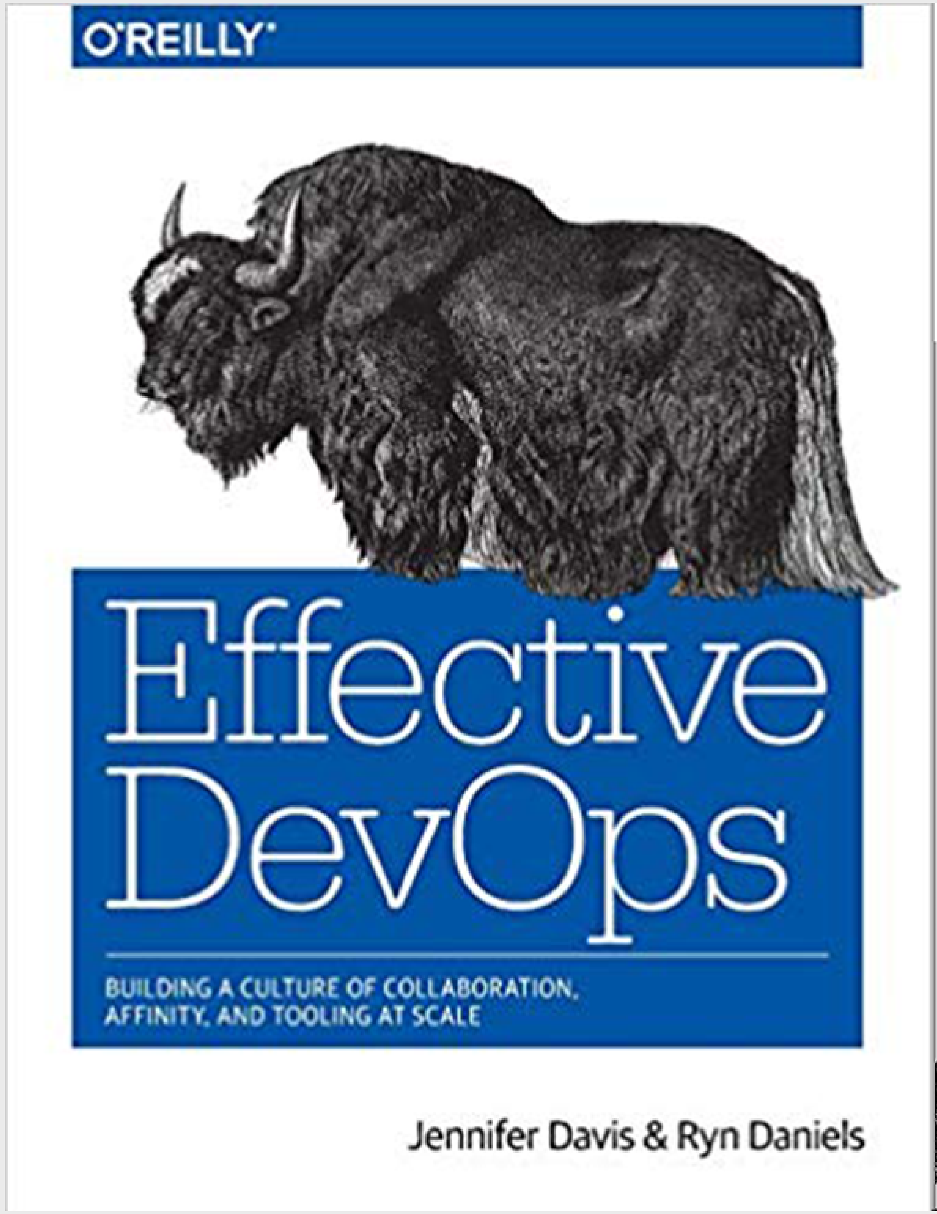
Microsoft

Prioritizing Trust while Creating Applications

Jennifer Davis, Cloud Advocate

she/her

@sigje

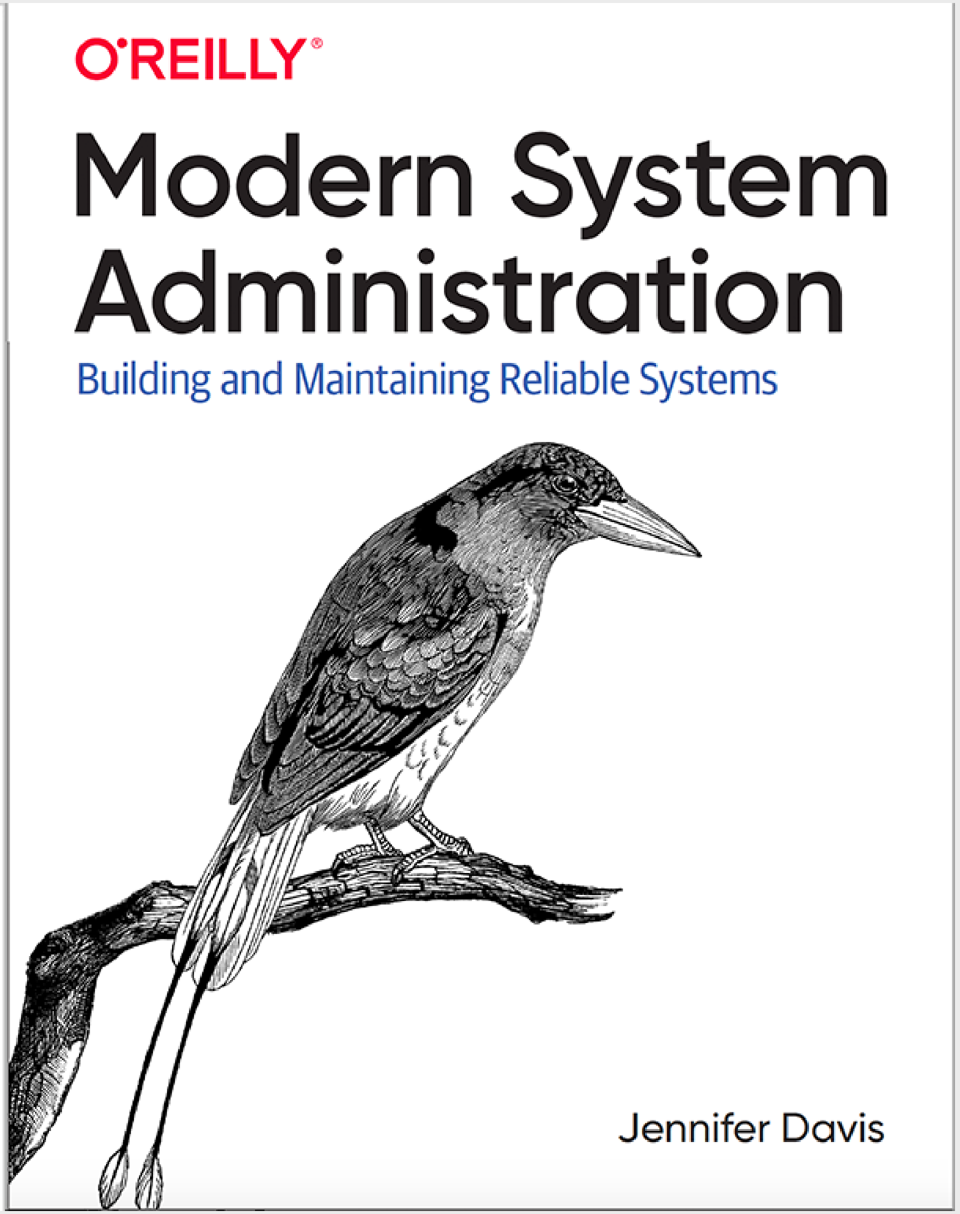


O'REILLY®

Effective DevOps

BUILDING A CULTURE OF COLLABORATION, AFFINITY, AND TOOLING AT SCALE

Jennifer Davis & Ryn Daniels



O'REILLY®

Modern System Administration

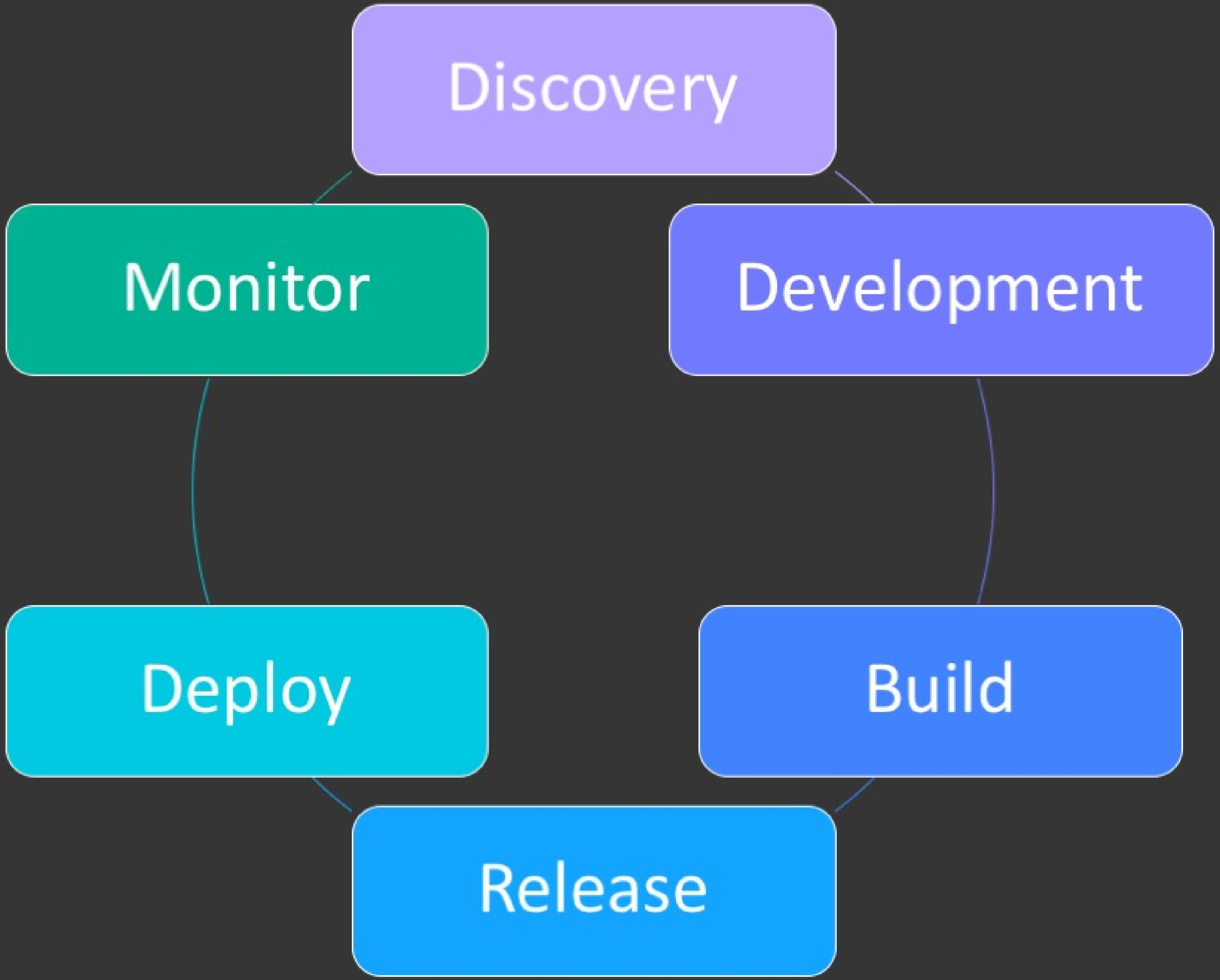
Building and Maintaining Reliable Systems

Jennifer Davis

Trust

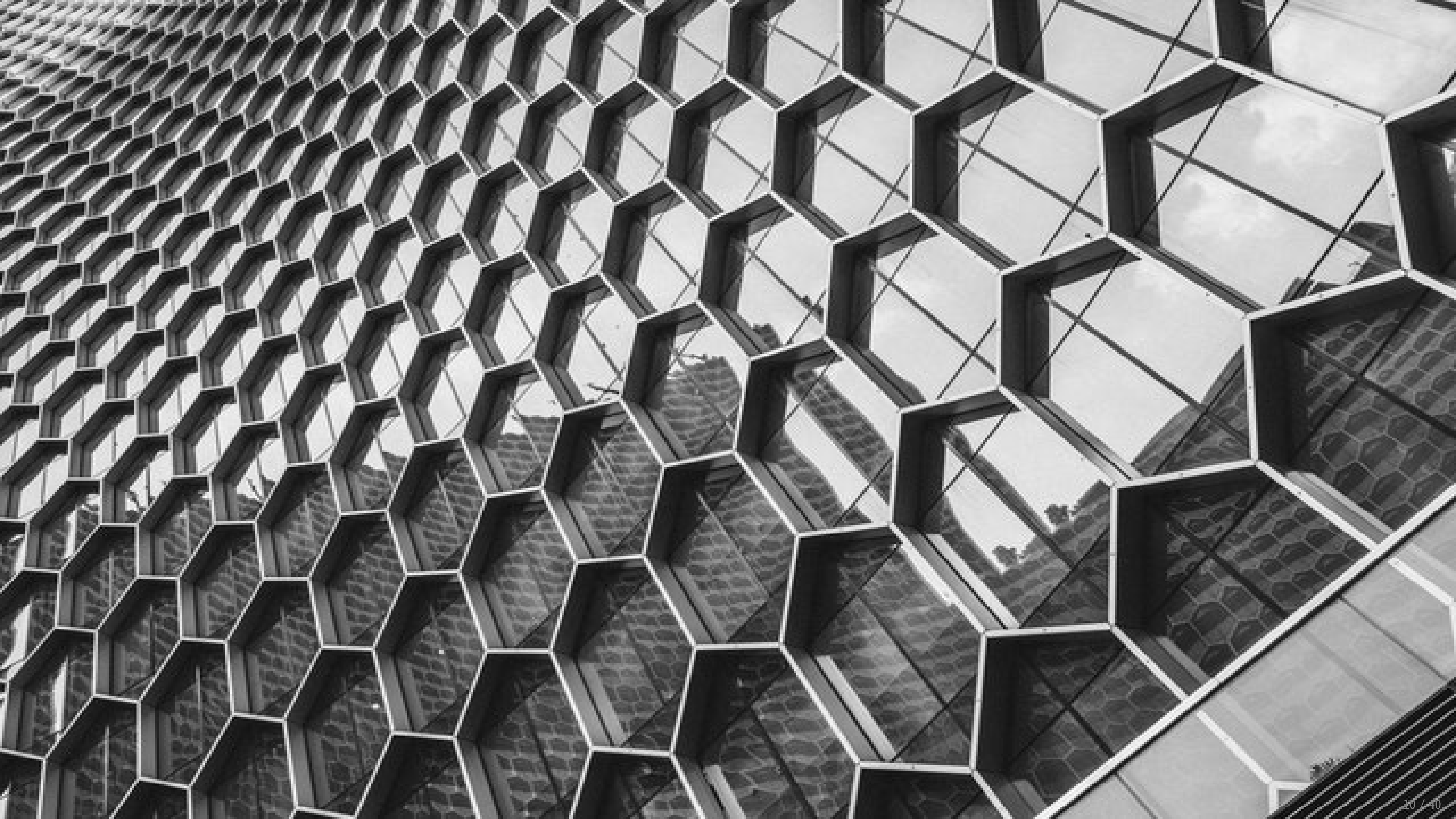
https://haveibeenpwned.com/

KODAK
TIMER
EASTMAN KODAK CO.
ROCHESTER, N.Y.
60
5
10
15
20
25
30
35
40
45
50
55


Discovery
Development
Build
Release
Deploy
Monitor

Agenda

- Establish Common Context
- Build Foundations
- Advancing Principles



Confidentiality

Availability

Integrity

Bug versus Flaw

Motivations

- Financial Gain
- Espionage/Strategic Gain
- Fun/Ideology/Grudge

Build Foundations

Defense in Depth

Snyk State of Open Source Security Report 2019

- 78% vulnerabilities in indirect dependencies
- 37% of open source developers no security testing in CI
- 54% docker image no security testing
- Top 10 docker images contain > 30 vulnerable system libraries

Source: https://snyk.io/opensourcesecurity-2019/

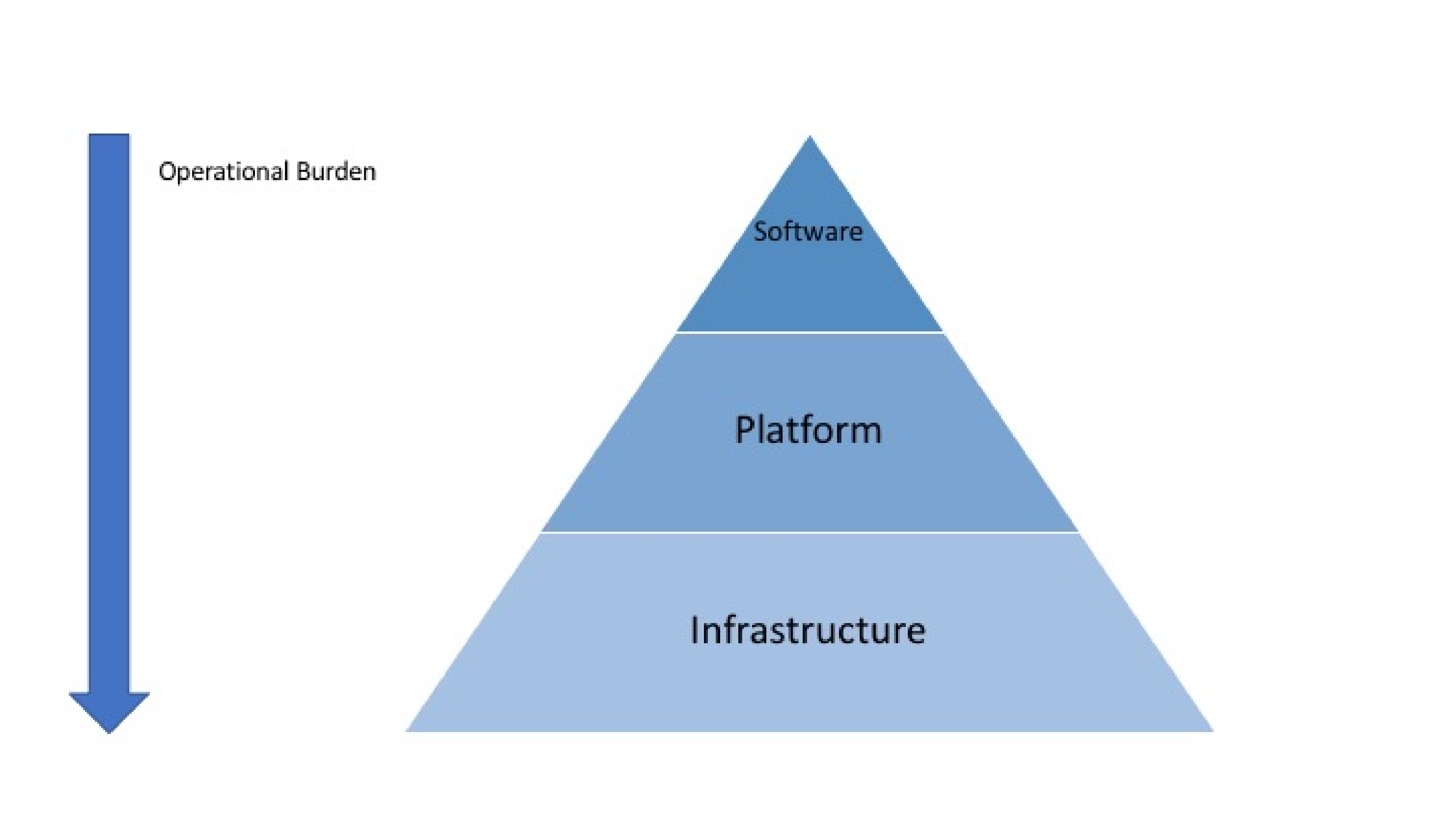
#WOCinTech Chat Attribution 2.0 Generic (CC BY 2.0)

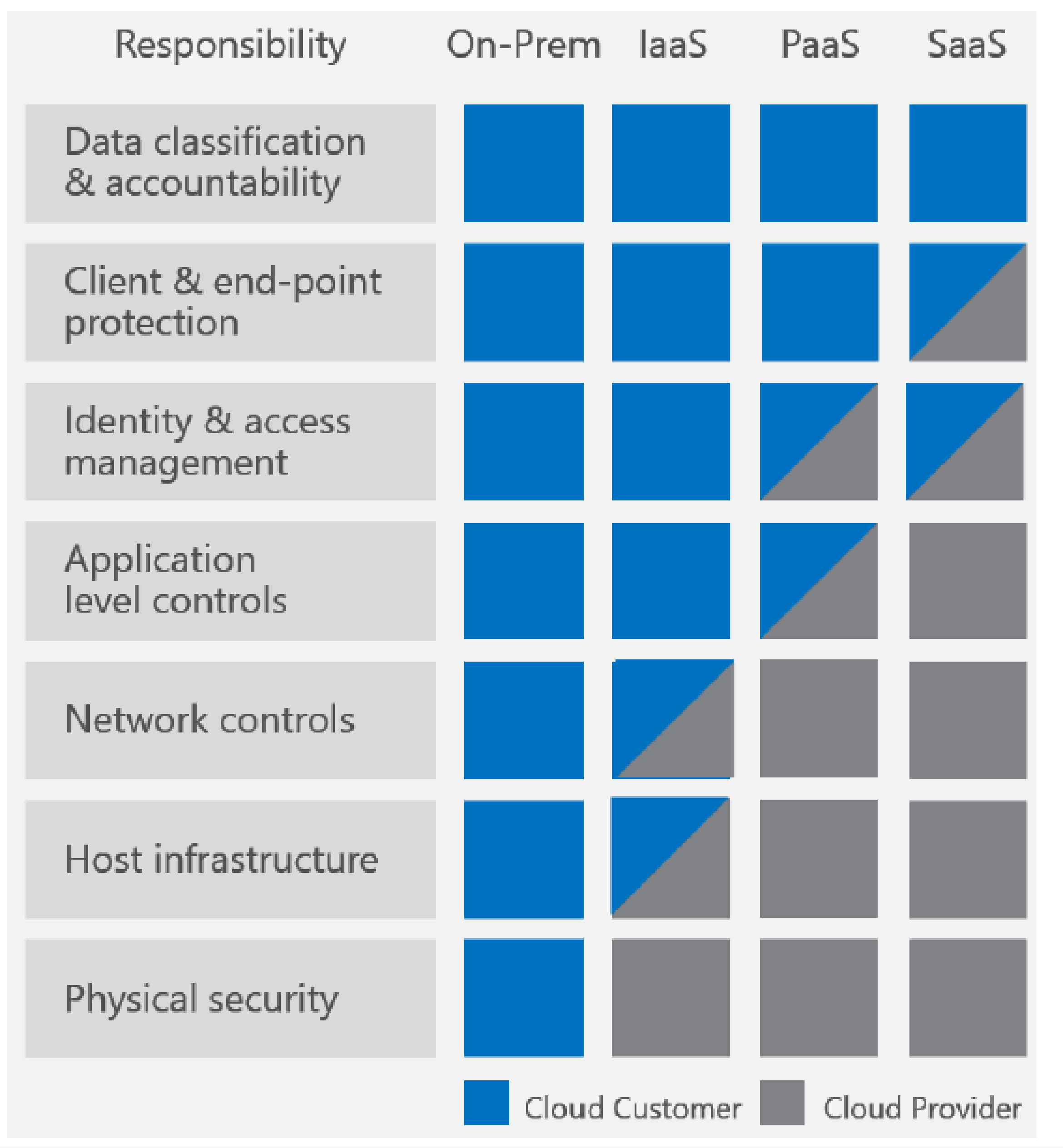
- What can a user see? do?
- What information is logged?
- Approach for failed logins

OWASP: Application Security Verification Standard Project

Threat Modeling

Architectural Trade-offs


Operational Burden
Software
Platform
Infrastructure

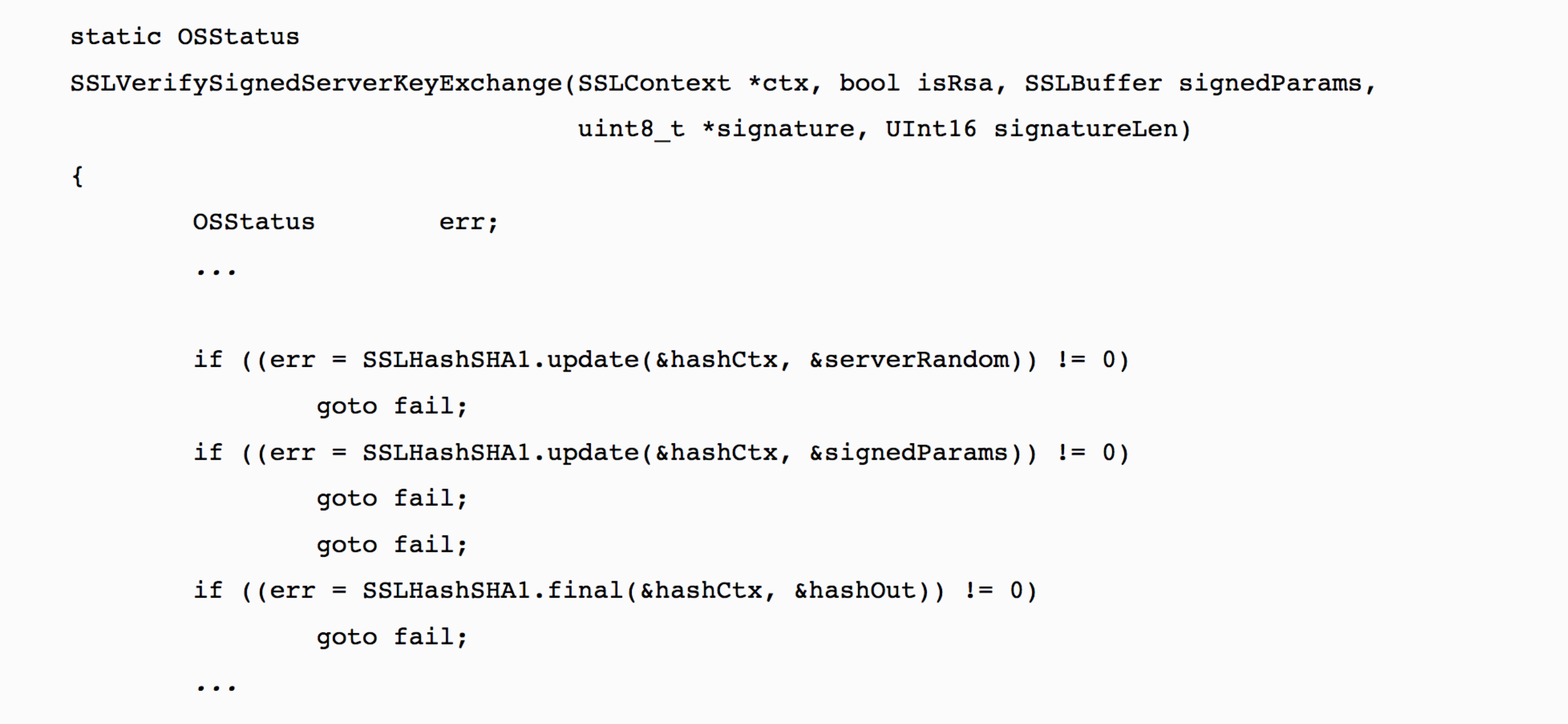


Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	◼
Network controls	🟦	◩	◼	◼
Host infrastructure	🟦	◩	◼	◼
Physical security	🟦	◼	◼	◼

🟦 Cloud Customer ◼ Cloud Provider

Testing Code

Static Code Analysis

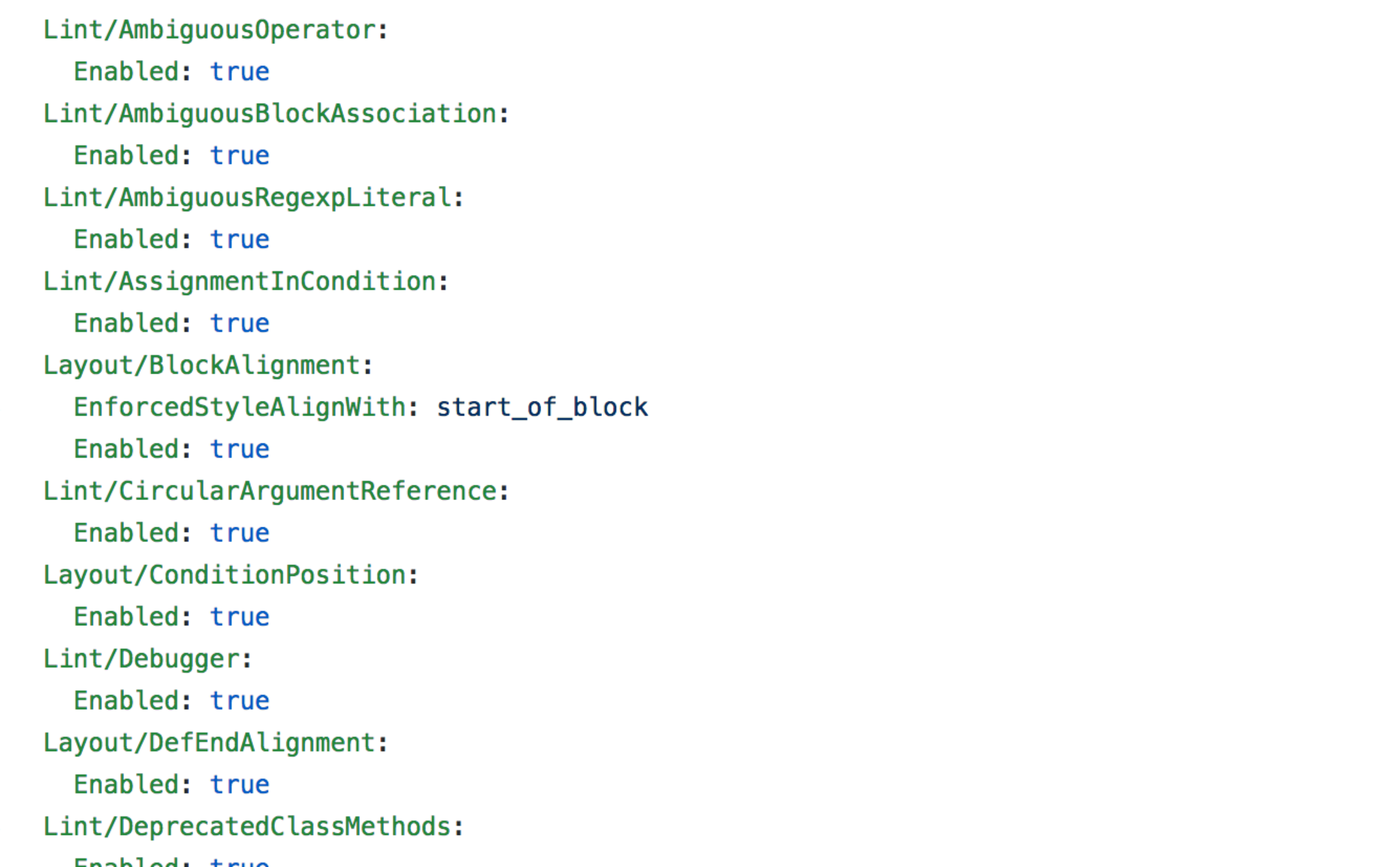


```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
        OSStatus        err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...
```

Source: https://www.imperialviolet.org/2014/02/22/applebug.htm

Coding Standards



```
Lint/AmbiguousOperator:
  Enabled: true
Lint/AmbiguousBlockAssociation:
  Enabled: true
Lint/AmbiguousRegexpLiteral:
  Enabled: true
Lint/AssignmentInCondition:
  Enabled: true
Layout/BlockAlignment:
  EnforcedStyleAlignWith: start_of_block
  Enabled: true
Lint/CircularArgumentReference:
  Enabled: true
Layout/ConditionPosition:
  Enabled: true
Lint/Debugger:
  Enabled: true
Layout/DefEndAlignment:
  Enabled: true
Lint/DeprecatedClassMethods:
  Enabled: true
```

Secure Code Reviews

Planning for Security Escalations

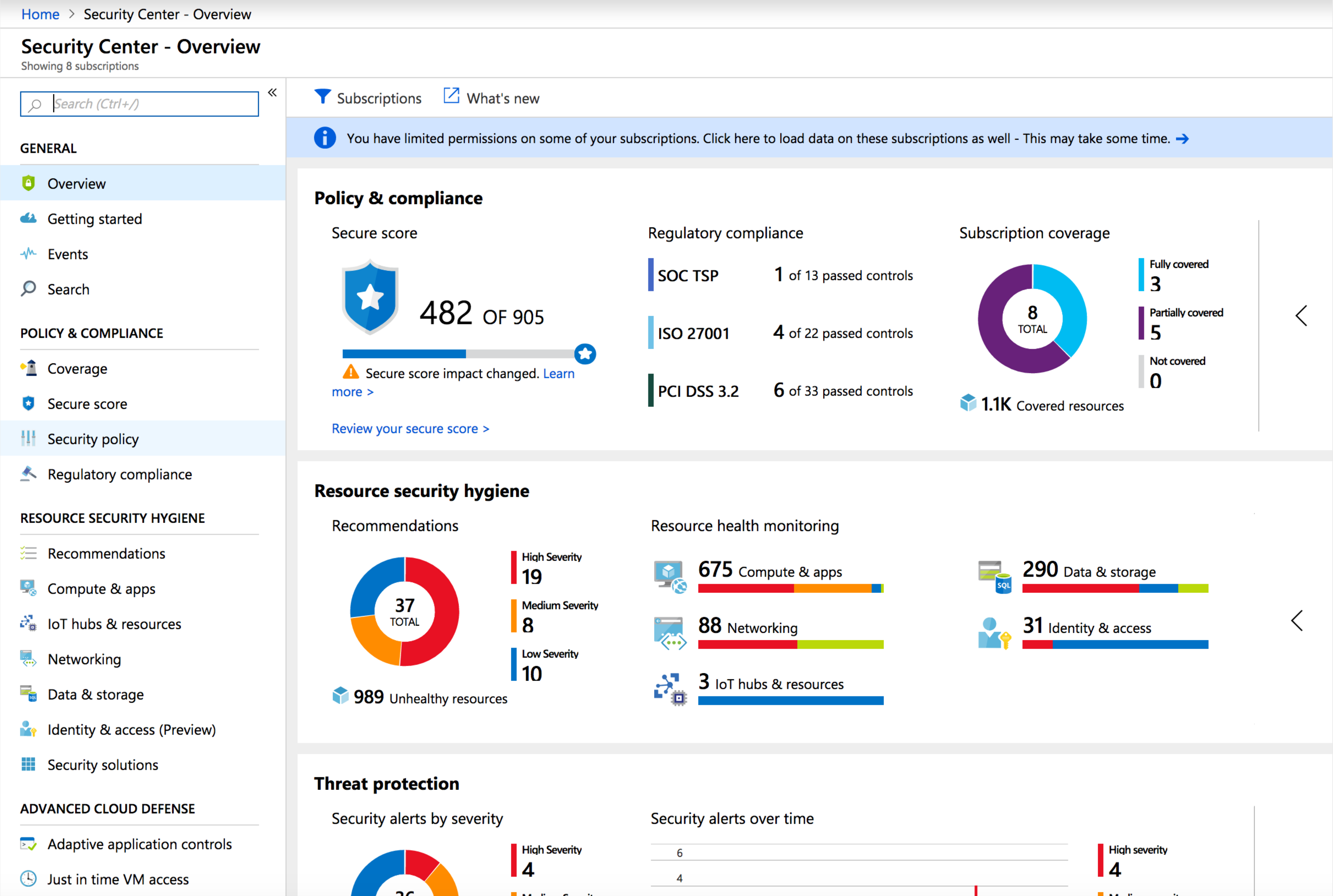
- Identify
- Assess
- Remediate

Incident Response Resource

- Building a Minimum Viable Response Plan: jhand.co/CreateResponsePlan

Leverage your platform's services

Recognize your platform's limits



Home > Security Center - Overview

Security Center - Overview

Showing 8 subscriptions

Search (Ctrl+/)

GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Secure score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- IoT hubs & resources
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access

Subscriptions What's new

You have limited permissions on some of your subscriptions. Click here to load data on these subscriptions as well - This may take some time. →

Policy & compliance

Secure score

482 OF 905

Secure score impact changed. Learn more >

Review your secure score >

Regulatory compliance

SOC TSP	1 of 13 passed controls
ISO 27001	4 of 22 passed controls
PCI DSS 3.2	6 of 33 passed controls

Subscription coverage

8 TOTAL

Fully covered	3
Partially covered	5
Not covered	0

1.1K Covered resources

Resource security hygiene

Recommendations

37 TOTAL

High Severity	19
Medium Severity	8
Low Severity	10

989 Unhealthy resources

Resource health monitoring

- 675 Compute & apps
- 88 Networking
- 3 IoT hubs & resources
- 290 Data & storage
- 31 Identity & access

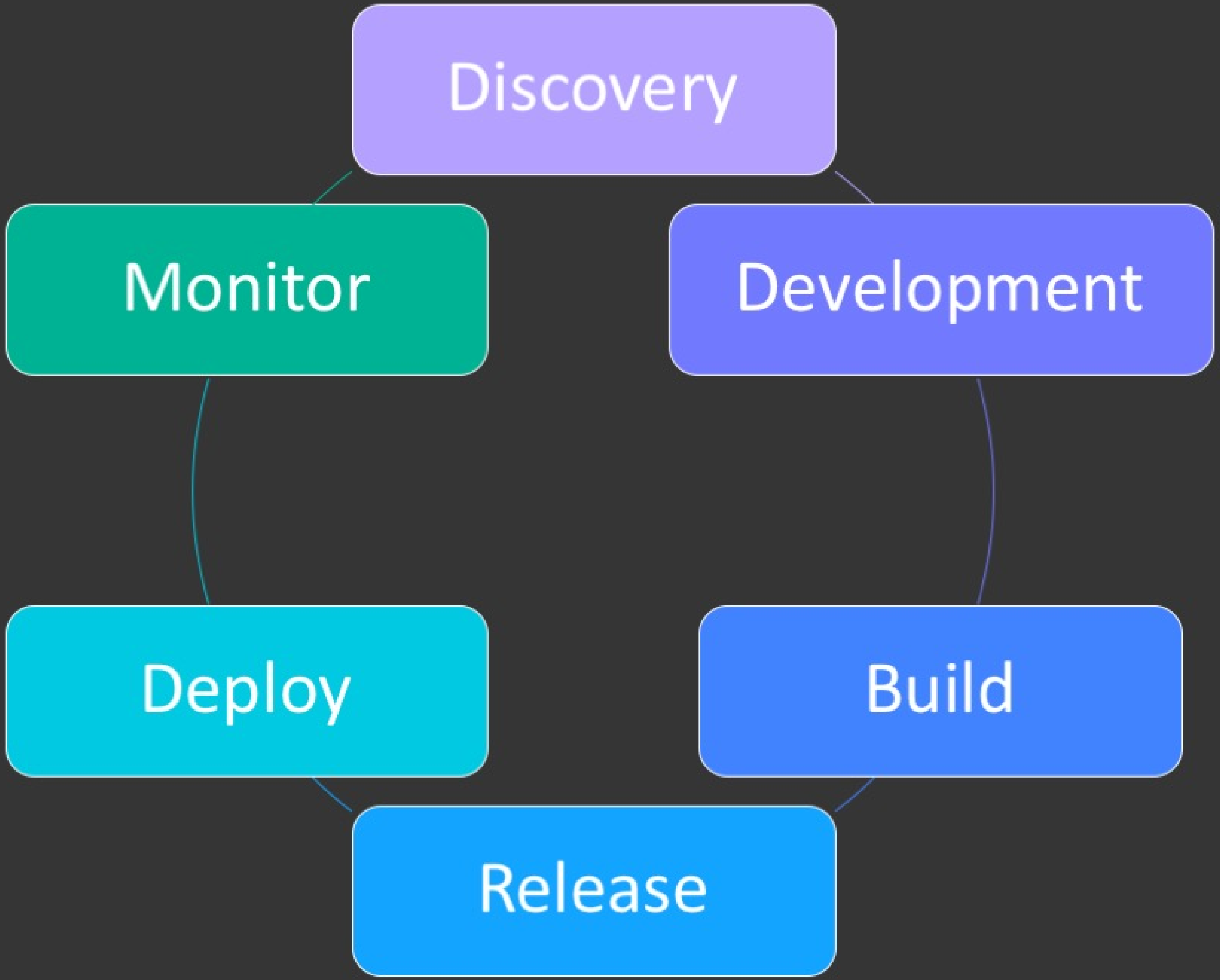
Threat protection

Security alerts by severity

High Severity 4

Security alerts over time

High severity 4



Discovery

Development

Build

Release

Deploy

Monitor

Advancing Principles

Bug Bounty Programs

Capture the Flag (CTF)

- CTF with Google
- CTF Circle - CTF distributed team for Nonbinary Folks and Women

Red Team Exercise

> *Fundamentally, if somebody wants to get in, they’re getting in…accept that. What we tell clients is: Number one, you’re in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated.*
>
> *- Michael Hayden, Former Director of NSA & CIA*

What's Next?

- Identify your security maturity
- Assess valuable practices
- Encourage learning security skills
- Incorporate feedback
- Update threat models

Security is everybody’s job!

Thank you

Email: jennifer@modernoperations.org

🐦 **@sigje**