Securing the Cloud

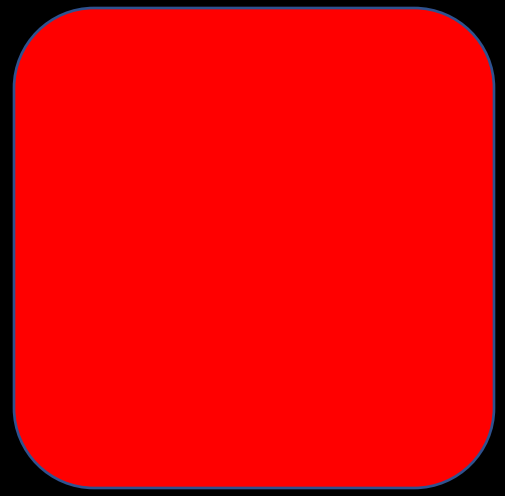
Tactics for Reducing Your Compromise Blast Radius

Blast Radius

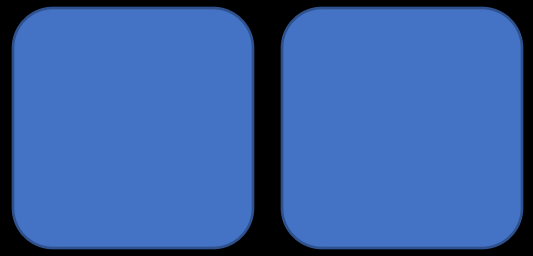
Blast Radius

the distance from the source of an adverse event that impacts a system

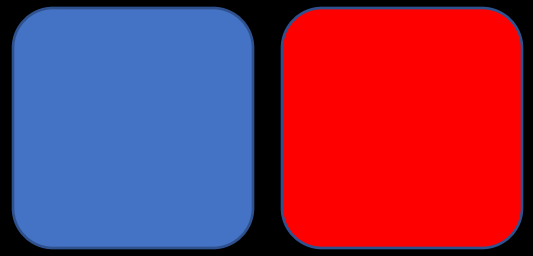
Your System



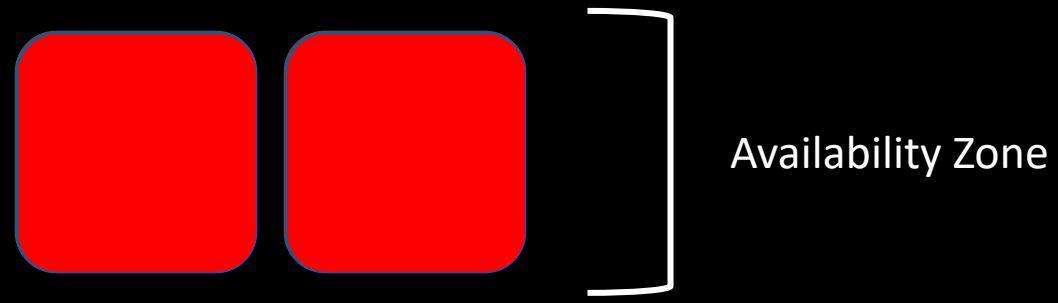
Your System



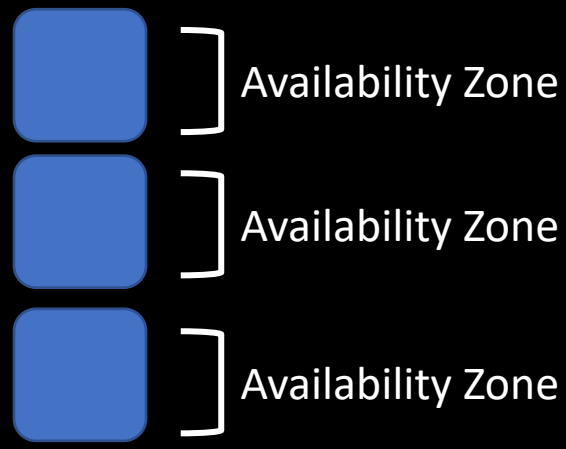
Your System



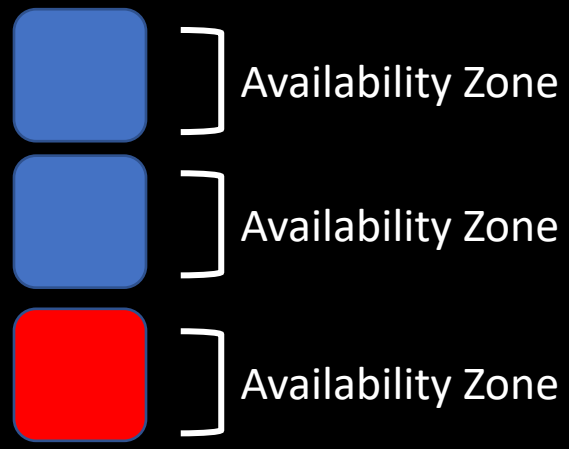
Your System



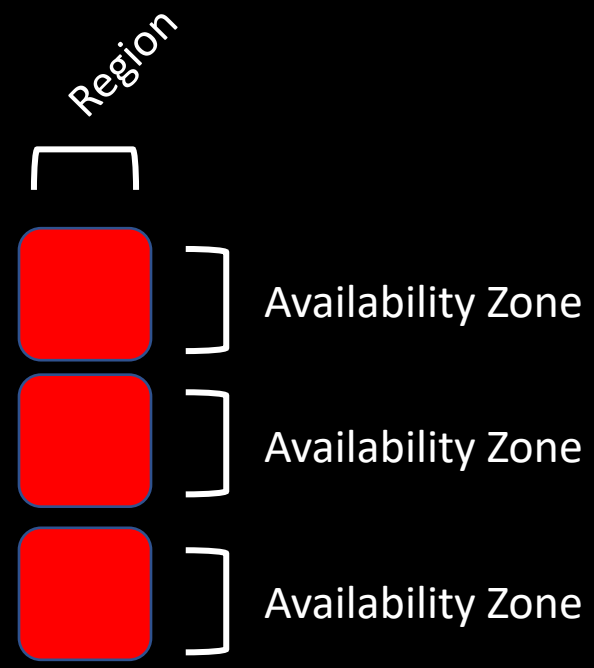
Your System



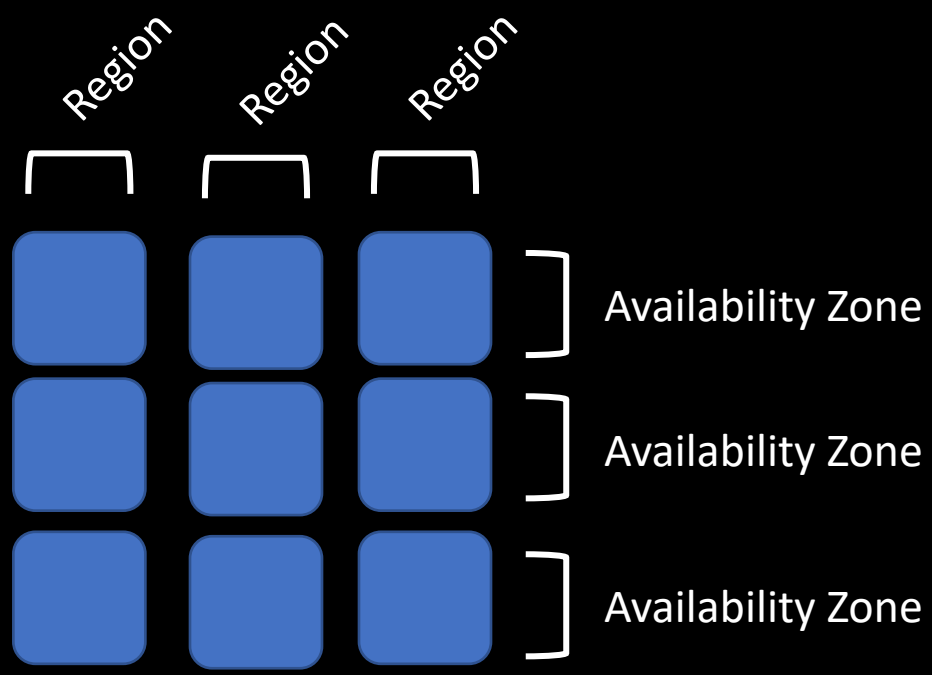
Your System



Your System


Region
Availability Zone
Availability Zone
Availability Zone

Your System

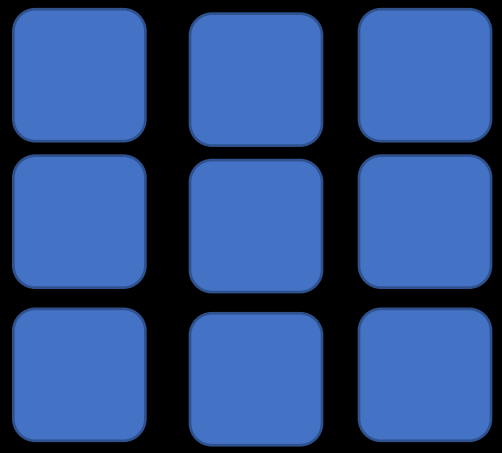

Region
Region
Region
Availability Zone
Availability Zone
Availability Zone

Your System

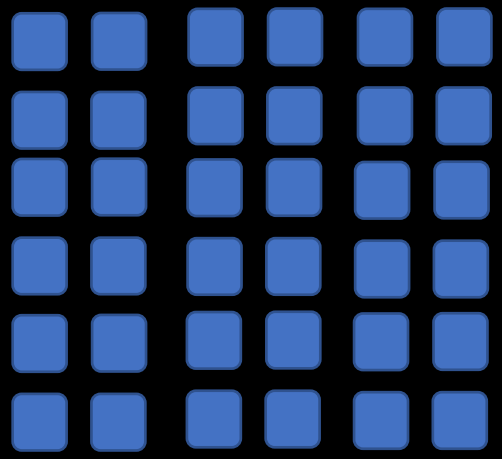
Cell-Based Architecture

Cell-Based Architecture

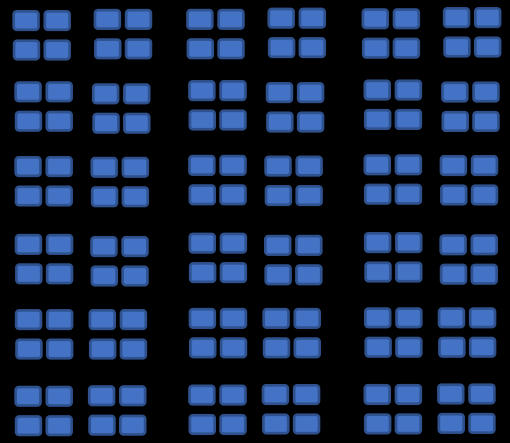
a resiliency-first approach to reducing blast radius



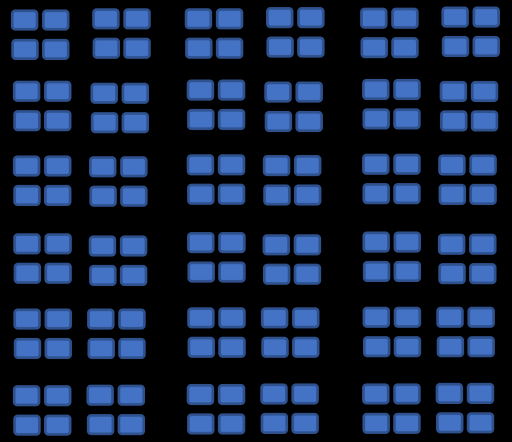
Your System



Your System



Your System



Your System

Benefits of Cell-Based Architecture

- Highly Scalable
- Redundancy in Everything
- Self-healing
- Compatible with Principal of Least Privilege
- Incremental but Continuous Deployment
- Easy to isolate bad actors
- Easy to reason about each cell

Cost of Cell-Based Architecture

- Deep reliance on Tooling
- More complex System
- Architecture may be incompatible with Legacy systems

AWS Well-Architected Framework

AWS Well-Architected Framework

Security Design Principals

Implement Strong Identity Foundation

Enable Traceability

Apply Security at All Layers

Automate Security Best Practices

Protect Data in transit and at Rest

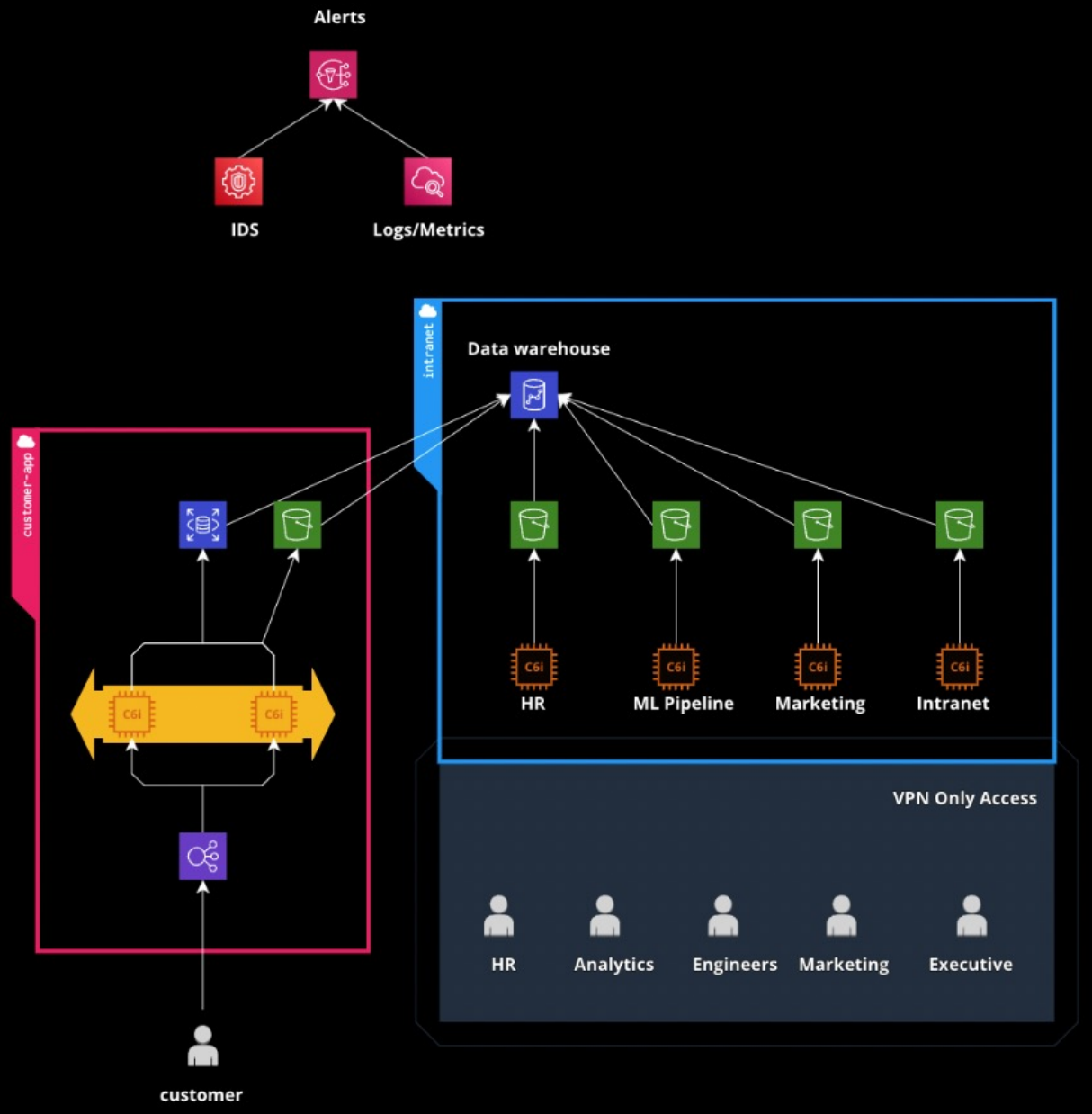
Keep People Away from Data

Prepare for Security Events

Zero Trust

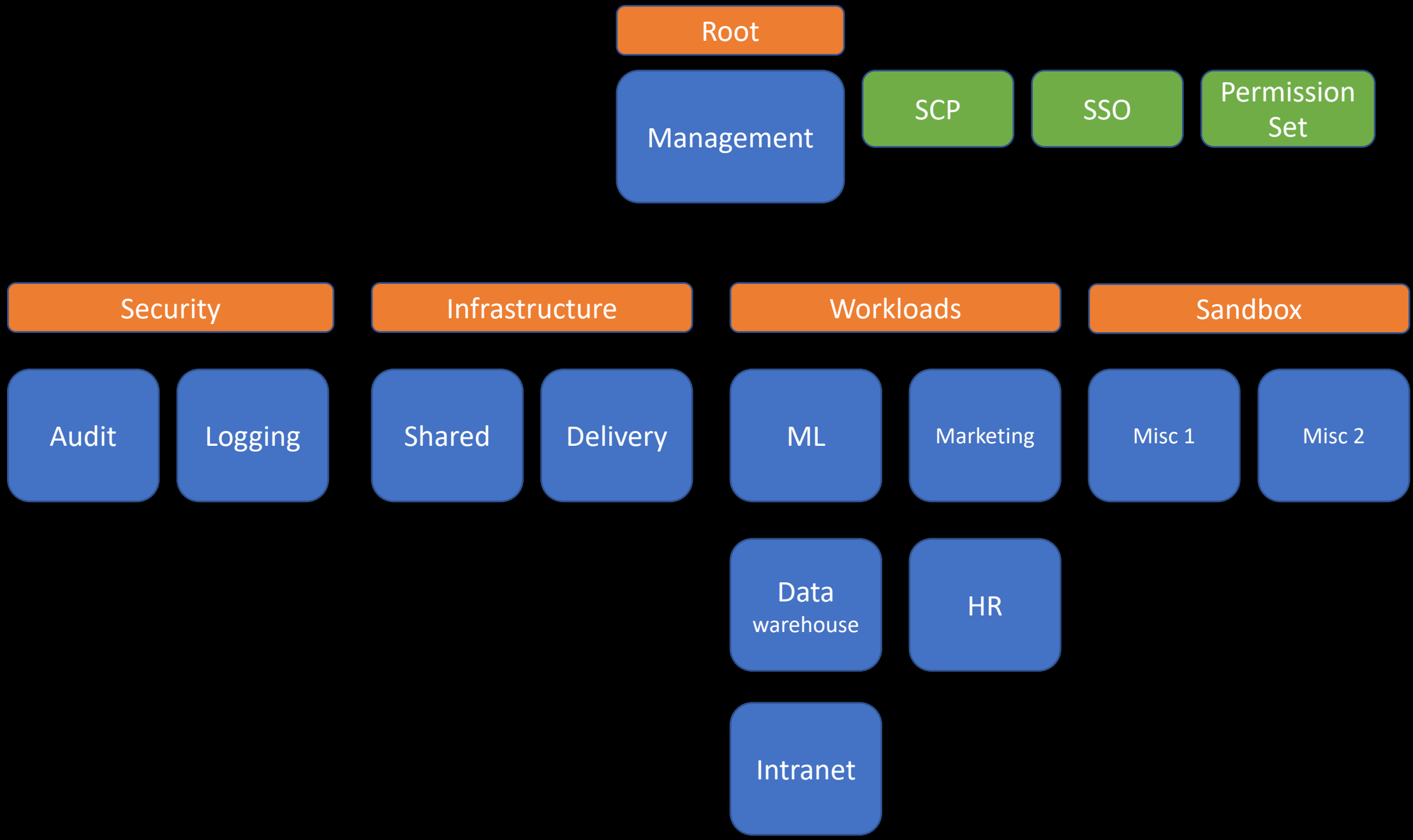
Prepare for Security Events

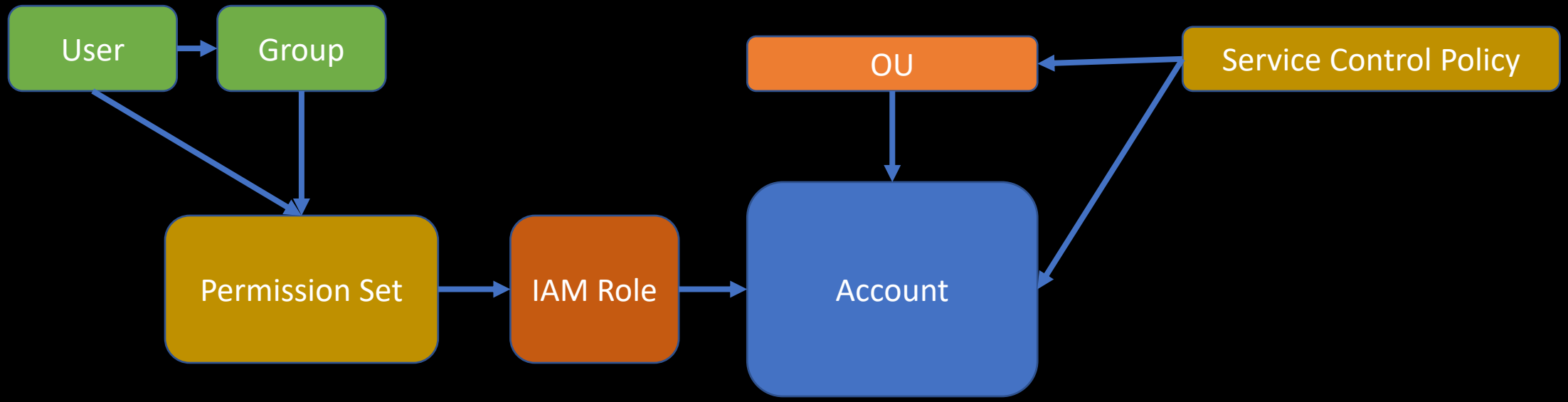
Your System

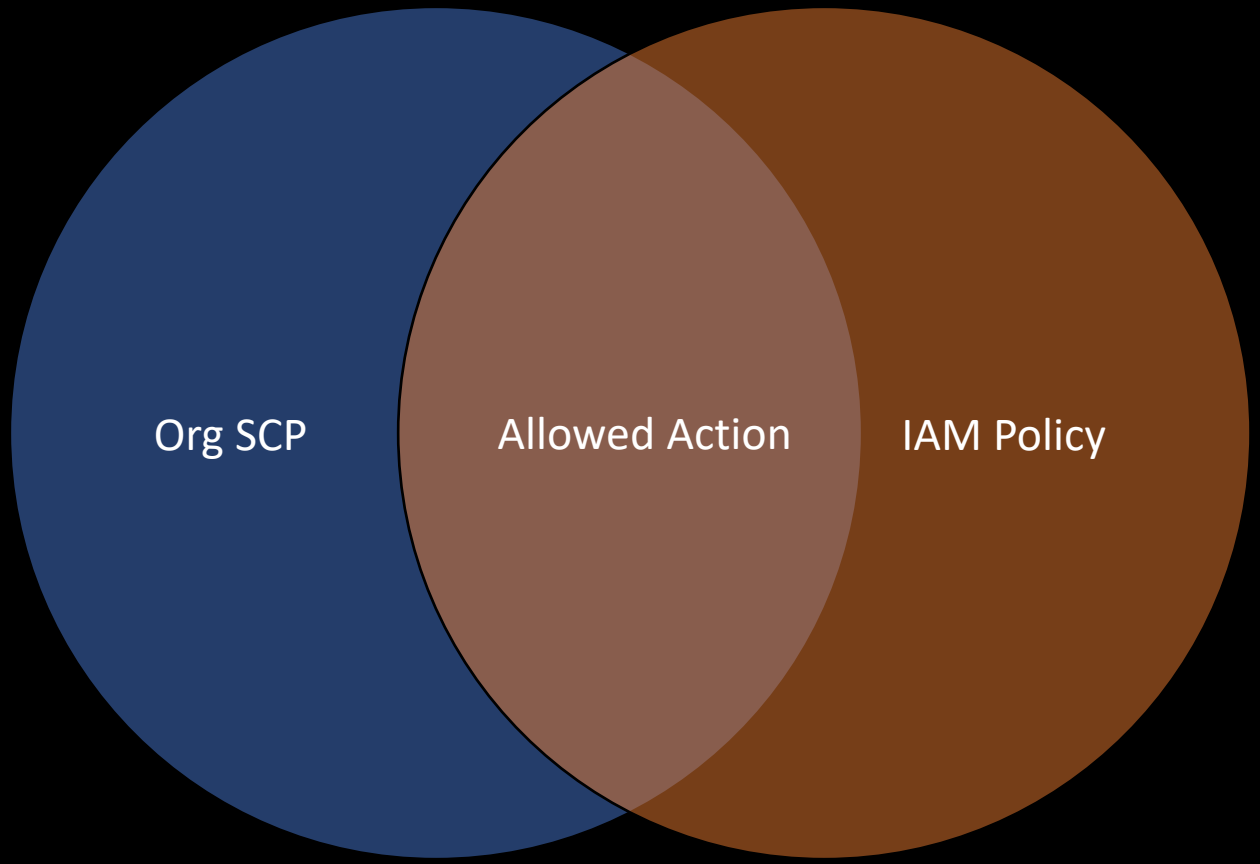

Alerts
IDS
Logs/Metrics
intranet
Data warehouse
customer-app
C6i
C6i
C6i
C6i
C6i
C6i
HR
ML Pipeline
Marketing
Intranet
VPN Only Access
HR
Analytics
Engineers
Marketing
Executive
customer

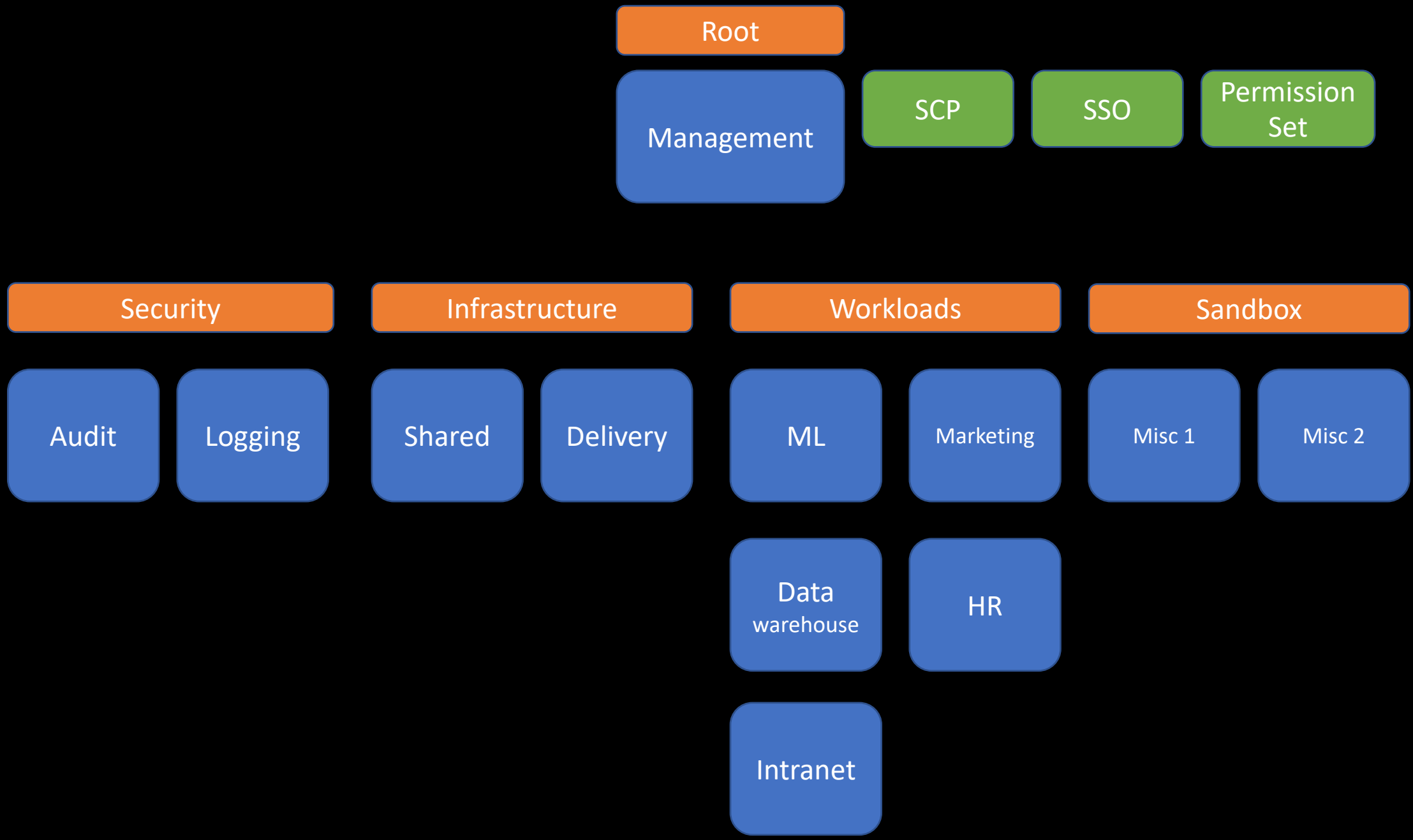
Reducing the blast radius

Multi-Account Organization

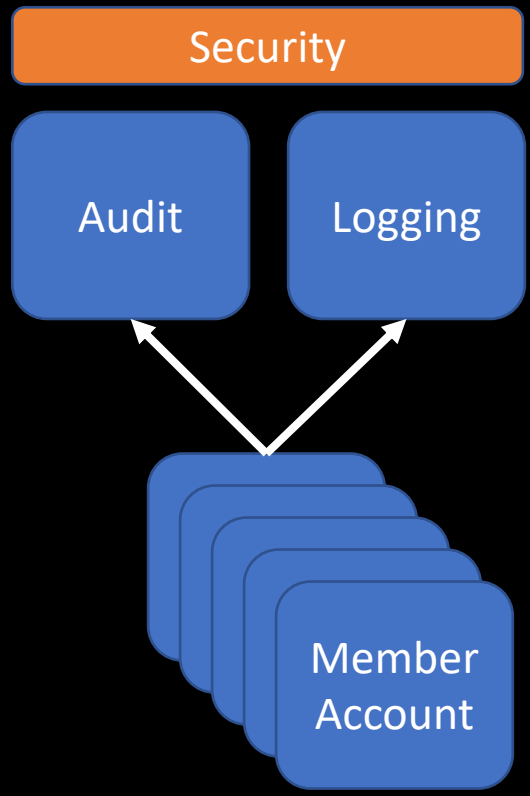

Root
Management
SCP
SSO
Permission Set
Security
Infrastructure
Workloads
Sandbox
Audit
Logging
Shared
Delivery
ML
Marketing
Misc 1
Misc 2
Data warehouse
HR
Intranet


User
Group
OU
Service Control Policy
Permission Set
IAM Role
Account

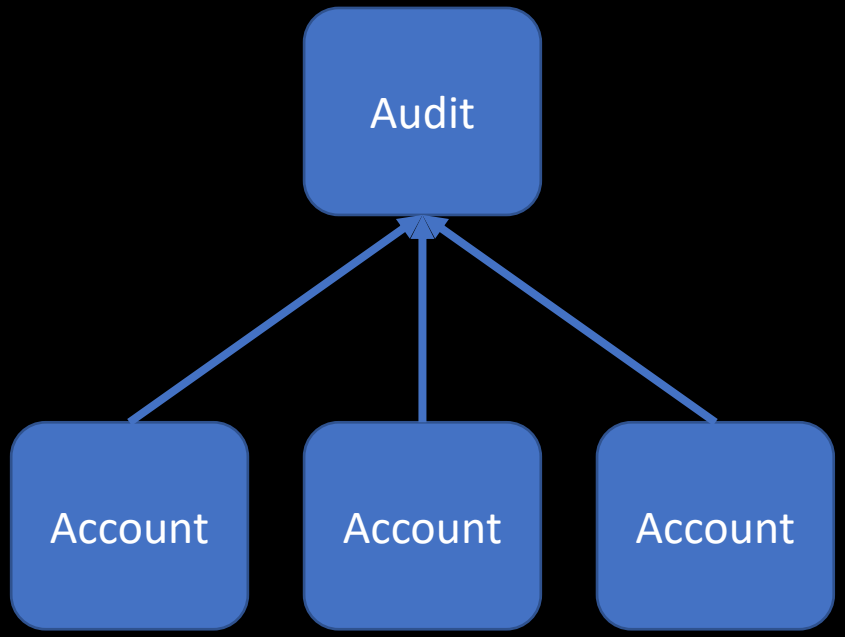

Org SCP
Allowed Action
IAM Policy

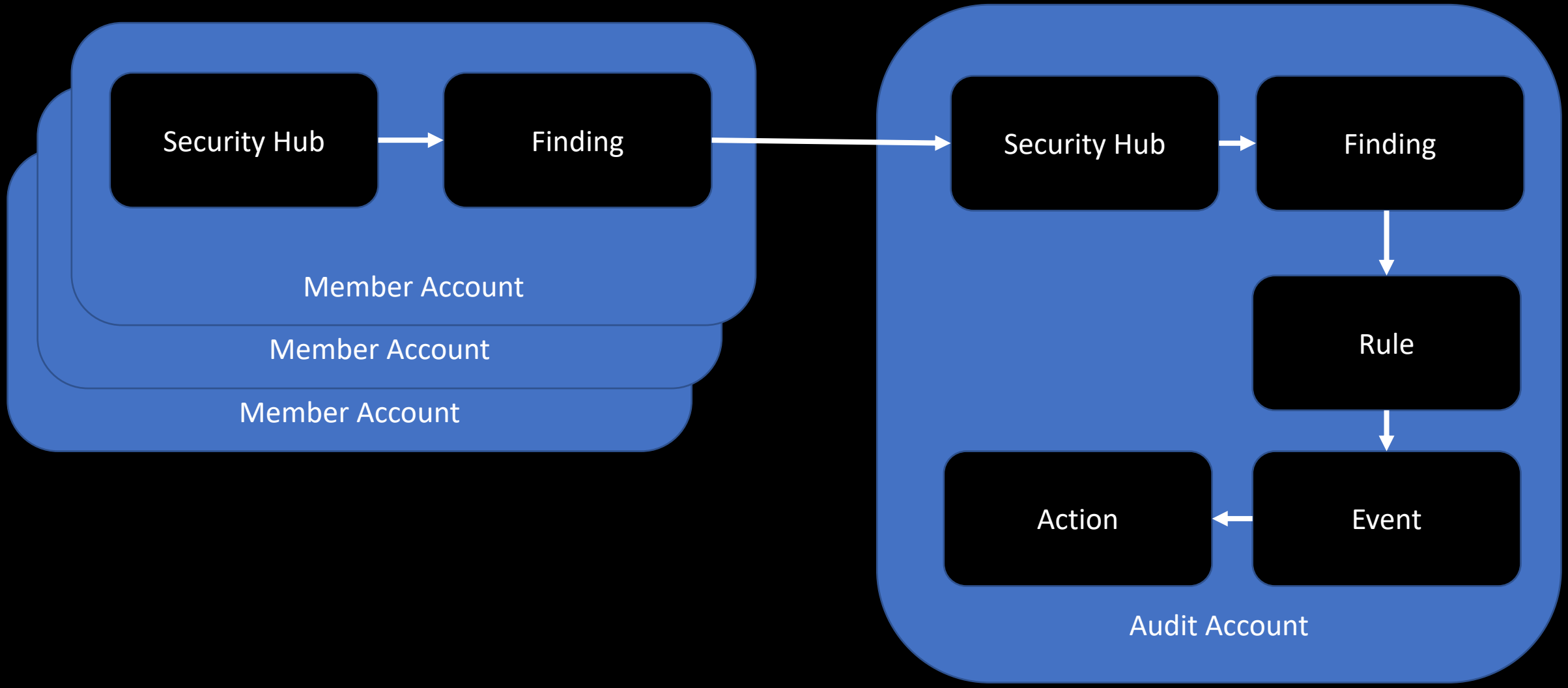

Root
Management
SCP
SSO
Permission Set
Security
Infrastructure
Workloads
Sandbox
Audit
Logging
Shared
Delivery
ML
Marketing
Misc 1
Misc 2
Data warehouse
HR
Intranet

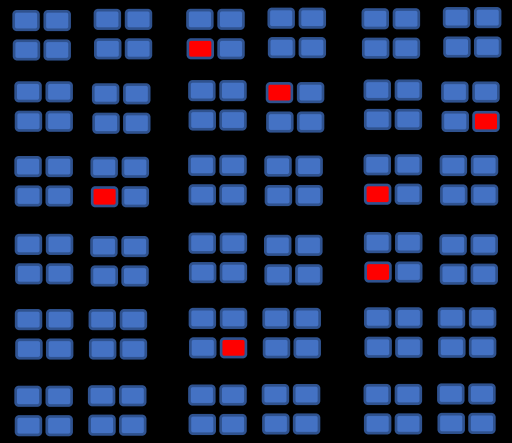
Cross Account Write Only Access


Security
Audit
Logging
Member
Account

Federated Anomaly Detection


Audit
Account
Account
Account


Security Hub
Finding
Member Account
Member Account
Member Account
Security Hub
Finding
Rule
Action
Event
Audit Account



Your System

Thank You

References

How AWS Minimizes the Blast Radius of Failures
https://www.youtube.com/watch?v=swQbA4zub20

Architecting for high availability on Amazon S3
https://www.youtube.com/watch?v=Qib1snR9FhA

AWS Well-Architected Security
https://www.youtube.com/watch?v=i-ErdXn9DFA

AWS Well-Architected Framework - Security
https://docs.aws.amazon.com/wellarchitected/latest/framework/sec-design.html