KILLING THE CYBER KILL CHAIN

BERNARD JAUREGUI – 01/08/2019

Real life Cyber Kill Chain with AWS

Agenda:

1. Part 1 – The Cyber Kill Chain
2. Part 2 – Defence in Depth with AWS

PART 1
CYBER KILL CHAIN

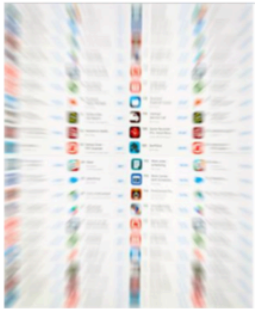
Security Strategies

Tim Rains
Regional Leader, Security & Compliance Business Acceleration
Worldwide Public Sector
Amazon Web Services

Protect & Recover Strategy

Endpoint Protection Strategy

Compliance as a Security Strategy



Application-centric Strategy

Identity-centric Strategy

Data-centric Strategy

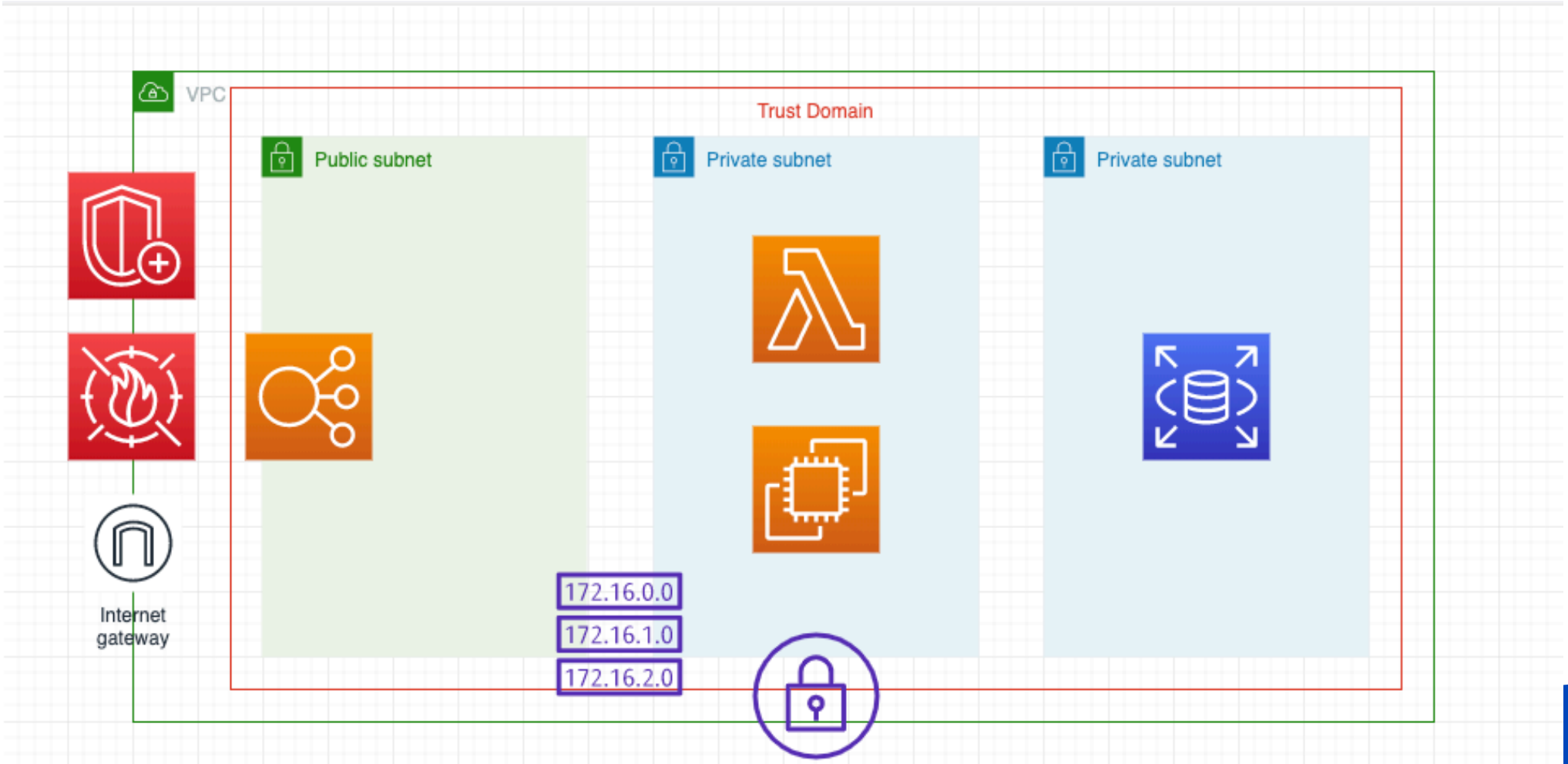
Security Clearances Strategy

Intrusion Kill Chain Strategy

POPULAR CYBERSECURITY STRATEGIES

COMPARATIVE STRATEGY SCORES

Strategy	Score
Protect & Recover	2
Security Clearances	2
Identity-centric	3
Data-centric	4
Compliance as a Security Strategy	5
Endpoint Protection	7
Application-centric	7
Intrusion Kill Chain	9



PROTECT & RECOVER

THE CHOCOLATE-FUDGE SECURITY STRATEGY

Unpatched vulnerabilities	• Potentially gives more time to patch • Users bring exploits through defenses
Security misconfigurations	• Can make it harder to find and exploit • Users bring exploits through defenses
Weak, leaked, stolen passwords	• Does not mitigate
Social engineering	• Does not mitigate
Insider threat	• Does not mitigate

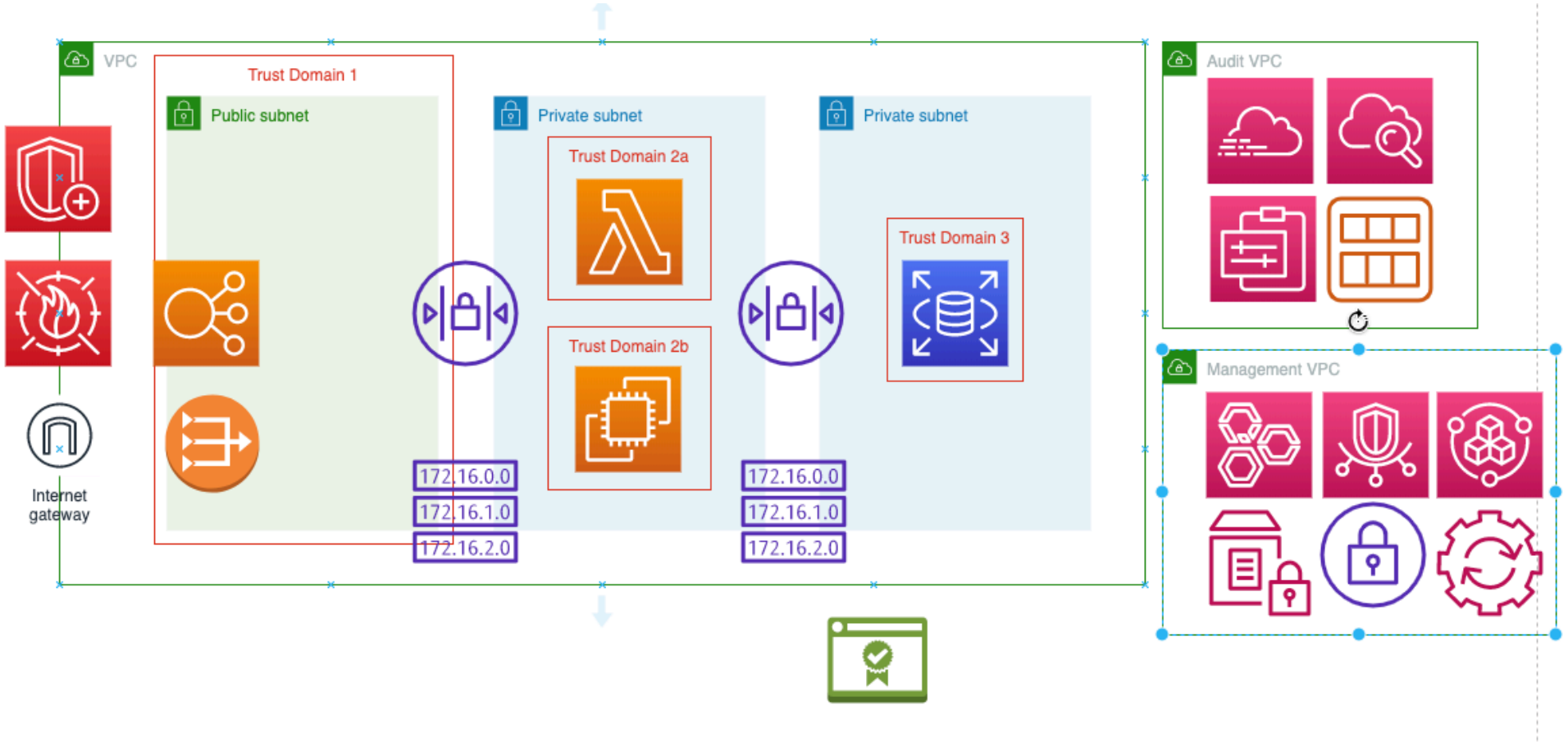
Good coverage (2pts)

Partial coverage (1pt)

Little or no coverage (0pts)

Cybersecurity fundamentals Score: 2/10

CYBER KILL CHAIN



Unpatched vulnerabilities	• Well managed vulnerability management program mitigates
Security misconfigurations	• Well managed vulnerability management program mitigates
Weak, leaked, stolen passwords	• Can implement effective mitigations
Social engineering	• Can mitigate in some scenarios by making it harder for attackers to be successful
Insider threat	• Can implement effective mitigations

Good coverage (2pts)

Partial coverage (1pt)

Little or no coverage (0pts)

Cybersecurity fundamentals Score: 9/10

SO WHAT IS THE CYBER KILL CHAIN?

Which
Kill Chain
to choose

- Intrusion Kill-Chain
- Cyber Security Kill-Chain
- ATT&CK for Enterprise
- Mitre Kill-Chain
- Lockheed Kill Chain
- Motiv Attack Chain

THERE ARE MANY VERSIONS

SO IN THE BEGINNING. . .

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins[*], Michael J. Cloppert[†], Rohan M. Amin, Ph.D.[‡]

Lockheed Martin Corporation

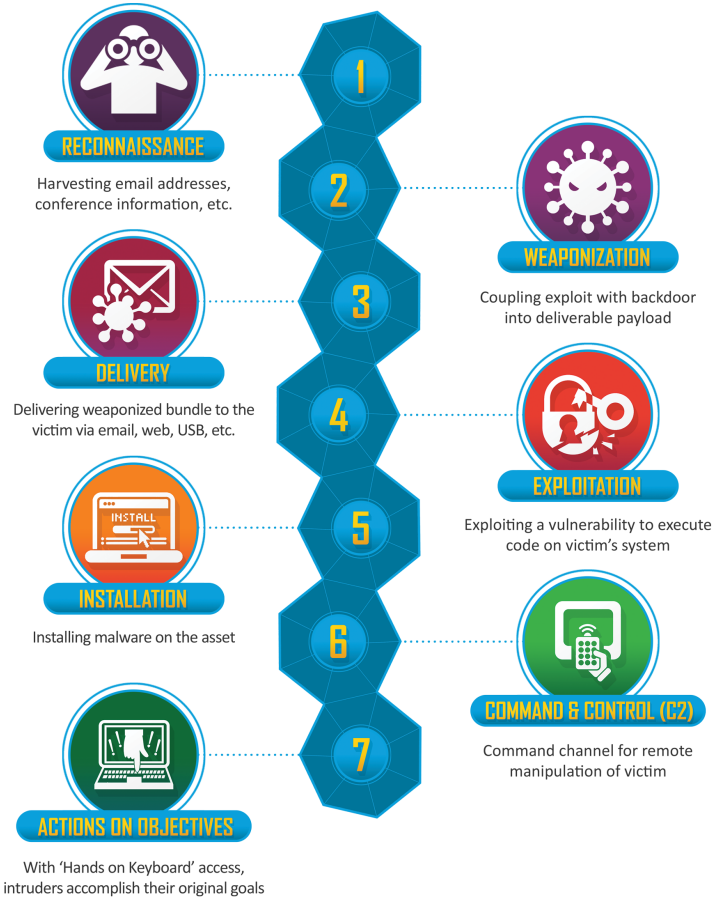
- **Find:** Locate the target
- **Fix:** Fix their location, make it difficult for them to move
- **Track:** Monitor their movement
- **Target:** Select an appropriate weapon or asset to use on the target to create desired effects
- **Engage:** Apply the weapon to the target
- **Assess:** Evaluate effects of the attack, including any intelligence gathered at the location

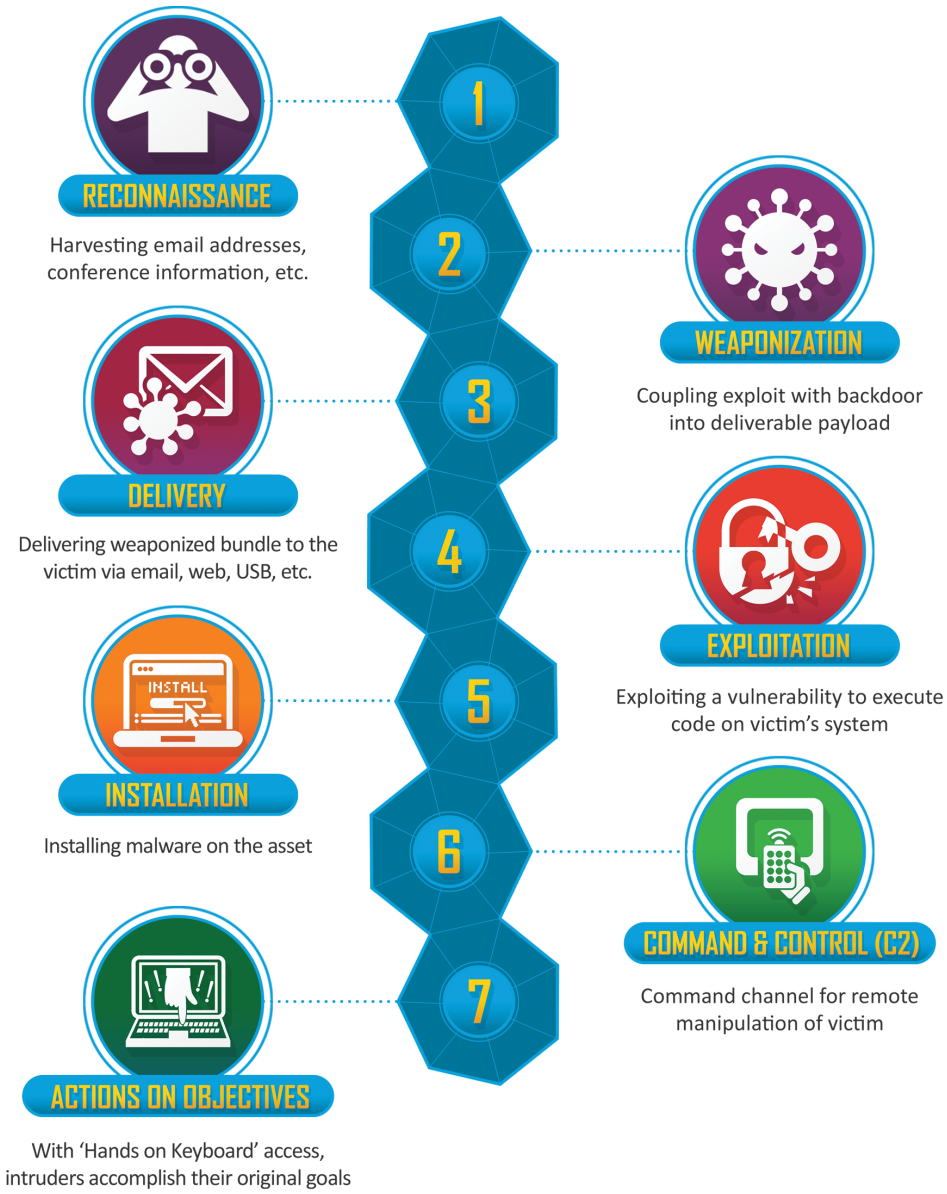
http://www.military-dictionary.org/F2T2EA

USAF ADVERSARY KILL CHAIN: F2T2EA

LOCKHEED MARTIN CYBER KILL CHAIN

- Seven steps
- Covers lifecycle of an attack
  - Starts before intrusion
  - Ends with the attacker achieving goals
- Is non-prescriptive
  - Not product focussed
  - Does not assume any technology
  - Flexible about attacker's objectives





Lockheed Martin CKC

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives

Other Kill Chain Steps

- Obfuscation
- Lateral Movement
- Credential Escalation
- Anti-Forensics
- Exfiltration
- Resurrection

THE CYBER KILL CHAIN IN 5 MINUTES

RECONNAISSANCE

- Observation
- Intelligence gathering
- Mapping the attack surface

- What are the endpoints
- What software stack is in use
- What security products are in use
- How do users identify themselves
- What is the likely architecture
- Stealing credentials

- Malware
- Phishing
- Leverage security vulnerabilities
- Pose as legitimate transaction

- Combinations of the above:
  - Pose as legitimate supplier invoice
  - Exploit PDF vulnerability
  - To escalate privilege
  - And install back door software

WEAPONIZATION

DELIVERY / INTRUSION

- Email
- USB media
- Compromised device (e.g. mouse)
- Unprotected features (e.g. File upload)
- FTP (!)
- PHP

- Exploiting vulnerabilities in:
  - Frameworks (PHP and anything based on PHP)
  - Unprotected administration features
  - Unpatched OS
  - Almost anything pre-pended with “legacy”
  - Zero Day Vulns

EXPLOITATION / PRIVILEGE ESCALATION

INSTALLATION

- Installing the means of compromise
- Back door software
- Tools for the next stage of the attack

- The aim is to maintain persistent access
- Create a “beach head”
- Further privilege escalation usually required

- Beach head established
- Beacon to Internet controller (often distributed)
- Establish comm's relay

- Provide expanded attack surface:
  - Hands on manual control
  - Payload insertion
  - Remote execution

- *Lateral Movement
  - Extend compromise
  - Further privilege escalation

- *Obscure activity

COMMAND AND CONTROL

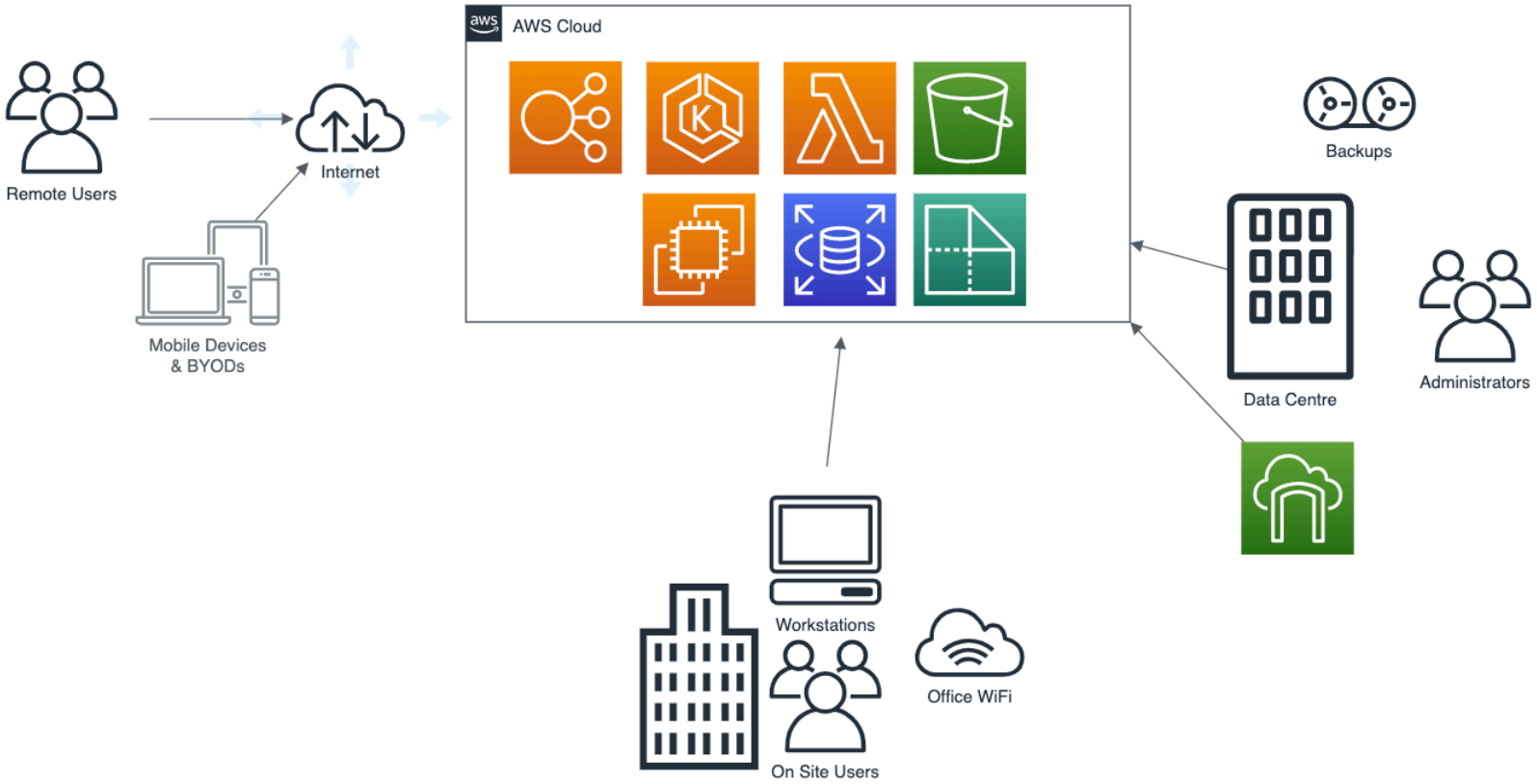
ACTIONS ON OBJECTIVES / EXFILTRATION

- Exfiltrate data
  - Collect
  - Encrypt
  - Establish comm's channel (e.g. DNS, Time, etc.)
  - Send
- Denial of Service (often a cover)
  - Distribute and arm payload
  - Execute on demand
- Jump box
- Data interference and manipulation


ZOMBIE
RESURRECTION

PART 2 - DEFENCE IN DEPTH

APPLYING THE CYBER KILL CHAIN IN PRACTICE



SYSTEM UNDER TEST

APPROACH

- What are we protecting & what is its value
- What is our threat model
- Who are the stakeholders
- What is our strategy

APPROACH

- What are we protecting & what is its value
- ~~What is our threat model~~
  - Cyber Kill Chain
- Who are the stakeholders
- ~~What is our strategy~~
  - Cyber Kill Chain

Cyber Kill Chain

gives us a lot

To Cover

- Large attack surface to consider
  - Seven Stages
  - Multiple opportunities
- We need:
  - A consistent approach
  - Shared language (terms)
  - Checks and balances

NO EASY ANSWERS

A GLOSSARY OF TERMS

- Characterizing Effects on the Cyber Adversary
  - By Deborah Bodeau and Richard Graubart, November 2013

MITRE

Characterizing Effects on the Cyber Adversary

A Vocabulary for Analysis and Assessment

Distinct aspects of a cyber defence strategy

- Detect
- Deny
- Disrupt
- Degrade
- Deceive
- Contain
- Respond
- Restore

WORDS OF MEANING

ENTER THE MATRIX

Phase	Detect	Deceive	Deny	Disrupt	Degrade	Contain	Respond	Restore	Learn
Reconnaissance									
Weaponization									
Delivery									
Exploitation									
Installation									
Command & Control									
Actions on Objectives									
Resurrection									

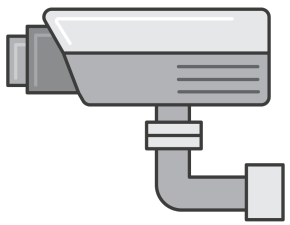
Phase	Detect	Deceive	Deny	Disrupt	Degrade	Contain	Respond	Restore	Learn
Reconnaissance	VPC Flow Logs Route 53								
Weaponization									
Delivery	AWS WAF								CloudWatch
Exploitation	Config Rules			Patch Management					CloudWatch Inspector
Installation	Inspector		RBAC (Cross Account) Organization Units						CloudWatch
Command & Control	VPC Flow Logs		CloudTrail Guard Rails						
Actions on Objectives			NACLs						
Resurrection			Autoscale Group Rotate Custom AMI's						

AWS SERVICES

FURTHER READING

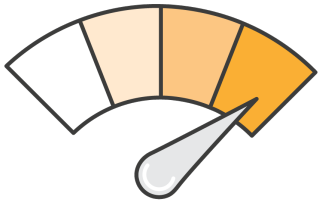
WHAT IS THE WELL-ARCHITECTED FRAMEWORK?

The Well-Architected Framework is designed to provide you with high-level guidance and best practices to help you build and maintain **secure**, **reliable**, **performant**, **cost optimized, and operationally excellent** applications in the AWS Cloud.



Security

Reliability



Performance Efficiency

Cost Optimization

Operational Excellence

				
Identity	**Detective control**	**Infrastructure security**	**Data protection**	**Incident response**
AWS Identity & Access Management (IAM)	AWS CloudTrail	Amazon EC2 Systems Manager	AWS Key Management Service	AWS Config Rules
AWS Organizations	AWS Config	AWS Shield	AWS CloudHSM	AWS Lambda
AWS Cognito	Amazon CloudWatch	AWS Web Application Firewall (WAF)	Server/Client Side Encryption	
AWS Directory Service	Amazon GuardDuty	Amazon Inspector	Certificate Manager	
AWS Single Sign-On	VPC Flow Logs	Amazon Virtual Private Cloud (VPC)	Secrets Manager	
	AWS Security Hub		S3 bucket policy, VPC Private Endpoints	

CLOUD ADOPTION FRAMEWORK

AWS REFERENCES

- White Papers and References
  https://aws.amazon.com/security/
  https://aws.amazon.com/compliance/
- Cloud Adoption Framework, Security Perspective
  https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf
- Well-Architected framework
  https://aws.amazon.com/architecture/well-architected/

KILLING THE CYBER KILL CHAIN

BERNARD JAUREGUI

Real life Cyber Kill Chain with AWS