IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Cloud Security Through Threat Modeling

Robert M. Zigweid
Director of Services for IOActive

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Key Points

- Introduction
- Threat Model Primer
- Assessing Threats
- Mitigating Threats
- Sample Threat Model Exercise
- Conclusions and Questions

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

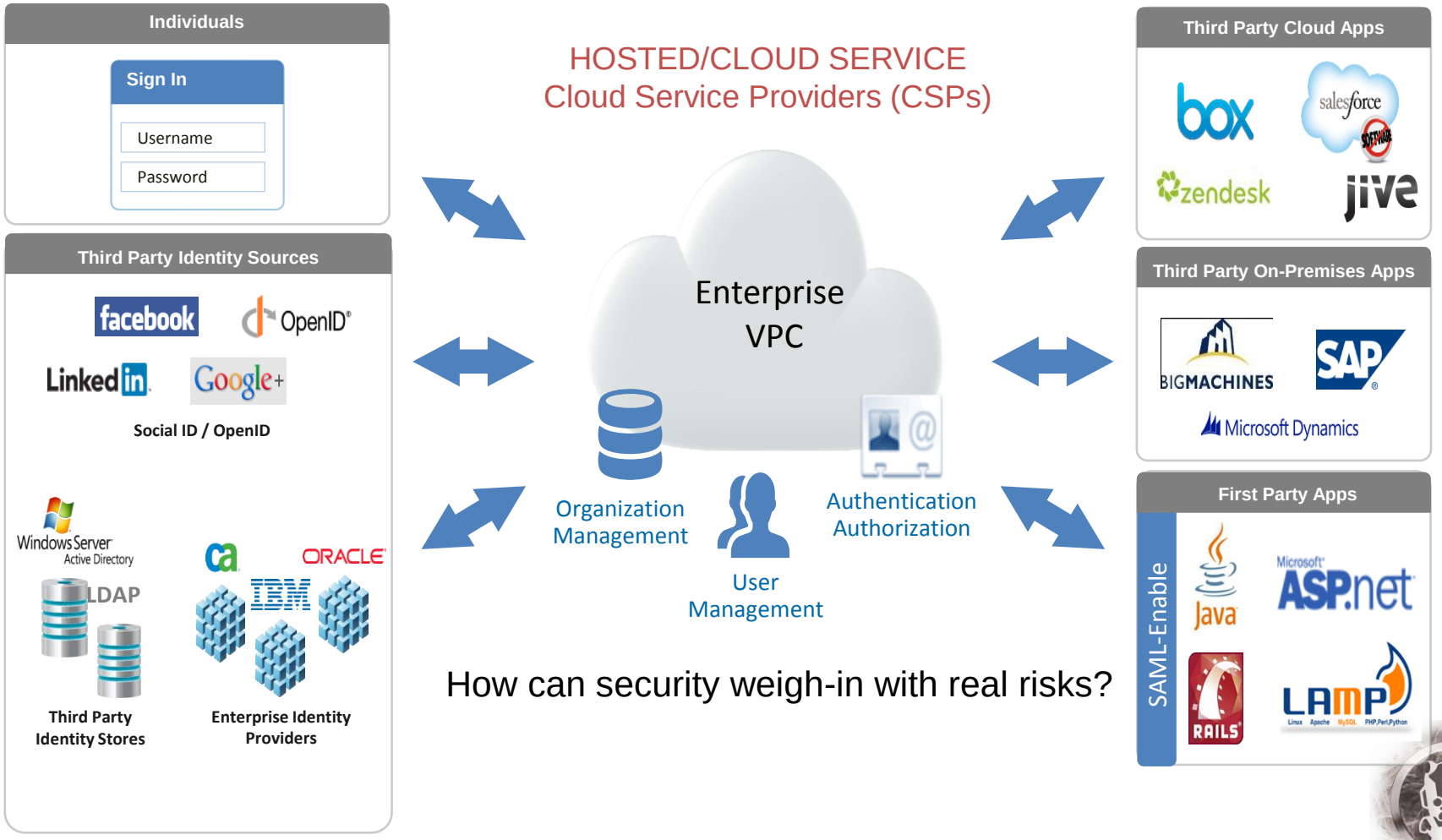
INTRODUCTION

Everything as a Service

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

FLEXIBILE AUTHENTICATION METHODS

MANAGED APP INTEGRATIONS Service Providers (SPs)

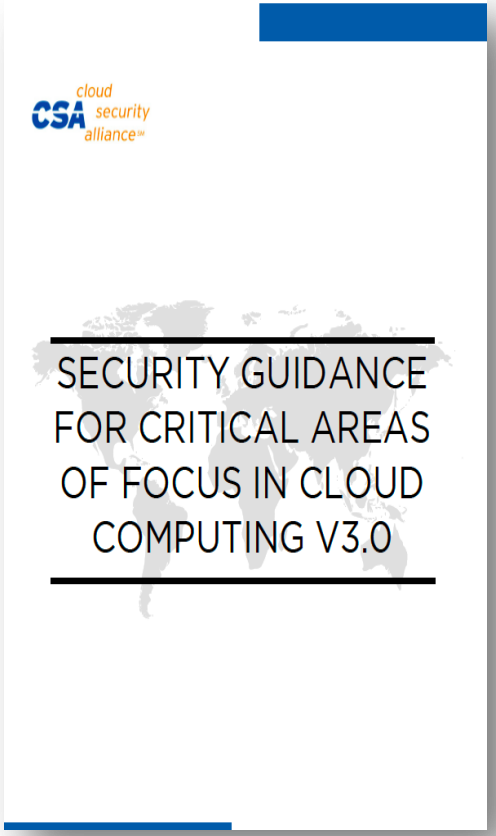


How can security weigh-in with real risks?

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Cloud Security Wisdom

This wisdom is captured best here:



IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Cloud Security Wisdom
What Is It?

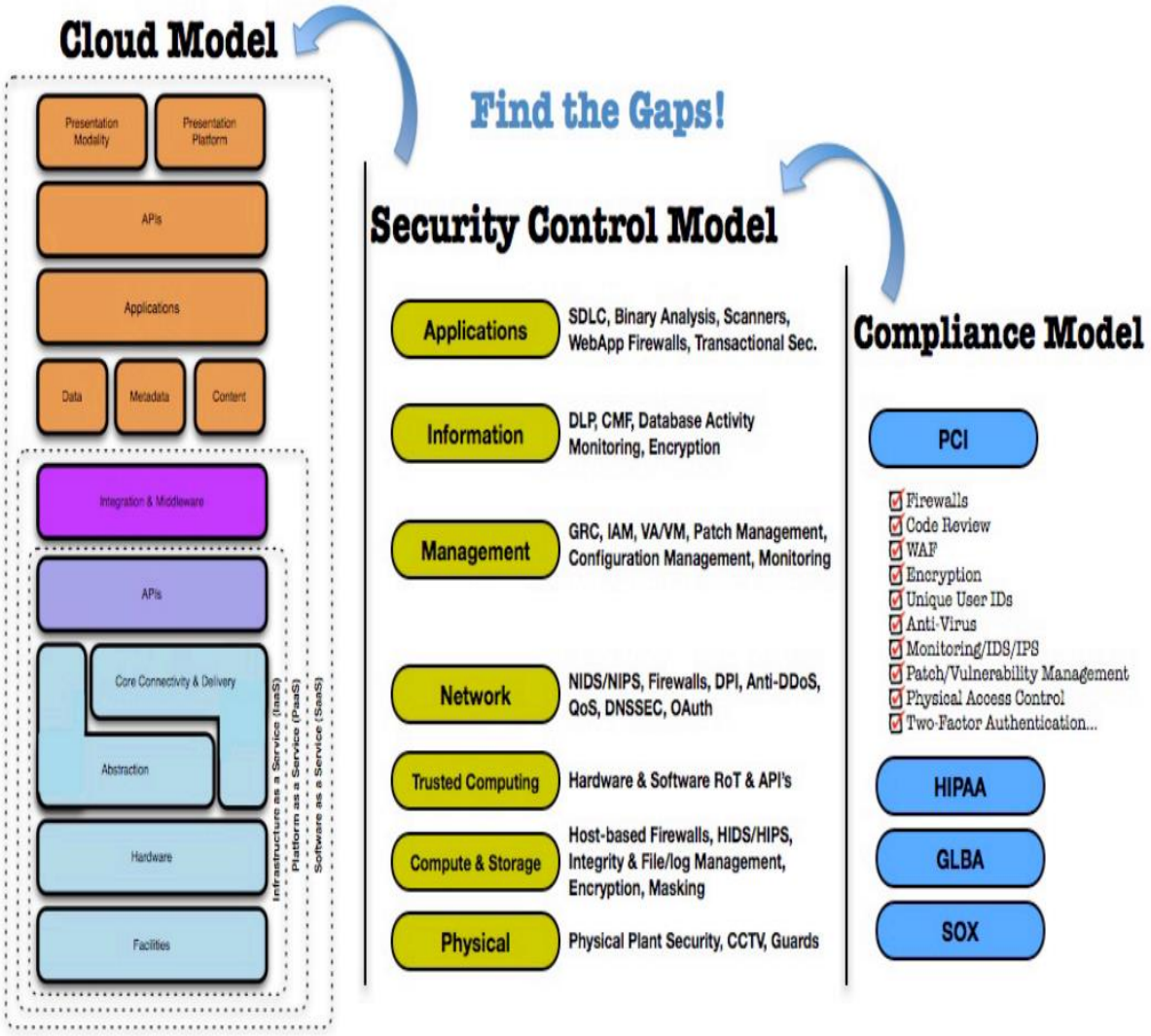
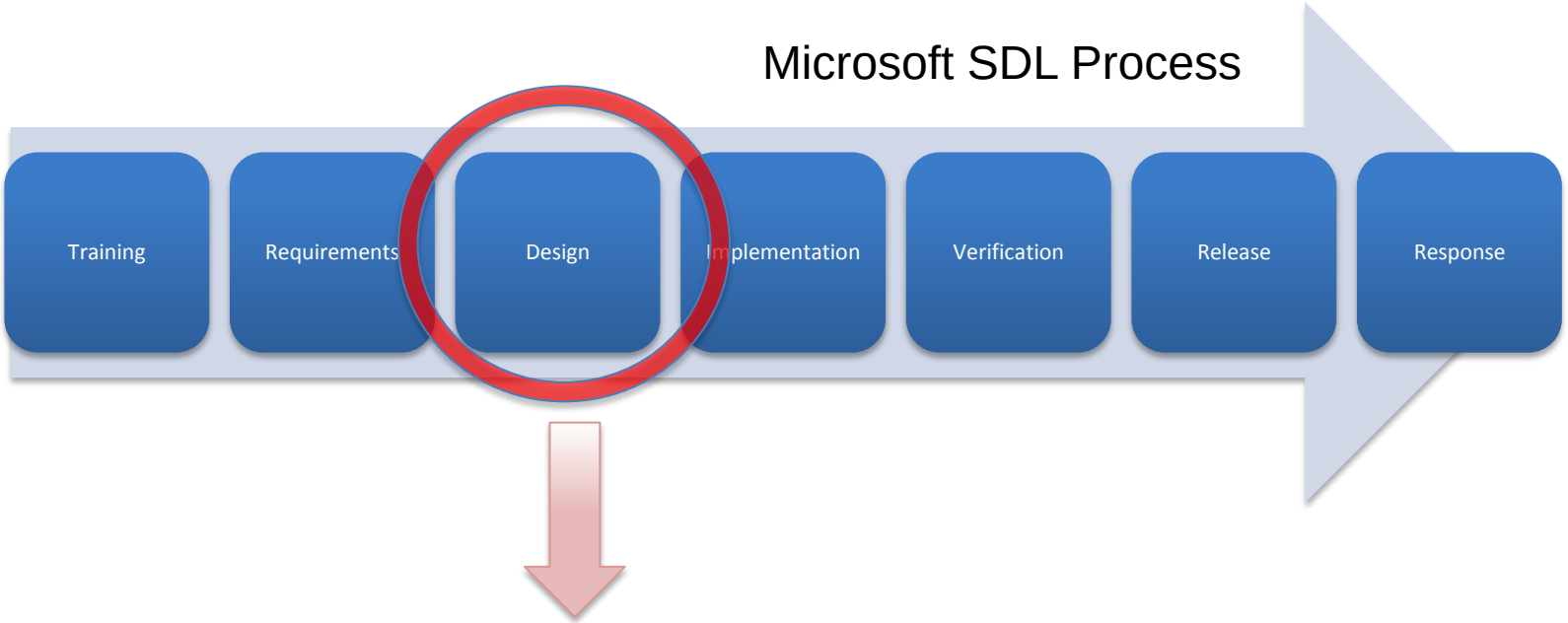


Figure 5—Mapping the Cloud Model to the Security Control & Compliance

Modeling Risks Programmatically



Developing Threat Models

- Structured approach
- Repeatable way to identify attack surfaces (i.e. risk)
- Develop mitigations and acceptance criteria
- Can be applied to anything–even Cloud environments

Threat Modeling Cloud Environments

DOMAIN 10 //
APPLICATION SECURITY

Threat analysis guidance provided in this domain

10.6 Recommendations

10.6.2 Risk Analysis Recommendations

- Risk analysis of the applications for security and privacy (confidentiality, integrity and availability) are undertaken, and threat models should be built and maintained.
- Risks from the perspective of development and deployment in the cloud should be analyzed and related threat models maintained.

…good thinking, now let's talk about how to create threat models

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

THREAT MODEL PRIMER

Why Threat Model?

- Threat modeling is not just for code
  - Anything can be Threat Modeled
  - Output will drive risk analysis and business decisions
- Implementing in the Cloud is still code
  - Deploying and managing servers is all software
  - It has driven the rise of Dev-Ops personnel

When to Threat Model

- Not a one time event
- Adding or removing assets/components
  - It is never too late!
- What you need to know before you start
  - What are you building?
  - What needs to be protected?
- You can be too early, especially on new projects

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Threat Modeling Tools

- The tool used is less important than the data recorded
- Using a tool already? Keep doing so!
- Whiteboards are a favorite
  - Do not forget longer term retention
- Data Flow Diagrams

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Assessment and Identifying Threats

- Identify Data Assets
  - Determine Each Assets Relative Value
- Identify Actors and Data Asset Visibility
  - Internal Personnel
  - CSP Personnel
  - Government?

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Assessment and Identifying Threats

- Data Flow Diagram
- Identify Points of Trust Boundaries
  - Points at which control changes
- Identify Points of Vulnerability
- Know Where Your Data Is
  - To the best of your visibility

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

ASSESSING THREATS

CSP Responsibilities–IaaS

- Hardware Layer
- Network Layer (IDS, DDoS, Guest Instances)
- Instance Access Control Rules

CSP Responsibilities–PaaS

- Hardware Layer
- Operating System Layer
- Network Layer
  - May not be inherited from IaaS
- Access Control Rules

CSP Responsibilities–SaaS

- All asset integrity and visibility is dependent upon the CSP regardless of service

CSP Threats–IaaS

- Data Visibility
  - Government requests
  - May be able to be mitigated
- Network Traffic Shaping and Manipulation
- Hypervisor Trust

CSP Threats–PaaS

- IaaS threats included
- Like a Managed Service Provider
  - Shared Root/Admin
- Less control over data
  - Depends on nature of PaaS
- Data Storage vs. Application Hosting
- Depends on how the data is used

CSP Threats–SaaS

- IaaS and PaaS threats included
- No guaranteed control over data
  - CSP must be completely trusted

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

MITIGATING THREATS

Mitigating CSP Threats–IaaS

- Data Storage
  - Storage location
  - Encryption and key management control
  - Avoid using ephemeral disks
- Authentication and Authorization
  - Use your own system whenever possible

Mitigating CSP Threats–IaaS

- Data transit
  - Encryption with your own certificates if possible
  - Pass through load balancers instead of terminating connections there
  - Includes administration
- Network segmentation and firewalls, if available

Mitigating CSP Threats–PaaS

- Monitor all access, regardless of who
  - It might not be a critical event–but then again, it might
- Use encrypted transit with your certificates/keys
  - Be careful where you store the private keys
- Encrypt before storing
- Log where possible

Mitigating CSP Threats–SaaS

- There is no control
- Deleted vs. non-visible
- Legal might help

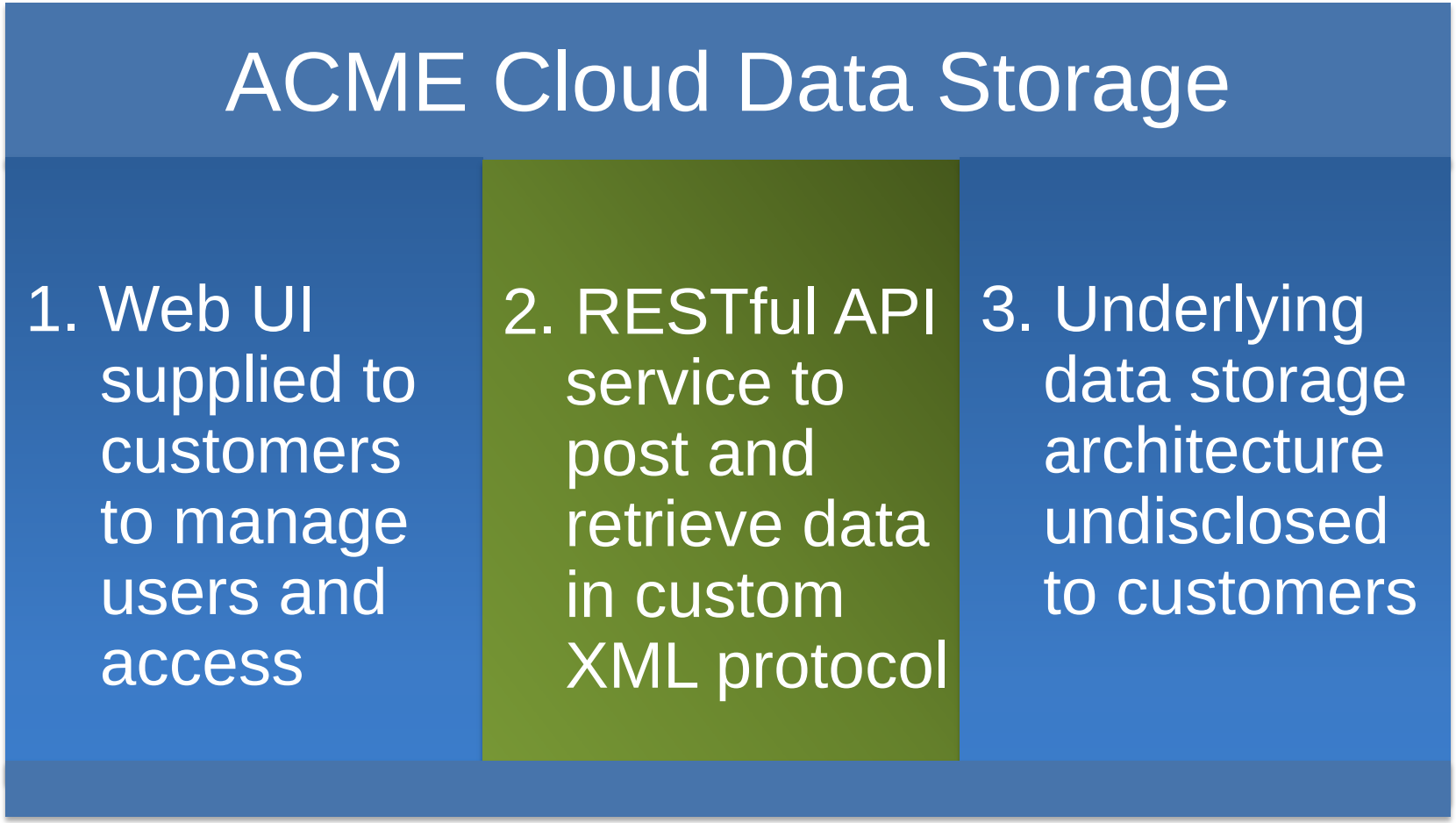
The Fun Part: Multiple Services

- Most Cloud implementations use multiple services
- Data Flow Diagrams show their worth
- It is necessary to break the components down
  - Take each service on its own merit
  - They might not be from the same CSP
    - Could be a good thing

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

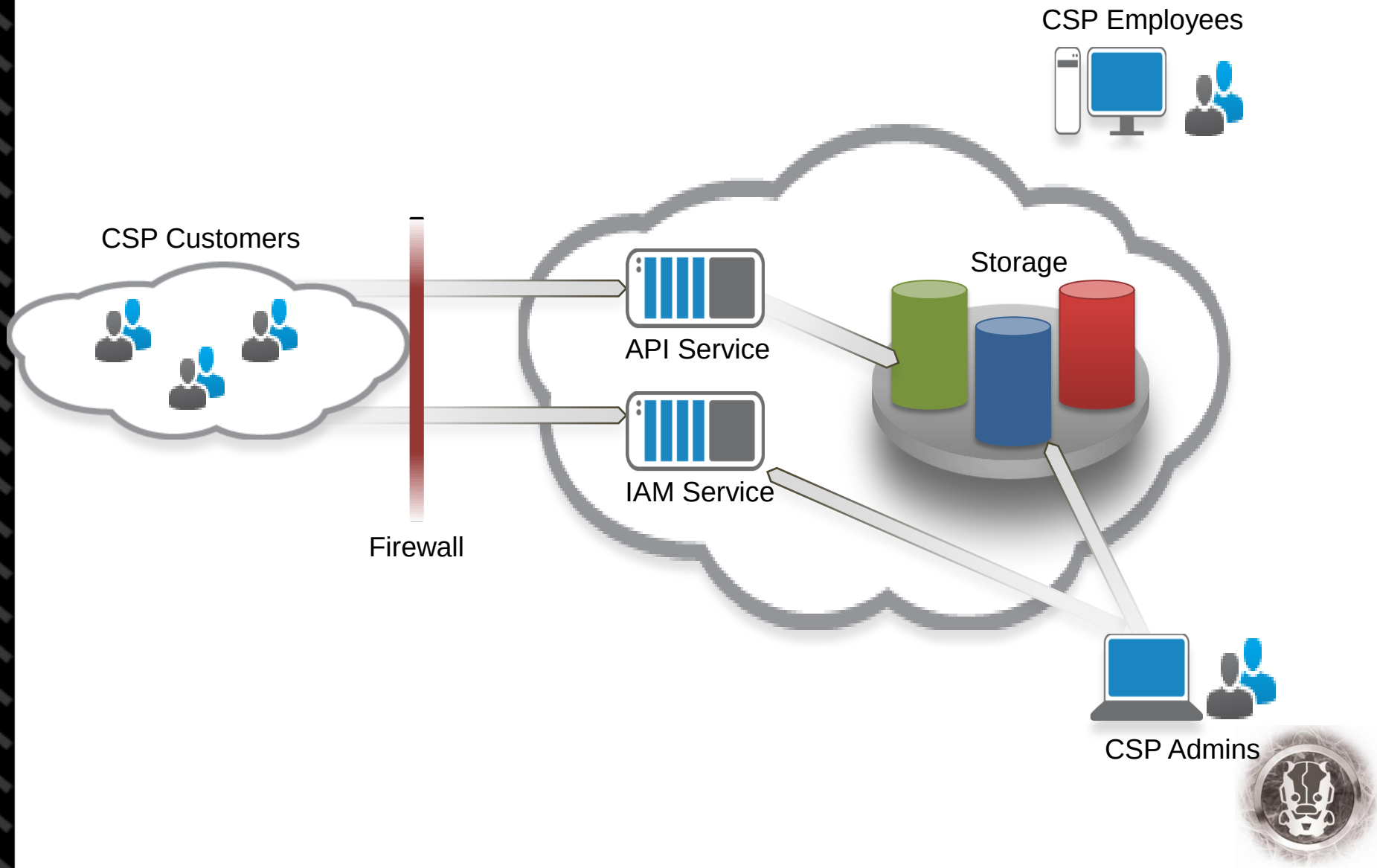
SAMPLE THREAT MODEL EXERCISE

Exercise: CSP Service Definition



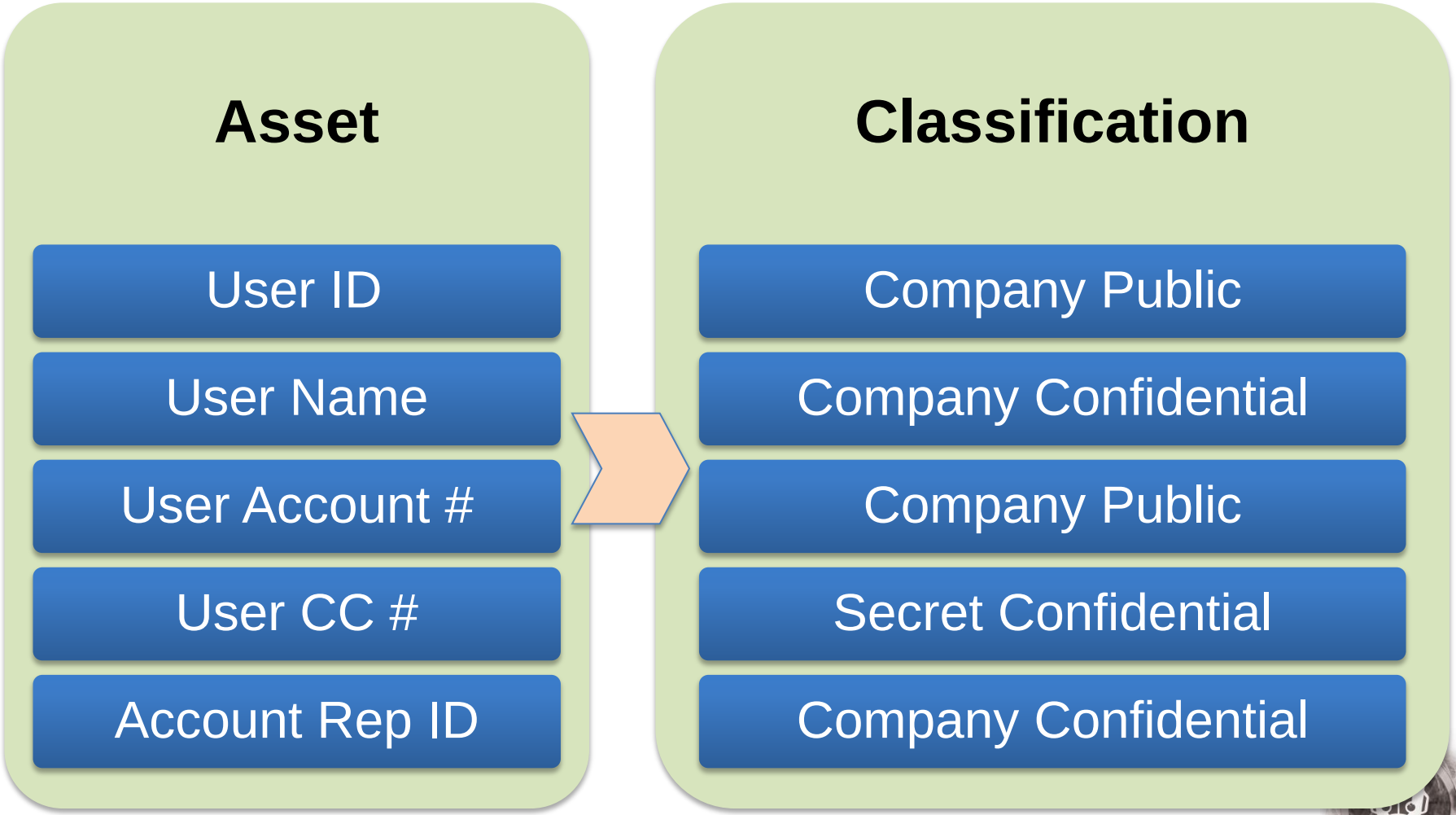
IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Exercise: Data Flow Diagram



IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Exercise: Identifying Assets

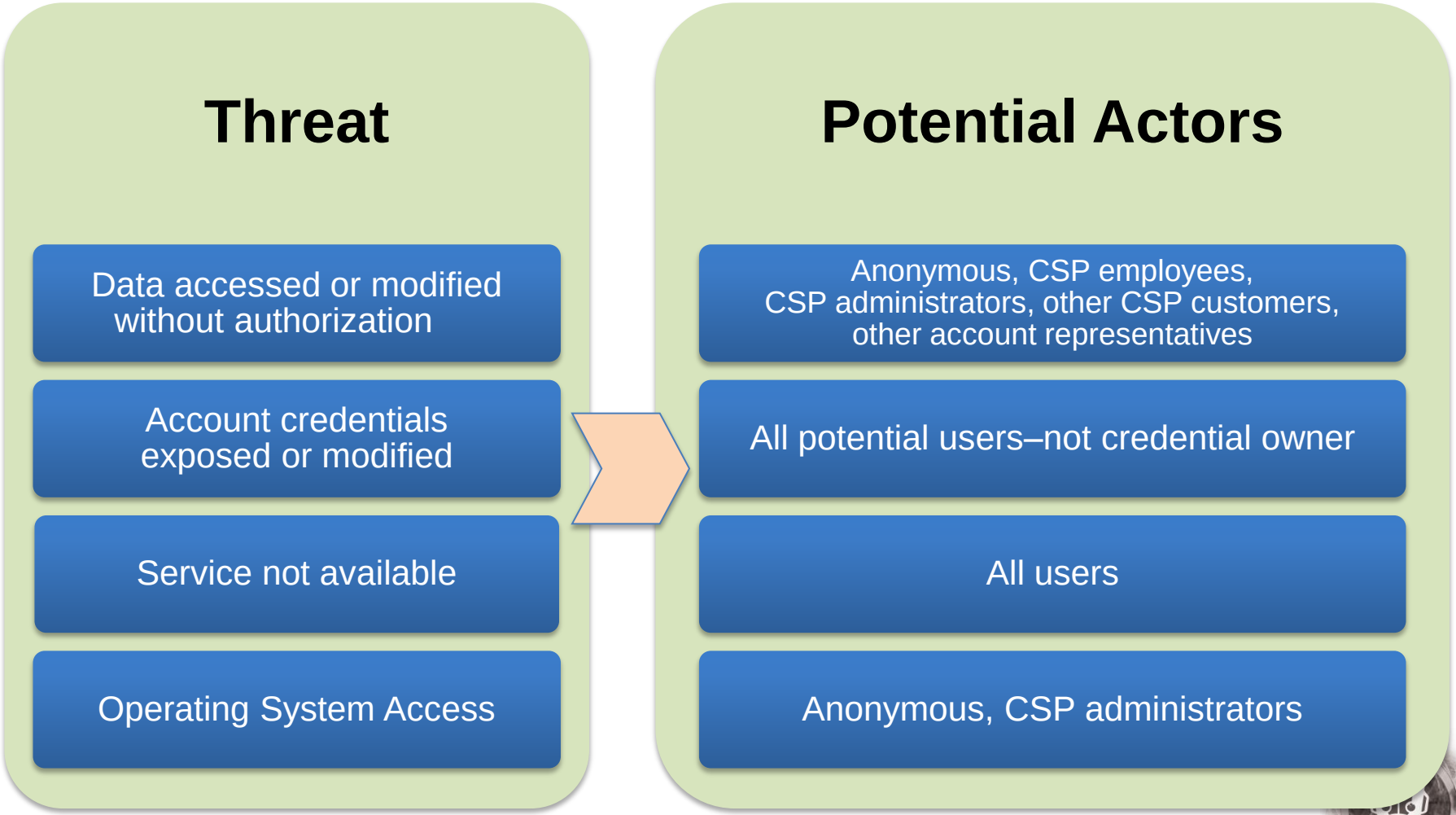


Exercise: Identifying Actors

Actors	Classification
Anonymous	Anyone not authenticated
Account Rep	Authenticated account representative
Account Manager	Account representative managers
Account Administrator	Controls account rep & managers access
CSP Personnel	CSP employees and administrators
CSP Customers	Other customers using similar interfaces

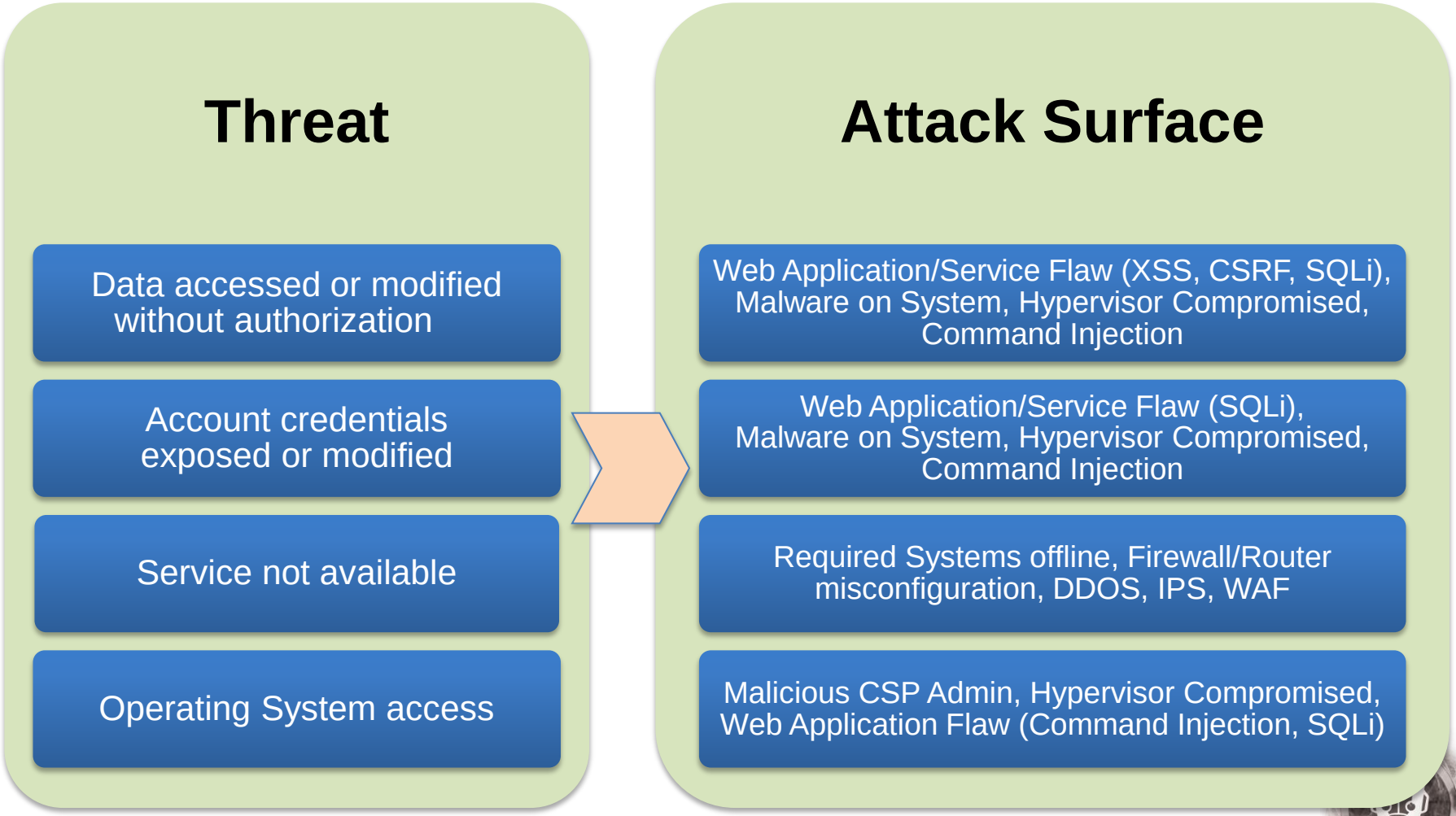
IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Exercise: Identifying Threats

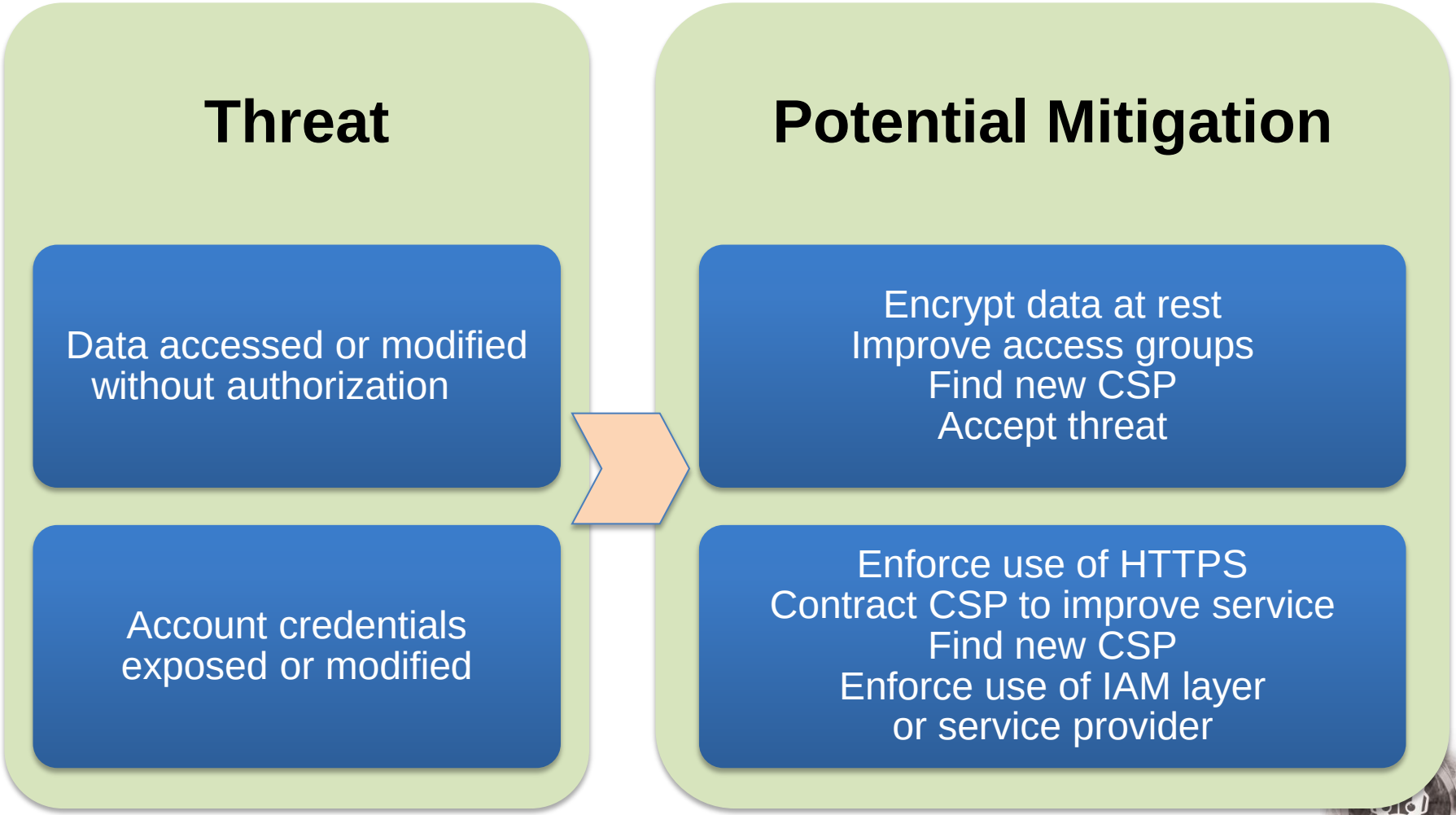


IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

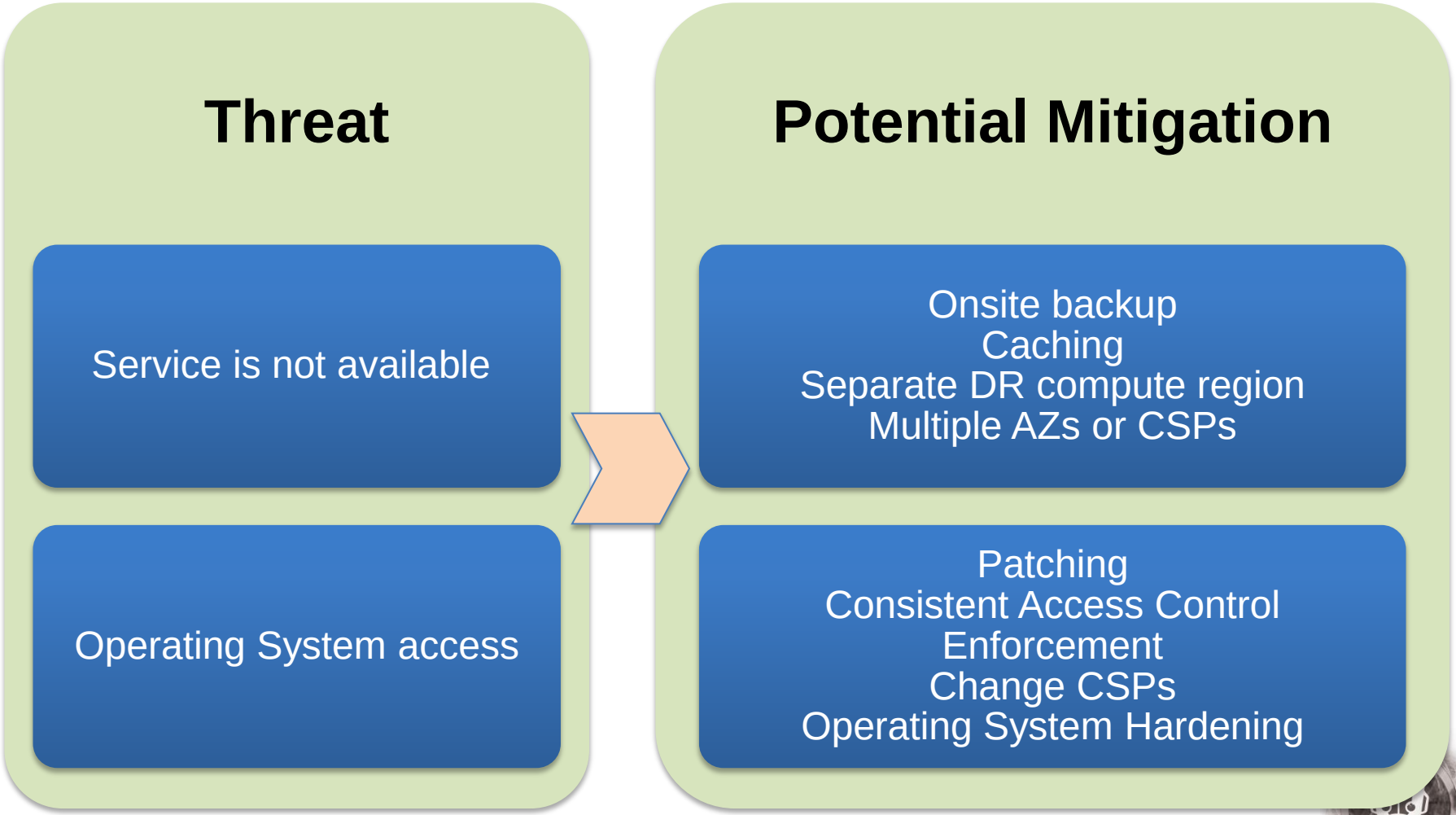
Exercise: Identifying the Attack Surface



Exercise: Mitigate or Accept



Exercise: Mitigate or Accept



IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

CONCLUSIONS AND QUESTIONS

Conclusions

- Risk vs. Reward
  - Identify risk to minimize it
  - Increase reward–leverage CSPs that work
- Cloud Projects will involve discrete backend services
  - Lots of API interaction at SaaS, PaaS, and IaaS levels
  - Focus on permissions, authentication, and authorizations
- Leverage legal contracts and compliance assurances

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Questions

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

Thank You!

Robert M. Zigweid
rzigweid@ioactive.com