AIRLOCK®

Airlock Partner-Tech-Community Online training

Episode 4 – June 2025

Airlock Anomaly Shield
Airlock IAM Config Automation

Agenda

15:00	Welcome	Friedrich Oesch
15:05	Anomaly Shield	Stefan Braun
15:45	Airlock IAM Config Automation	Urs Zurbuchen
16:30	Q&A	
17:45	End	

All times in CEST (UTC+2)

Airlock Partner-Tech-Community

- WAAP and Access Management
  - Technical disciplines
  - Protocols
  - Integration
  - 3rd-party products
  - Web technologies
- Engineers at our partners are a **key resource**

Goals for *Airlock Partner-Tech-Community*

Confidence

Know How

Solution Design

Successful Projects

Profit

Already available

Presentations

Videos

Academy

Forum

Strong Pre-Sales Team

Friedrich Oesch
Senior Security Consultant

Stefan Braun
Senior Security Consultant

Urs Zurbuchen
Senior Security Consultant

Feedback survey will follow after this session.

partner-tech-community@airlock.com
for further wishes and topics.

AIRLOCK®

Airlock Anomaly Shield

Quick start

Stefan Braun
Senior Airlock Security Consultant

Anomaly Shield

Field-proven protection against automated attacks as a part of Airlock WAAP

Mutual complementation

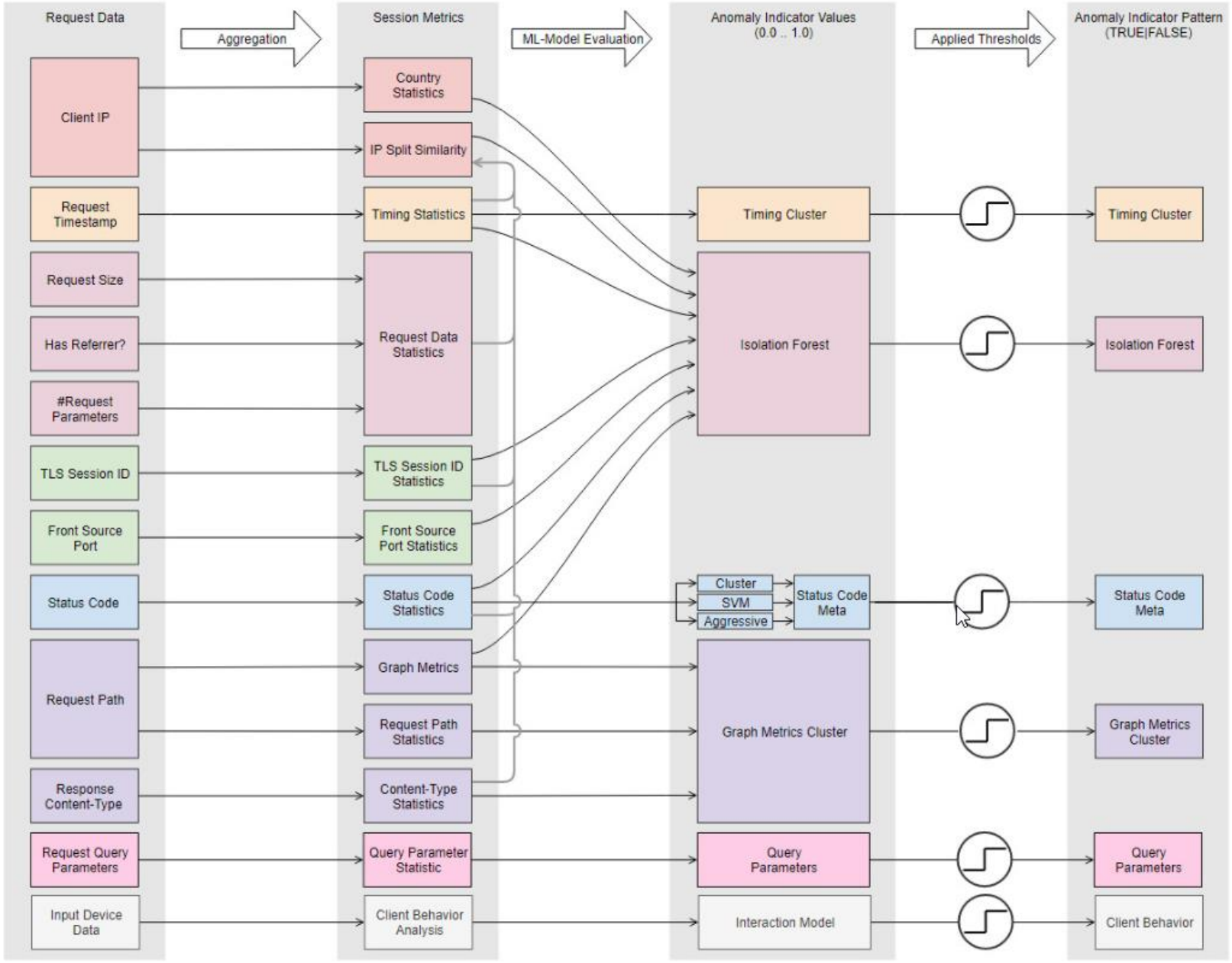
Airlock Gateway

Deny Rules
IP Blacklists

+

AI based Anomaly
Session Detection +
advances Bot Defense

ML – Anomaly Shield



Anomaly Indicators

- Timing Cluster
- Isolation Forest
- Status Code Meta
- Graph Metrics Cluster
- Query Parameters
- Client Behavior

PhD in Data Science??

Save yourself the time!

What changed in 8.4?

Starting with Anomaly Shield

35 days wait

Too much effort

Manual configuration

In production only

Interpretation of results

Airlock Anomaly Shield

Set up

10 min.

- Check prerequisites (e.g. session handling)
- Switch on Anomaly Shield
- Exclude pentests and vulnerability scans

Collect

< 1 day

- Automatic data collection
- At least 500 sessions
- As much “real" traffic as possible from the productive environment.

Configure

10 min.

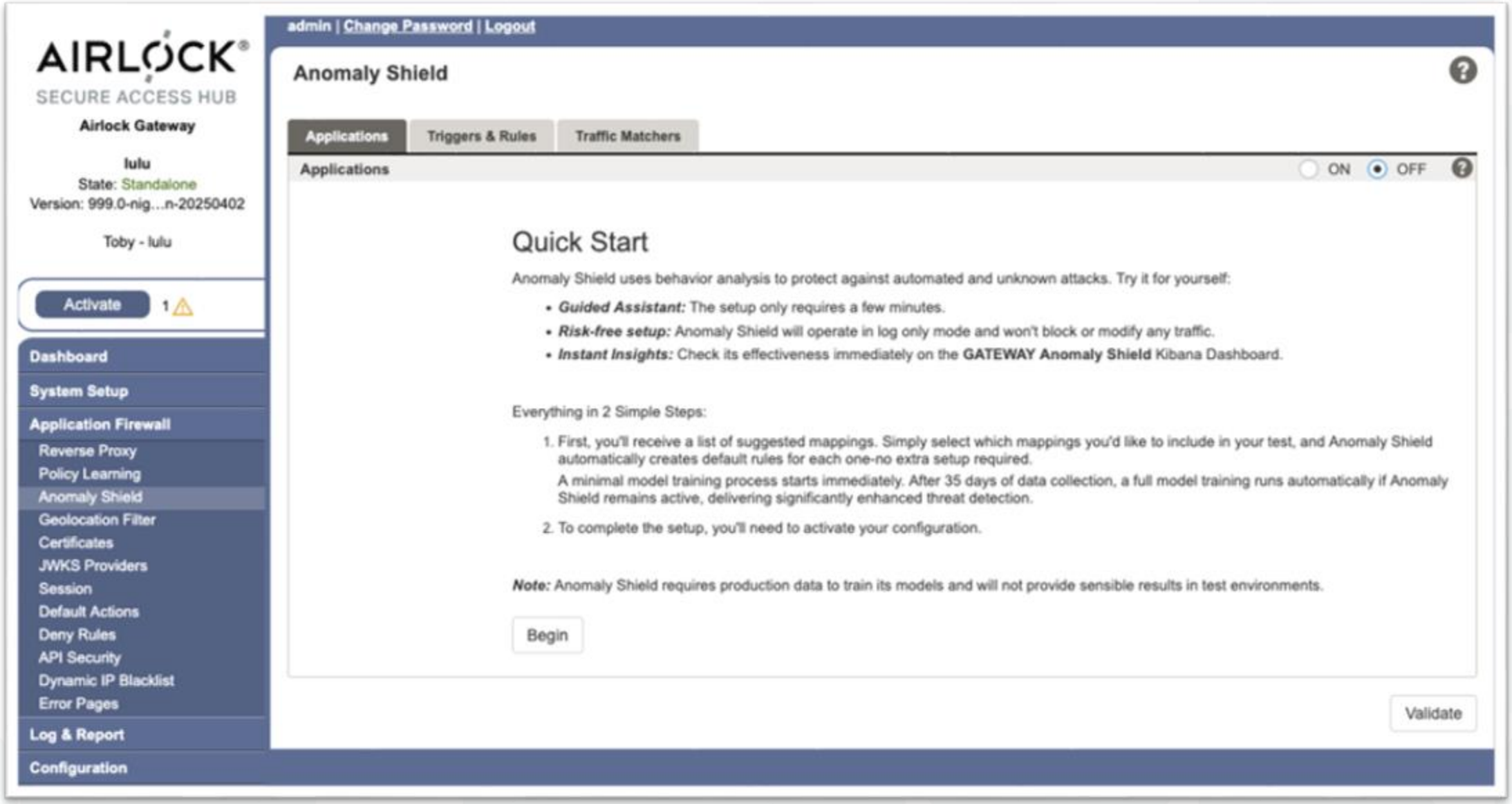
- Use default sensor configuration
- Start training
- Use generated model

Protect

Continuous Monitoring

- Protection is active
- Usual monitoring + SIEM
- Kibana and Elastic Search
- Adjust sensitivity if necessary
- No re-learning for normal app adjustments

Quick Start with Anomaly Shield



Quick Start with Anomaly Shield

Mapping recommendation

Immediate training

No license required

Automatic configuration

Log-only

Less than 5 minutes

Query Parameter Model with Body Parameters

Broken Access Control
(A01:2021)

Injection
(A03:2021)

Security Misconfiguration
(A05:2021)

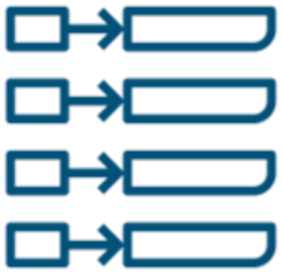
Identification and Authentication Failures
(A07:2021)

Software and Data Integrity Failures
(A08:2021)

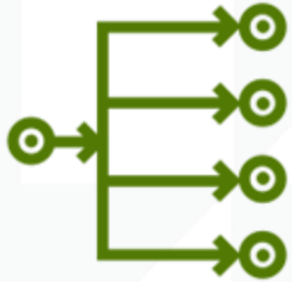
Server-Side Request Forgery
(A10:2021)

Many attacks target exposed web forms

Anomaly detection on forms



Anomalies may be the number of body parameters



Anomalies may be the number of values in a body parameter

Properties of the Parameter Model

Name unchanged

Authenticated Users

No configuration

Power Users

Overload protection

Effective against password spraying and credential stuffing

Migration to Gateway 8.4

ColdDB automatic upgrade

Model retraining required

QPM Model requires 35 days of data to train.
We recommend to enable automatic retraining

Q & A – your feedback please

AIRLOCK®

For additional information:

Your personal contact:

Stefan Braun
Senior Security Consultant
Application Security Solutions
Tel.: +49 1515 6866 821
Email: stefan.braun@airlock.com

AIRLOCK®

Airlock IAM
Config Automation

How to get started and never stop going ☺

Urs Zurbuchen
Senior Security
Consultant

The Plan

- Switch to YAML config
- Structure of the YAML config
- Picking up speed: easy config changes
- By the power of Git
- Config Snippets

Why A New Config Format ?

- medusa-configuration.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<medusaConfiguration xmlns="http://www.ergon.ch" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ergon.ch medusa-config.xsd" medusa-version="8.4">
  <plugin class="com.airlock.iam.admin.app.application.configuration.Adminapp" id="adminapp" uuid="a25f0193-6c34-44eb-9708-cf7ac234cca3">
    <pluginProperty name="accessControl">
      <plugin uuidref="2e2e41d5-5bca-450b-bc88-b1c0b273a9ba"/>
    </pluginProperty>
    <pluginProperty name="administrators">
      <plugin uuidref="b0ade70b-10fb-4e58-8b72-7abc93085a55"/>
    </pluginProperty>
 <plugin class="com.airlock.iam.admin.application.configuration.administrators.AdministratorsConfiguration" id="Administrator Settings"
uuid="b0ade70b-10fb-4e58-8b72-7abc93085a55">
    <pluginProperty name="administratorsManagement">
      <plugin uuidref="100ae66b-d6be-4127-9131-a973e9d8ad74"/>
    </pluginProperty>
    <pluginProperty name="authenticator">
      <plugin uuidref="27742242-f509-4d12-a7e1-14fbd3e50604"/>
    </pluginProperty>
    <pluginProperty name="passwordService">
      <plugin uuidref="e56b902c-42ad-46ec-9380-2112394625f4"/>
    </pluginProperty>
  </plugin>
```

- Not API
- Not automation-friendly

Start with YAML Config Format

- Convert to YAML config

```
iam config convert -i <instance>
for f in instances/<instance>/{.activated-configs,workingcopies}/*.xml
do
  echo $f
  iam config convert -f "$f" -o "${f/xml/yaml}"
done
rm instances/<instance>/{.activated-configs,workingcopies}/*.xml
```

- Change instance to YAML config

```
grep -q ^iam.config.format instances/<instance>/instance.properties
rc=$?
[[ ${rc} -eq 0 ]] && sed -i -e 's,iam.config.format *= *.*,iam.config.format = yaml,'
instances/<instance>/instance.properties
[[ ${rc} -ne 0 ]] && echo 'iam.config.format = yaml' >>
instances/<instance>/instance.properties
```

Revert to XML Config Format

- Change instance to XML config

```
sed –i –e 's,iam.config.format *= *.*,iam.config.format = xml,'
instances/<instance>/instance.properties
iam reset –i <instance>
sudo systemctl restart airlock-iam-<instance>
```

- Convert to XML config
  - In Config Editor, drag & drop YAML config
  - Activate

YAML Structure & File Format

- Documentation
  - https://docs.airlock.com/iam/latest/index/1738063554373.html#Basic_YAML_document_structure
- Top-level types – defined
  - Global config (aka Main settings)
  - Loginapp
  - Adminapp
  - Transaction Approval
  - API Policy Service
  - Server (aka Service Container)
- Other top-level types
  - Unconnected plugins

Plugin ID

- Technical identifier
  - Alphanumeric + dash (-), underline (_), dot (.)
  - Not required ! unless used by a reference
- If missing
  - Auto-generated as <plugin_name-random_string> for internal use by Config Editor
  - Written to config file upon activation in Config Editor
- References

```
ref: <plugin-id>
```

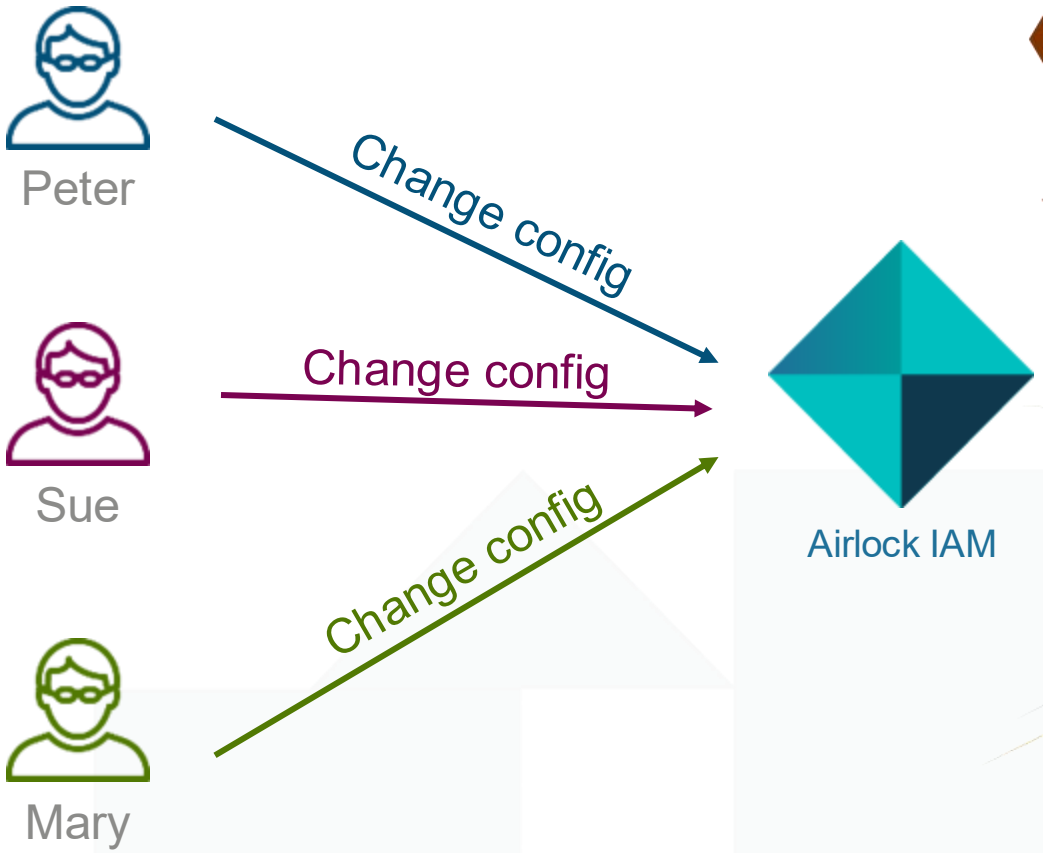
  - Forward references are ok
  - Warning:
    Upon activation, Config Editor moves definition to first use

Edit YAML

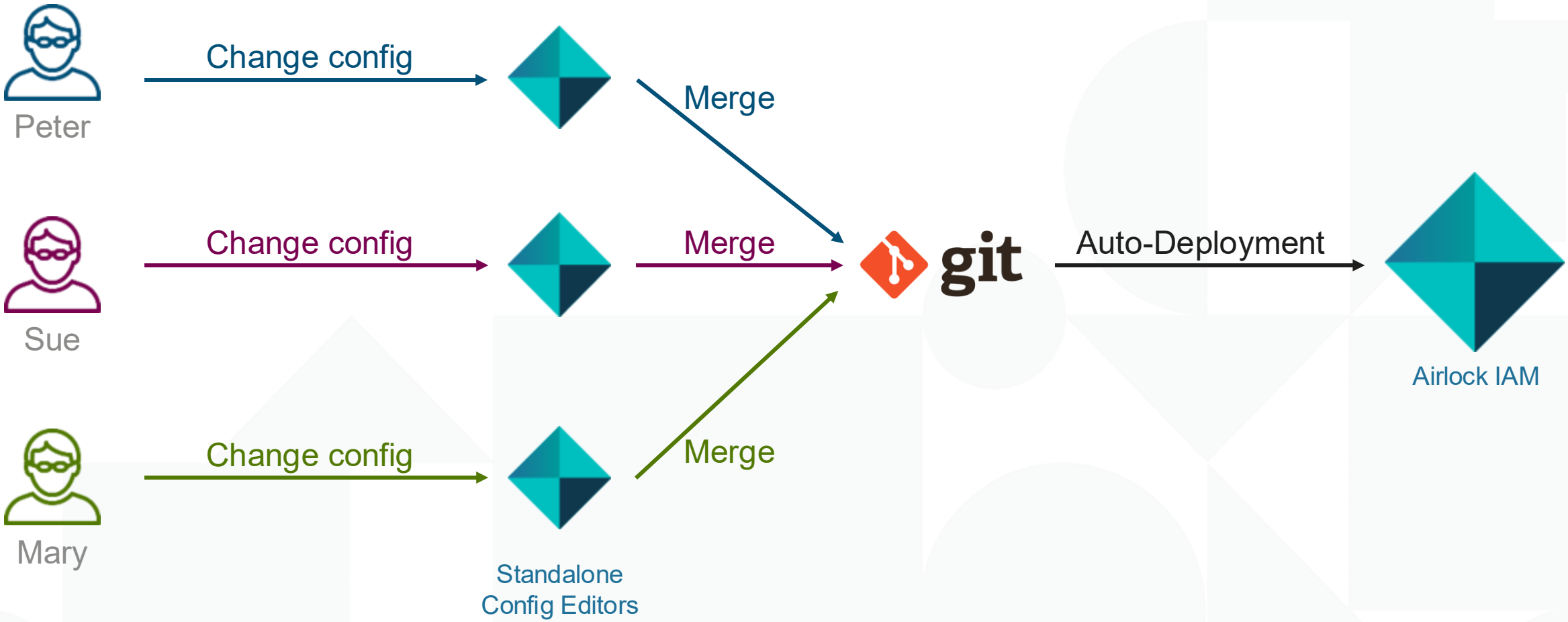
- Visual Studio Code
  - Extension: YAMLfmt for Visual Studio
  - Show all commands (Ctrl-Shift P): Format Document with -> Configure Default Formatter -> YAMLfmt
- Split full YAML config into separate files
  - First split manually
  - Later, use split2files to split into same files
  - Lookout for split2files repository on GitHub (to be published)

```
usage: split2files.py [-h] [-b BASE] [-t TMPDIR] [-k] [-l] [-r] [-v] [-L LEVEL] [-V] file
Split2files - Update Airlock IAM config split into files from iam-config.yaml
positional arguments:
  file                  path to IAM YAML config file
options:
  -h, --help            show this help message and exit
  -b, --base BASE       path to directory with split files
  -t, --tmpdir TMPDIR   path to directory for resulting files (default: ./tmp)
  -k, --keep            if specified, keep files in tmpdir and do not update "base" (default: no)
  -l, --list-ids        if specified, list found plugin ids and containing file (default: no)
  -r, --remove-ids      if specified, remove unreferenced plugin ids from output (default: no)
```

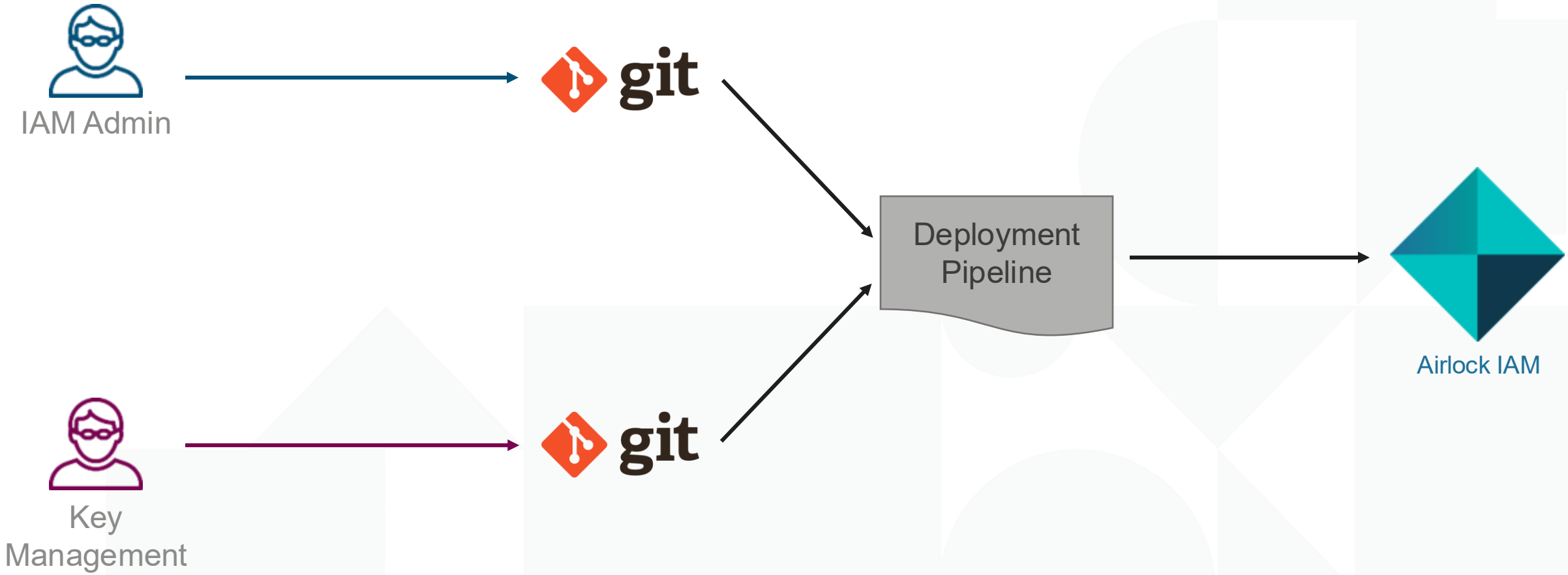
Multi-Admin Support



Multi-Admin Support



Different Responsibilities



Config snippet

- The config snippet for «Identity Proofing with Airlock IAM» will be published here:
  - https://github.com/airlock/airlock-iam-examples/tree/main/identity-proofing-with-airlock-iam

Feedback survey will follow after this session

partner-tech-community@airlock.com
for further wishes and topics

AIRLOCK®

Airlock

Airlock Partner-Tech-Community

partner-tech-community@airlock.com