InfoSec Capability Model

Access Admin

Administration

Directory

Identity

Provisioning

Synchronization

Access Control

Risk-Based Authentication

Authentication

Authorization

Federation

Policy-based Access

SSO

Federation

Multi/2Factor Authentication

Boundary

Firewall

Network Access Control

Proxy

Segmentation

System 2 System

User Connectivity

VPN

WAF

Content Control

Anti-Spam

Anti-Virus/malware

Data Encryption

Data Loss

Drive/Vol Encryption

Email Behavior Analysis

Email URL Protection

Phishing Education

Phishing Protection

Sandboxing

URL Filtering/Listing

Cryptography

Digital Signatures

Encryption

Key Management

Public Keys/Asymmetric

Secret Orchestration

Detection

Anomoly Detection

Endpoint Detection

Host Detection

Logging

Managed Security Provider

Network Detection

Security Event

Wireless Detection

Governance

Assurance

Awareness

Incident

Training

IAM Governance

Access Certification

Cloud Access

IAM Forensics

Privileged Access

Program

Arch & Engineering

Capacity

Planning

Policy

Strategy

Threat & Vulnerability

Asset Control

Compliance Monitoring

Mobile Application

Mobile Device

Patching

Research/Intelligence

Vulnerability

DAST

SAST/CAS

Endpoint Forensics

SERVICE or FUNCTION

MANAGEMENT CAPABILITY

InfoSec Capability Model

Access Admin

Administration Directory Identity Provisioning Synchronization

Access Control

Risk-Based Authentication Authentication Authorization Federation Policy-based Access SSO Federation Multi/2Factor Authentication

Boundary

Firewall Network Access Control Proxy Segmentation System 2 System User Connectivity VPN WAF

Content Control

Anti-Spam Anti-Virus/malware Data Encryption Data Loss Drive/Vol Encryption **Email Behavior Analysis** Email URL Protection Phishing Education **Phishing Protection** Sandboxing URL Filtering/Listing

Cryptography

Digital Signatures Encryption Key Management Public Keys/Asymmetric Secret Orchestration

Detection

Anomoly Detection **Endpoint Detection** Host Detection Logging Managed Security Provider Network Detection Security Event Wireless Detection

Governance

Assurance Awareness Incident Training

IAM Governance

Access Certification Cloud Access IAM Forensics Privileged Access

- Below baseline
 - Baseline
 - Above baseline
- N Not applicable

MANAGEMENT CAPABILITY

SERVICE or FUNCTION

Program

Arch & Engineering Capacity **Planning** Policy Strategy

Threat & Vulnerability

В Asset Control Compliance Monitoring Mobile Application Mobile Device В Patching Research/Intelligence В Vulnerability В DAST SAST/CAS

Capability Mapping to the CyberSecurity Framework

	Access Admin
1	Administration
	Directory
	Identity
	Provisioning
	Synchronization

Access Control		
Risk-Based Authentication	PR	
Authentication	PR	
Authorization	PR	
Federation	PR	
Policy-based Access	PR	
SSO	PR	
Federation	PR	
Multi/2Factor Authentication	PR	

Boundary		
Firewall		PR
Network Access Cor	ntrol	PR
Proxy	DE	PR
Segmentation		PR
System 2 System		PR
User Connectivity		PR
VPN		PR
WAF		PR

Content Control			
Anti-Spam			PR
Anti-Virus/malv	vare		PR
Data Encryptio	n		PR
Data Loss	DE	ID	PR
Drive/Vol Encryption		PR	
Email Behavior Anal DE		PR	
Email URL Pro	tectio	n	PR
Phishing Educa	ation		PR
Phishing Prote	ction		PR
Sandboxing		DE	PR
URL Filtering/L	isting	DE	PR

Cryptography	
Digital Signatures	PR
Encryption	PR
Key Management	PR
Public Keys/Asymmetric	PR
Secret Orchestration	PR

Detection		
Anomoly Detection	DE	
Endpoint Detection	DE	
Host Detection	DE	
Logging	DE	
Managed Security Provide	DE	
Network Detection	DE	
Security Event	DE	
Wireless Detection	DE	

Governance		
Assurance		PR
Awareness		PR
Incident	RE	RS
Training		PR

IAM Governance	
Access Certification	PR
Cloud Access	PR
IAM Forensics	RS
Privileged Access	PR

Program
Arch & Engineering
Capacity
Planning
Policy
Strategy

Threat & Vulnerability			
Asset Control			ID
Compliance Mo	onitor	ing	PR
Mobile Applica	tion	PR	ID
Mobile Device		PR	ID
Patching			PR
Research/Intelligence		ID	
Vulnerability	DE	PR	ID
DAST			ID
SAST/CAS			ID
Endpoint Forer	nsics		RS

CSF 1.1 Functions		
ID	Identify	
PR	Protect	
DE Detect		
RS	Respond	
RE	Recover	

MANAGEMENT CAPABILITY
SERVICE or FUNCTION

Network
WAF
Firewall
Network Detection
API Gateway
Segmentation
Authentication
Authorization
Logging
In-Transit Protection

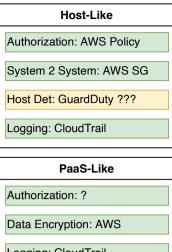
Host-Like
Authorization
System 2 System
Host Detection
Logging
PaaS-Like
raa3-Like
Authorization
Data Encryption

PaaS-Like
Authorization
Data Encryption
Logging

Data Services
Authorization
Drive/Vol Encryption
Data Encryption
Data Loss
Logging

Security Ops
Logging
Security Event
Anomoly Detection
Compliance Monitoring
Patching
Vulnerability

Network
WAF: AWS WAF
Firewall: AWS Firewall
Net Detection: GuardDuty
API Gateway: AWS API GW
Segmentation: AWS
Authentication: AWS Cognito
Authorization: AWS Policy
Logging: CloudTrail
In-Transit Protection: TLS



Logging: CloudTrail
Data Services
2
Authorization: AWS Policy
Drive/Vol Encryption: AWS
Data Encryption: AWS
Data Loss
Data 2033
Logging

Security Ops
Logging: CloudTrail
Security Event: CloudWatch
Anomoly Detection: GuardDuty
Compliance Mon: Inspector
Patching: AWS
Vulnerability: Inspector

InfoSec Capability Model

File:InfoSecCapabilityModel

Version: 1.0

Date:2022/03/15

http://www.secretchipmunk.com