Shared Signals

TO MAKE ZERO TRUST WORK – WE NEED TO TALK WITH EACH OTHER

Rasmus Schewenius Lund, Solutions Engineer

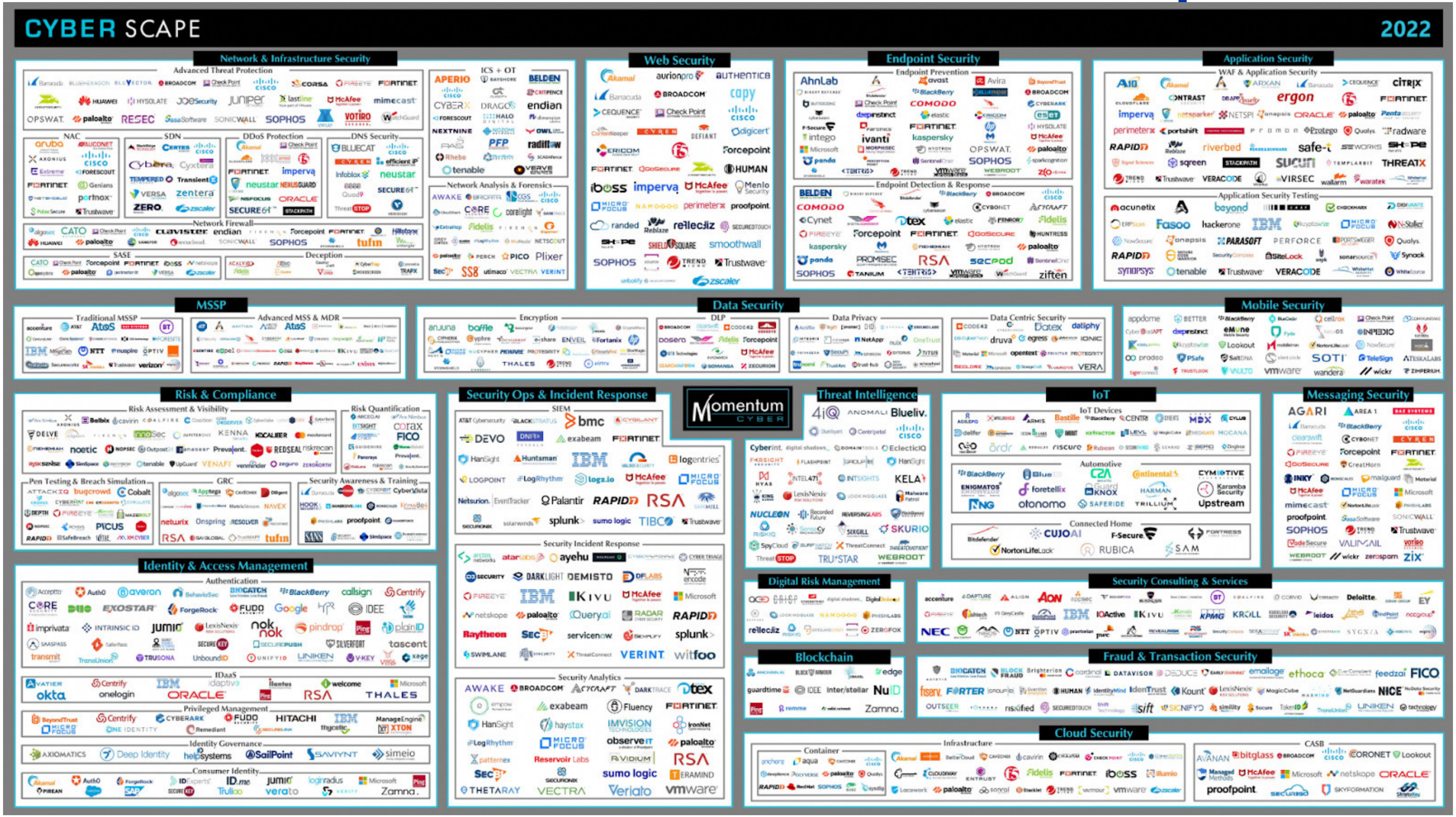
SailPoint®

ПРИВЕТ
Hello
Bonjour
你好
Hallo
Hi!
HOLA
ホア
Salut
OLÁ
HI!

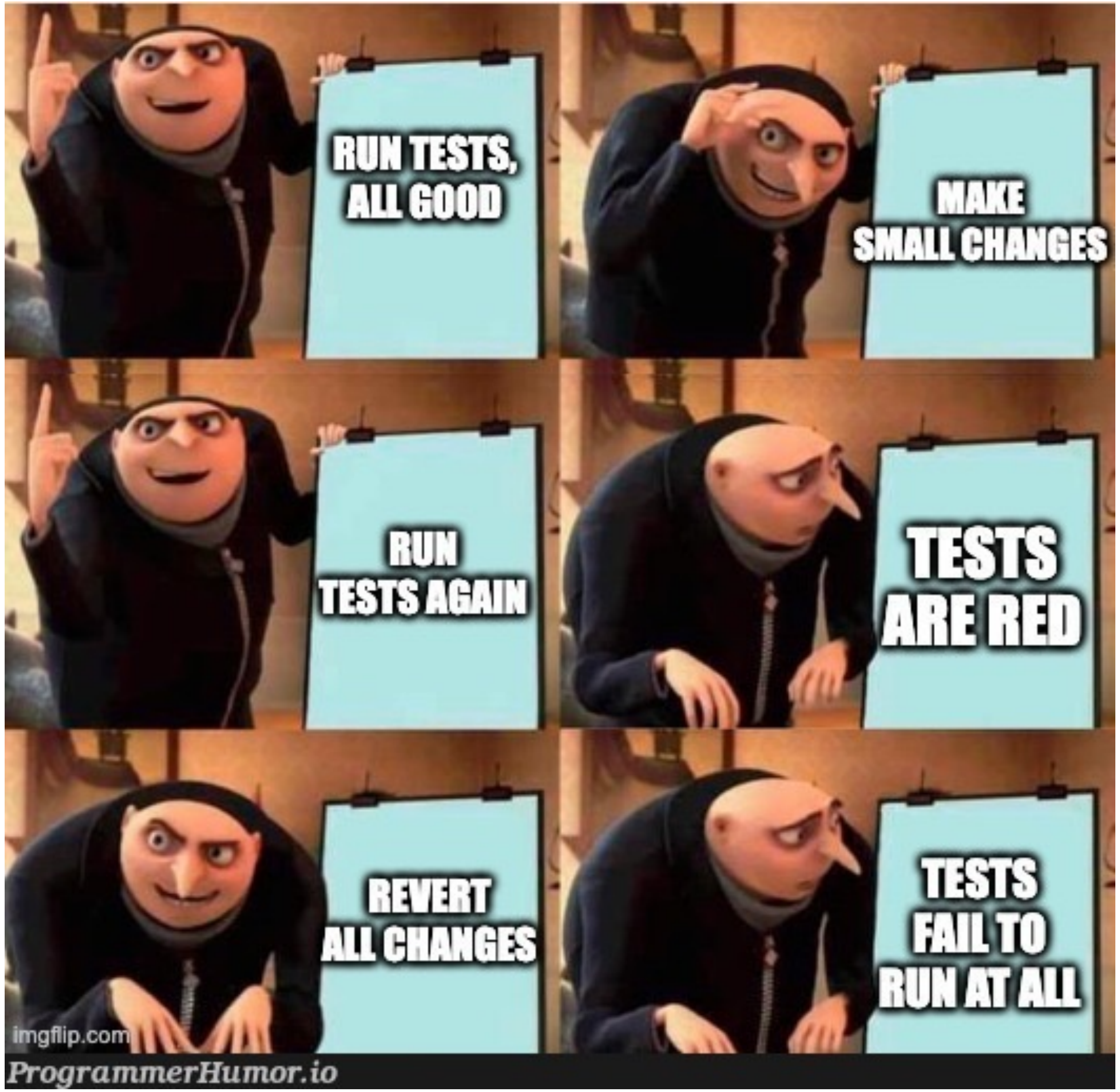
Why is this important?

© 2023 SailPoint Technologies, Inc. All rights reserved.

Have a look at the vendor landscape...



You can cobble stuff together (but its not that easy)



Let’s talk about standards

SCIM

SAML

OAuth / OpenID

FIDO2 / Passkeys

Mature

FastFed

Shared Signals

Verifiable Credentials

SCIM Reloaded

Emerging

© 2023 SailPoint Technologies, Inc. All rights reserved.

Shared Signals

OpenID®

What is it?

Pub/Sub method for sharing real-time events about identities and their context

Why is it useful?

Enables the sharing of security events, state changes, and other signals between security systems and allows them to take protective action.

How common is it?

Still emerging, but major vendors are working on interop support of the standard

https://openid.net/wg/sharedsignals/

© 2023 SailPoint Technologies, Inc. All rights reserved.

Shared Signals Framework

OpenID®

Goal:

Enable the sharing of security events, state changes, and other signals between related and/or dependent systems in order to:

- Manage access to resources and enforce access control restrictions
- Prevent malicious actors from leveraging compromises
- Enable coordination to detect and respond to incidents

Google

amazon web services™

Microsoft

THALES

SailPoint

ORACLE

Prove

TESLA

Foreign & Commonwealth Office

coinbase

vericlouds™

vmware®

onelogin

DUO

okta

verizon media

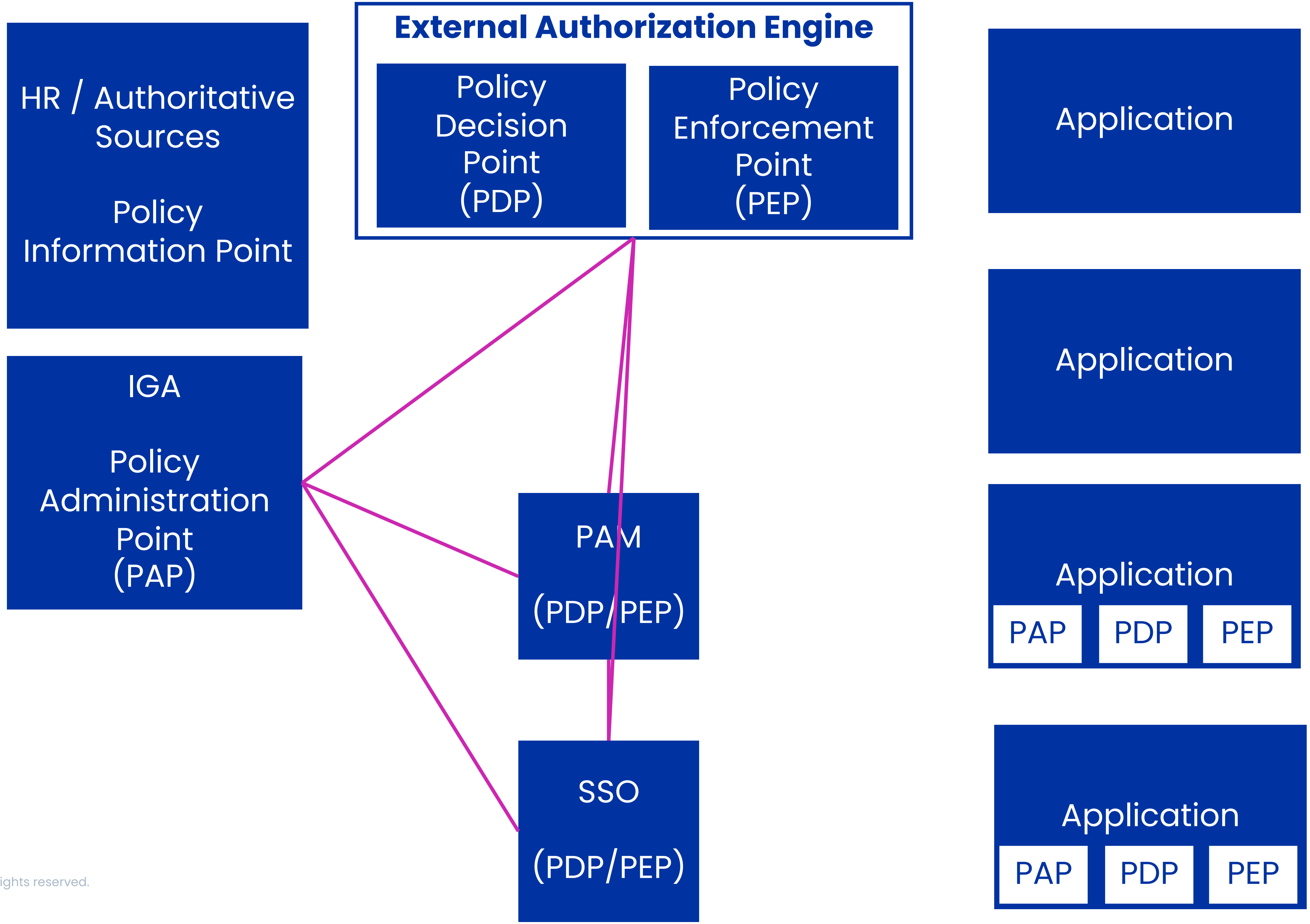
RSA

intuit

PingIdentity®

BlackBerry

yubico



External Authorization Engine

Policy Decision Point (PDP)

Policy Enforcement Point (PEP)

HR / Authoritative Sources

Policy Information Point

IGA

Policy Administration Point (PAP)

PAM

(PDP/PEP)

SSO

(PDP/PEP)

Application

Application

Application

PAP PDP PEP

Application

PAP PDP PEP

© 2023 SailPoint Technologies, Inc. All rights reserved.

The zero-trust security problem

- Users simultaneously logged in to hundreds of services
- Independent sources of truth for various information:
  - Device compliance and security
  - User credentials and authentication
  - User authorization
  - Compromised Credentials
  - Behavioral analytics

Interesting events:

- Modification in user repository
- Access request grant
- User attribute change
- User credential compromise
- User device update
- Fraud detected

Reactions:

- Session revocation
- Forced reauthentication
- Forced password reset
- Reissue credentials
- Modification of profile data

Copyright © SailPoint Technologies Holdings, Inc. 2021. All rights reserved.

Subjects in SSF Events

Subject

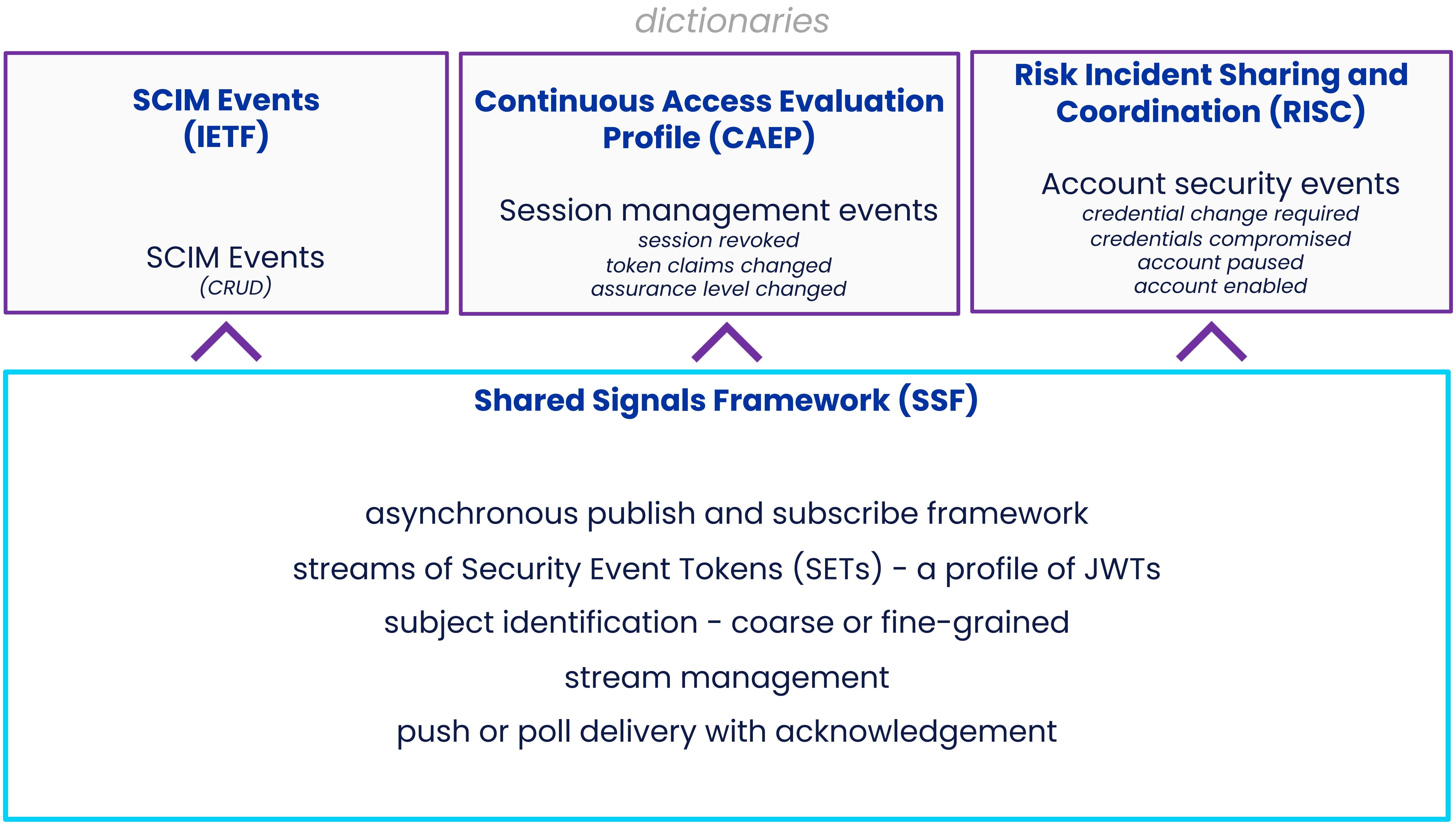
Stream

Event

Transmitter

Receiver

Copyright © SailPoint Technologies Holdings, Inc. 2021. All rights reserved.



dictionaries

SCIM Events (IETF)

SCIM Events

(CRUD)

Continuous Access Evaluation Profile (CAEP)

Session management events

session revoked
token claims changed
assurance level changed

Risk Incident Sharing and Coordination (RISC)

Account security events

credential change required
credentials compromised
account paused
account enabled

Shared Signals Framework (SSF)

asynchronous publish and subscribe framework

streams of Security Event Tokens (SETs) - a profile of JWTs

subject identification - coarse or fine-grained

stream management

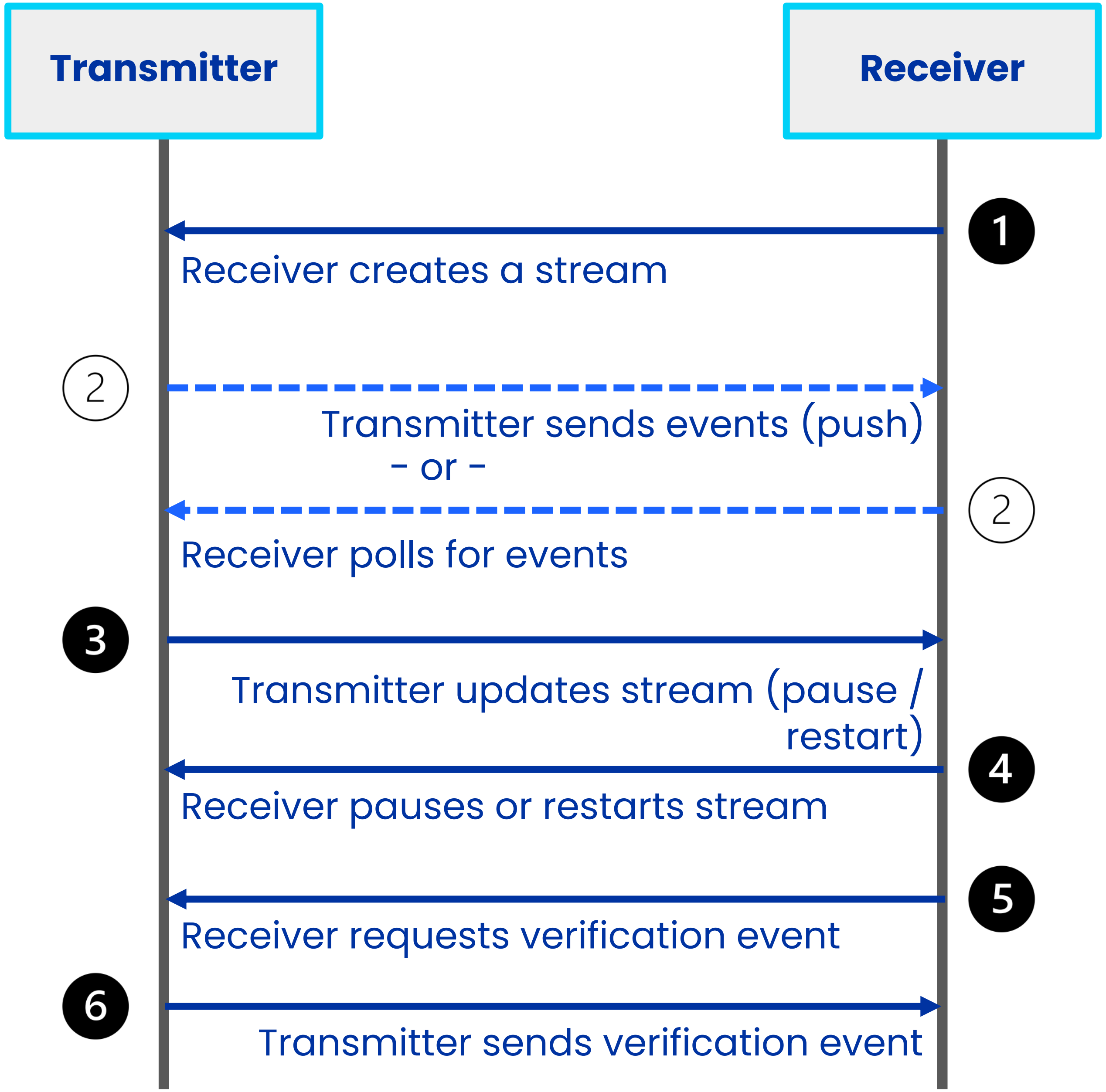
push or poll delivery with acknowledgement

management & transports

Copyright © SailPoint Technologies Holdings, Inc. 2021. All rights reserved.

Stream controls

- Event types are negotiated during stream creation
- Push and poll delivery methods
- Verification events to check liveness of the stream



Transmitter

Receiver

1 Receiver creates a stream

2 Transmitter sends events (push)

- or -

2 Receiver polls for events

3 Transmitter updates stream (pause / restart)

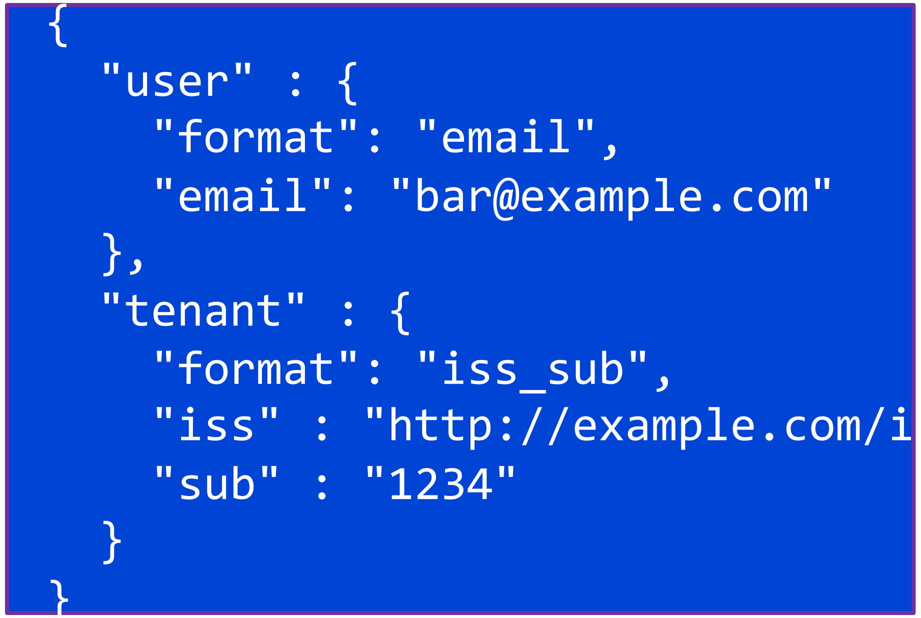
4 Receiver pauses or restarts stream

5 Receiver requests verification event

6 Transmitter sends verification event

Subjects in SSF Events

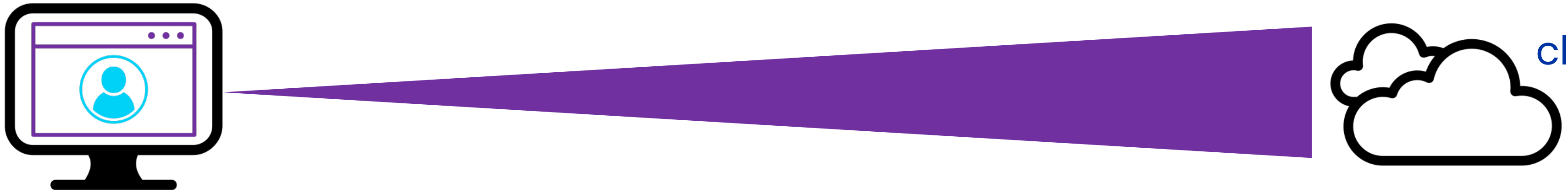
- **Simple** subjects: email, phone number, unique identifier, etc.
- **Complex** subjects:



```
{
  "user" : {
    "format": "email",
    "email": "bar@example.com"
  },
  "tenant" : {
    "format": "iss_sub",
    "iss" : "http://example.com/i
    "sub" : "1234"
  }
}
```

More on event subjects

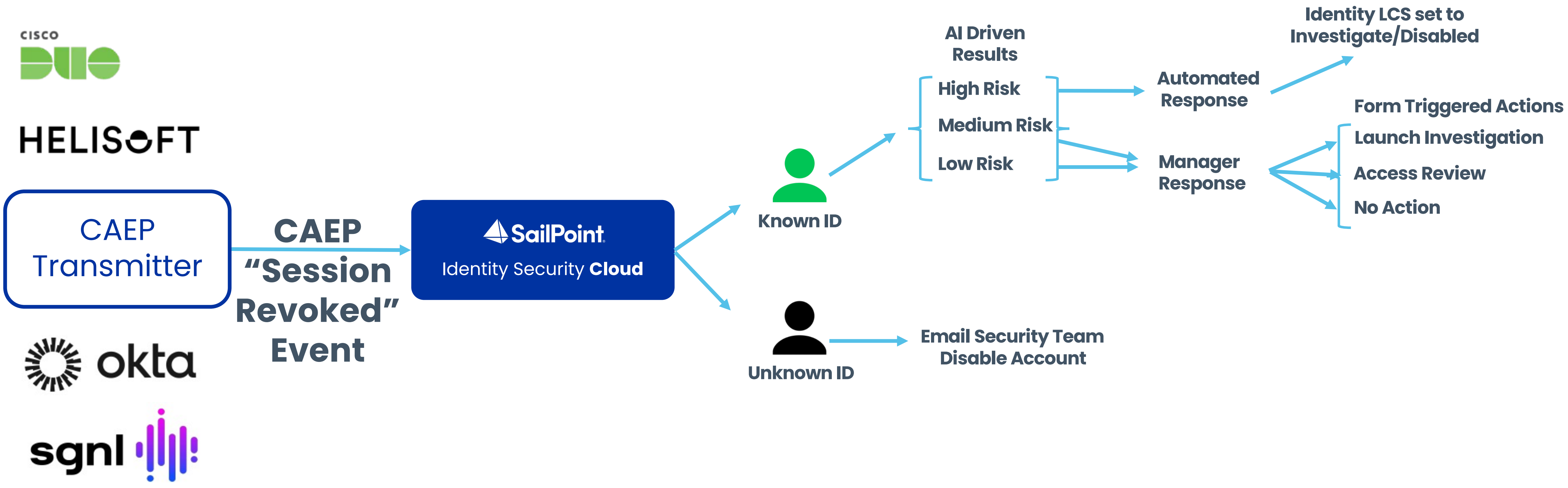
- Specific subjects may be added to or removed from streams
- Authorization may be user-specific
- Subjects may be implicitly included in streams
- A subject value always relates to one principal, but it may be coarse-grained or fine-grained



specific session of a
specific user on a
specific device

cloud service
tenant

Example: Receiving Events



CAEP Transmitter

CAEP "Session Revoked" Event

SailPoint Identity Security Cloud

Known ID

AI Driven Results

High Risk

Medium Risk

Low Risk

Automated Response

Identity LCS set to Investigate/Disabled

Manager Response

Form Triggered Actions

Launch Investigation

Access Review

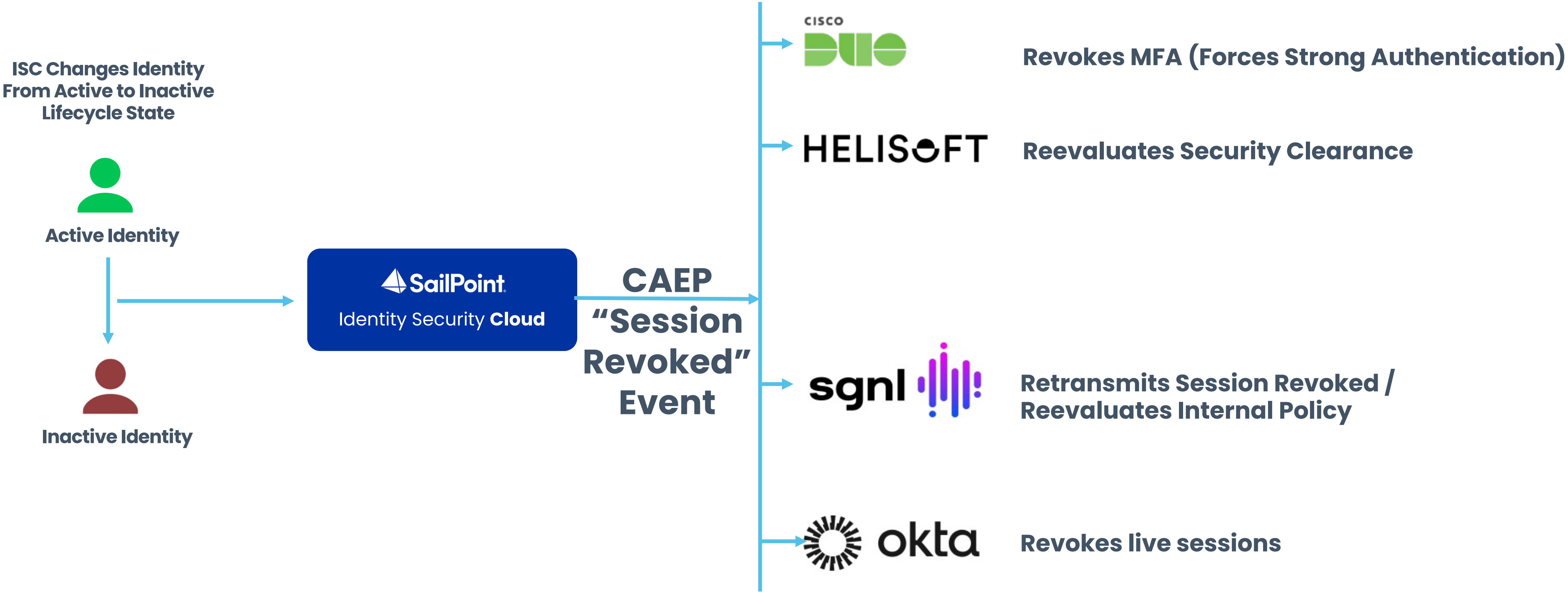
No Action

Unknown ID

Email Security Team Disable Account

© 2024 SailPoint Technologies, Inc. All Rights Reserved.

Example: Transmitting Events



ISC Changes Identity
From Active to Inactive
Lifecycle State

Active Identity

Inactive Identity

SailPoint
Identity Security **Cloud**

CAEP
“Session
Revoked”
Event

CISCO DUO — Revokes MFA (Forces Strong Authentication)

HELISOFT — Reevaluates Security Clearance

sgnl — Retransmits Session Revoked / Reevaluates Internal Policy

okta — Revokes live sessions

2024 SailPoint Technologies, Inc. All Rights Reserved.

SailPoint

Thank You!

Want to read more?

- https://openid.net/wg/sharedsignals/
- https://sharedsignals.guide/
- https://github.com/openid/sharedsignals

Want to get in contact?

Email:
rasmus.lund@sailpoint.com
LinkedIn:
https://linkedin.com/in/rscheweniuslund

©2024 SailPoint Technologies, Inc. All rights reserved.