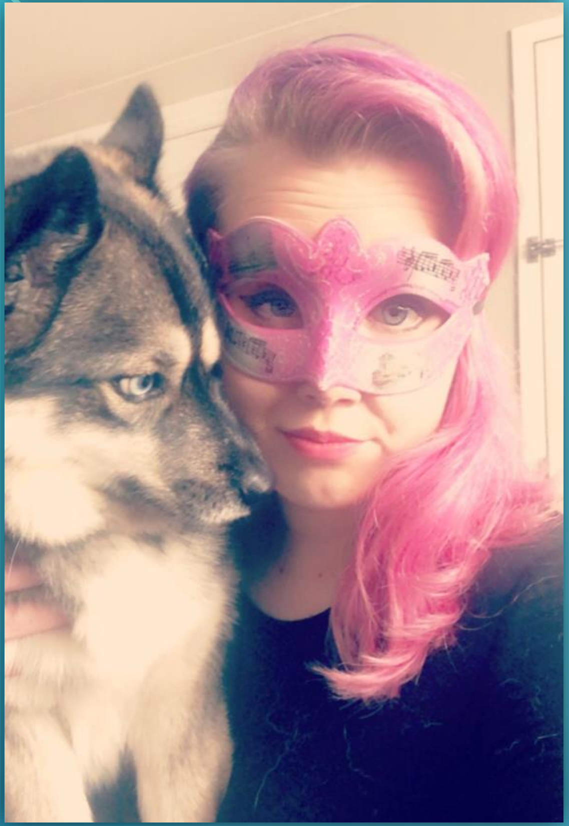
“CLOUD”Y WITH A CHANCE OF BREACH

HOW TO LEVERAGE THE CIS TOP 20 IN CLOUD ENVIRONMENTS

In-Security Newscast

Dowe Pwnem & Howe Network

WHO ARE WE?



Tricia A. Howard

@TriciaKicksSaaS

Marketing Manager, HolistiCyber

Protector of Darth the Pomsky

Micah K. Brown

@MicahKBrown

Gave the Food Hacking Talk at Derbycon 2019!

SOME CHALLENGES FOR CLOUD

CLOUD SPRAWL (COST, DATA PRIVACY, COMPLEXITY)

MISCONFIGURED ASSETS (WIDE OPEN STORAGE)

IN SOME CASES LACK OF CONTROLS IN CLOUD ENVIRONMENT

VIRTUAL ASSET HIJACK

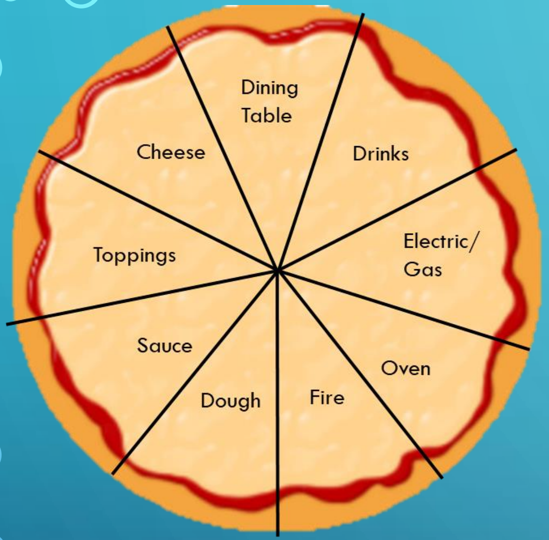
GOVERNANCE / RESOURCE

AVAILABILITY OF CLOUD EXPERTISE

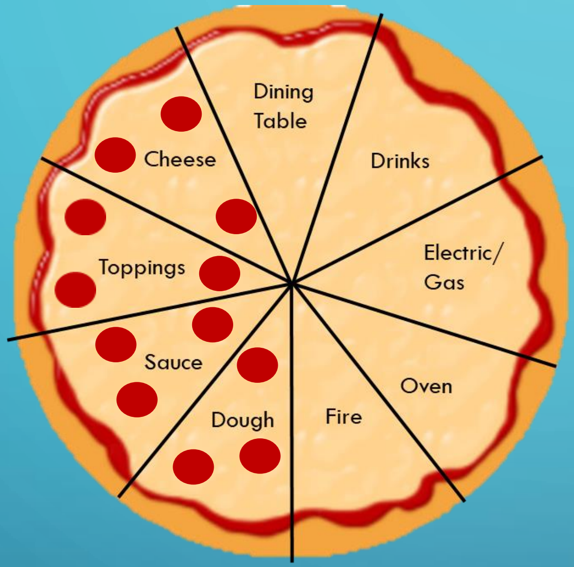
VENDOR LOCK IN

RELIANCE ON VENDOR FOR UPTIME

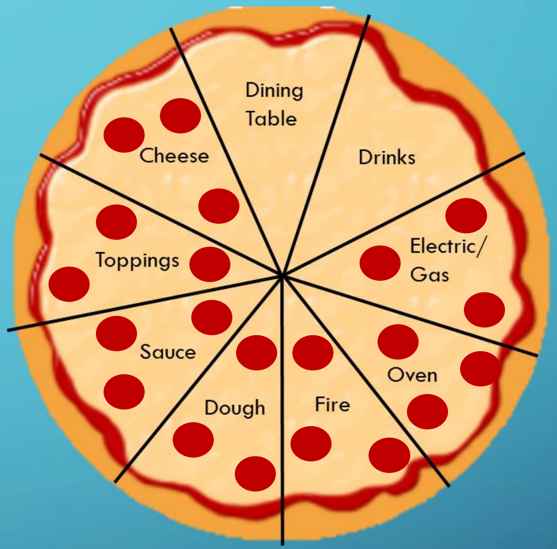
CLOUD OVERVIEW VIA PIZZA:
CHEESE – YOU MANAGE, PEPPERONI – VENDOR MANAGES



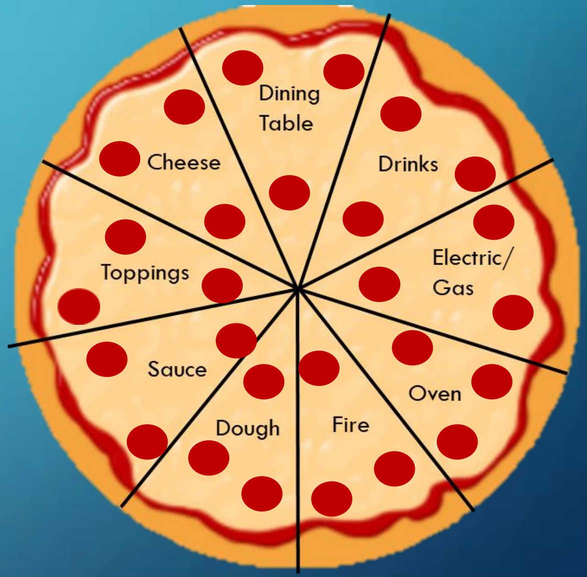
ON-PREM
(MADE AT HOME)



IAAS
(TAKE AND BAKE)

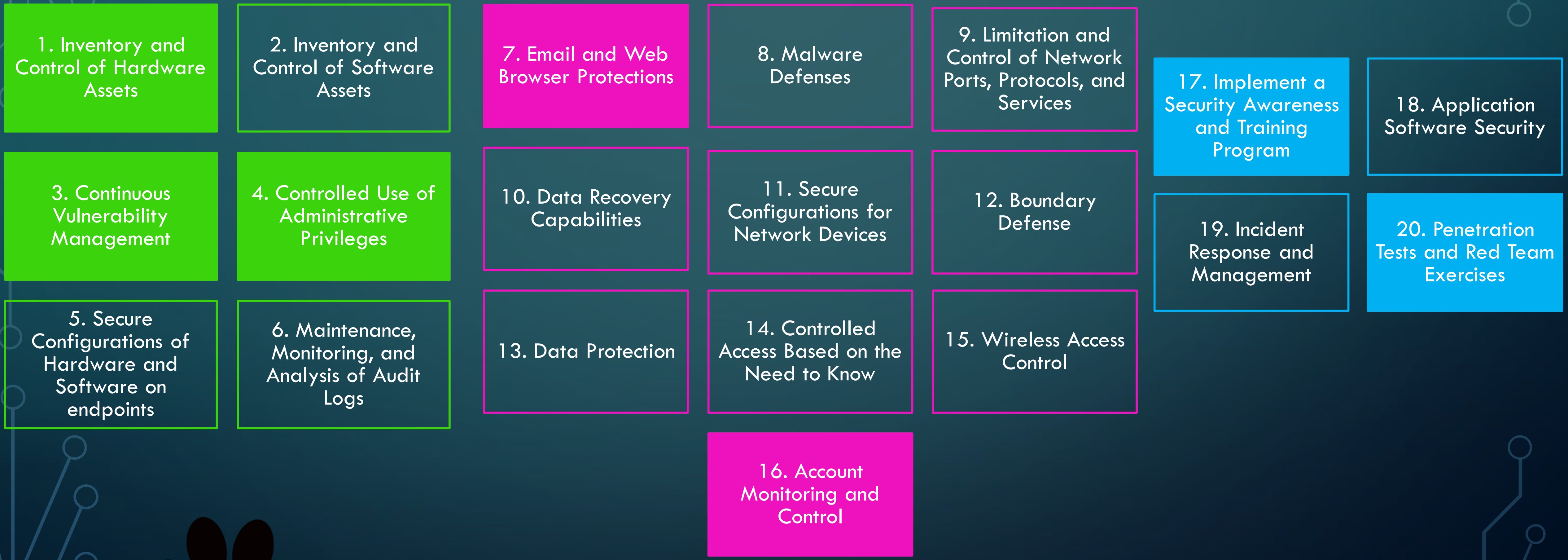


PAAS
(DELIVERY)



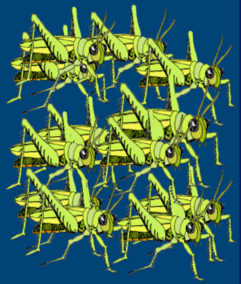
SAAS
(DINING OUT)

CIS CONTROLS



1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configurations of Hardware and Software on endpoints
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

7 DAY SECURITY FORECAST

SAT	SUN	MON	TUE	WED	THU	FRI
						
HI UV WARNING	CLEAR SKIES	WARM FRONT	COLD FRONT	SWARM OF LOCUSTS OF OLD TESTAMENT PROPORTIONS	SMALL TORNADO WARNING	THUNDERSTORMS WITH CHANCE OF HAIL
17: Security Awareness and Training	**1: Inventory and Control of Hardware Assets**	**4: Controlled Use of Admin Privileges**	**7: Email and Web Browser Protection**	**20: Penetration Tests and Red Team Exercises**	**16: Account Monitoring and Control**	**3: Continuous Vulnerability Management**

GRAPHIC KEY

1: Inventory and Control of Hardware Assets IaaS PaaS SaaS

Basic Controls

Foundational Controls

Organizational Controls

IaaS	Infrastructure as a Service	PaaS	Most of the controls apply
PaaS	Platform as a Service	PaaS	Some of the controls apply
SaaS	Software as a Service	PaaS	None of the controls apply

17: Implement a Security Awareness and Training Program

IaaS | PaaS | SaaS

- Perform ‘Skills Gap’ analysis and create training to address
- Implement Security Awareness program
- Update content regularly
- Secure authentication
- Phishing simulations and identification
- Social Engineering
- Handling sensitive information
- Unintentional data disclosure
- Identify and report security events

1: Inventory and Control of Hardware Assets

IaaS PaaS SaaS

IaaS, PaaS: Build Strong Asset Inventory

- Automate Active and Passive Discovery tools to build up asset list (CMDB)
- Augment CMDB with DHCP Logging
- Regular update CMDB and search for systems that do not have a CI

IaaS, PaaS: Virtual computers contain many parts virtual disk, network cards, other components. Common naming convention can make your job a lot easier

IaaS, PaaS: Regular audit for unauthorized devices

IaaS, PaaS: Strong port level ACL controls

IaaS, SaaS: Strong Certificate Management

4: Controlled Use of Administrative Privileges

IaaS PaaS SaaS

- Maintain inventory of admin accounts
- Align with your password policy
- Separation of admin and normal user accounts
- Protect admin accounts with MFA for ALL admin access
- Use dedicated 'systems' for all admin accounts (jump servers)
- IaaS, PaaS: Control access to scripting / programing tool to business use
- Log, Alert, Report: changes to Admin Users / Admin Groups
- Log, Alert, Report: failed auth of Admin Users

7: Email and Web Browser Protection

IaaS PaaS SaaS

- Standardize on approved email clients (software and browsers) and restrict rest.
- Disable unauthorized browser or email client plug-ins
- Limit use of scripting in emails
- IaaS, PaaS: Enforce Network-based URL Filters
- IaaS, PaaS: Limit web browsing and email on cloud assets to what is required
  - Log all URL requests
- IaaS, PaaS: Use DNS Filtering
- IaaS, PaaS: Use DMARC and enable Receiver Side Verification
- IaaS, PaaS: Block unnecessary file types
- IaaS, PaaS: Sandbox all email attachments*

IT'S
INTERMISSION
TIME, Folks!

20: Penetration Tests and Red Team Exercises

IaaS PaaS SaaS

- Establish Penetration Testing Program
- Conduct regular external and Internal Penetration Tests
- Perform periodic red team exercise
- Test for presence of unprotected systems info and artifacts
- Create a test bed for elements for those devices not typically tested
- Use vulnerability scanning and penetration testing tools together
- Ensure penetration tests are documented in machine readable format
- Control, monitor, and alert access accounts associated with penetration tests

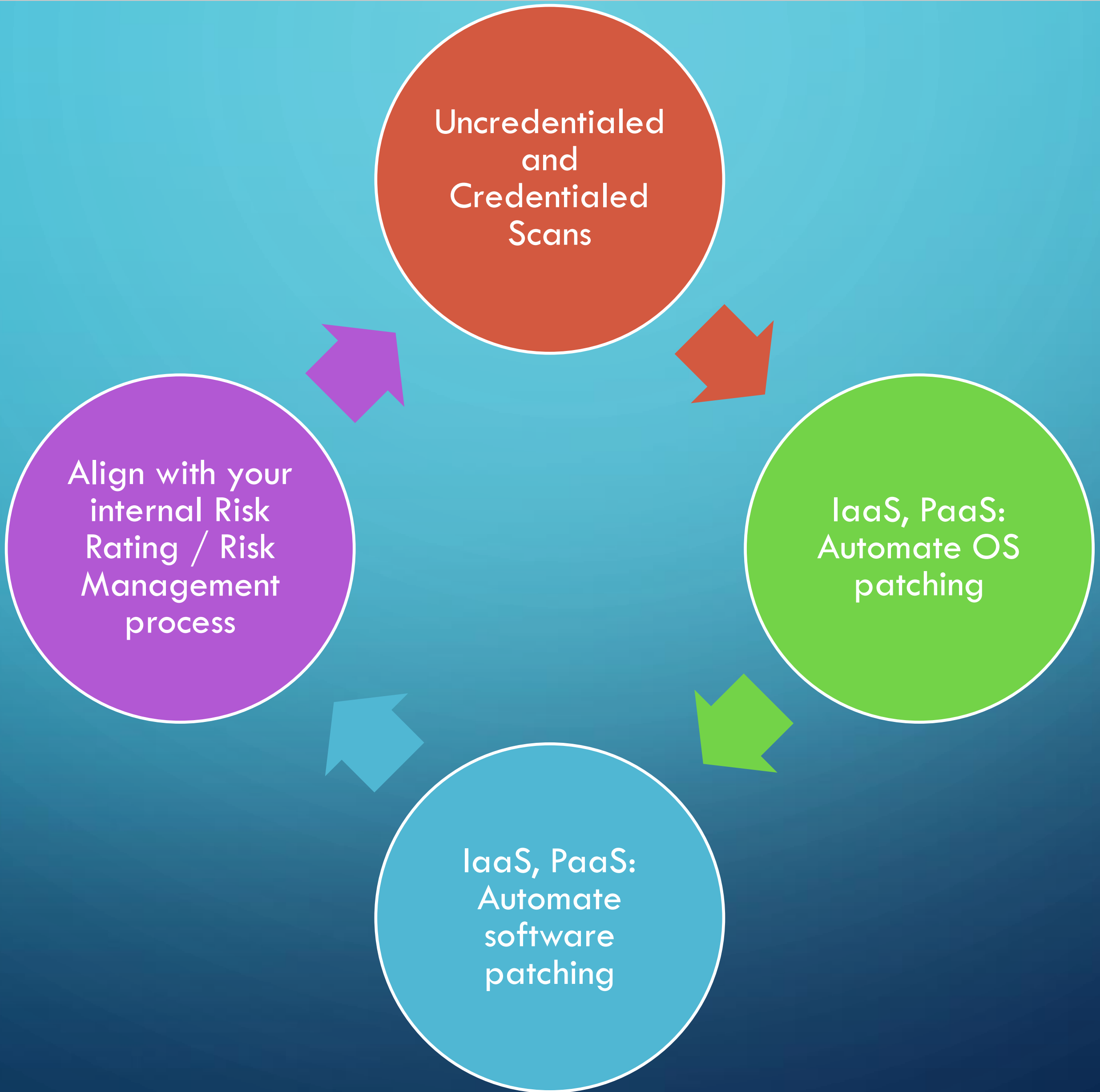
16: Account Monitoring and Control

IaaS PaaS SaaS

- Maintain inventory of authentication systems
- Configure centralized point of authentication
- Require MFA
- Encrypt / hash authentication credentials
  - IaaS, PaaS: Encrypt transmission of authentication attempts
- Maintain inventory of accounts
- Establish account revocation
- Disable unassociated / dormant accounts
- Ensure accounts have expiration date
- IaaS: Lock system after time of activity
- Monitor / Alert attempt to access deactivated accounts
- Alert on anomaly deviations in account login behavior

3: Continuous Vulnerability Management

IaaS PaaS SaaS



Uncredentialed and Credentialed Scans

IaaS, PaaS: Automate OS patching

IaaS, PaaS: Automate software patching

Align with your internal Risk Rating / Risk Management process

Thank you for your time and support. Questions?

Stay cloudy San Diego!