MICRO STRATEGIES

Security First!

Alfresco Virtual DevCon 2020, Day 2 [September 16, 2020]

Jason Jolley – Director, Application Development

@jasonjolley ✉ jjolley@microstrat.com

Technology Solutions. Business Results.

Objective

To empower Alfresco development teams to implement their solutions in a secure manner.

Agenda

SECURITY REQUIREMENTS

SECURE DEVELOPMENT

CLOUD SECURITY

RESOURCES

Security Requirements

- Understand Current State Security
- Authentication
- Authorization
- Content Security
- Regulations
- Governance
- Controlled Distribution
- Redaction
- Annotation
- Compliance
- Going Paperless
- Business Continuity
- Business Process
- Automation
- Auditing
- Detect mass downloads or deletions
- Viruses & Malware

Alfresco and Security

- Core Alfresco Features
- Alfresco Enterprise Viewer
- Alfresco Governance Services
- Alfresco Cloud
- Alfresco Encrypted Content Store

- Core Alfresco Architecture
- SAML Single Sign-On
- Identity Services
- Vulnerability Alerts
- Partner Solutions

Alfresco and Security Tips & Tricks

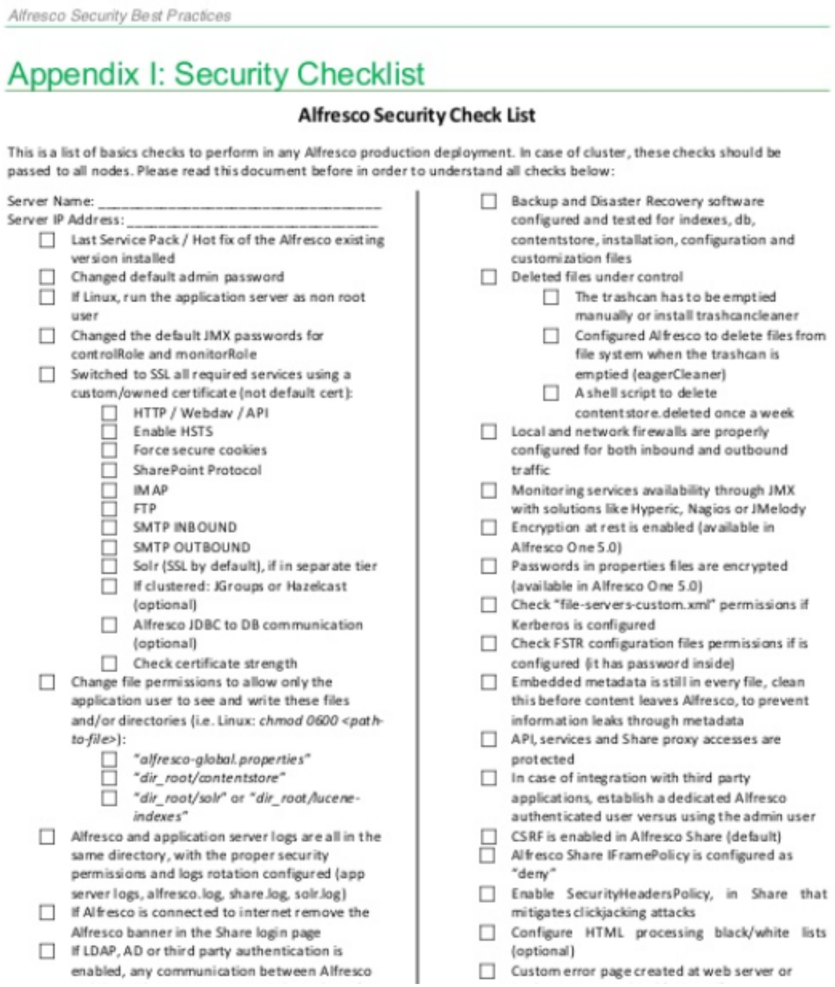
Alfresco Security Best Practices Checklist

https://www.slideshare.net/toniblyx/alfresco-security-best-practices-check-list-only

Alfresco's configuration can be tweaked in many ways. The Alfresco Security Best Practices Checklist presented by Toni de la Fuente details recommended configurations.

This document is five years old, but still has many useful recommendations. For example:

- Disable Unneeded services
- Change File Permissions
- Encrypt Passwords



Alfresco Security Best Practices

Appendix I: Security Checklist

Alfresco Security Check List

This is a list of basics checks to perform in any Alfresco production deployment. In case of cluster, these checks should be passed to all nodes. Please read this document before in order to understand all checks below:

Server Name: ________________________________
Server IP Address: ______________________________

- □ Last Service Pack / Hot fix of the Alfresco existing version installed
- □ Changed default admin password
- □ If Linux, run the application server as non root user
- □ Changed the default JMX passwords for controlRole and monitorRole
- □ Switched to SSL all required services using a custom/owned certificate (not default cert):
    - □ HTTP / Webdav / API
    - □ Enable HSTS
    - □ Force secure cookies
    - □ SharePoint Protocol
    - □ IMAP
    - □ FTP
    - □ SMTP INBOUND
    - □ SMTP OUTBOUND
    - □ Solr (SSL by default), if in separate tier
    - □ If clustered: JGroups or Hazelcast (optional)
    - □ Alfresco JDBC to DB communication (optional)
    - □ Check certificate strength
- □ Change file permissions to allow only the application user to see and write these files and/or directories (i.e. Linux: *chmod 0600 <path-to-file>*):
    - □ *"alfresco-global.properties"*
    - □ *"dir_root/contentstore"*
    - □ *"dir_root/solr"* or *"dir_root/lucene-indexes"*
- □ Alfresco and application server logs are all in the same directory, with the proper security permissions and logs rotation configured (app server logs, alfresco.log, share.log, solr.log)
- □ If Alfresco is connected to internet remove the Alfresco banner in the Share login page
- □ If LDAP, AD or third party authentication is enabled, any communication between Alfresco

- □ Backup and Disaster Recovery software configured and tested for indexes, db, contentstore, installation, configuration and customization files
- □ Deleted files under control
    - □ The trashcan has to be emptied manually or install trashcancleaner
    - □ Configured Alfresco to delete files from file system when the trashcan is emptied (eagerCleaner)
    - □ A shell script to delete contentstore.deleted once a week
- □ Local and network firewalls are properly configured for both inbound and outbound traffic
- □ Monitoring services availability through JMX with solutions like Hyperic, Nagios or JMelody
- □ Encryption at rest is enabled (available in Alfresco One 5.0)
- □ Passwords in properties files are encrypted (available in Alfresco One 5.0)
- □ Check "file-servers-custom.xml" permissions if Kerberos is configured
- □ Check FSTR configuration files permissions if is configured (it has password inside)
- □ Embedded metadata is still in every file., clean this before content leaves Alfresco, to prevent information leaks through metadata
- □ API, services and Share proxy accesses are protected
- □ In case of integration with third party applications, establish a dedicated Alfresco authenticated user versus using the admin user
- □ CSRF is enabled in Alfresco Share (default)
- □ Alfresco Share IFramePolicy is configured as "deny"
- □ Enable SecurityHeadersPolicy, in Share that mitigates clickjacking attacks
- □ Configure HTML processing black/white lists (optional)
- □ Custom error page created at web server or

Alfresco and Security Tips & Tricks

Additional Alfresco Security presentations with valuable tips and tricks:

Alfresco Security Best Practices Guide

https://www.slideshare.net/toniblyx/alfresco-security-best-practices-guide

Tech Talk Live #110: Alfresco Security Best Practices & Tips

https://youtu.be/qEFHmsEV4bc

Alfresco DevCon 2019: Encryption at-rest and in-transit

https://www.slideshare.net/toniblyx/alfresco-devcon-2019-encryption-atrest-and-intransit

Developer Security Myths

1. Security is just a task.
2. Security is just a feature.
3. You need to be a security expert.
4. We have a security team so we’re okay.
5. This project is a small target. Hackers won’t bother.
6. We need to overhaul everything to be secure.
7. Security can wait until the end.

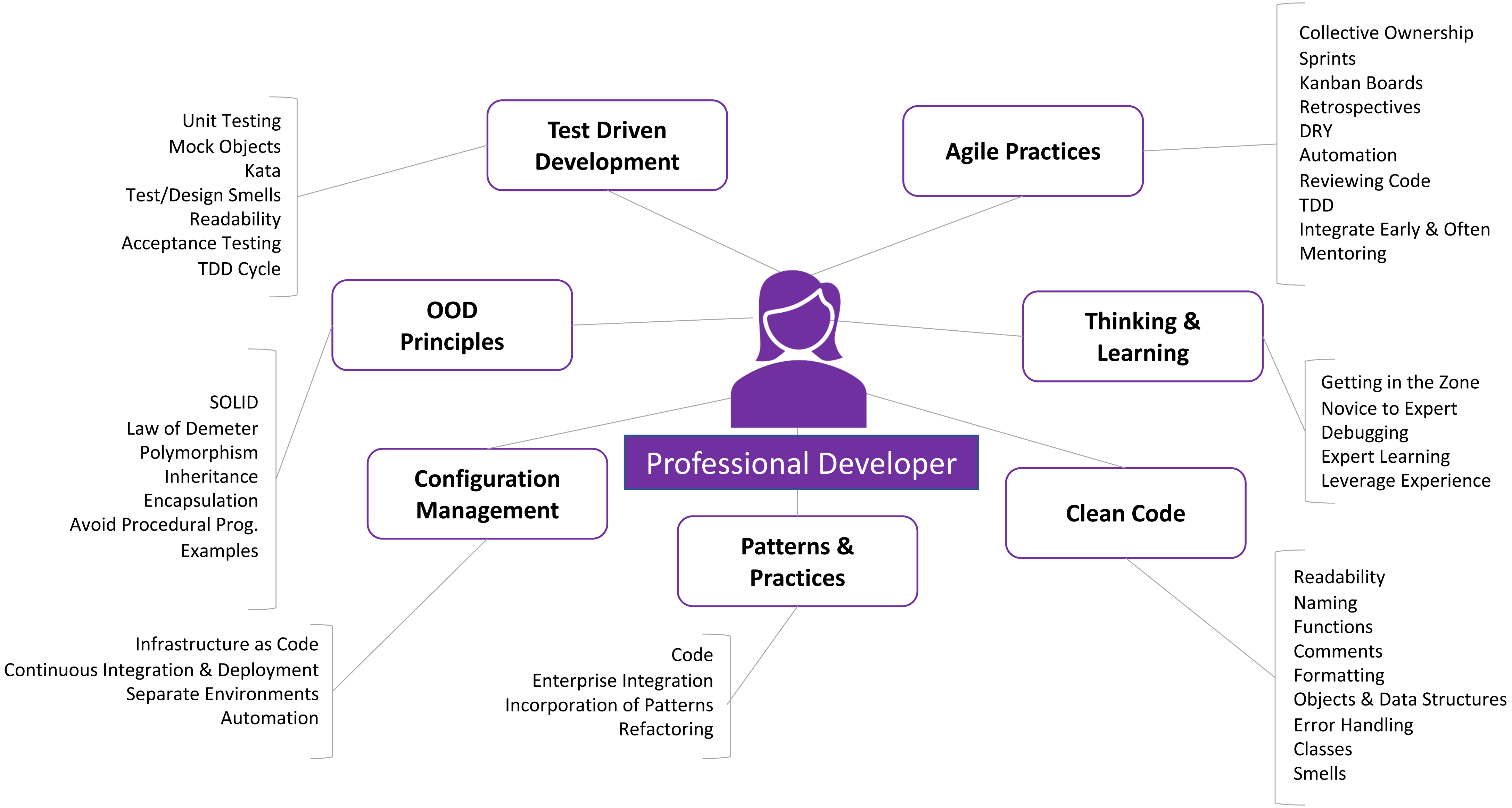
Building A Secure Development Culture

- ❑Security Training
- ❑Onboarding/Offboarding Checklist
- ❑Add Security to your Agenda
- ❑Be Ready for an Incident
- ❑Have an Escalation Path
- ❑Have a Contained Sandbox

Have a Developer Code of Conduct

1. Only Ship Quality Software
2. Stable Productivity
3. Inexpensive Adaptability
4. Continuous Improvement
5. Fearless Competence
6. Extreme Quality
7. QA Will Find Nothing!
8. Automation
9. Honest Estimates
10. Say No When We Can't Commit
11. Continuous Aggressive Learning
12. Mentor Each Other
13. Not Be A Knowledge Silo
14. Be Safe

*This list is influenced by Robert C. Martin's presentation: "The Reasonable Expectations of your CTO"
https://vimeo.com/54025415



Professional Developer

Test Driven Development
- Unit Testing
- Mock Objects
- Kata
- Test/Design Smells
- Readability
- Acceptance Testing
- TDD Cycle

Agile Practices
- Collective Ownership
- Sprints
- Kanban Boards
- Retrospectives
- DRY
- Automation
- Reviewing Code
- TDD
- Integrate Early & Often
- Mentoring

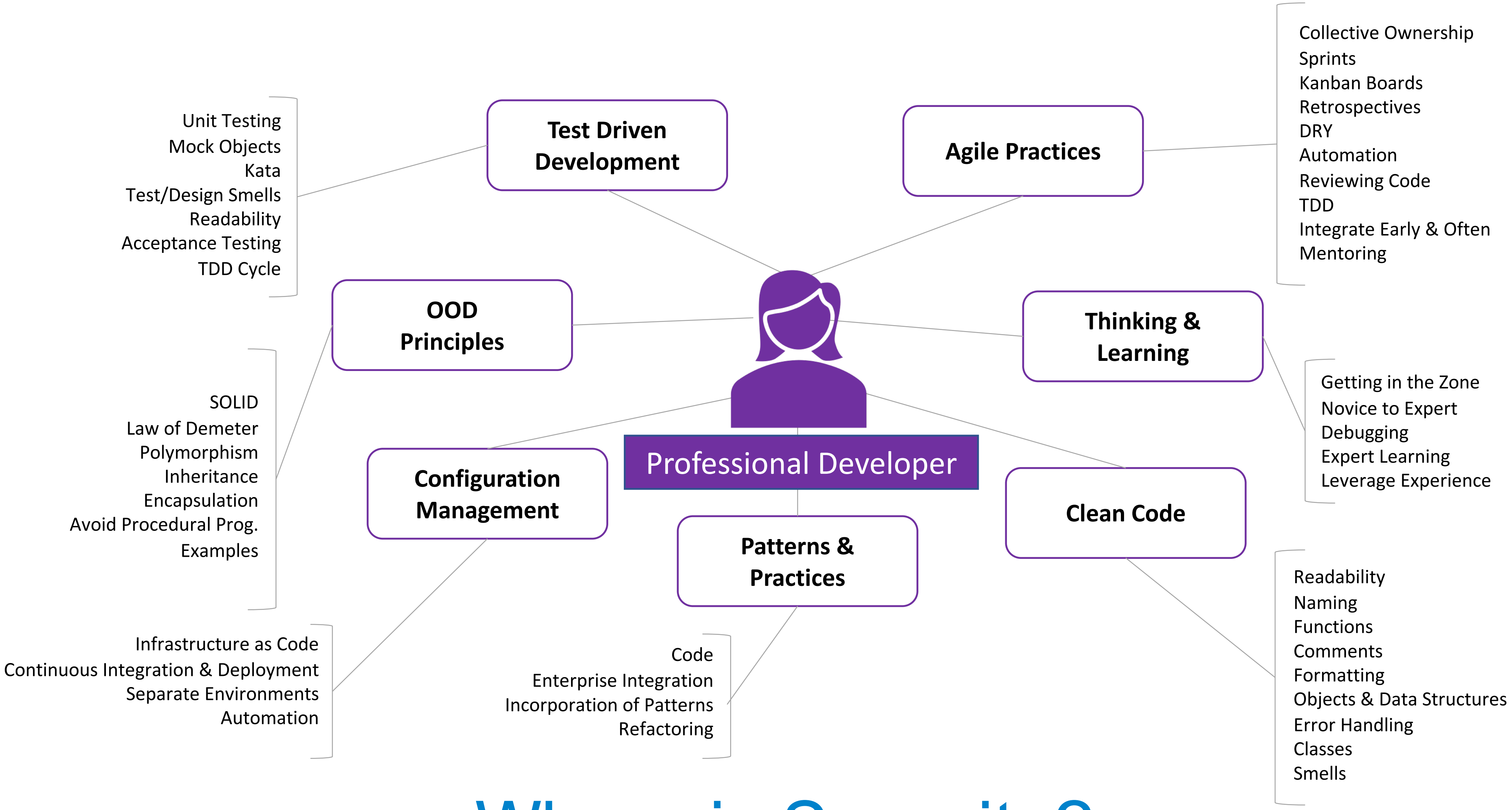
OOD Principles
- SOLID
- Law of Demeter
- Polymorphism
- Inheritance
- Encapsulation
- Avoid Procedural Prog.
- Examples

Thinking & Learning
- Getting in the Zone
- Novice to Expert
- Debugging
- Expert Learning
- Leverage Experience

Configuration Management
- Infrastructure as Code
- Continuous Integration & Deployment
- Separate Environments
- Automation

Patterns & Practices
- Code
- Enterprise Integration
- Incorporation of Patterns
- Refactoring

Clean Code
- Readability
- Naming
- Functions
- Comments
- Formatting
- Objects & Data Structures
- Error Handling
- Classes
- Smells



Professional Developer

Test Driven Development

Unit Testing
Mock Objects
Kata
Test/Design Smells
Readability
Acceptance Testing
TDD Cycle

Agile Practices

Collective Ownership
Sprints
Kanban Boards
Retrospectives
DRY
Automation
Reviewing Code
TDD
Integrate Early & Often
Mentoring

OOD Principles

SOLID
Law of Demeter
Polymorphism
Inheritance
Encapsulation
Avoid Procedural Prog.
Examples

Thinking & Learning

Getting in the Zone
Novice to Expert
Debugging
Expert Learning
Leverage Experience

Configuration Management

Infrastructure as Code
Continuous Integration & Deployment
Separate Environments
Automation

Patterns & Practices

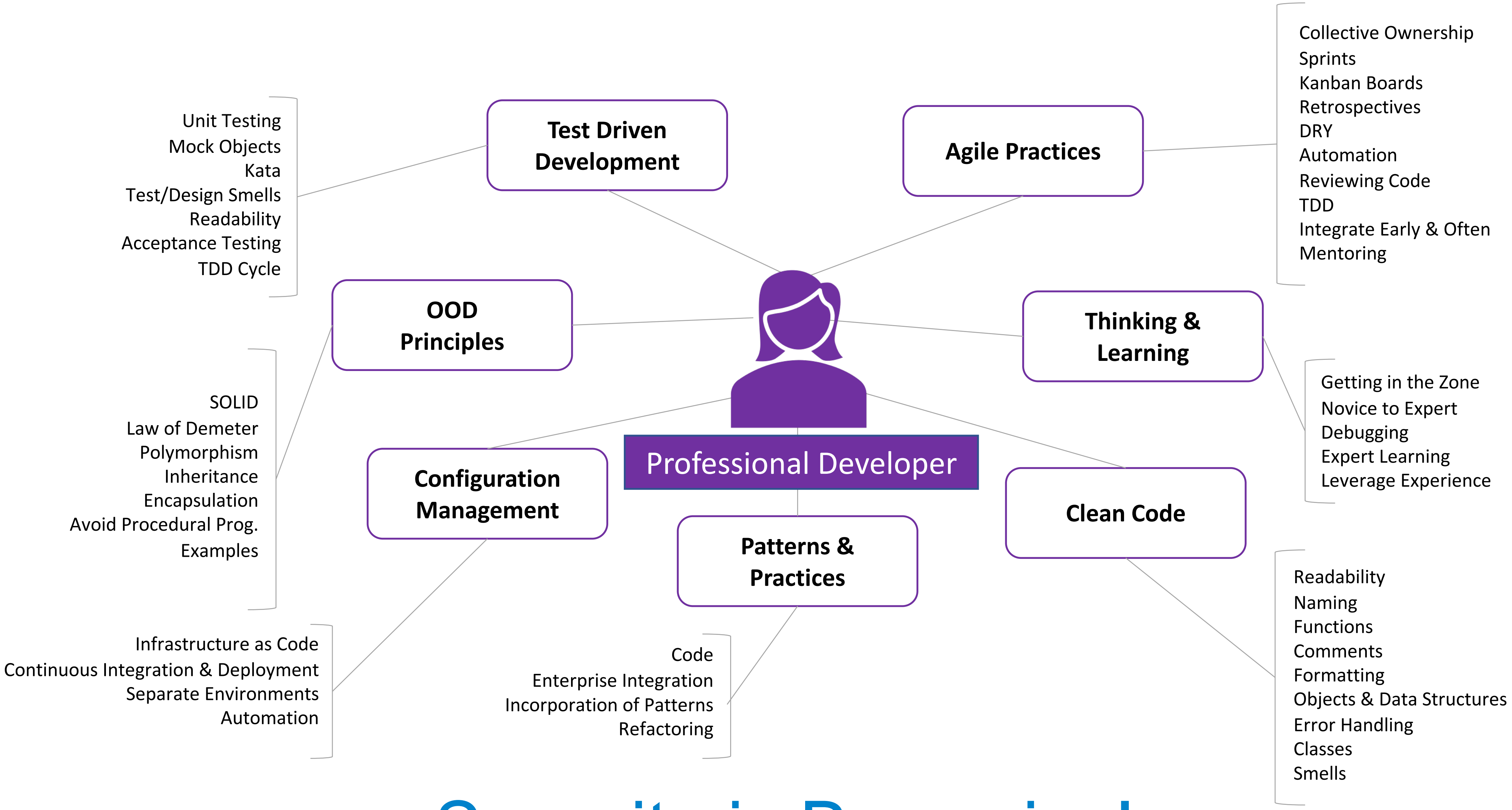
Code
Enterprise Integration
Incorporation of Patterns
Refactoring

Clean Code

Readability
Naming
Functions
Comments
Formatting
Objects & Data Structures
Error Handling
Classes
Smells

Where is Security?

MICRO STRATEGIES
Technology Solutions. Business Results.



Professional Developer

Test Driven Development

Unit Testing
Mock Objects
Kata
Test/Design Smells
Readability
Acceptance Testing
TDD Cycle

Agile Practices

Collective Ownership
Sprints
Kanban Boards
Retrospectives
DRY
Automation
Reviewing Code
TDD
Integrate Early & Often
Mentoring

OOD Principles

SOLID
Law of Demeter
Polymorphism
Inheritance
Encapsulation
Avoid Procedural Prog.
Examples

Thinking & Learning

Getting in the Zone
Novice to Expert
Debugging
Expert Learning
Leverage Experience

Configuration Management

Infrastructure as Code
Continuous Integration & Deployment
Separate Environments
Automation

Patterns & Practices

Code
Enterprise Integration
Incorporation of Patterns
Refactoring

Clean Code

Readability
Naming
Functions
Comments
Formatting
Objects & Data Structures
Error Handling
Classes
Smells

Security is Pervasive!

Secure Development – Automated Builds

- ❑Manage the Security Risk of Using Third-Party Components
  - ❑“Dependency Management”
- ❑Use Approved Tools
- ❑Perform Static Analysis Security Testing
- ❑Perform Dynamic Analysis Security Testing
- ❑Penetration Testing
- ❑Track New Vulnerabilities, Release Notes

Secure Development – Monitoring & Analytics

- ❑Safe Logging
- ❑Log Collection, Archival & Access
- ❑Define Metrics and Compliance Reporting
- ❑Triggered Alerts

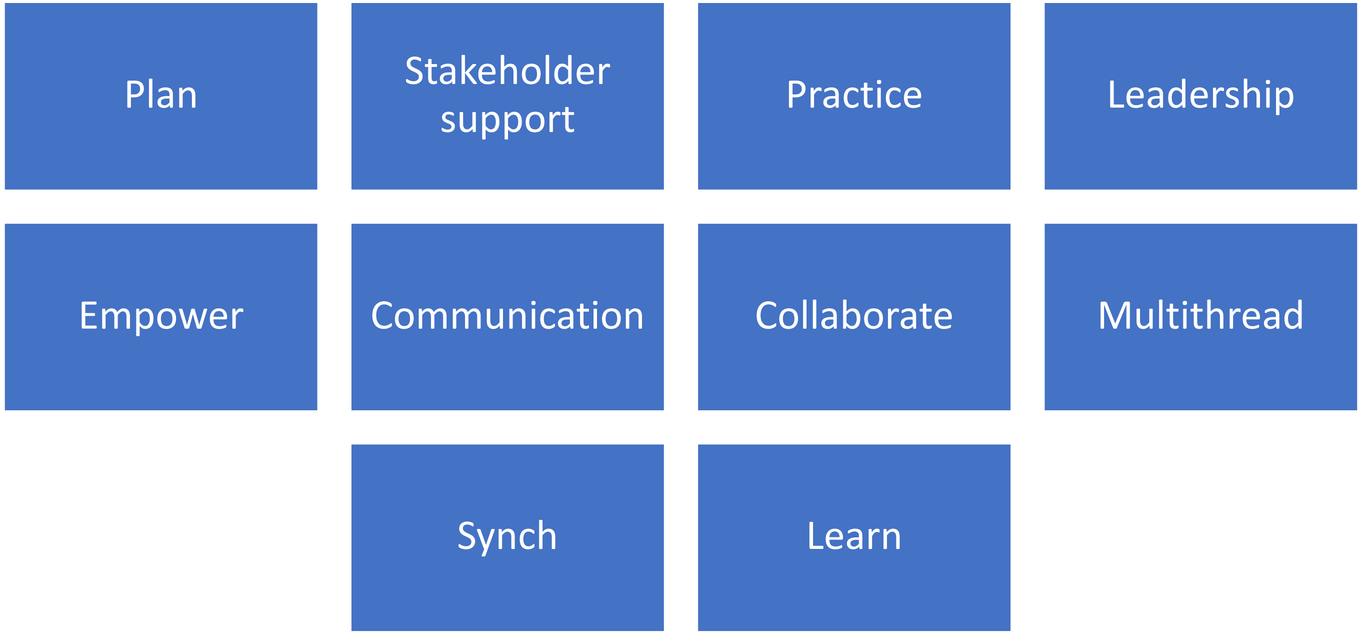
Secure Development – Incident Response

“Better to have, and not need, than to need, and not have”

F. Kafka

Secure Development – Incident Response

Any organization looking to establish their own incident response plan can benefit from the below best practices:



Plan

Stakeholder support

Practice

Leadership

Empower

Communication

Collaborate

Multithread

Synch

Learn

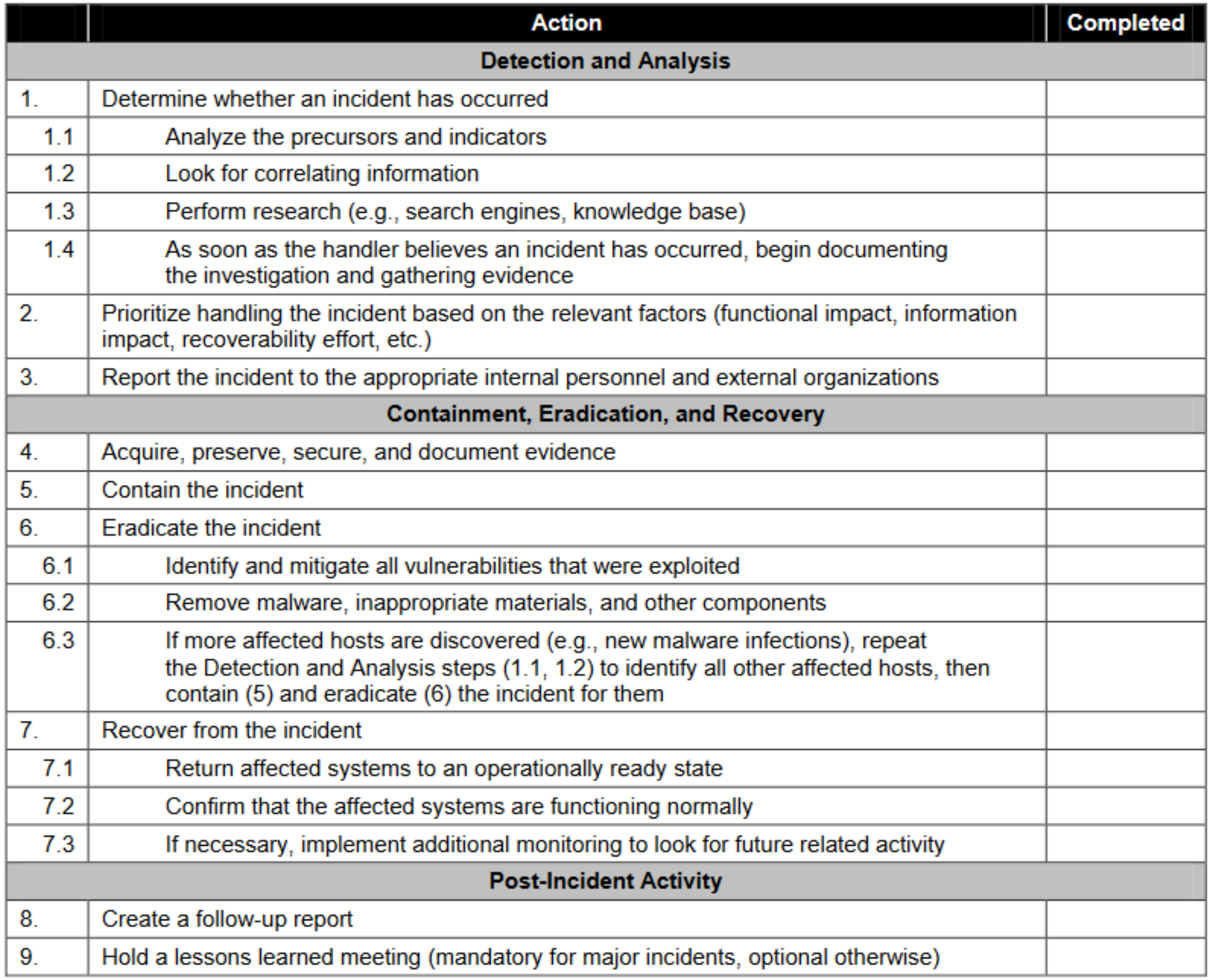
https://msrc-blog.microsoft.com/2019/07/01/inside-the-msrc-building-your-own-security-incident-response-process/

Secure Development – Incident Handling Checklist

Computer Security Incident Handling Guide

Incident Handling Checklist

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf



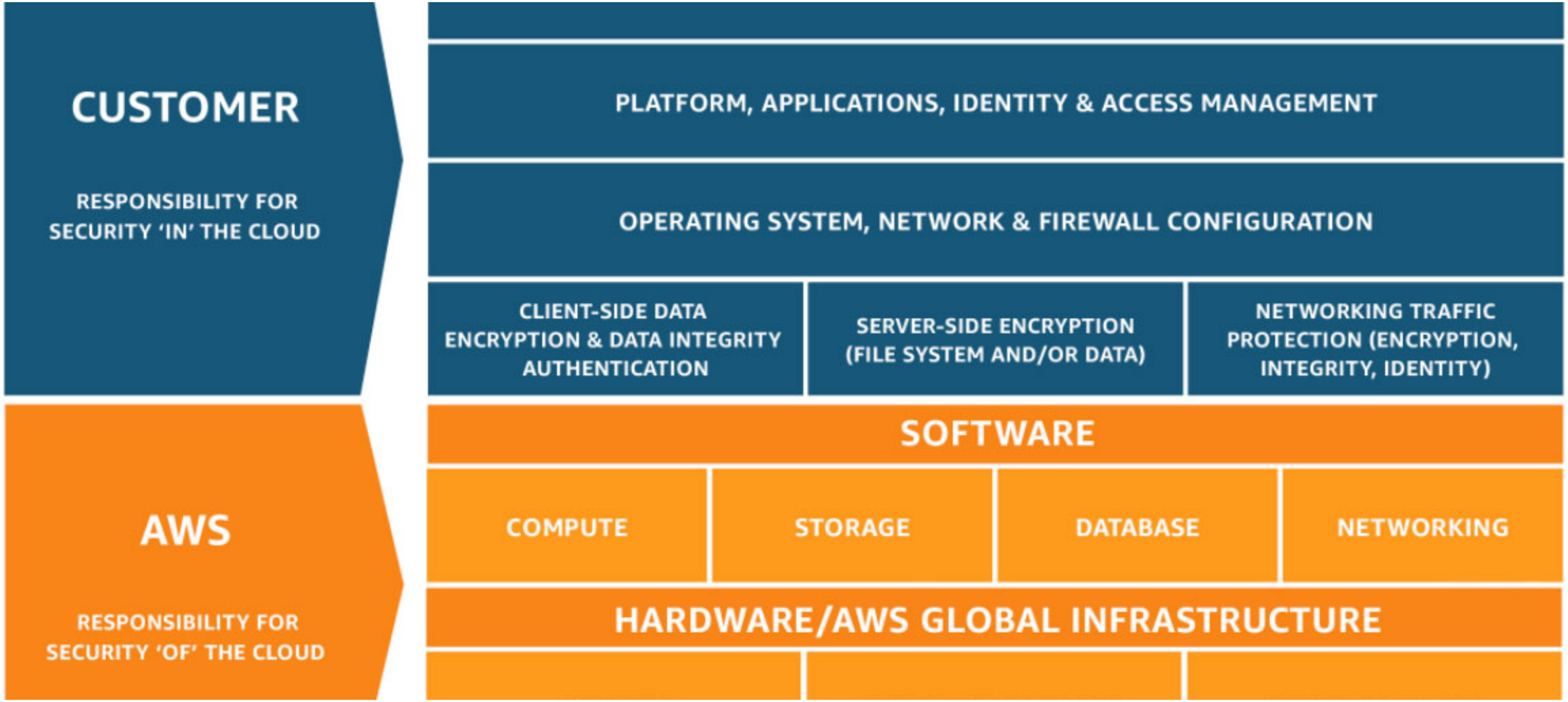
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Shared Responsibility Model

In the cloud, security is a partnership with your vendor.

You need to be aligned on security responsibilities.

Shared Responsibility Model - AWS



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

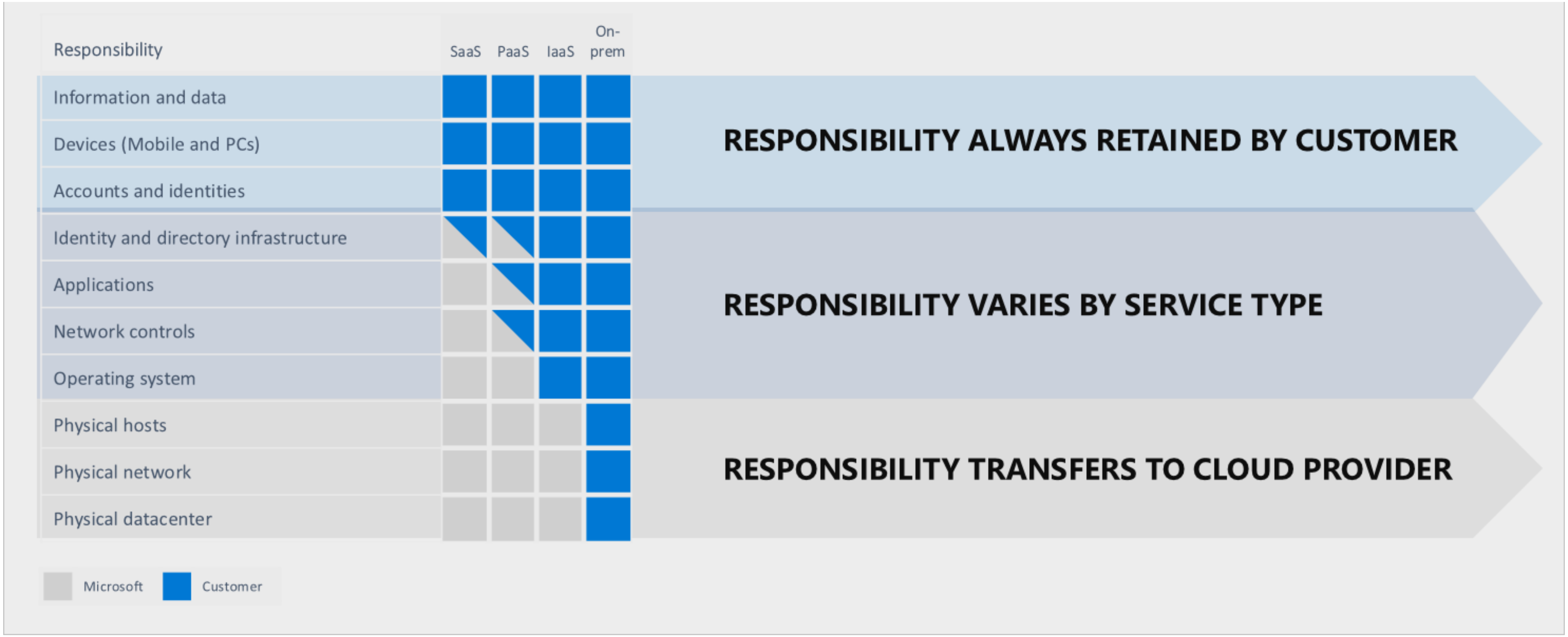
STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

Shared Responsibility Model - Azure



Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	■	■	■	■
Devices (Mobile and PCs)	■	■	■	■
Accounts and identities	■	■	■	■
Identity and directory infrastructure	◪	◪	■	■
Applications	□	◪	■	■
Network controls	□	◪	■	■
Operating system	□	□	■	■
Physical hosts	□	□	□	■
Physical network	□	□	□	■
Physical datacenter	□	□	□	■

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

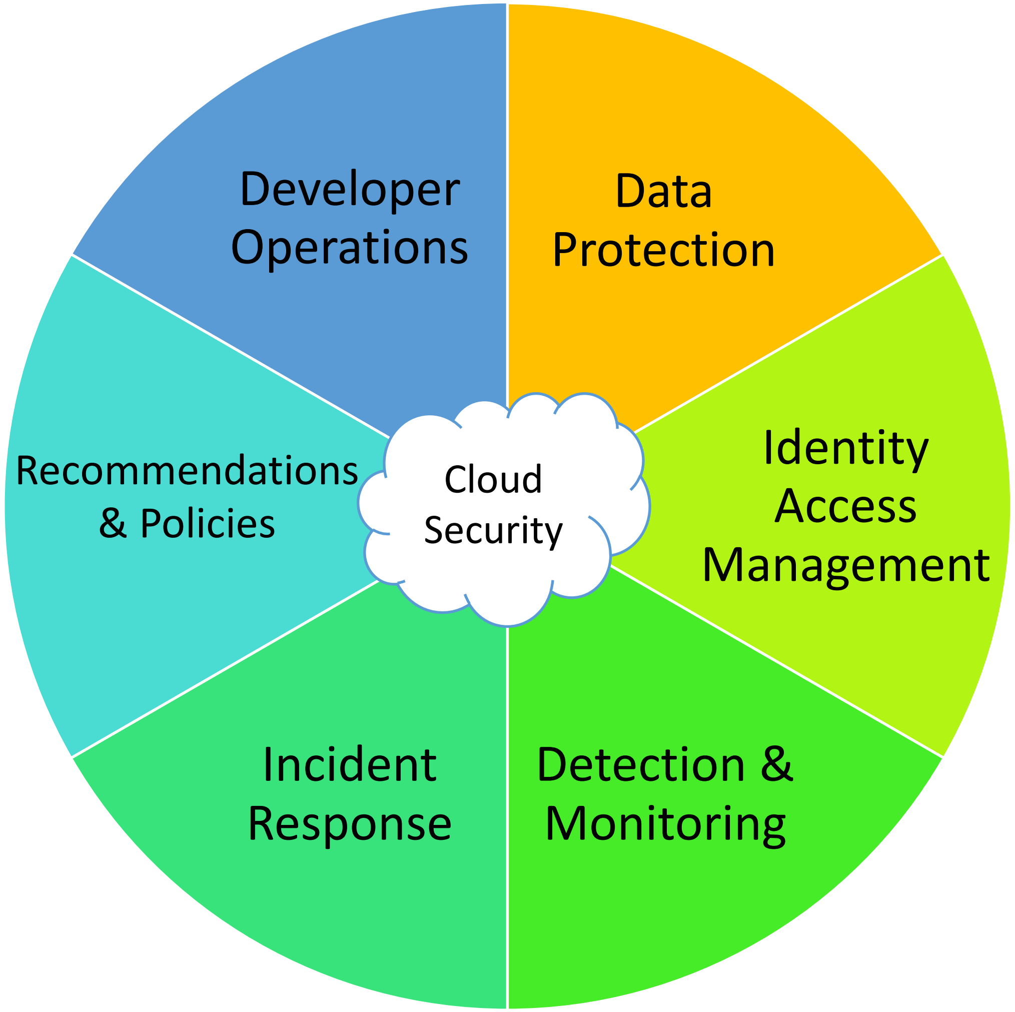
RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

□ Microsoft ■ Customer

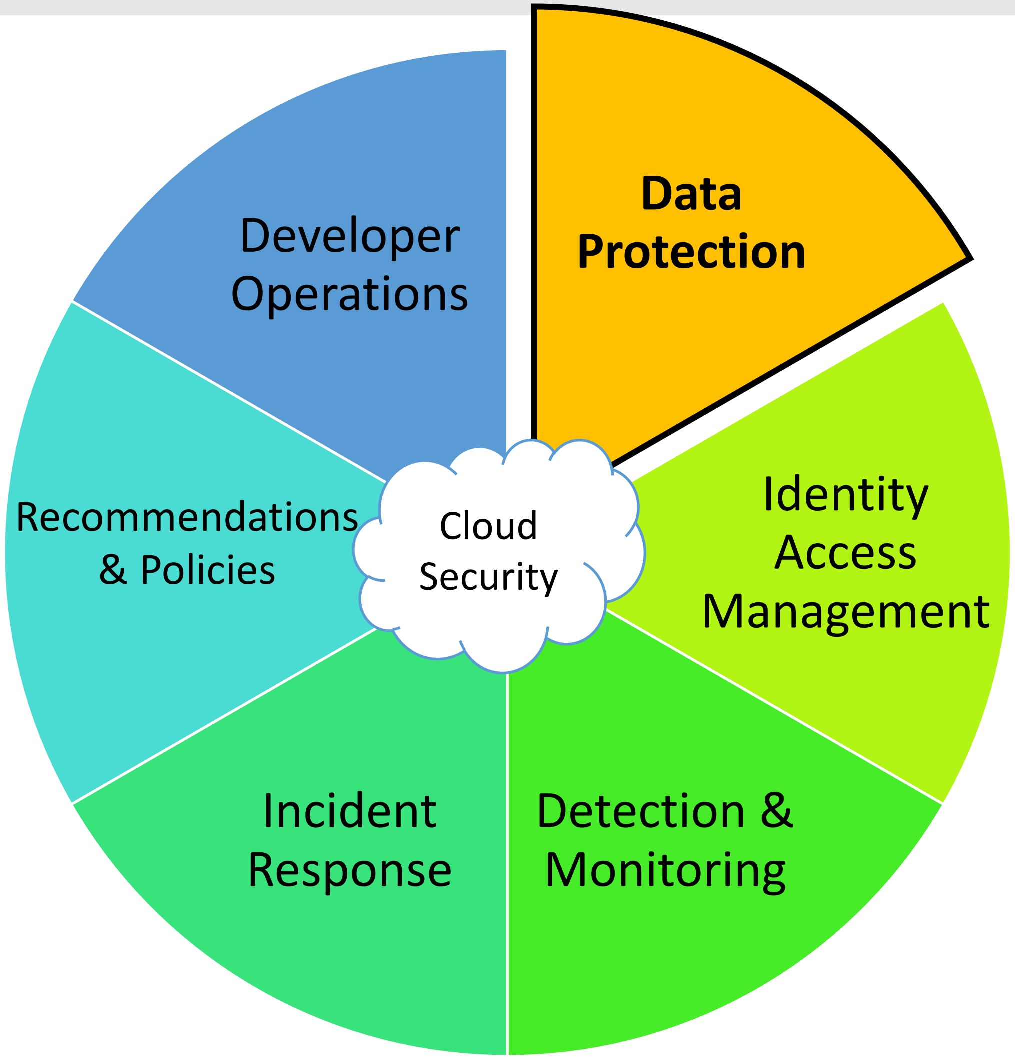
Cloud Security

Most Cloud Vendors have similar Security Concerns.

These concerns can be grouped into six areas.



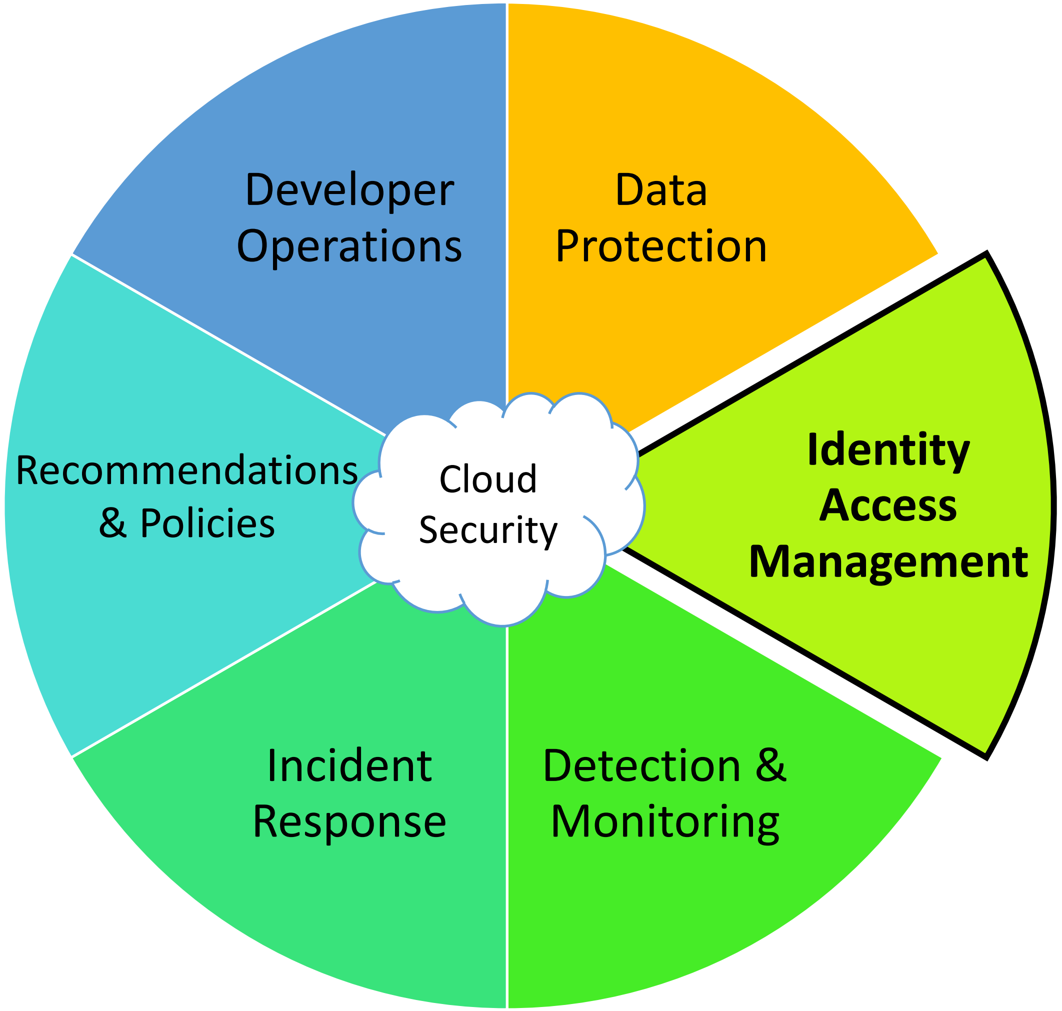
Cloud Security Basics – Data Protection



- ❑ Encrypt data at rest
- ❑ Encrypt data in transit
- ❑ Protect data in use
- ❑ Use mechanisms to keep people away from data

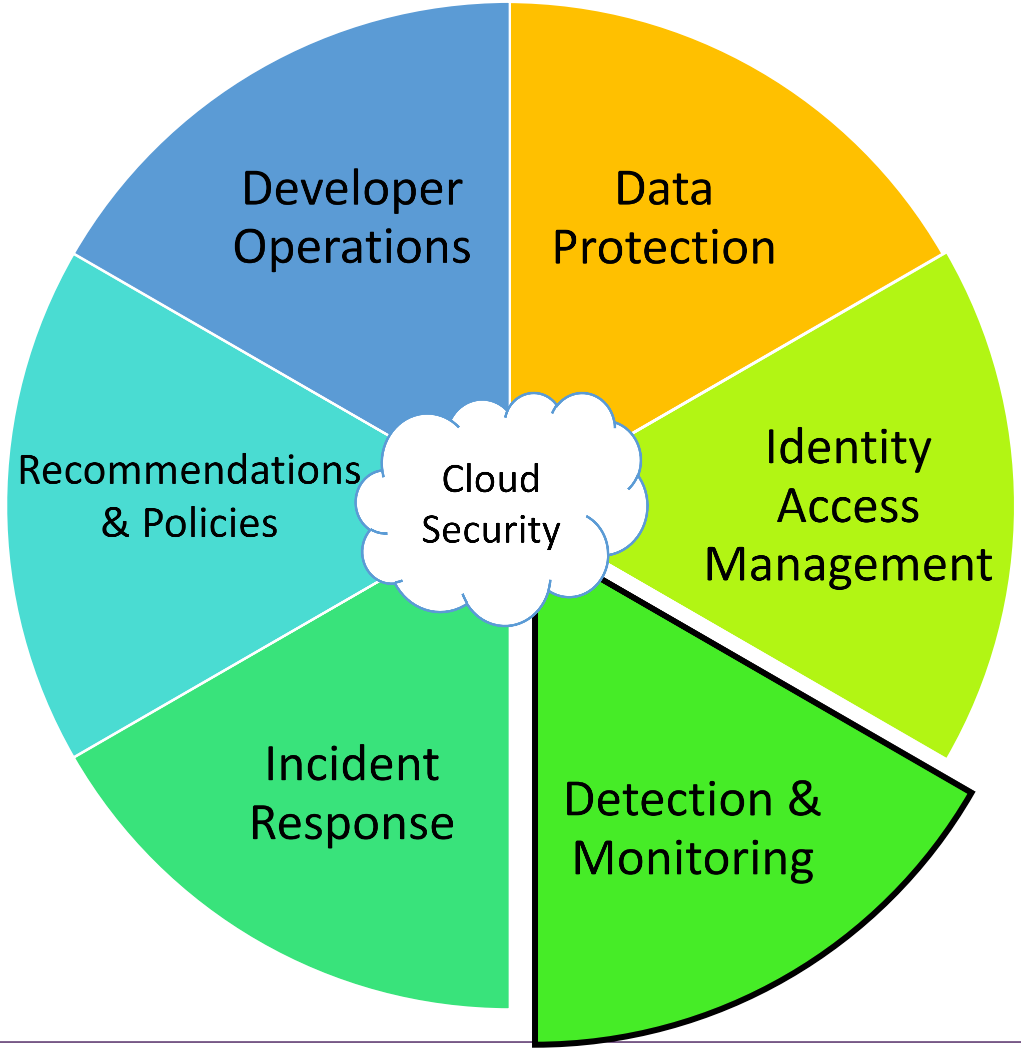
MICRO STRATEGIES
Technology Solutions. Business Results.

Cloud Security Basics – Identity Access Management



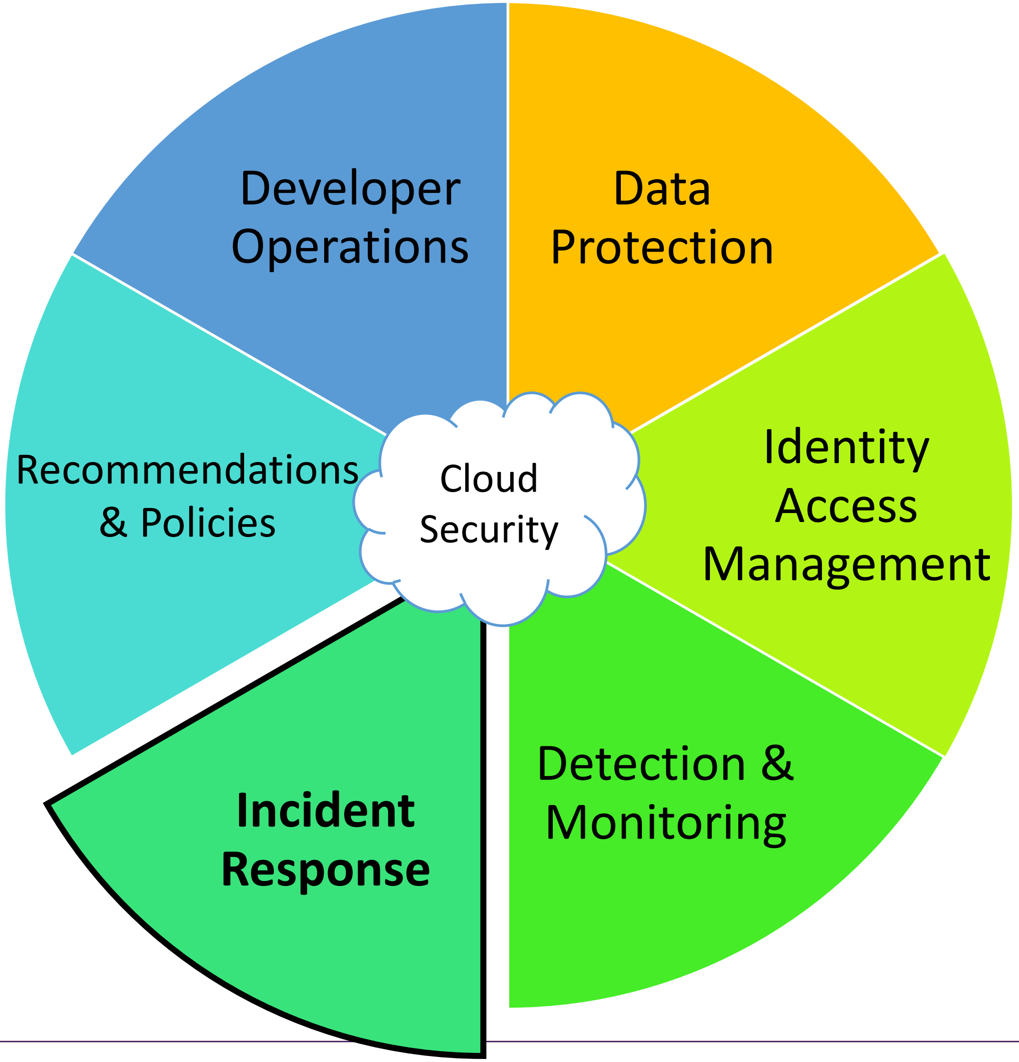
- ❑Secure your account
- ❑Use Centralized Identity Provider
- ❑Use Multi-Factor Authentication
- ❑Store Secrets Securely

Cloud Security Basics – Detection & Monitoring



- ❑Service and Application logging
- ❑Monitoring and Alerts
- ❑Investigate Events
- ❑Use Analytics to discover malicious behavior
- ❑Automatic Escalation of Events

Cloud Security Basics – Incident Response



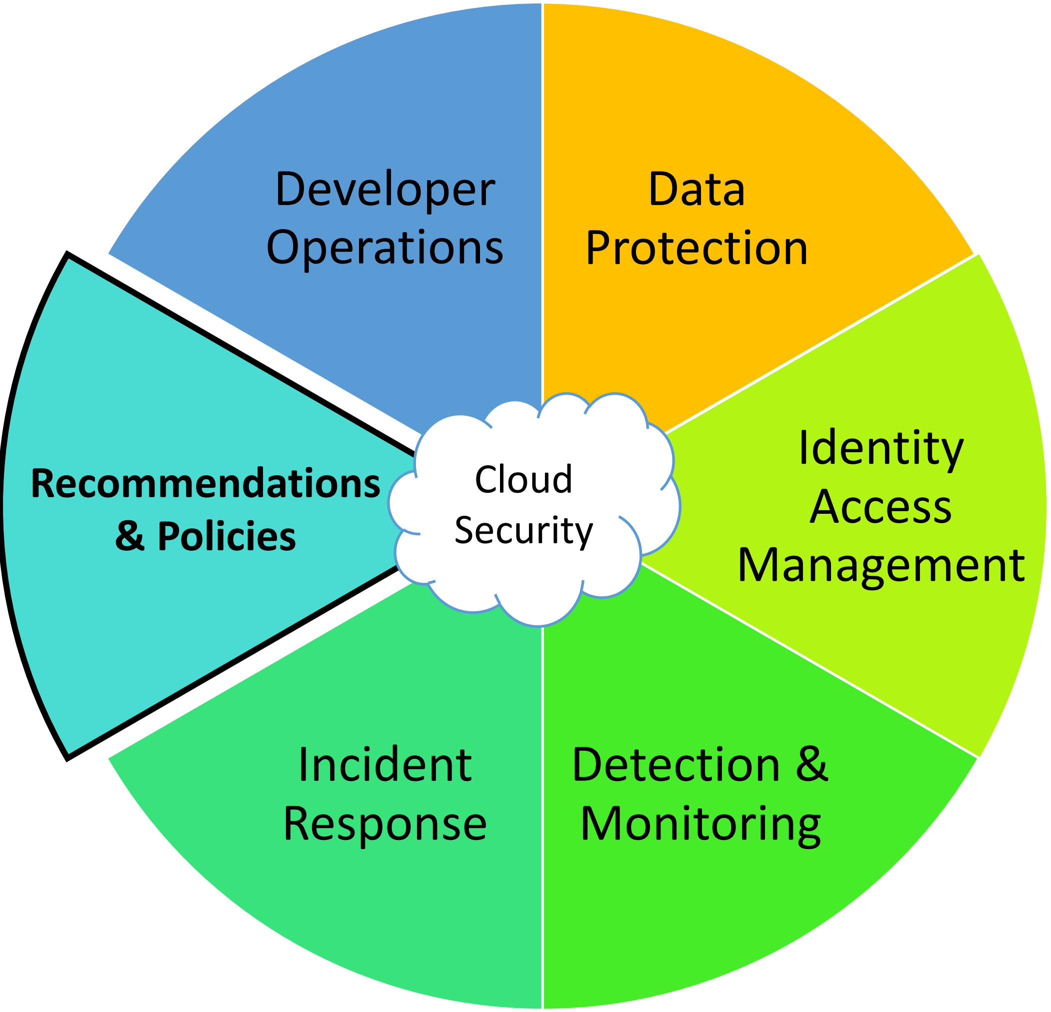
❑ Have an Incident Plan

❑ Practice Responding to Events

❑ Ensure security contacts are valid and notified.

❑ Automate Responses where possible

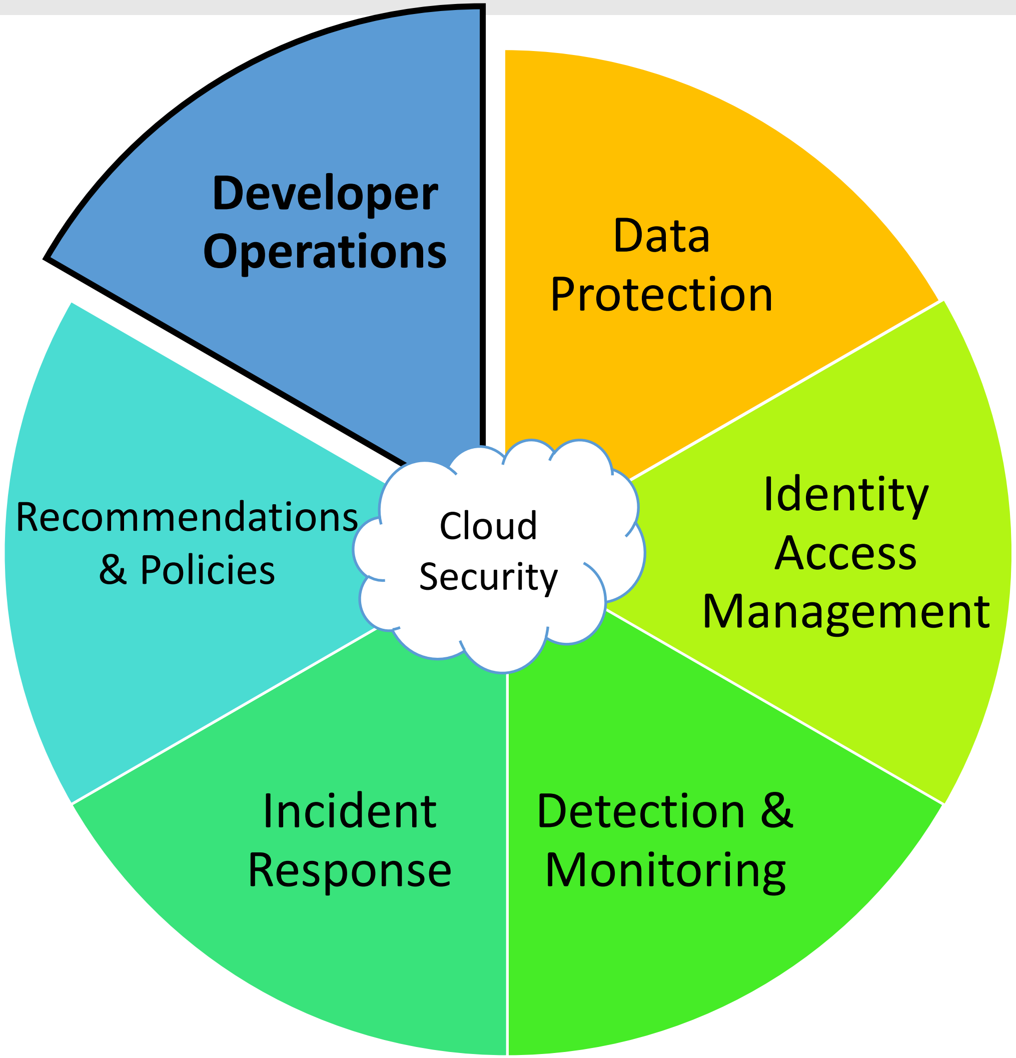
Cloud Security Basics – Recommendations & Policies



- ❑Follow Vendor Recommendations
- ❑Patch everything
- ❑Secure Endpoints, Firewall, Network
- ❑Define & Audit Policies

MICRO STRATEGIES
Technology Solutions. Business Results.

Cloud Security Basics – Developer Operations



- ❑Infrastructure as Code
- ❑Continuous Integration & Deployment/Delivery
- ❑Automation
- ❑Release Management
- ❑Auto-Scale & Load Testing
- ❑Security Testing

Additional References and Recommended Reading

Setting up authentication and security

https://docs.alfresco.com/6.2/concepts/auth-intro.html

Alfresco Security Best Practices Guide

https://www.slideshare.net/toniblyx/alfresco-security-best-practices-guide

Tech Talk Live #110: Alfresco Security Best Practices & Tips

https://youtu.be/qEFHmsEV4bc

Alfresco DevCon 2019: Encryption at-rest and in-transit

https://www.slideshare.net/toniblyx/alfresco-devcon-2019-encryption-atrest-and-intransit

Additional References and Recommended Reading

AWS Security Checklist

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Checklist.pdf

AWS Well-Architected Framework
https://aws.amazon.com/architecture/well-architected/

AWS Well-Architected Framework: Security Pillar

https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf

AWS Shared Responsibility Model

https://aws.amazon.com/compliance/shared-responsibility-model/

Additional References and Recommended Reading

Microsoft

Azure operational security checklist

https://docs.microsoft.com/en-us/azure/security/fundamentals/operational-checklist

Microsoft Security Development Lifecycle

https://www.microsoft.com/en-us/securityengineering/sdl/practices

Planning and operations guide

https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide

Shared responsibility in the cloud

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Additional References and Recommended Reading

IBM **Cloud**

Cloud-native security practices in IBM Cloud
https://www.ibm.com/cloud/architecture/files/ibm-cloud-security-white-paper.pdf

IBM Cloud Security: An Essential Guide

https://www.ibm.com/cloud/learn/cloud-security

IBM Cloud Security https://www.ibm.com/security/cloud

Shared responsibilities for using IBM Cloud offerings

https://cloud.ibm.com/docs/overview?topic=overview-shared-responsibilities

Additional References and Recommended Reading

Google Cloud

Google Cloud security best practices center

https://cloud.google.com/security/best-practices

Best practices for enterprise organizations

https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations

Google Cloud security foundations guide

https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

Thank You!

Alfresco Virtual DevCon 2020, Day 2 [September 16, 2020]

Jason Jolley – Director, Application Development

@jasonjolley jjolley@microstrat.com

Technology Solutions. Business Results.