LevelOps

User persona

Security team

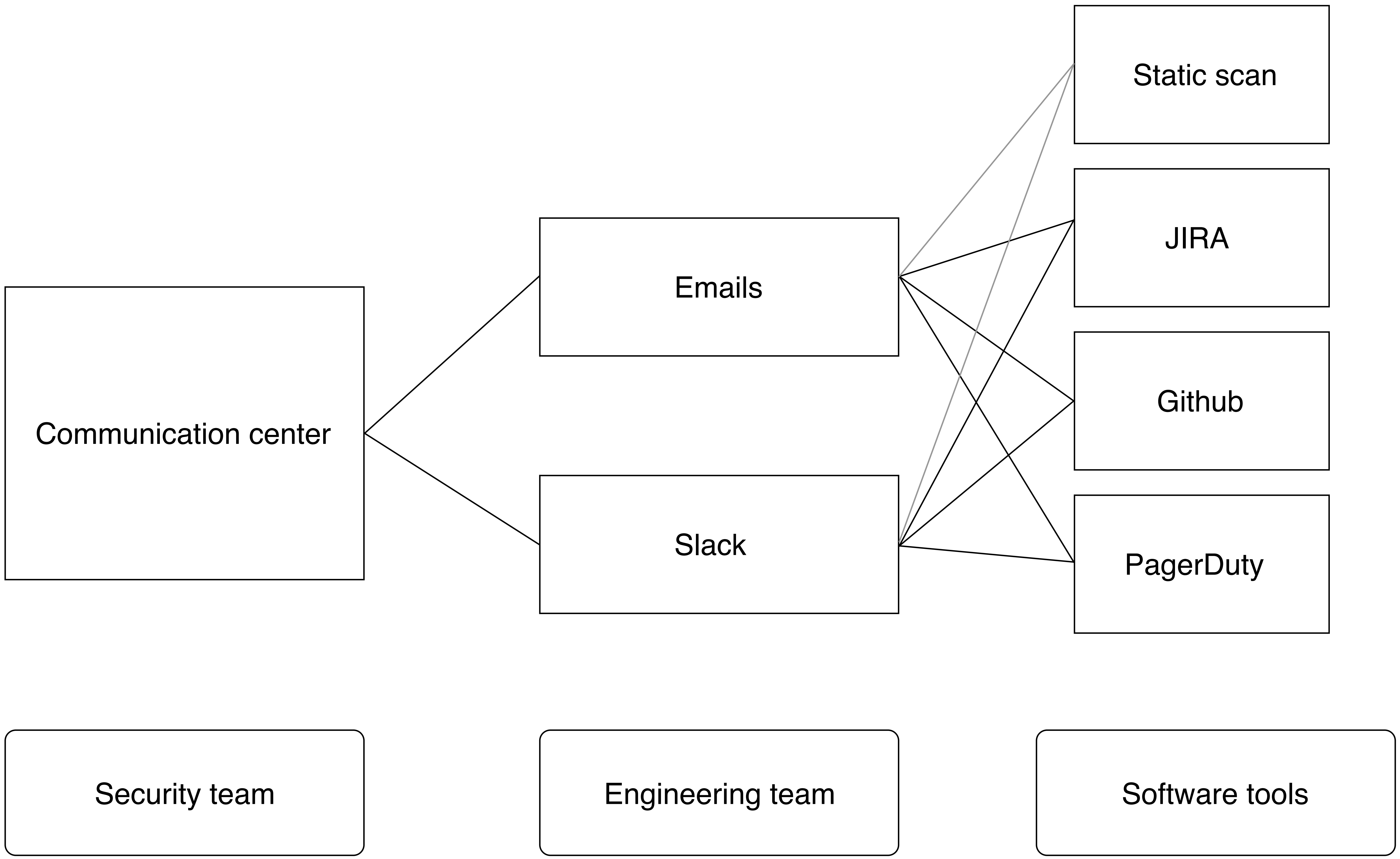
A security team at a software company evaluate, identify, triage, and resolve security vulnerabilities:

- Be responsible for multiple ENG teams' security posture of their code base. This includes the cloud infrastructure security, application security, and networking security. They tend to perform or outsource static / dynamic code testing as well as build system-based static code analysis to gate the security posture of their cloud products.
- Manage and are held accountable for the security of the entire company as well as the entire suite of products. Not only do they have to be on top of all security problems they also have to be able to quickly respond to issues that have been caught in production.
- Each team member is responsible for and specialized in a specific functional area in security. For example, one team member might be specifically in charge of mobile products and has extensive knowledge about the landscape of mobile pen testing, amongst others.
- When a security vulnerability has been discovered, they proactively communicate to the ENG team and work with them to resolve the vulnerability.

ENG team

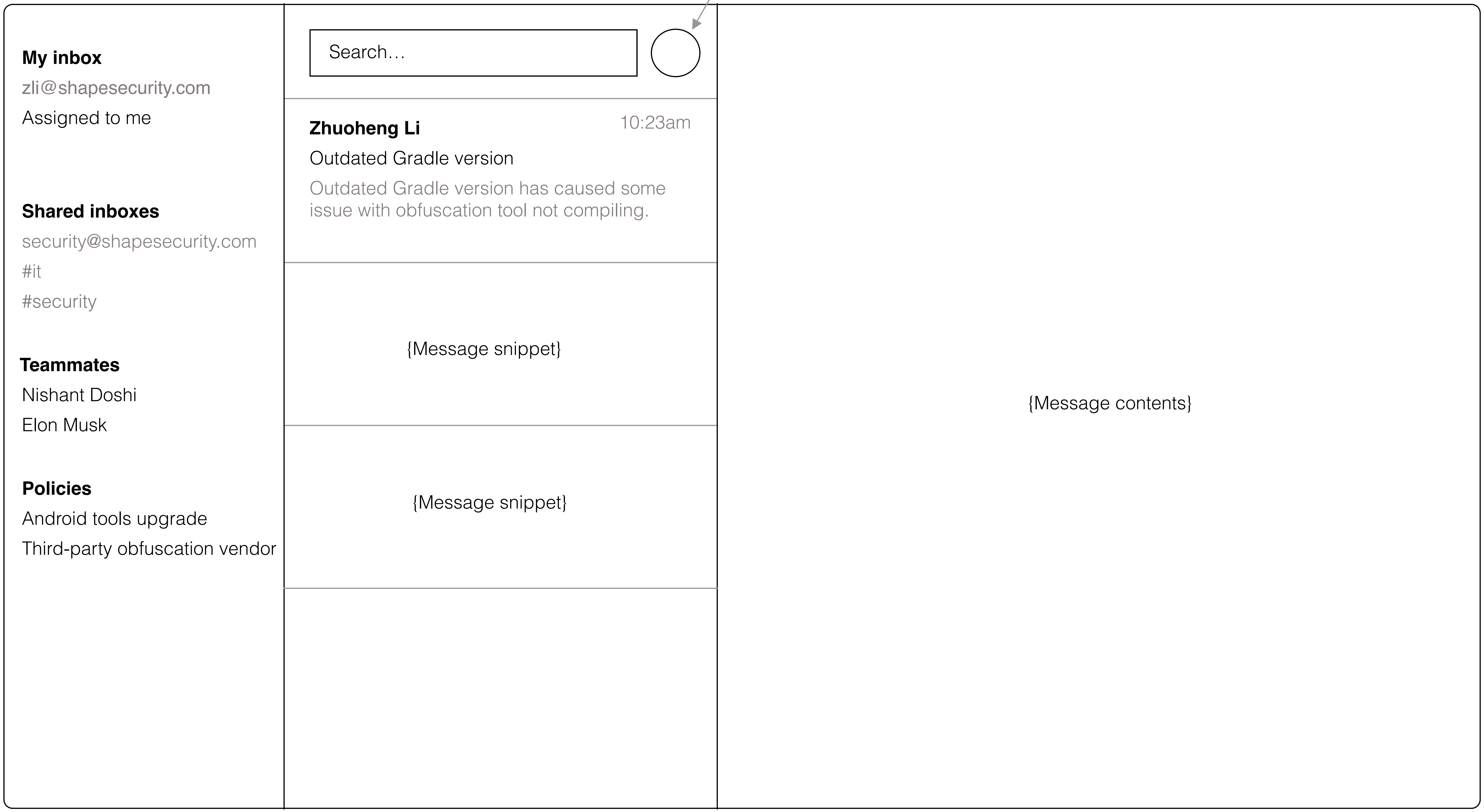
An ENG team at a software company:

- Are responsible for a specific functionality of a product.
- Do not necessarily have strong awareness of security coding practices.
- Have the tendency to catch / delegate security issues to the security team. Therefore, interaction with the security team is at a limited capacity.
- Often too busy with prioritizing issues that have values on the functionality level.


Static scan
JIRA
Emails
Communication center
Github
Slack
PagerDuty
Security team
Engineering team
Software tools

Communication center

Primary users are security team members



Users can filter for questionnaires, links, and messages

My inbox

zli@shapesecurity.com

Assigned to me

Shared inboxes

security@shapesecurity.com

#it

#security

Teammates

Nishant Doshi

Elon Musk

Policies

Android tools upgrade

Third-party obfuscation vendor

Search…

Zhuoheng Li 10:23am

Outdated Gradle version

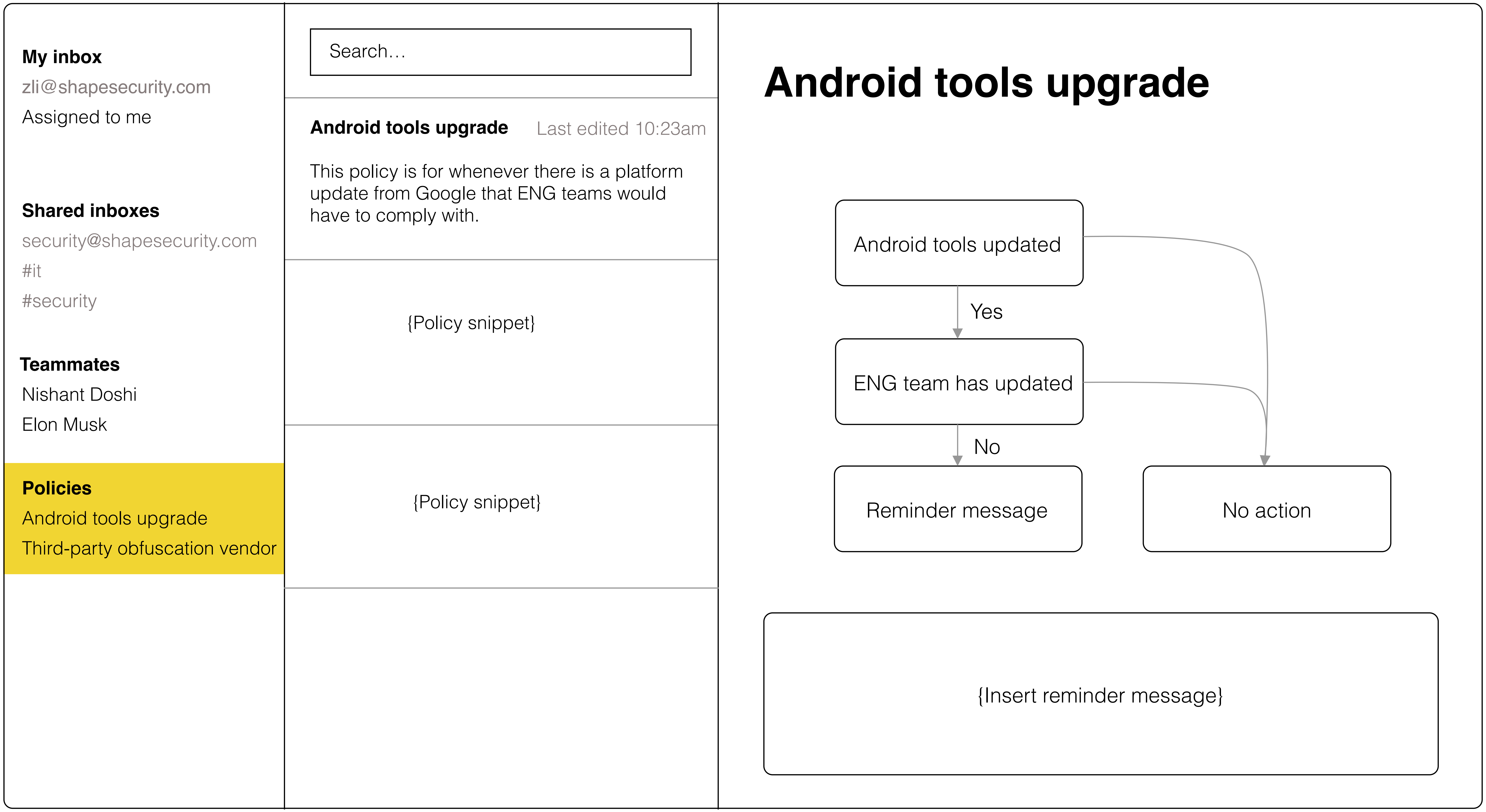
Outdated Gradle version has caused some issue with obfuscation tool not compiling.

{Message snippet}

{Message snippet}

{Message contents}

Programmatic communication



Android tools upgrade Last edited 10:23am

This policy is for whenever there is a platform update from Google that ENG teams would have to comply with.

{Policy snippet}

{Policy snippet}

Android tools upgrade

{Insert reminder message}

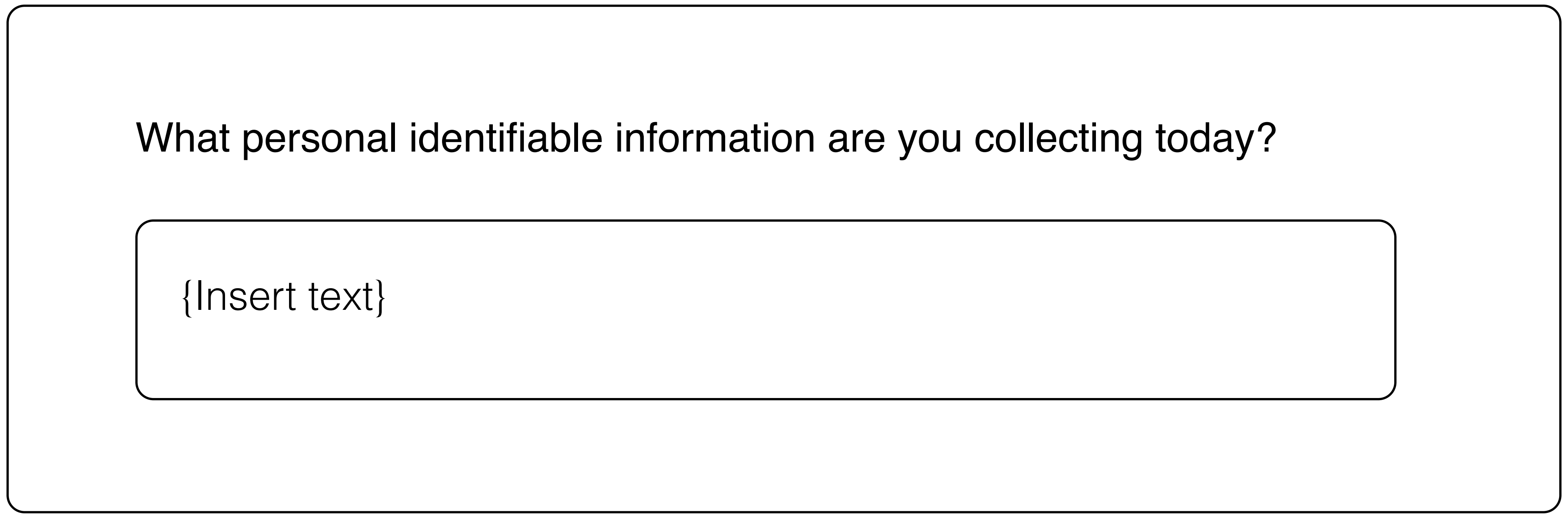
Questionnaire

Questionnaires can be used for:

- Risk assessments (e.g. of security practices amongst engineering teams)
- Public opinions (e.g. security feedback, tools selection)
- PII assessments

Areas for consideration:

- Simple for users to fill out, even in out-of-band communication channel.
- Basic functionalities to build a simple questionnaire with a maximum of 5 questions. Any more questions than that warrants a more sophisticated survey tool that Security team can link into a message.



What personal identifiable information are you collecting today?

{Insert text}

Basic questionnaires builder options include:

- Free responses
- Multiple choice
- Checkbox

Capturing out-of-band communication

Primary users are engineering teams

Slack

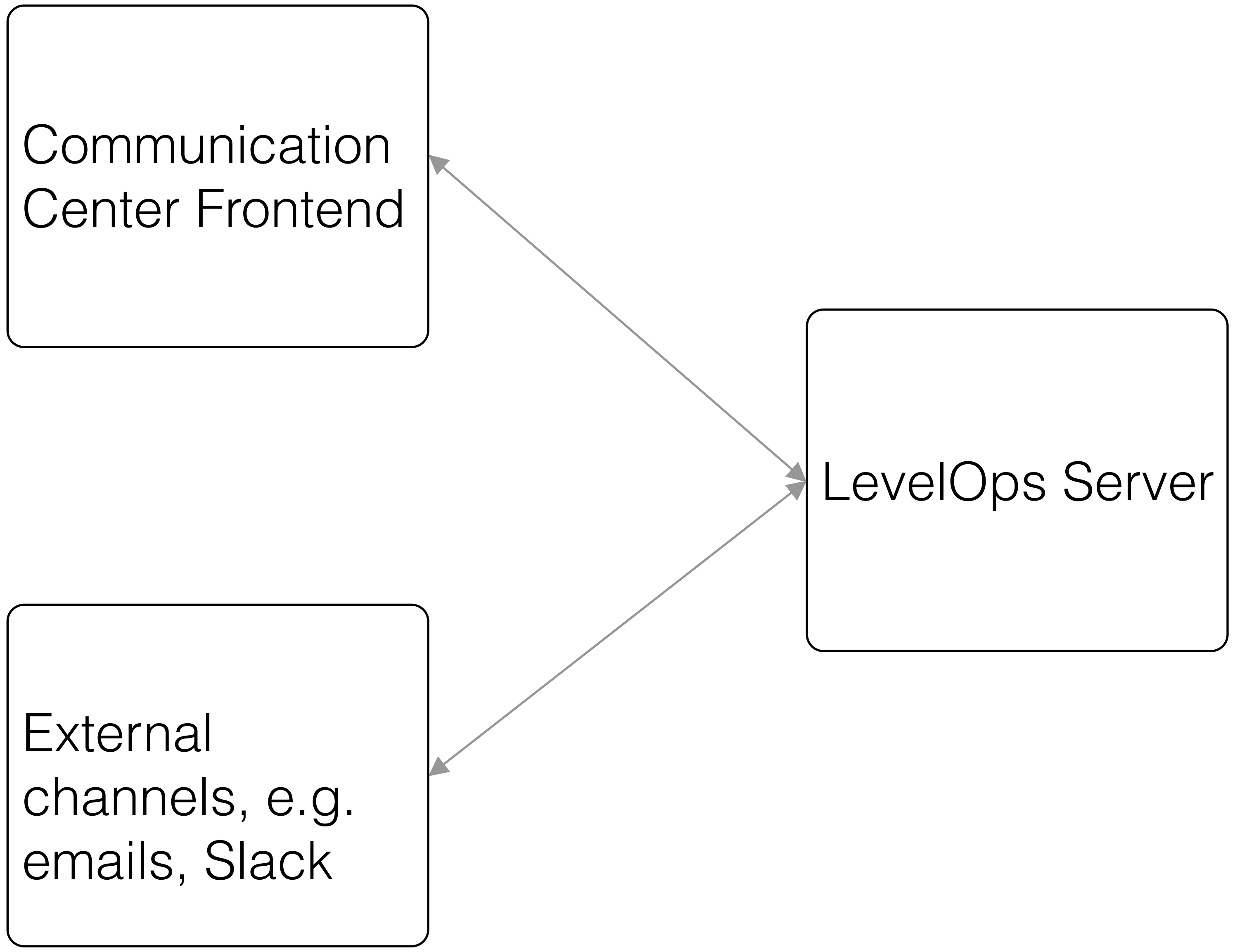
#mobile-eng

@levelops We received an automated report from the static scan that there is a vulnerability in our recent feature. We believe this is a false alarm.

Emails

To: nishant@shapesecurity.com
cc: levelops@shapesecurity.com

API endpoints



Communication Center Frontend

LevelOps Server

External channels, e.g. emails, Slack

1. External channel communicating with LevelOps server and send the messages for display on Communication Center.

Slack POST /v1/messages/

```
{ subject: string,
  contentType: (questionnaire, cleartext, links),
  contents: { value: string,
                   responses: (optional for questionnaire)
                 }
  threadId: number (identify which thread is coming from),
  messageId: number,
  priority: number
  automated: { value: false,
                      policyNumber: N/A
                    }
  assignee: (optional) string
  origin: { channel: (Communication Center, Slack, emails),
                meta: ‘’#mobile-eng’’
              }
}
```

2. Communication Center sending to external channels

Slack GET /v1/messages/ with similar JSON schema.

Leveraging data

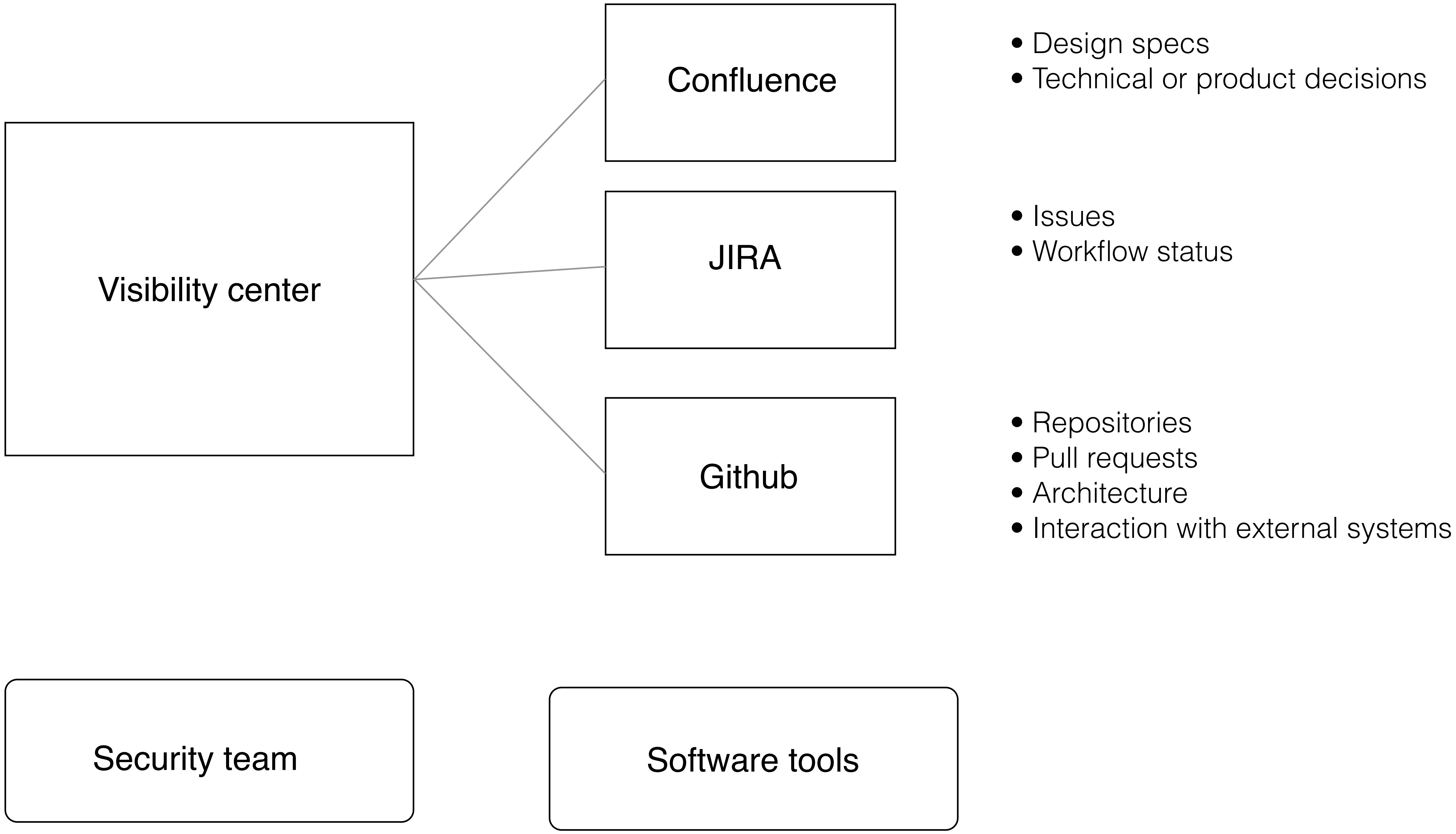
1. Automated priority.

Given the frequency, keywords, etc. in a given communcation thread, we can extract an organizational level priority of these messages for individual security team members.

2. Policy recommendation

If a similar issue has occurred multiple times, a recommended policy is generated for Security team to decide whether they should make it a long-term enforcement.

Visibility center



- Design specs
- Technical or product decisions

- Issues
- Workflow status

- Repositories
- Pull requests
- Architecture
- Interaction with external systems

Mobile SDK

Flagged vulnerabilities

- Very Important - NullPointer exception vulnerabilities (Link to Github here)
- Important - Outdated build tools used for Android app (Link to Github here) (Jira ticket) (Confluence page)

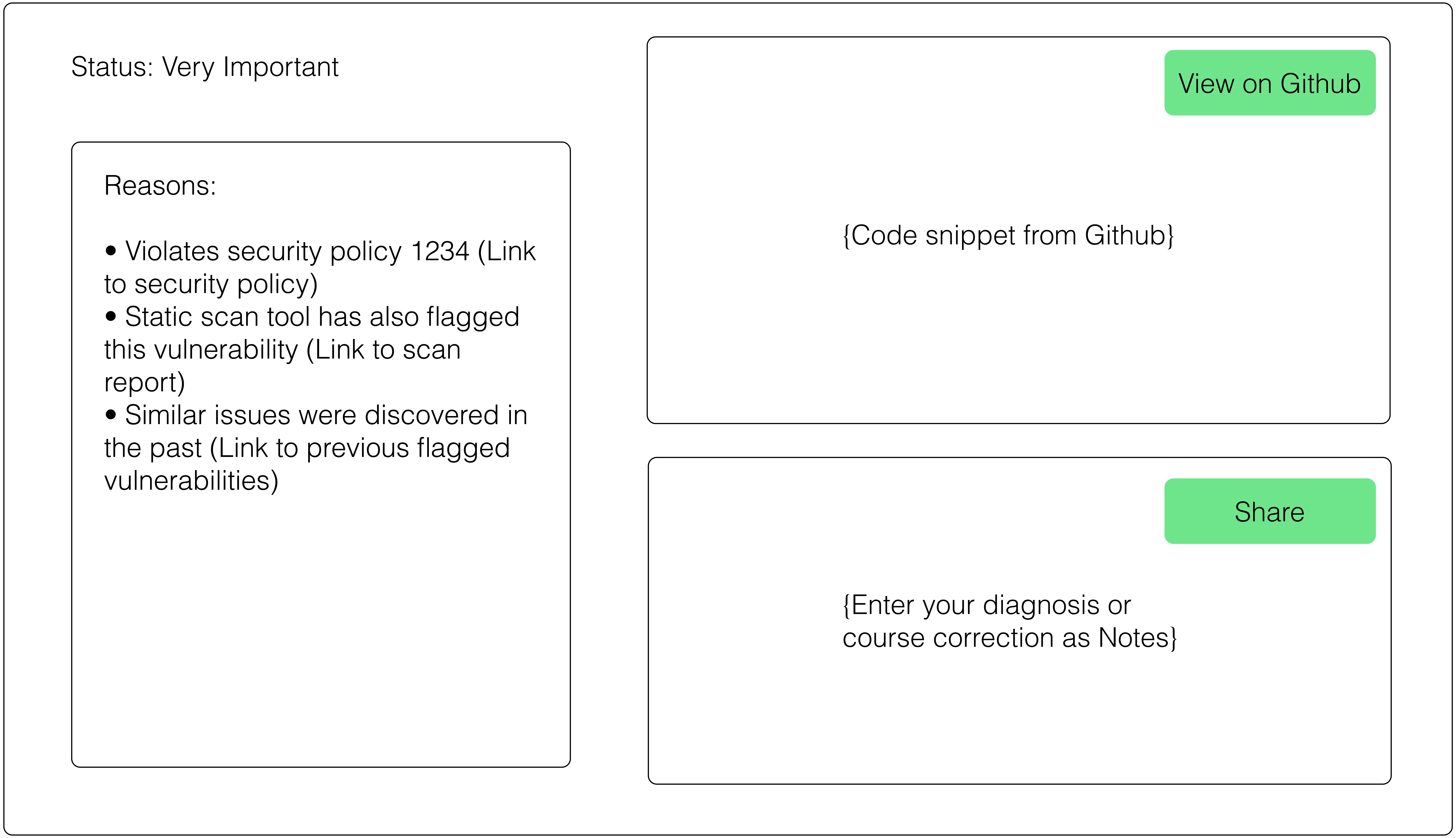
Security tasks

- Very Important - SDK 3.4 release (Jira ticket) (Confluence page / Design spec)
- Important - SDK 3.x dynamic instrumentation testing (Jira ticket) (Confluence page / Design spec)

AWS infrastructure security

{Externally connected data to demonstrate any form of security vulnerabilities of third-party tools}

Flagged vulnerabilities



Status: Very Important

Reasons:

- Violates security policy 1234 (Link to security policy)
- Static scan tool has also flagged this vulnerability (Link to scan report)
- Similar issues were discovered in the past (Link to previous flagged vulnerabilities)

{Code snippet from Github}

{Enter your diagnosis or
course correction as Notes}