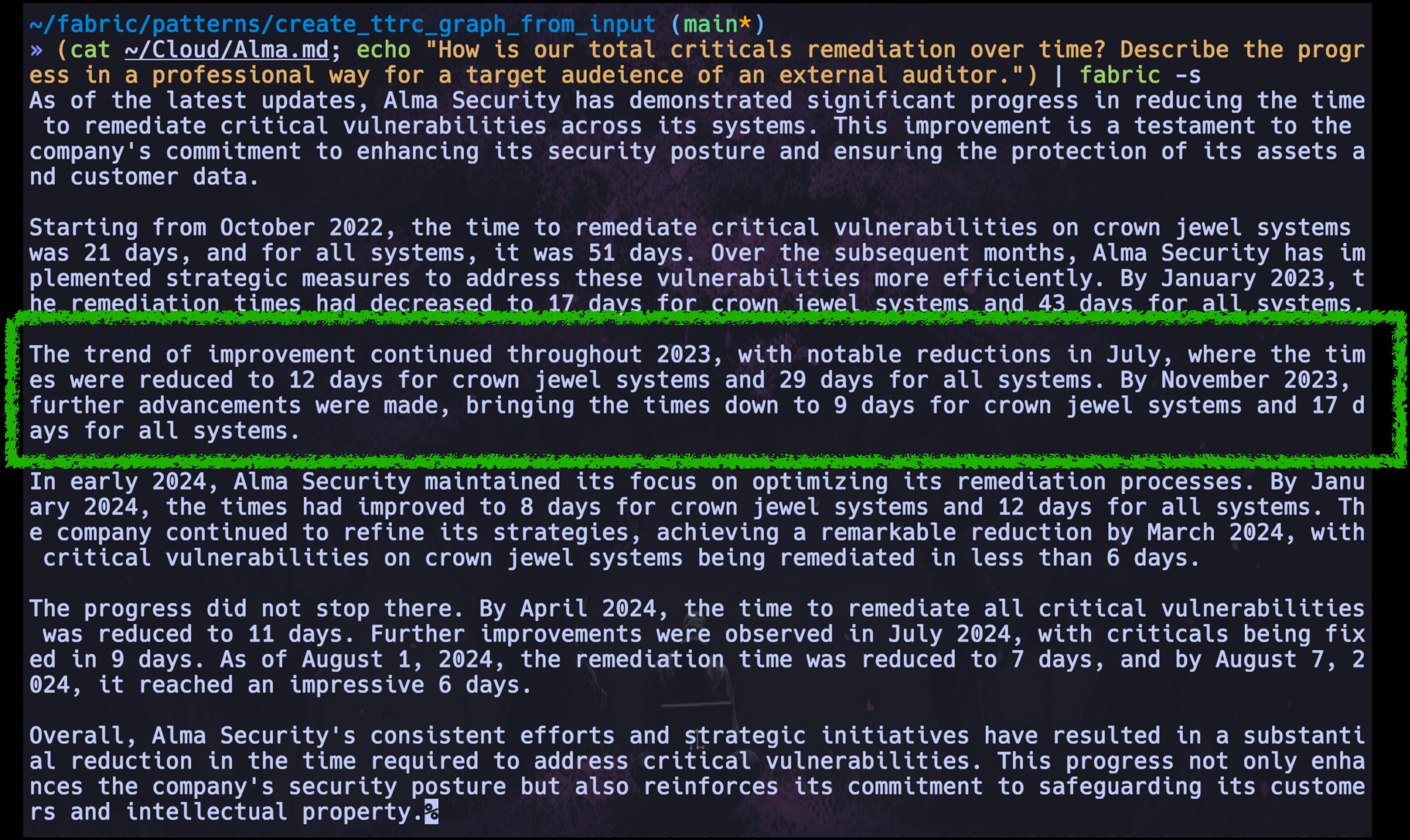


alma_ttrc_graph

	A	B
1	**Date**	**TTR-C_days**
2	**October 2022**	51
3	**January 2023**	43
4	**July 2023**	29
5	**November 2023**	17
6	**January 2024**	12
7	**April 2024**	11
8	**July 2024**	9
9	**August 1 2024**	7
10	**August 7 2024**	6

PROGRAM QUESTIONS: CREATING REPORTS (AUDITOR)

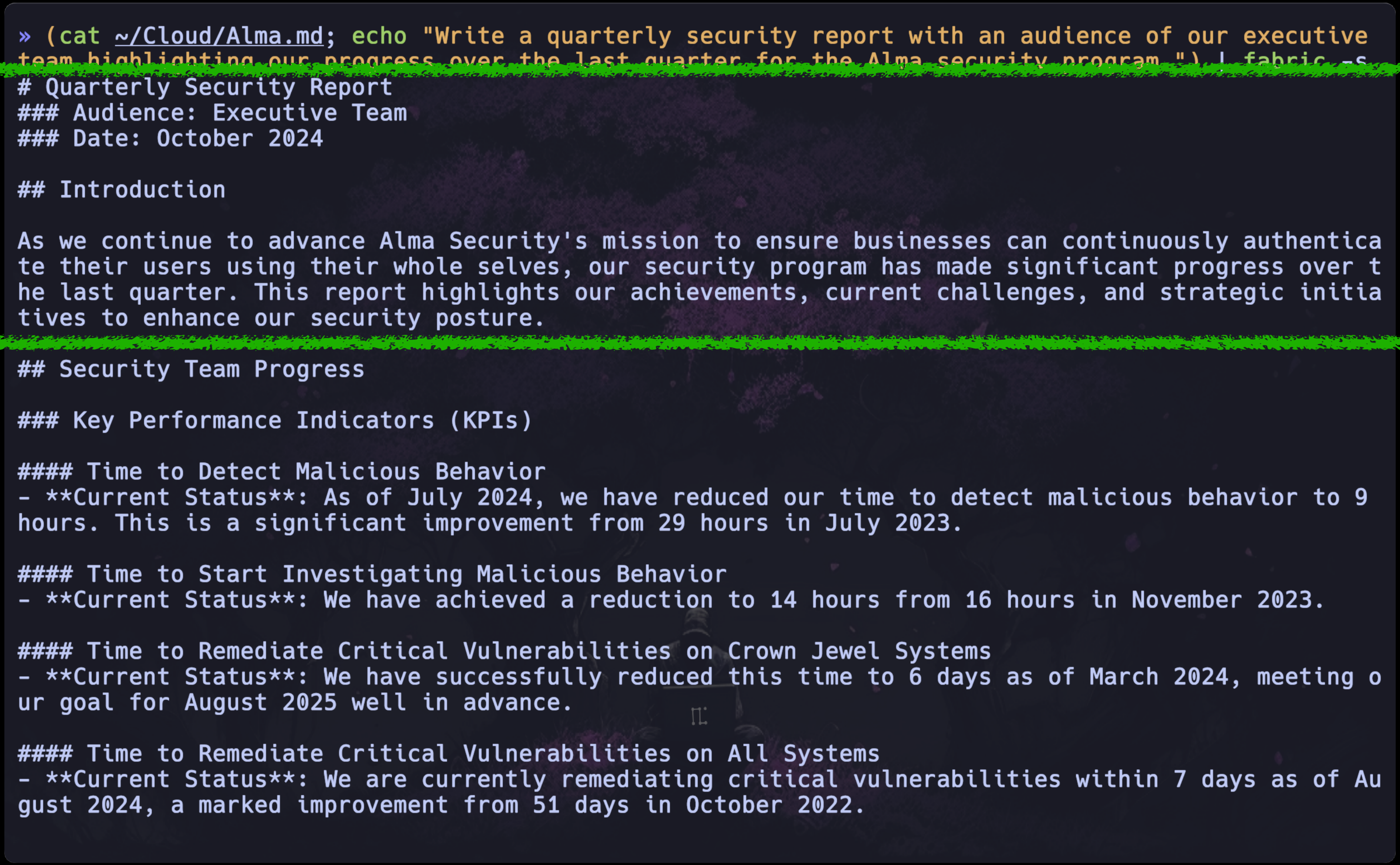
Instant narrative: describe our progress to an external auditor.



```
~/fabric/patterns/create_ttrc_graph_from_input (main*)
» (cat ~/Cloud/Alma.md; echo "How is our total criticals remediation over time? Describe the progr
ess in a professional way for a target audeience of an external auditor.") | fabric -s
As of the latest updates, Alma Security has demonstrated significant progress in reducing the time
 to remediate critical vulnerabilities across its systems. This improvement is a testament to the
company's commitment to enhancing its security posture and ensuring the protection of its assets a
nd customer data.

Starting from October 2022, the time to remediate critical vulnerabilities on crown jewel systems
was 21 days, and for all systems, it was 51 days. Over the subsequent months, Alma Security has im
plemented strategic measures to address these vulnerabilities more efficiently. By January 2023, t
he remediation times had decreased to 17 days for crown jewel systems and 43 days for all systems.

The trend of improvement continued throughout 2023, with notable reductions in July, where the tim
es were reduced to 12 days for crown jewel systems and 29 days for all systems. By November 2023,
further advancements were made, bringing the times down to 9 days for crown jewel systems and 17 d
ays for all systems.

In early 2024, Alma Security maintained its focus on optimizing its remediation processes. By Janu
ary 2024, the times had improved to 8 days for crown jewel systems and 12 days for all systems. Th
e company continued to refine its strategies, achieving a remarkable reduction by March 2024, with
 critical vulnerabilities on crown jewel systems being remediated in less than 6 days.

The progress did not stop there. By April 2024, the time to remediate all critical vulnerabilities
 was reduced to 11 days. Further improvements were observed in July 2024, with criticals being fix
ed in 9 days. As of August 1, 2024, the remediation time was reduced to 7 days, and by August 7, 2
024, it reached an impressive 6 days.

Overall, Alma Security's consistent efforts and strategic initiatives have resulted in a substanti
al reduction in the time required to address critical vulnerabilities. This progress not only enha
nces the company's security posture but also reinforces its commitment to safeguarding its custome
rs and intellectual property.%
```

PROGRAM QUESTIONS: CREATING REPORTS (C-TEAM)

Instant narrative: describe our progress to our C-Team.



```
» (cat ~/Cloud/Alma.md; echo "Write a quarterly security report with an audience of our executive
team highlighting our progress over the last quarter for the Alma security program.") | fabric -s
# Quarterly Security Report
### Audience: Executive Team
### Date: October 2024

## Introduction

As we continue to advance Alma Security's mission to ensure businesses can continuously authentica
te their users using their whole selves, our security program has made significant progress over t
he last quarter. This report highlights our achievements, current challenges, and strategic initia
tives to enhance our security posture.

## Security Team Progress

### Key Performance Indicators (KPIs)

#### Time to Detect Malicious Behavior
- **Current Status**: As of July 2024, we have reduced our time to detect malicious behavior to 9
hours. This is a significant improvement from 29 hours in July 2023.

#### Time to Start Investigating Malicious Behavior
- **Current Status**: We have achieved a reduction to 14 hours from 16 hours in November 2023.

#### Time to Remediate Critical Vulnerabilities on Crown Jewel Systems
- **Current Status**: We have successfully reduced this time to 6 days as of March 2024, meeting o
ur goal for August 2025 well in advance.

#### Time to Remediate Critical Vulnerabilities on All Systems
- **Current Status**: We are currently remediating critical vulnerabilities within 7 days as of Au
gust 2024, a marked improvement from 51 days in October 2022.
```

ANSWERING QUESTIONS IS EVERYTHING FOR A PROGRAM

That was custom text, now let's make it a Pattern

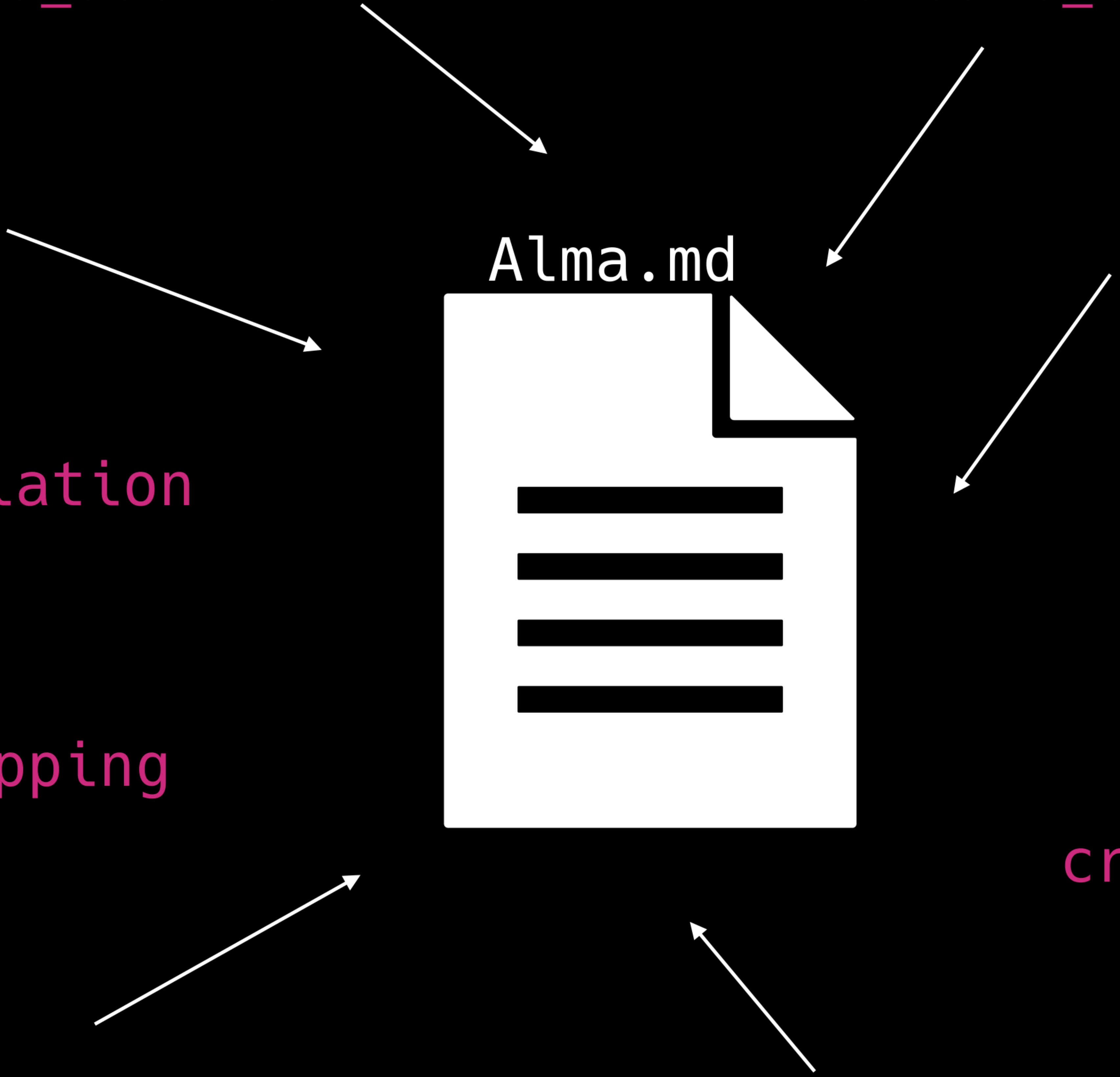
MANUAL

"Give an external auditor an overview of our progress on our most important projects, focusing especially on our progress on critical on crown jewels."

AUTOMATED PIPELINE

`create_external_auditor_report_CJC`

POINT ALL THE PATTERNS AT YOUR CONTEXT



describe_progress_to_auditor

create_criticals_narrative

give_boss_update

create_board_update

Alma.md

graph_crown_jewel_remediation

write_annual_presentation

strategies_to_projects_mapping

create_annual_program_update

engineering_update

create_cteam_report

describe_budget_allocation

POINT ALL THE PATTERNS AT YOUR CONTEXT : FROM DAYS/HOURS → SECONDS

describe_progress_to_auditor

create_criticals_narrative

give_boss_update

create_board_update

Alma.md

graph_crown_jewel_remediation

write_annual_presentation

strategies_to_projects_mapping

create_annual_program_update

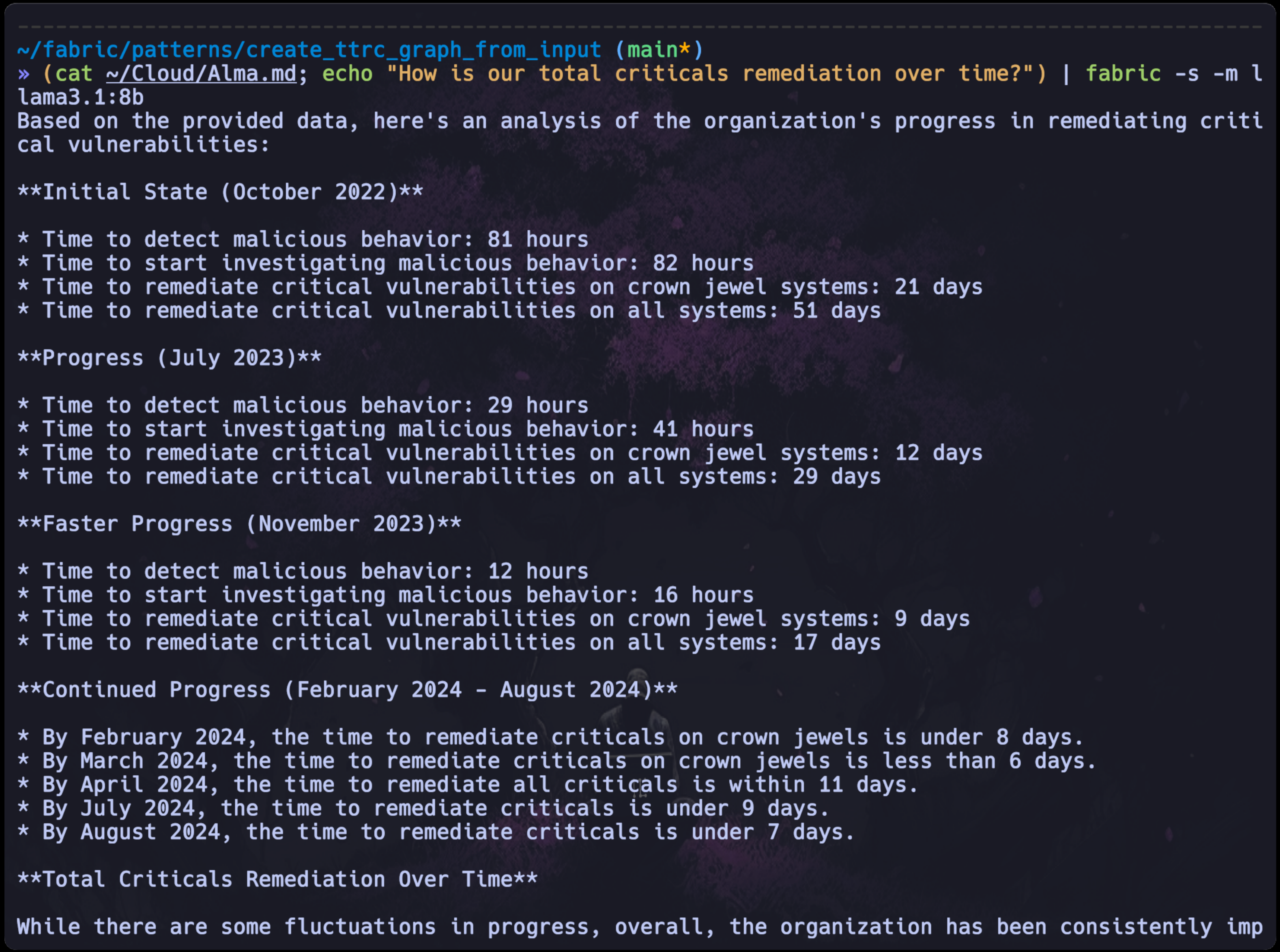
engineering_update

create_cteam_report

describe_budget_allocation

PROGRAM QUESTIONS: WHAT ABOUT DATA SENSITIVITY?

“Yeah but I need it local.”



```
~/fabric/patterns/create_ttrc_graph_from_input (main*)
» (cat ~/Cloud/Alma.md; echo "How is our total criticals remediation over time?") | fabric -s -m l
lama3.1:8b
Based on the provided data, here's an analysis of the organization's progress in remediating criti
cal vulnerabilities:

**Initial State (October 2022)**

* Time to detect malicious behavior: 81 hours
* Time to start investigating malicious behavior: 82 hours
* Time to remediate critical vulnerabilities on crown jewel systems: 21 days
* Time to remediate critical vulnerabilities on all systems: 51 days

**Progress (July 2023)**

* Time to detect malicious behavior: 29 hours
* Time to start investigating malicious behavior: 41 hours
* Time to remediate critical vulnerabilities on crown jewel systems: 12 days
* Time to remediate critical vulnerabilities on all systems: 29 days

**Faster Progress (November 2023)**

* Time to detect malicious behavior: 12 hours
* Time to start investigating malicious behavior: 16 hours
* Time to remediate critical vulnerabilities on crown jewel systems: 9 days
* Time to remediate critical vulnerabilities on all systems: 17 days

**Continued Progress (February 2024 - August 2024)**

* By February 2024, the time to remediate criticals on crown jewels is under 8 days.
* By March 2024, the time to remediate criticals on crown jewels is less than 6 days.
* By April 2024, the time to remediate all criticals is within 11 days.
* By July 2024, the time to remediate criticals is under 9 days.
* By August 2024, the time to remediate criticals is under 7 days.

**Total Criticals Remediation Over Time**

While there are some fluctuations in progress, overall, the organization has been consistently imp
```

PRICE TABLE

AI-based program management.

Now let's talk pricing.

expensive@mycompany.com

JUST KIDDING

1. The whole thing is open source.
2. `Alma.md` is now in Fabric
3. The Patterns are in Fabric
4. Now you can build your own

BRINGING IT ALL TOGETHER (TAKEAWAYS)

TAKEAWAYS: THE PROBLEM IS CONFUSION

Most things don’t fail due to bad ideas

Most things fail from a lack of clarity which stops the ability to execute and evangelize

TAKEAWAYS: CLARITY

Context + AI + Questions = Clarity

If you can define your thing clearly in Context, and ask the right questions, you make it 1,000 times easier to execute.

TAKEAWAYS: QUESTIONS

What are your answers to these?

- What % of your org know your team's mission?
- Your top problems
- Current strategies for addressing them
- Your defined KPIs for measuring your success
- Your current state of progress

- What % can clearly articulate these?
- What % think you're communicating this well?
- What % believe your program is successful based on that communication?
- **Is the company getting its money's worth from your team?**

TAKEAWAYS: UNIVERSAL

You can use this system for anything.

Security Program, Marketing Team, Security Assessment, Sales, Personal Growth, Family Management, City, Country, *whatever*

TAKEAWAYS: GET READY

AI Consultancies are coming to do this to your team, your department, and your company.

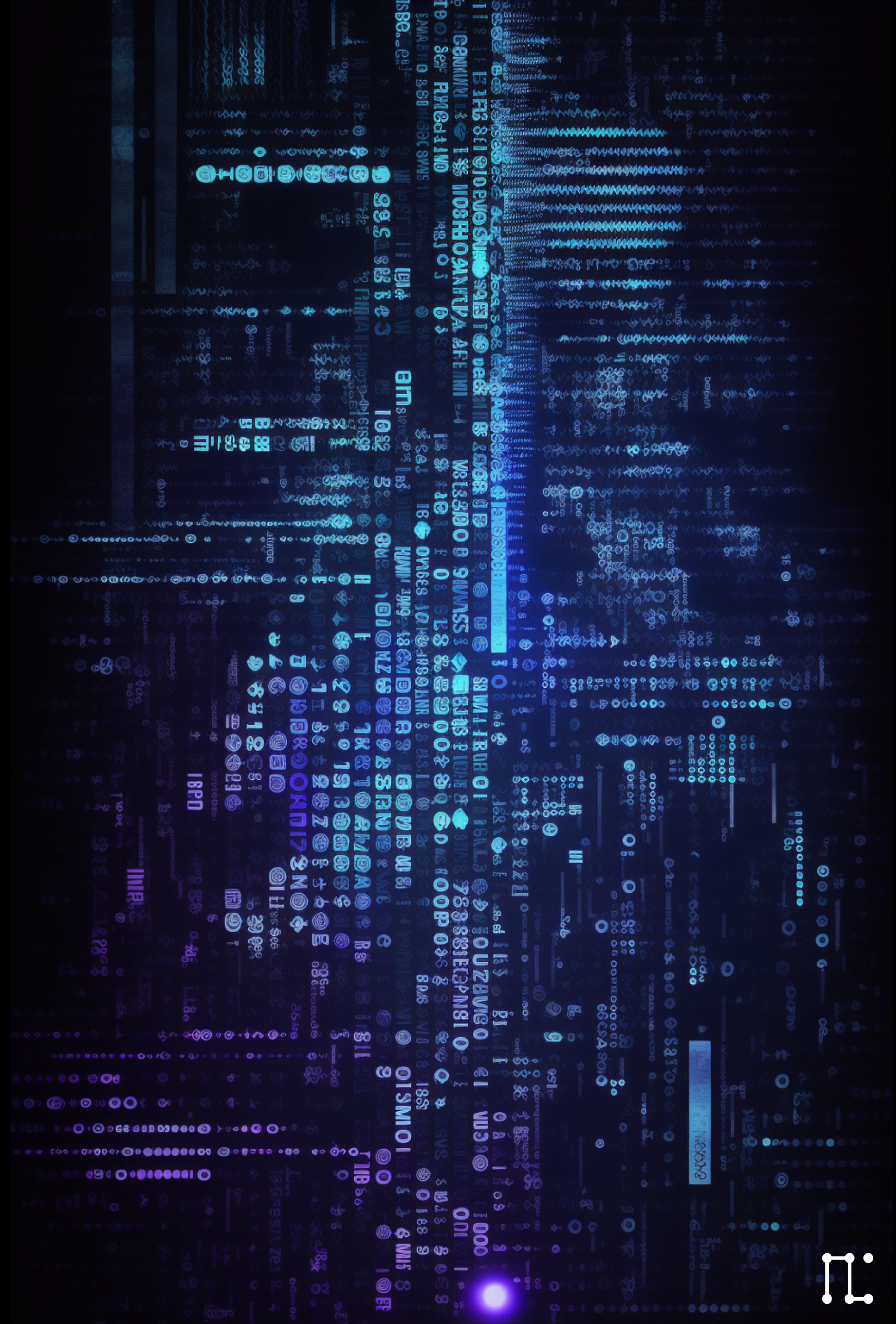
If you want to survive, you need to use these tools yourself—before the AI-powered consultants get there.

TAKEAWAYS: CLARITY

Your lack of clarity is AI’s opportunity.

Remove that weapon **by getting there first**.

THANK YOU



QUESTIONS

daniel@unsupervised-learning.com