

# *The 20 Critical Security Controls: How You Doing?*

**Randy Marchany**

CISO, Virginia Tech

marchany@vt.edu

<https://security.vt.edu>

Twitter: @randymarchany



# *Most Common Security Mistakes Made by Individuals (2001)*

- Poor password management
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- Not installing anti-virus software ✓
- Laptops on the loose
- Blabber mounts (file access open to the world)
- Plug and Play without protection
- Not reporting security violations
- Always behind the times (OS, application patches)
- Keeping an eye out inside the organization

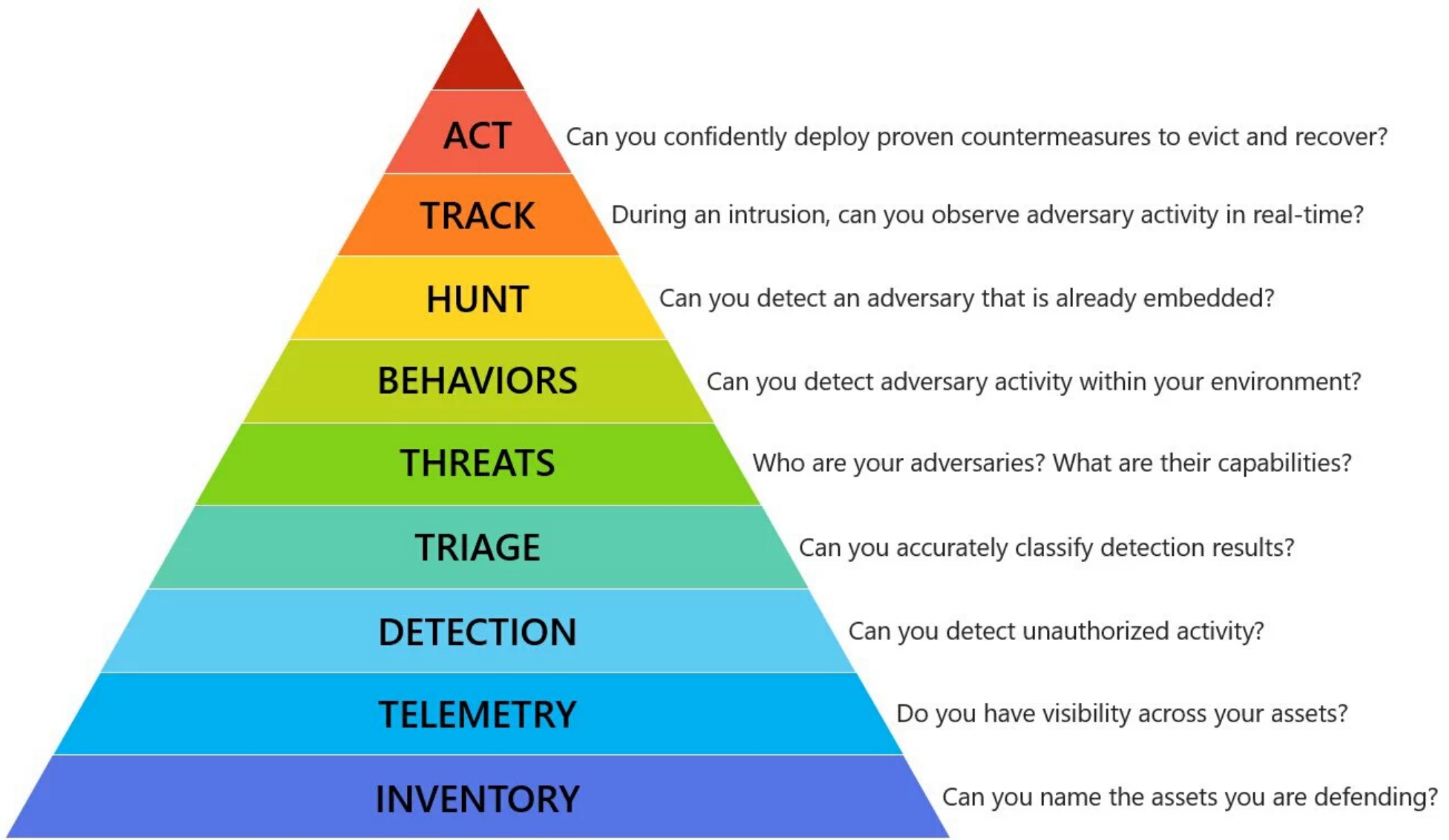
# Net Access isn't Equal

- Some areas have no internet access
- Some areas have poor internet access
  - <https://it.vt.edu/resources/home-internet-tips.html>
- ISP rate based charge structure
- Campus WiFi Parking lots
  - <https://vtnews.vt.edu/notices/it-nis-driveupwifi.html>
- EDITORIAL COMMENT – My Opinion only (Flame Retardant Suit On)
  - #WFH shows the Net has become a utility.
  - It should be regulated as such.
  - 21<sup>st</sup> Century version of Rural Electrification Project

# *Hacker Attack Goals*

Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
  - **ATTACK** other sites using hacked assets
  - **DESTRUCTION** of company data (deletion or ransomware).
- 
- **DEFEND** accordingly



Source: Matt Swann, <https://github.com/swannman/ircapabilities>

TCTC 2021

Marchany Copyright  
2021



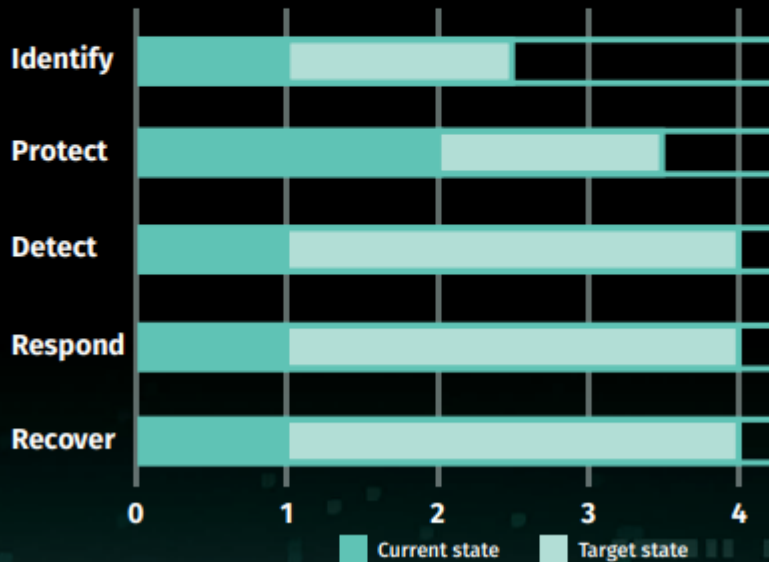
# 1 Find Frameworks that Fit

# 2 Map Controls to the Framework

# 3 Manage and Assess Risk

# 4 Measure Maturity and Progress

Use a risk-based approach to prioritize security controls to reach a desired target state. Developing a roadmap allows to measure maturity and progress over time.



Risk Acceptance

# 5 Monitor and Measure Security

To continuously improve security effectiveness:

- Establish and measure meaningful security metrics.
- Monitor those metrics frequently enough to minimize incident impact.
- Take action rapidly and efficiently to effectively improve overall security.

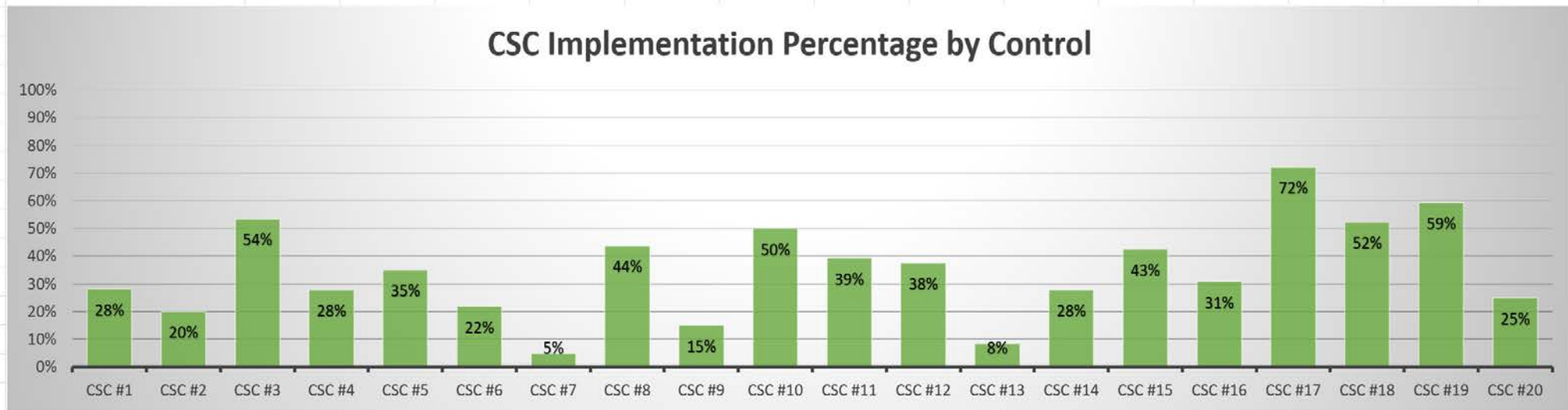
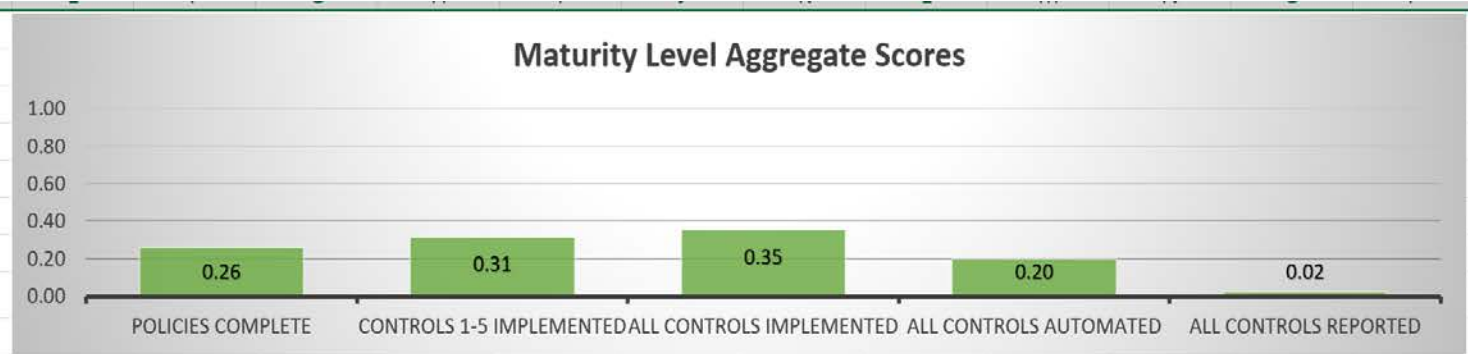
The CIS Controls have proven to be an effective starting point for selecting key security metrics.

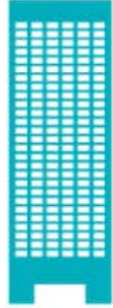
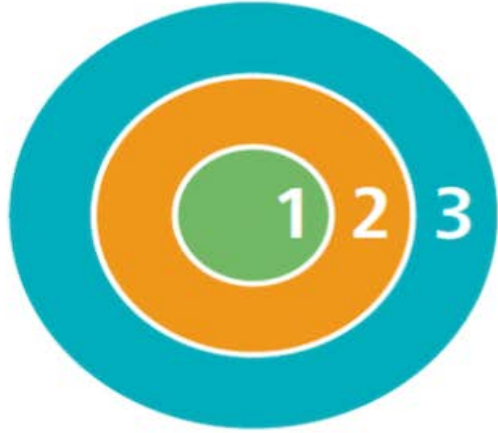
Establish continuous monitoring guidelines that define which controls should be monitored on a weekly, monthly, or on an ongoing basis.

Frequency	CIS Control	Example Measure
Continuous and Ongoing	(1) Inventory of Devices	Percentage of unauthorized assets that have not been removed from the network, quarantined, or added to the inventory in a timely manner
	(3) Continuous VA and Remediation	Percentage of vulnerabilities that have not been remediated in a timely manner
Weekly	(6) Maintenance, Monitoring, Analysis of Logs	Percentage of assets that are not configured to aggregate appropriate logs to a SIEM or log analytic tools for correlation and analysis
	(9) Limitation/Control of Ports, Services	Percentage of hardware assets that are not configured to require only network ports, protocols, and services with validated business needs
Monthly	(2) Software Inventory	Percentage of high-risk business applications that have not been physically or logically segregated from other business systems
	(5) Secure Configurations	Percentage of assets that do not have a documented, standard security configuration

# Gap It! Audiscripts.com

Maturity level:	Description:	Score:
Level One	Policies Complete	0.26
Level Two	Controls 1-5 Implemented	0.31
Level Three	All Controls Implemented	0.35
Level Four	All Controls Automated	0.20
Level Five	All Controls Reported	0.02
<b>Maturity Rating*:</b>		<b>1.15</b>
*Rating is on a 0-5 scale.		





### **Implementation Group 3**

A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls



### **Implementation Group 2**

An organization with moderate resources and cybersecurity expertise to implement Sub-Controls



### **Implementation Group 1**

An organization with limited resources and cybersecurity expertise available to implement Sub-Controls



## Basic

- 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 Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

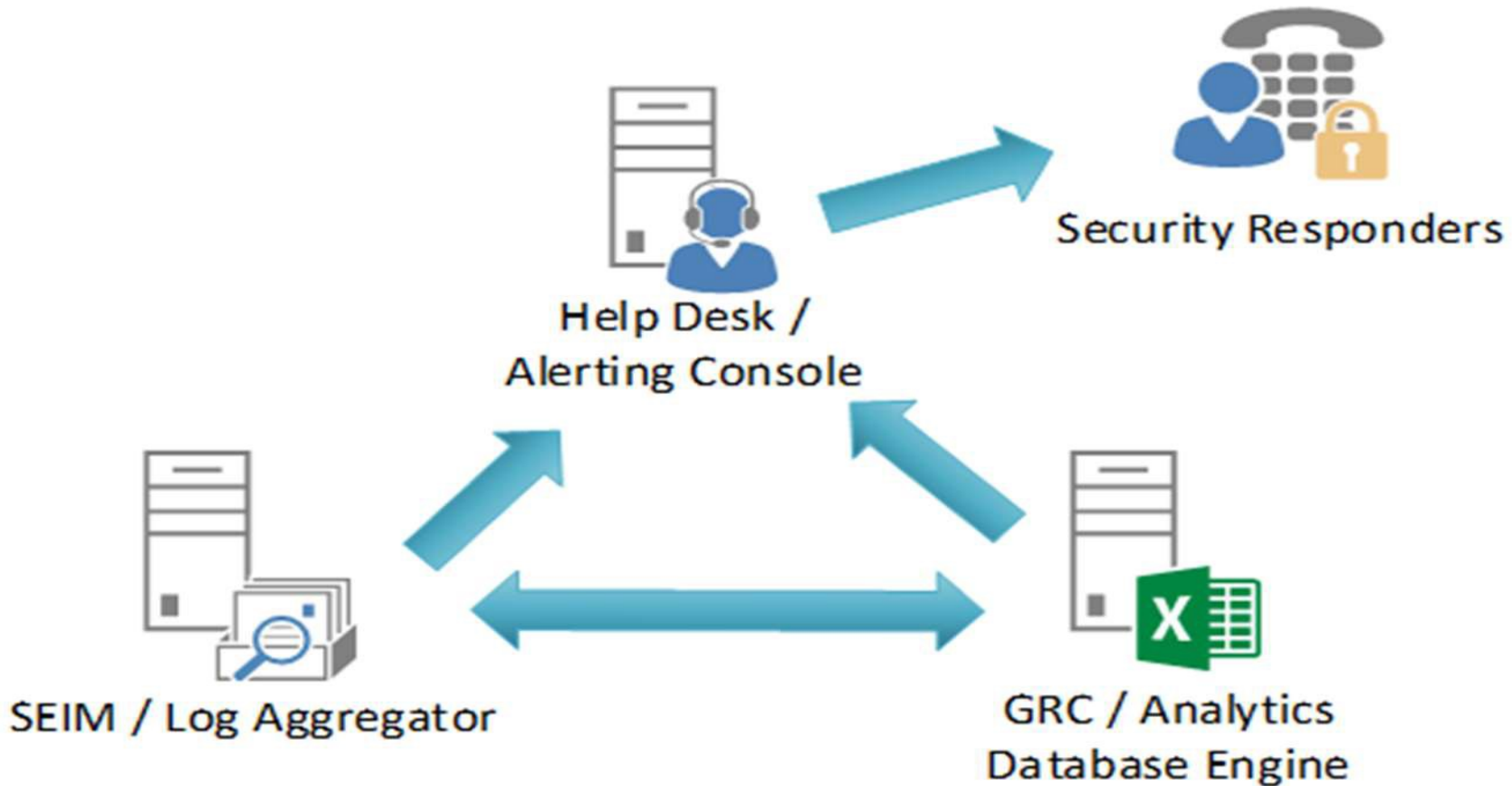
## Foundational

- 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 Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

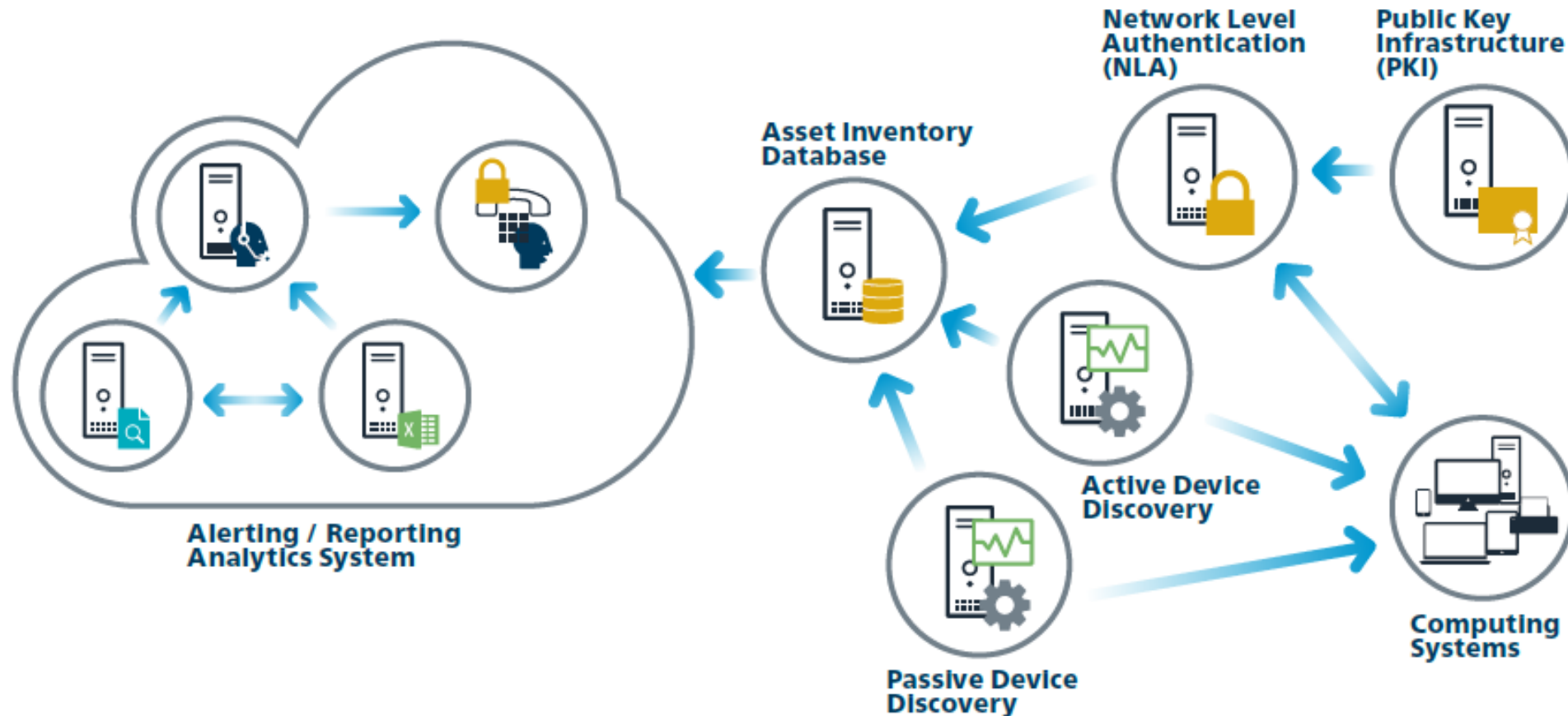
## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

# CSC Alerting/Reporting/Analytics

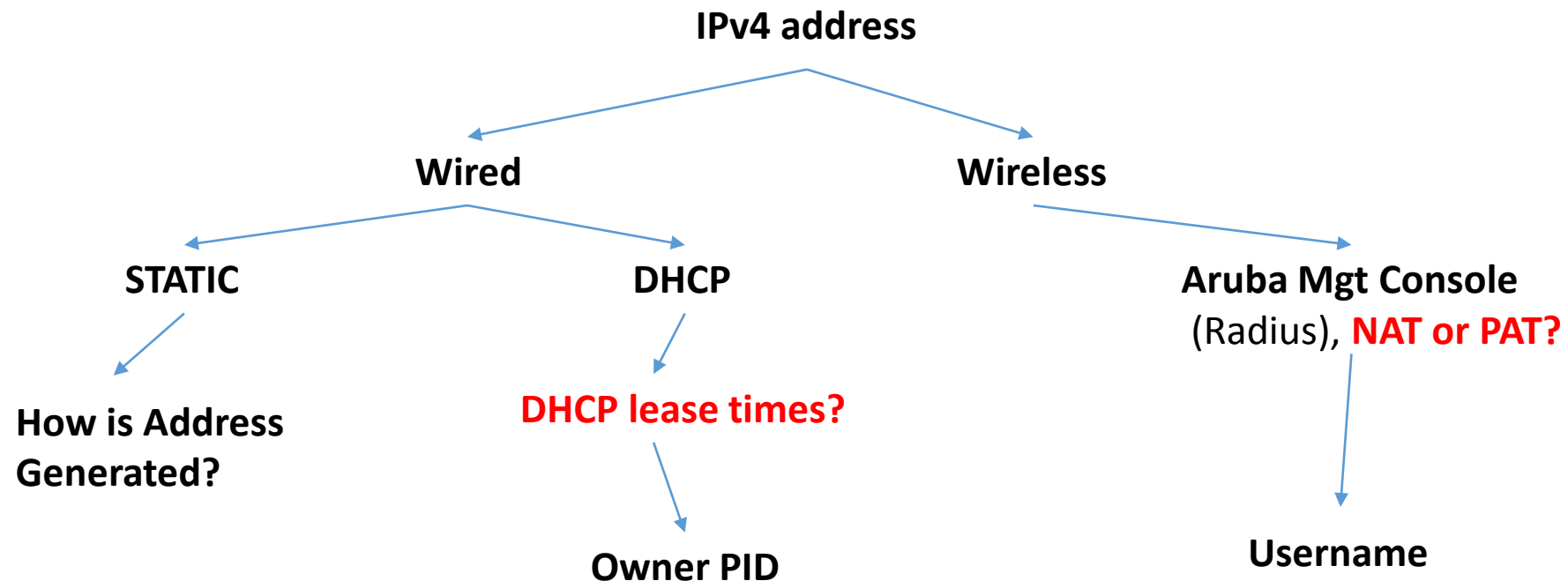


# CSC 1 - Inventory & Control of HW Assets



# Control 1 - Finding Waldo

- Given an IP address, can you locate it and find the owner?



# *CSC 1: Hardware Inventory WFH WTF?*

- Can't inventory what's not yours. Or can you?
- Can you “disconnect” a host from your network?
  - ISP will get abuse complaints not your org.



Sony's X93D HDR with Android TV

7



TOTO's CW993VA/TCF993WA

10



LifeSmart's BLEND™ Light Bulb

2



LG's Styler

6



LG's G5 Friends Rolling Bot

8



Samsung's AddWash Washing Machine

9



Dyson's Pure Cool Link purifier fan

4



LifeSmart's Smart Light Switch

3



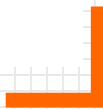
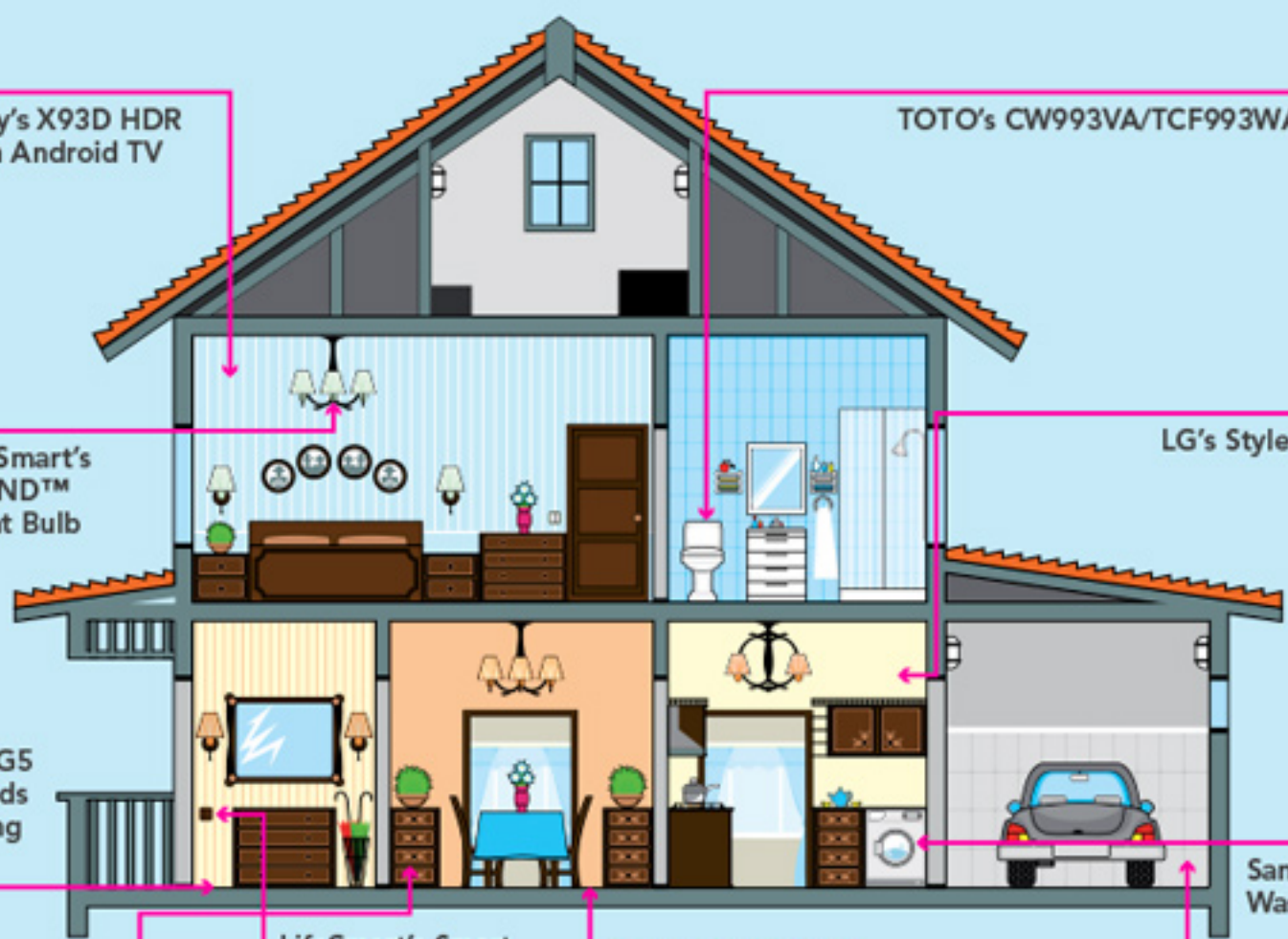
Samsung's VR9050 ROBOT VC with Cyclone Force, 70W

5

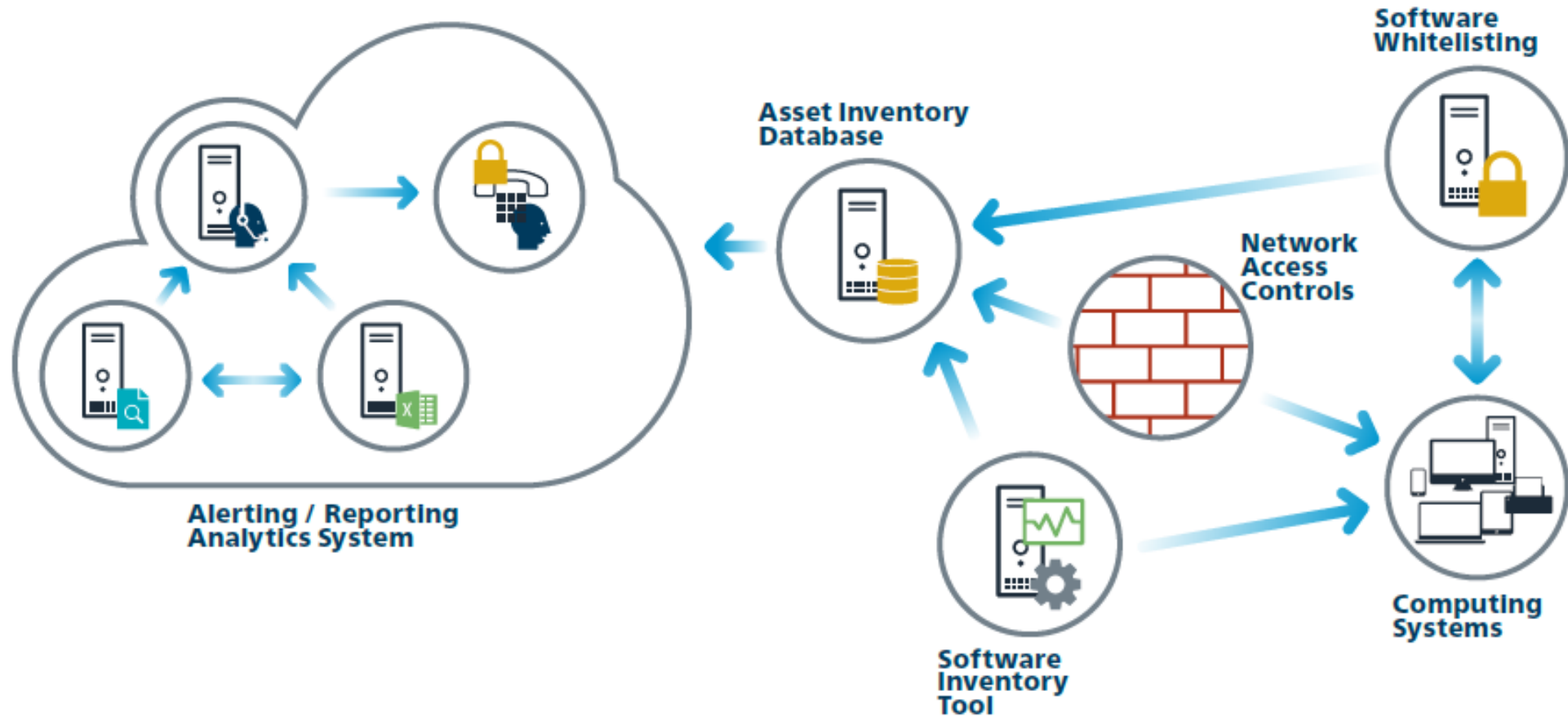


LifeSmart's Wireless Camera

1



# CSC 2 - Inventory & Control of SW Assets



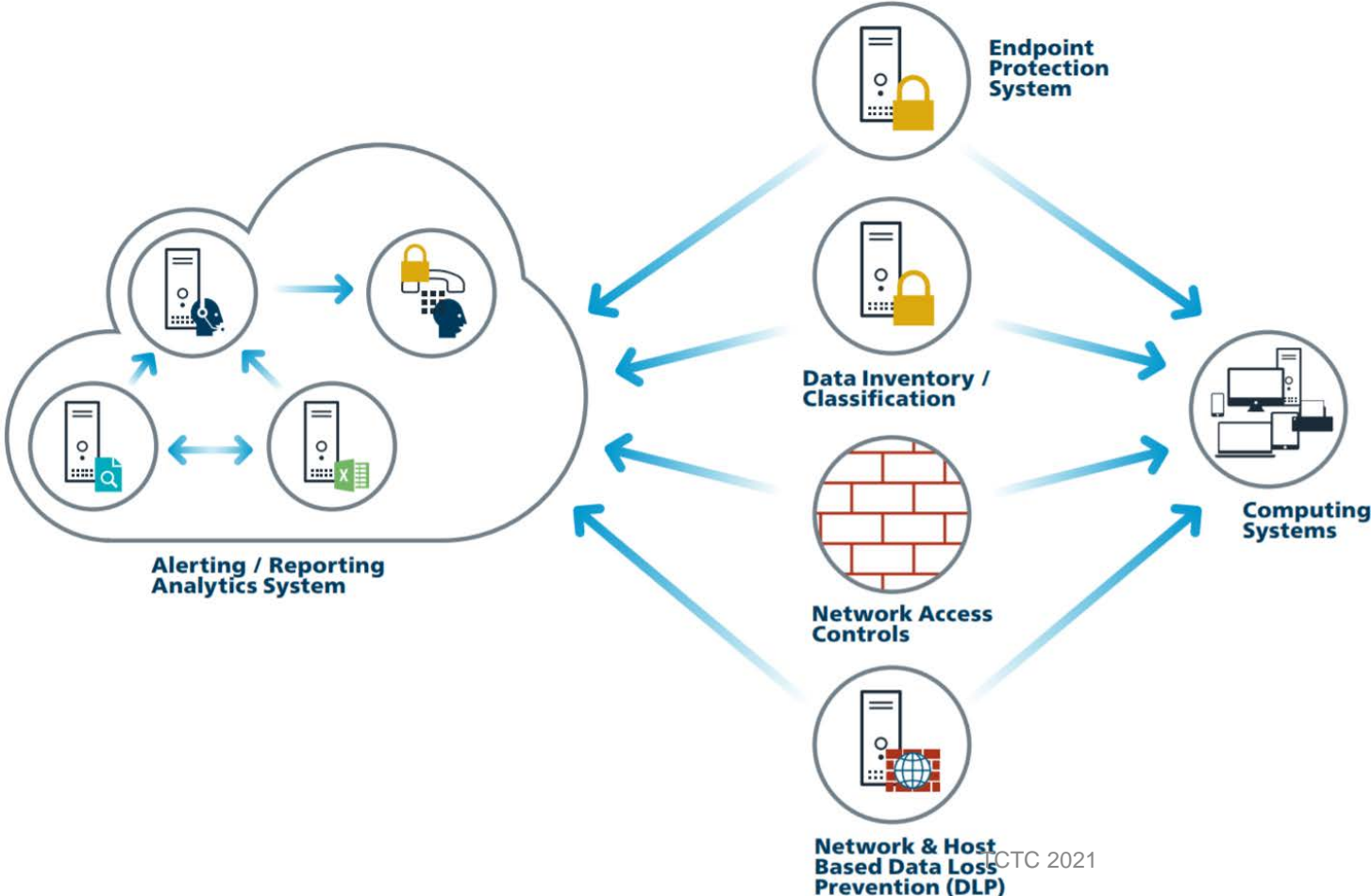
# *Your Work Computer Became Your Home Computer*

- What happens to software inventory?
- WFH not new but # of WFH computers has INCREASED
- Will your company tools work outside of your work network?
  - Active Directory?
  - Authentication? 2 factor?
  - Software Licensing?
  - Virtual Private Network (VPN)?

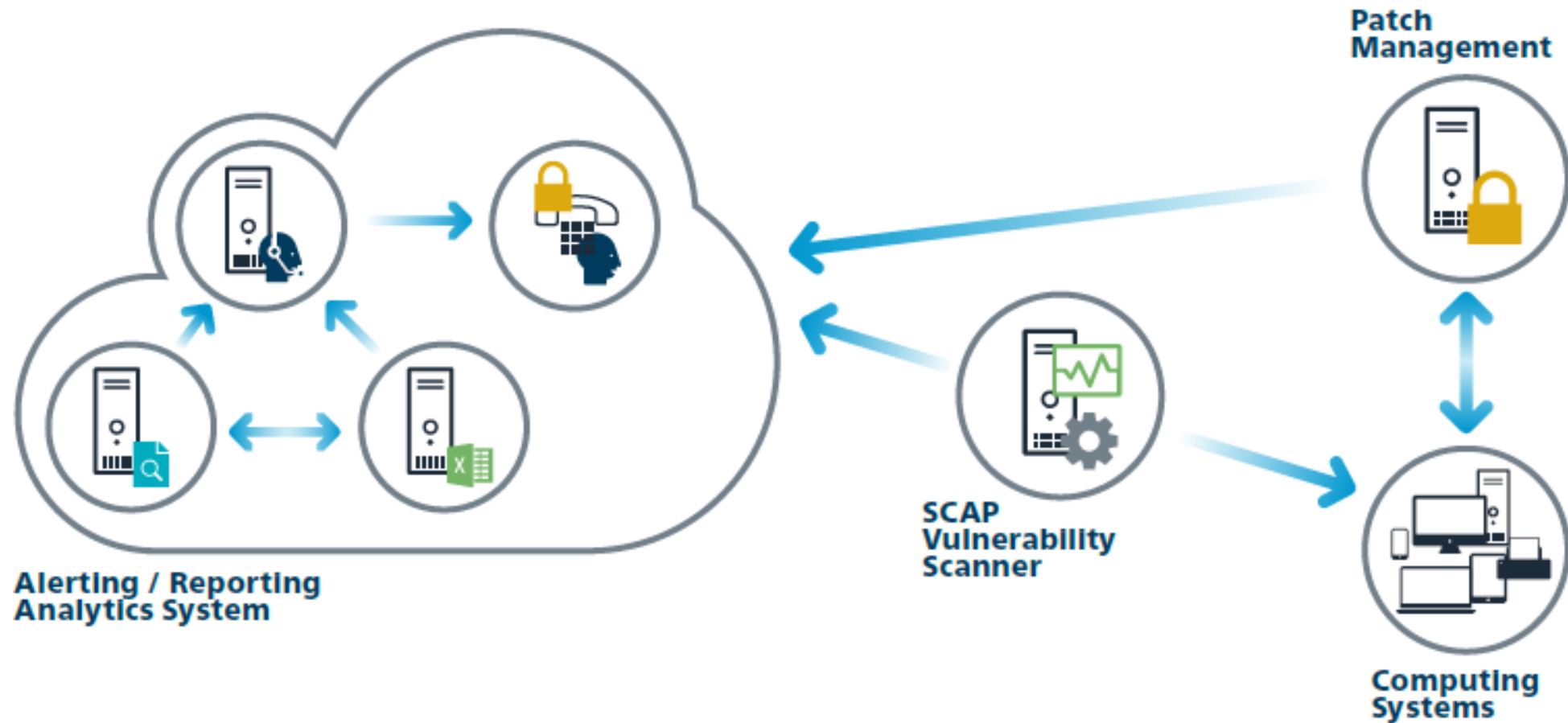


# CSC 13 - Data Protection

## CIS Control 13: System Entity Relationship Diagram



# CSC 3 - Continuous Vulnerability Mgt

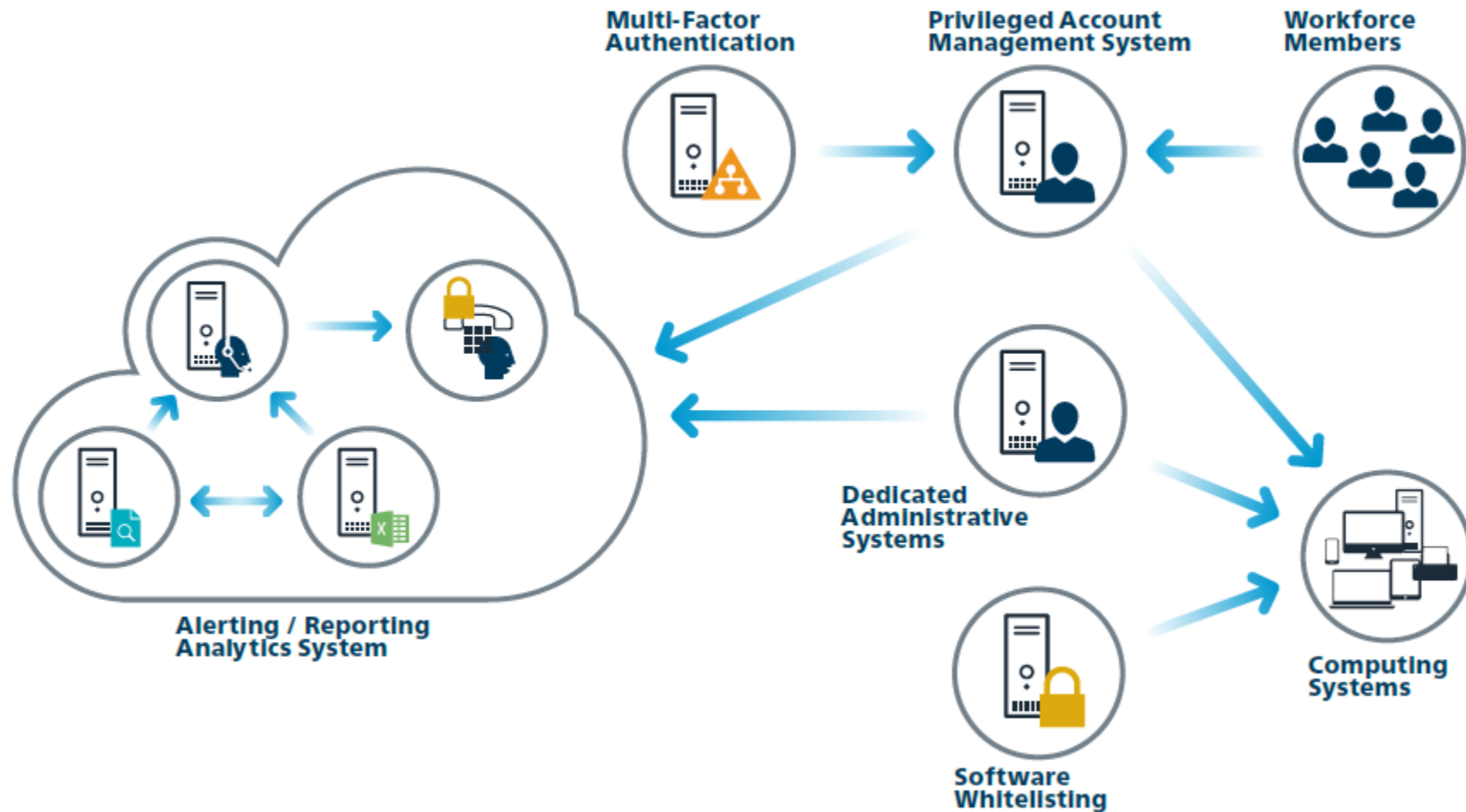




# *WFH Part Deux*

- Can your IT scan computers at your house?
  - May be blocked by your ISP
  - May work in a “pull” mode where the client initiates the scan request

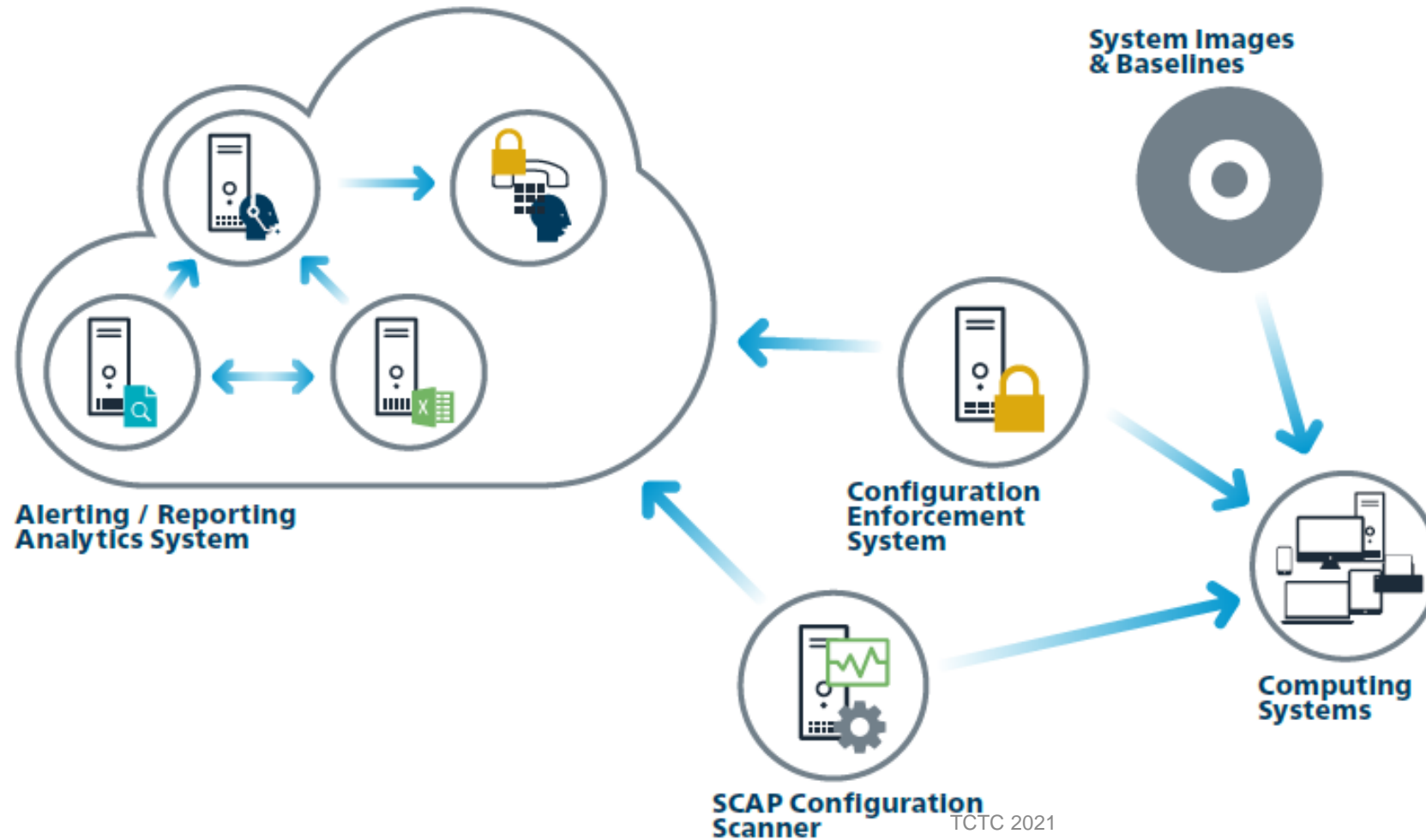
# CSC 4 - Controlled Use of Admin Privs



# CSC vs WFH

- Does your home computer meet any regulatory requirements imposed on the data you use?
- If you use your home computer for work, you should follow your office's security requirements on it.
- **Create a separate userid for work stuff.** Keeps personal separate from work.
  - Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.
  - When you're done #WFH, you can delete that account

# CSC 5 - Secure Config for HW, SW





STANDARDS	WHAT TO DO	L	M	H	CSC
Patching	Apply security patches within 30 days of publish. BigFix is recommended. Use a supported OS version.	✓	✓	✓	3
Whole Disk Encryption	Use FileVault2 for Mac. Use BitLocker for Windows. Consider Veracrypt if applicable. Recommended for low-risk endpoints.		✓	✓	13
Malware Protection	Install antivirus (e.g., Windows Defender) and configure to automatically update and run scheduled scans.	✓	✓	✓	8
Backup	Backup local user data at least weekly. Consider using Network Backup Service.	✓	✓	✓	10
Inventory	Register your endpoint with departmental inventory system.	✓	✓	✓	1



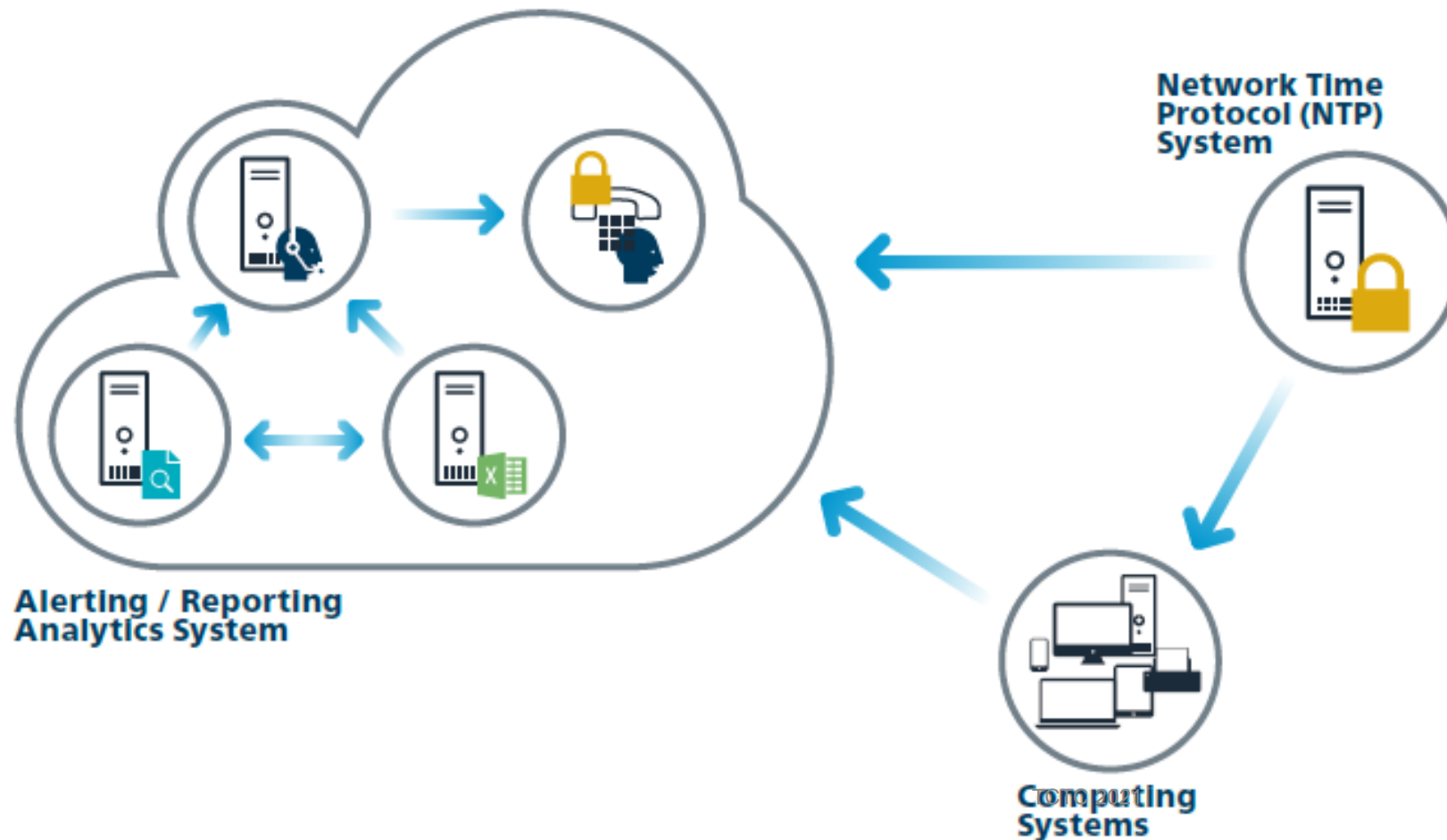
STANDARDS	WHAT TO DO	L	M	H	CSC
Firewall	Enable host-based firewall in default deny mode and permit only the minimum necessary services.	✓	✓	✓	9
Equipment Disposal	All university-owned equipment must go through Surplus Property for disposal.	✓	✓	✓	1
Credentials and Access Control	Configure workstations and laptops to prohibit anonymous access. Enforce password age, length, and complexity. Require password-protected screen savers, with a recommended 15-minute time for inactivity, or lock device before leaving it unattended.	✓	✓	✓	4, 16
Configuration Management	Install BigFix or equivalent (Kaseya)			✓	3, 5
Regulated Data Security Controls	Implement PCI DSS, FISMA, or export controls as applicable.			✓	12 13 14
Centralized Logging	Forward logs to a remote log server. Use of the university's centralized log server is recommended (required for division of IT endpoints). Review logging standard for additional requirements.			✓	6

2021

Marchany Copyright  
2021

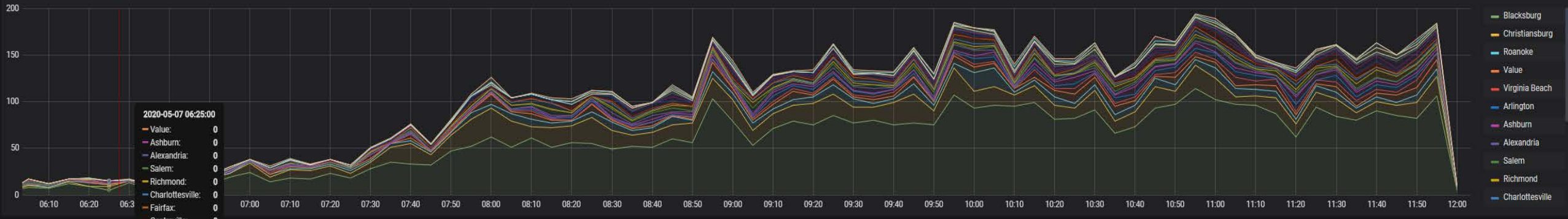


# CSC 6 - Maintenance, Monitoring & Analysis of Logs

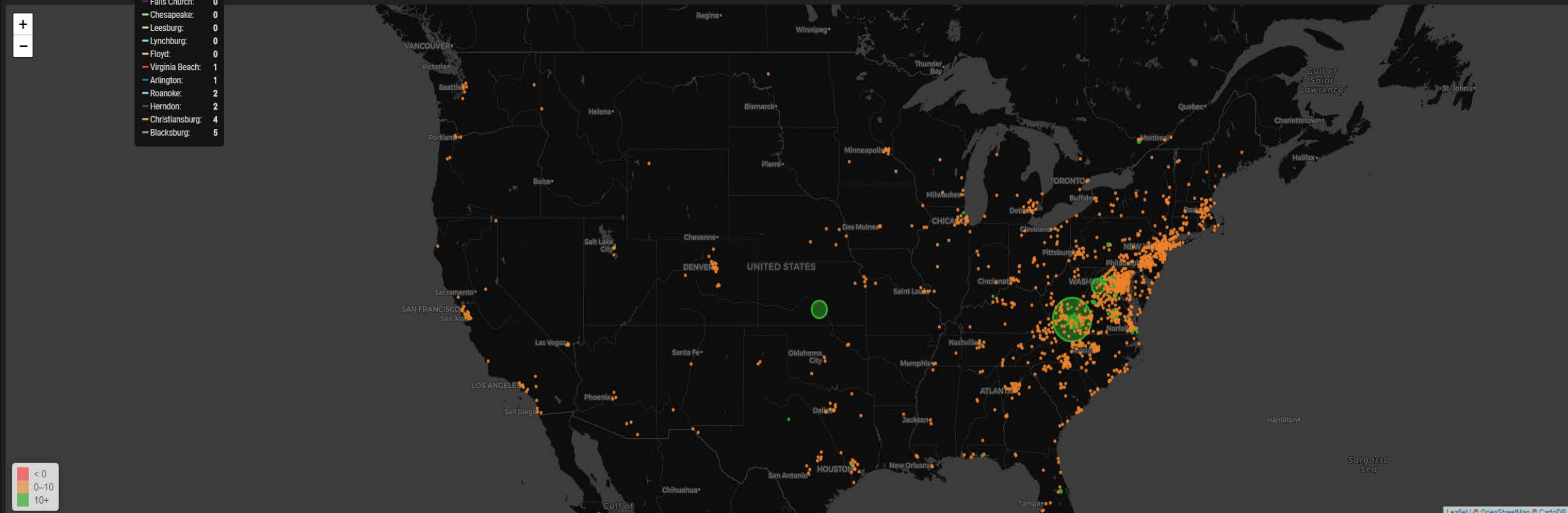




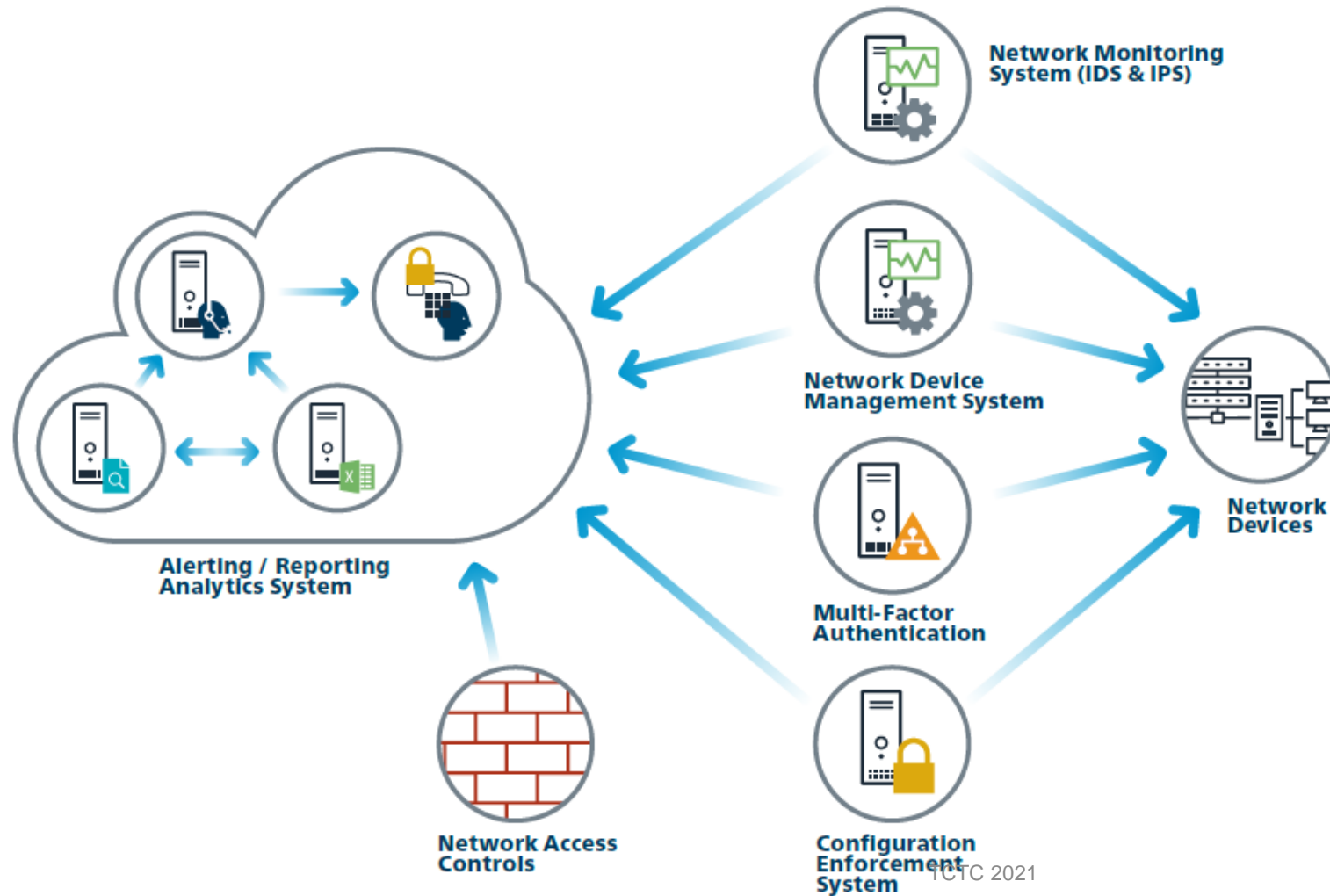
Cities



World Map



# CSC 12 - Boundary Defense



© 2021

Marchany Copyright  
2021

# *Border? What Border?*

- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- Internet 3.0 – mobile servers (containers, serverless), mobile endpoints (laptops, phones, tablets, IoT, ICS)
- WFH has moved us to Internet 3.0
- Data and Identity become the new border

# CIS Benchmarks

- Operating Systems
- Server Software
- Cloud Providers
- Mobile Devices
- Network Devices
- Desktop Software
- Multi Function Print ...

- Linux
- Microsoft Windows
- UNIX

Currently showing Operating Systems [Go back to showing ALL](#)

**Operating Systems**

**Amazon Linux**  
Expand to see related content ↓

**Download CIS Benchmark** →

CIS Hardened Image and Remediation Kit also available

Linux

**Operating Systems**

**Apple OS**  
Expand to see related content ↓

**Download CIS Benchmark** →

UNIX

**Operating Systems**

**CentOS Linux**  
Expand to see related content ↓

**Download CIS Benchmark** →

CIS Hardened Image and Remediation Kit also available

Linux

**Operating Systems**

**Debian Linux**  
Expand to see related content ↓

**Download CIS Benchmark** →

CIS Hardened Image and Remediation Kit also available

Linux

# *CSC Map to CIS Benchmarks*

- Pick appropriate CIS Benchmark
- Map benchmark to Framework
  - Example: NIST 800-171 -> CSC
  - <https://library.educause.edu/resources/2016/9/nist-sp-800-171-compliance-template>
- Cut commands out of benchmark doc, paste into flat file to create security configuration script file – mods may be needed

### 1.7.1.4 Ensure permissions on /etc/motd are configured (Scored)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.


#### Rationale:

If the `/etc/motd` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

#### Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644`:

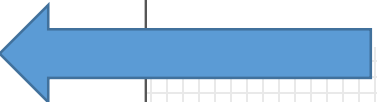
```
# stat /etc/motd
Access: (0644/-rw-r--r--)  Uid: (   0/   root)  Gid: (   0/   root)
```



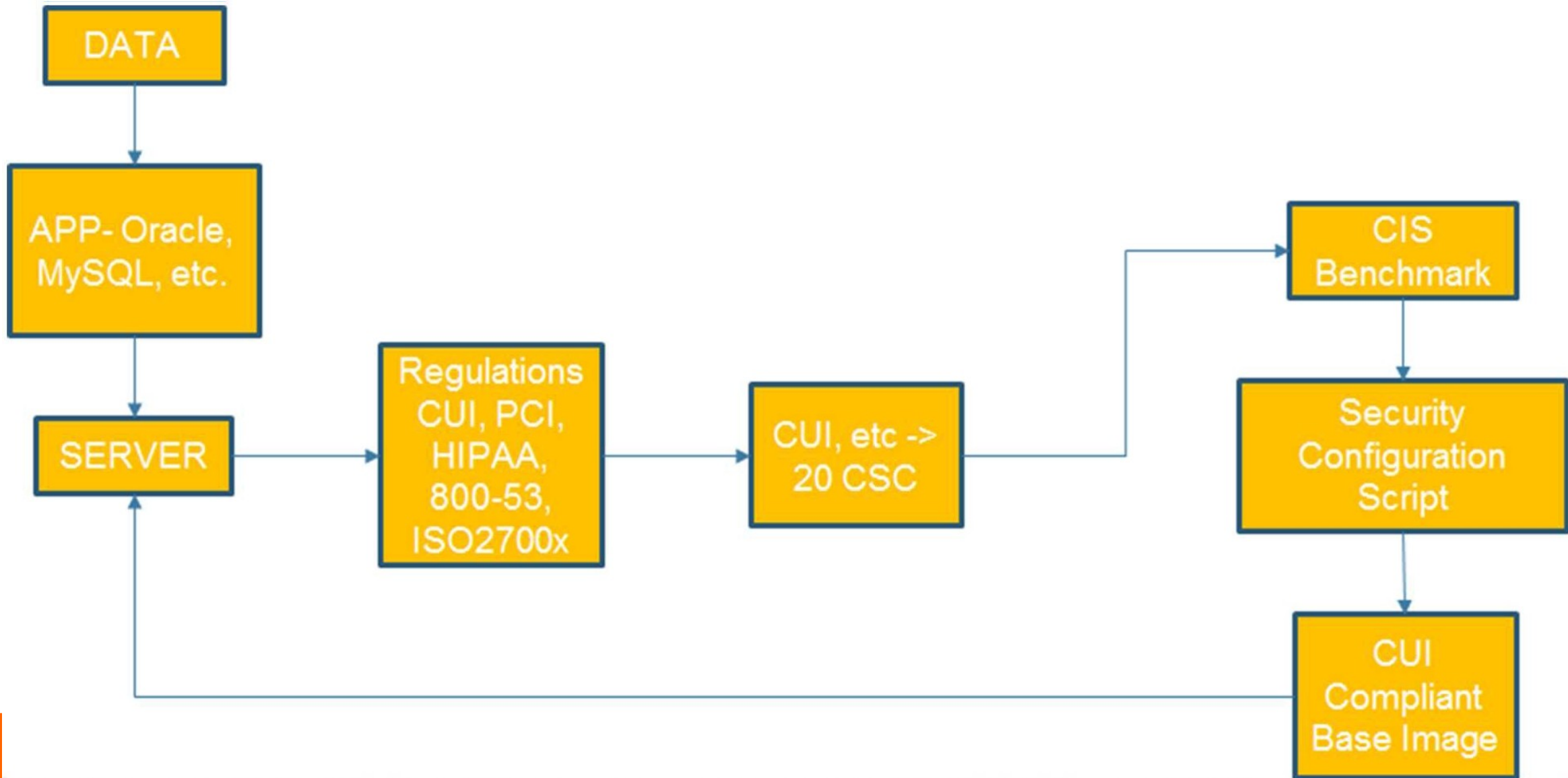
#### Remediation:

Run the following commands to set permissions on `/etc/motd`:

```
# chown root:root /etc/motd
# chmod 644 /etc/motd
```



#### CIS Controls:



v8 CIS Control Number - Proposed	v8 CIS Control Number - Previous	v8 CIS Control Title	v7.1 CIS Control Title	v7.1 CIS Control Number
1	1	Inventory and Control of Hardware Assets	Inventory and Control of Hardware Assets	1
2	2	Inventory and Control of Software Assets	Inventory and Control of Software Assets	2
3	5	Secure Configuration of Assets, Network Infrastructure, and Applications	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	5 and 9.4 only
4	4	Account Management	Controlled Use of Administrative Privileges Account Monitoring and Control	4, 16
5	4	Access Control Management	Controlled Use of Administrative Privileges Account Monitoring and Control	4, 16
6	12	Data Protection	Boundary Defense, Data Protection, Controlled Access Based on the Need to Know	12, 13, 14
7	3	Continuous Vulnerability Management	Continuous Vulnerability Management	3
8	6	Audit Log Management	Maintenance, Monitoring and Analysis of Audit Logs	6
9	7	Email and Web Browser Protections	Email and Web Browser Protections	7
10	8	Malware Defenses	Malware Defenses	8
11	10	Data Recovery	Data Recovery Capabilities	10
12	11	Network Infrastructure Management	Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	11
13	13/14	Network Monitoring and Defense	Controlled Access Based on the Need to Know, Boundary Defense	14, 12
14	17	Security Awareness and Skills Training	Implement a Security Awareness and Training Program	17
15	Y	Service Provider Management	N/A	N/A
16	18	Application Software Security	Application Software Security	18
17	19	Incident Response Management	Incident Response and Management	19
18	20	Penetration Testing	Penetration Tests and Red Team Exercises	20
	X	<del>Secure Configuration of Servers, Applications, and Services</del>	<del>Limitation and Control of Network Ports, Protocols and Services</del>	0
	45	<del>Wireless Access Control</del>	<del>Wireless Access Control</del>	45



# *What Changed?*

- From 20 Controls to 18 Controls
  - Rolled 2 controls into a 3<sup>rd</sup> control
- Added **Service Provide Management** control to deal with Cloud services
  - For cloud-specific guidance, refer to the CIS Cloud Companion Guide - <https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/>
- Reorganized the 1<sup>st</sup> 3 controls into an “Inventory” set of controls
  - CSC 1 – Hardware Inventory
  - CSC 2 – Software Inventory
  - CSC 3 – Sensitive Data Inventory



# *Summary*

- 20 Critical Security Controls provide a bridge between security frameworks, industry and local standards and operational actions.
- Start with the Basic set
- Version 8 coming out late spring 2021

# References

- <https://www.auditscripts.com/free-resources/critical-security-controls/>
- <https://cisecurity.org>
- <https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/>
- <https://www.sans.org/security-resources/posters/security-leadership-cis-controls/55/download>
- <https://github.com/62726164> - netscan fast scanner
- Slides 10, 11, 15, 17, 18, 20, 22, 24, 26 used with permission