The 20 Critical Security Controls: From Framework to Operational to Implementation

Randy Marchany

CISO, Virginia Tech

marchany@vt.edu

https://security.vt.edu

Twitter: @randymarchany

VIRGINIA TECH™

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

EDU (now) vs. Corporate Structure (future)

- **Administrative** – the process that runs the institution (**CORP**)
  - Payroll, HR, Purchasing, Facilities, Legal, etc.
  - **Security model closest to corporate model**
- **Academic/Instructional** – the process that supports teaching/learning (**ISP**)
  - Learning Mgt Systems such as CANVAS, Blackboard, Moodle
  - Course Delivery systems – Zoom, Webex, etc.
  - Heavily BYOD – all flavors, types
  - **Security model closest to an ISP**
- **Research** – **hybrid** of the previous 2
  - Intellectual Property protection, High risk, visibility
  - **Security model is a hybrid of corporate and ISP**

Hacker Attack Goals

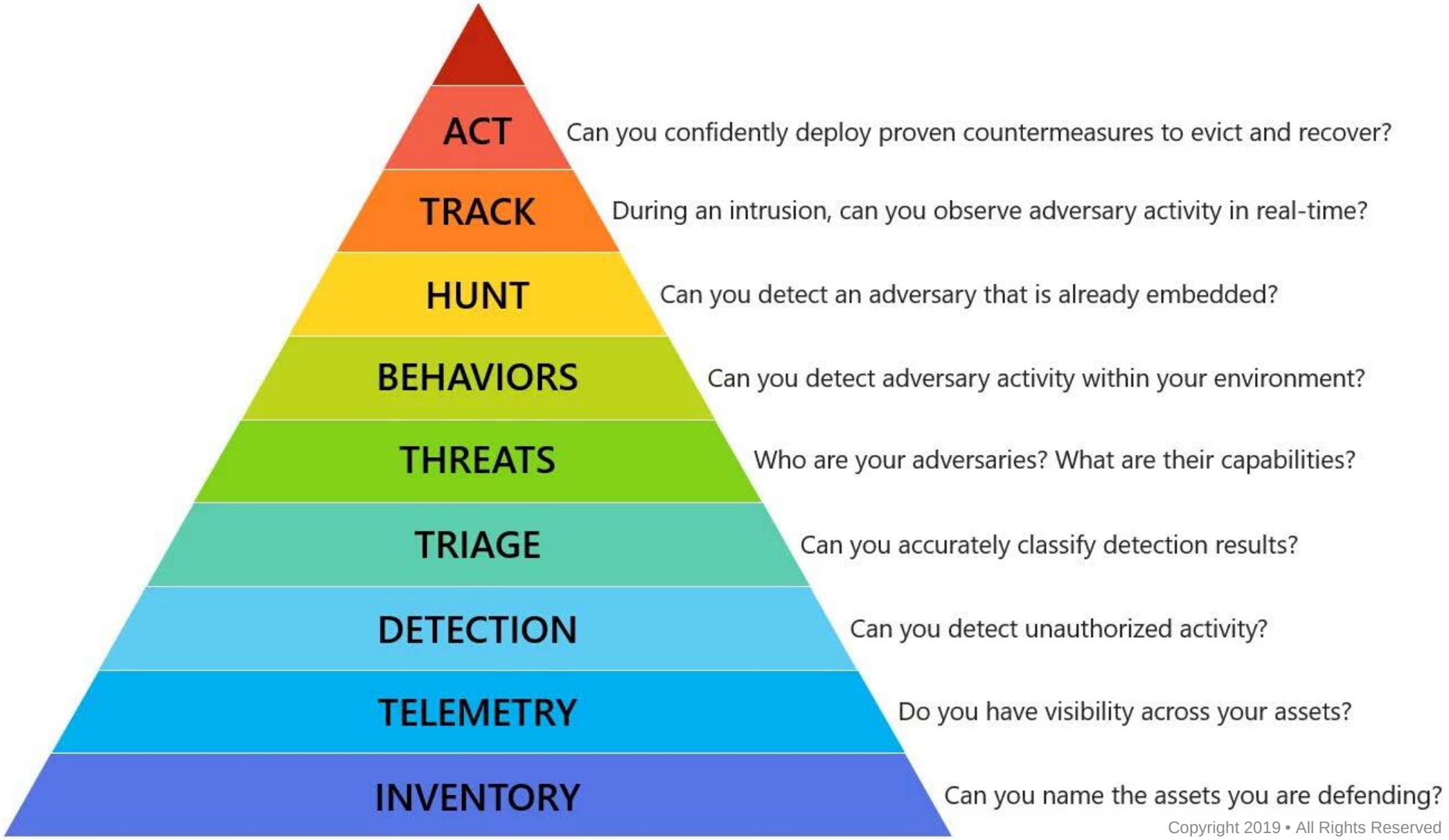
Hacker attack goals are 1 or more of the following:

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

- **DEFEND** accordingly

What are You Defending? What Should You Defend?

- Systems? Not really but that's what we thought should be defended.
- Networks? Safe answer.
- DATA – what we should be defending.



From Framework to Standards

- Start with your Framework
  - ISO27001 -> NIST 800-53a
  - https://www.auditscripts.com/free-resources/critical-security-controls/, click on Master Mapping spreadsheet
- Standard -> Controls
  - <your standard here> (NIST 800-53a) -> 20 CSC
- Controls -> Commands
  - CSC -> CIS Benchmarks -> shell commands

Discussion

- •70% of the 800-171 control numbers map to the 20 Critical controls.
- •Which ones have you done already?
- •Determine the scope
- •Just the CUI systems or the whole net?

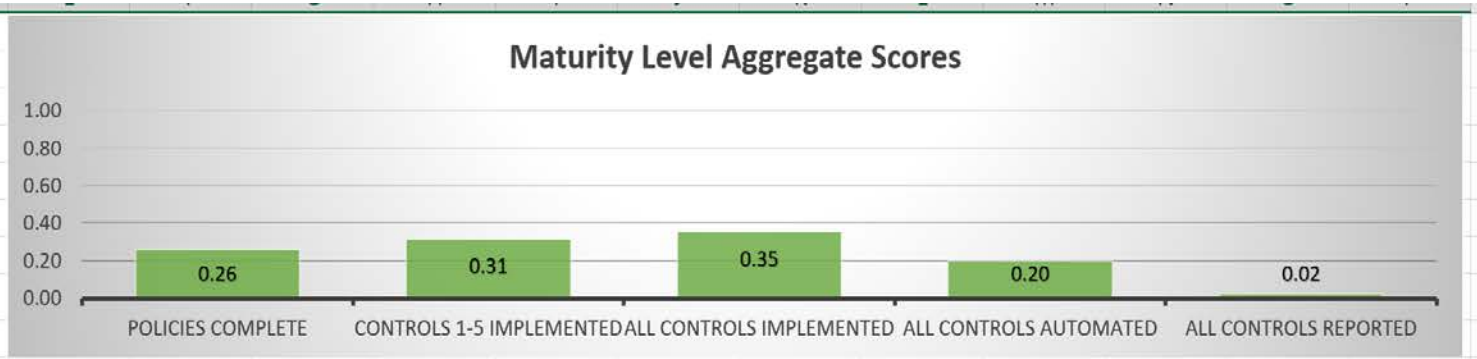
VIRGINIA TECH

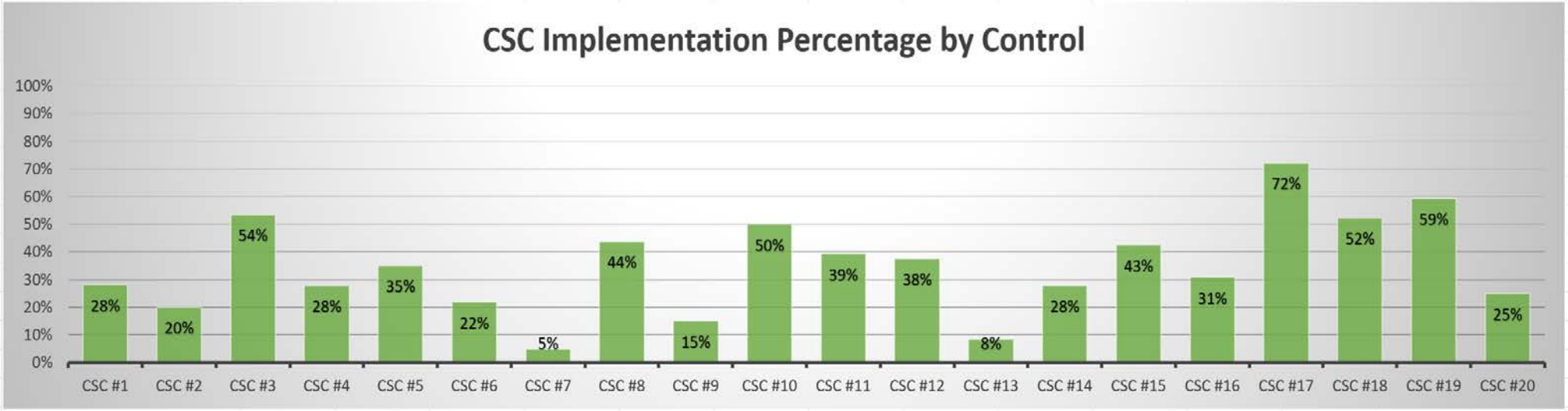
Gap It!

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

Maturity Rating*:	1.15

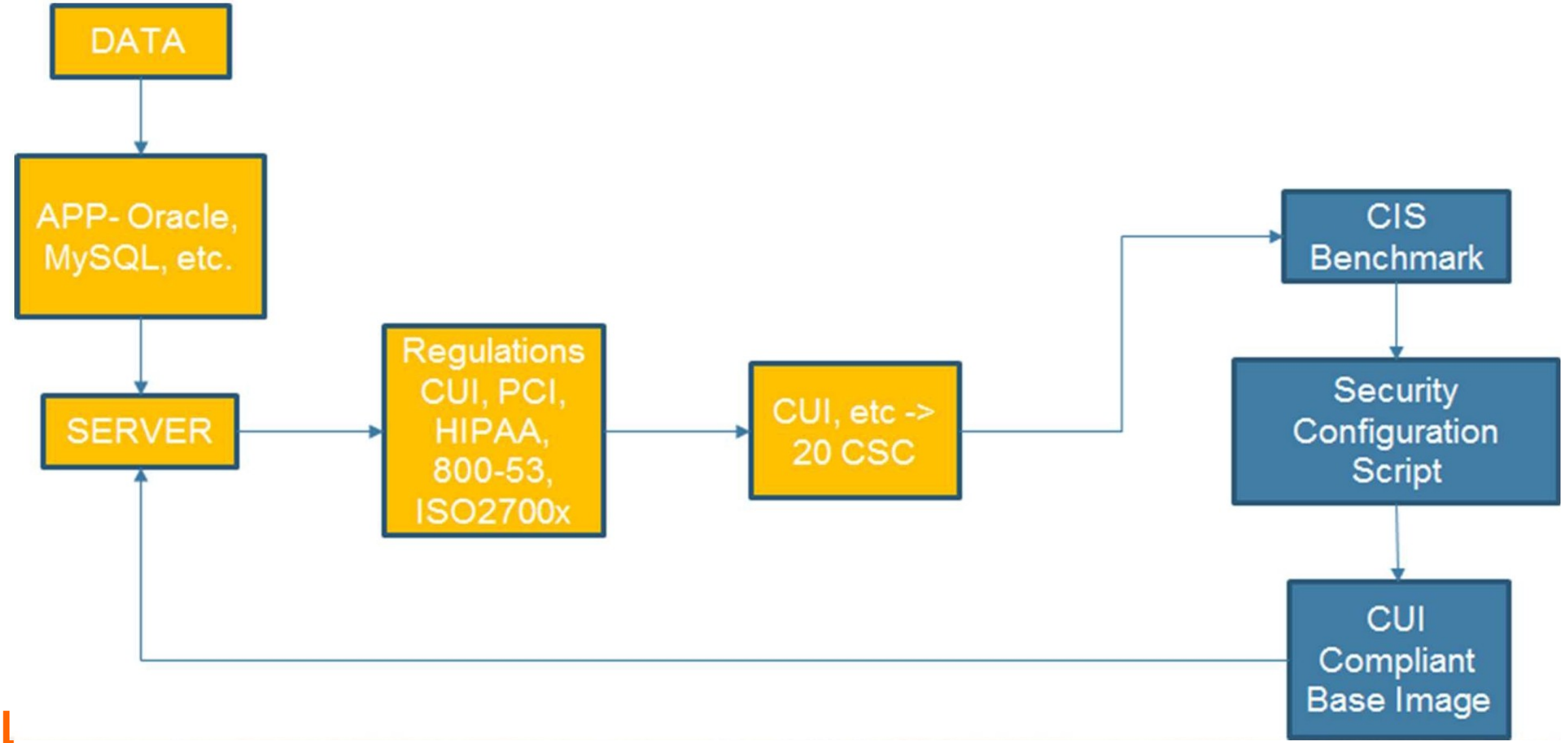
*Rating is on a 0-5 scale.



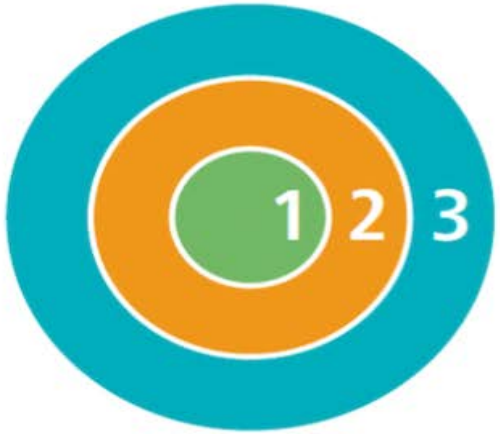


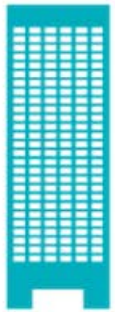
ReadMe | Dashboard | CSC #1 | CSC #2 | CSC #3 | CSC #4 | CSC #5 | CSC #6 | CSC #7 | CSC #8 | CSC #9 | CSC #10 | CSC # ...

VIRGINIA TECH



VIRGINIA TECH





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

VIRGINIA TECH

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

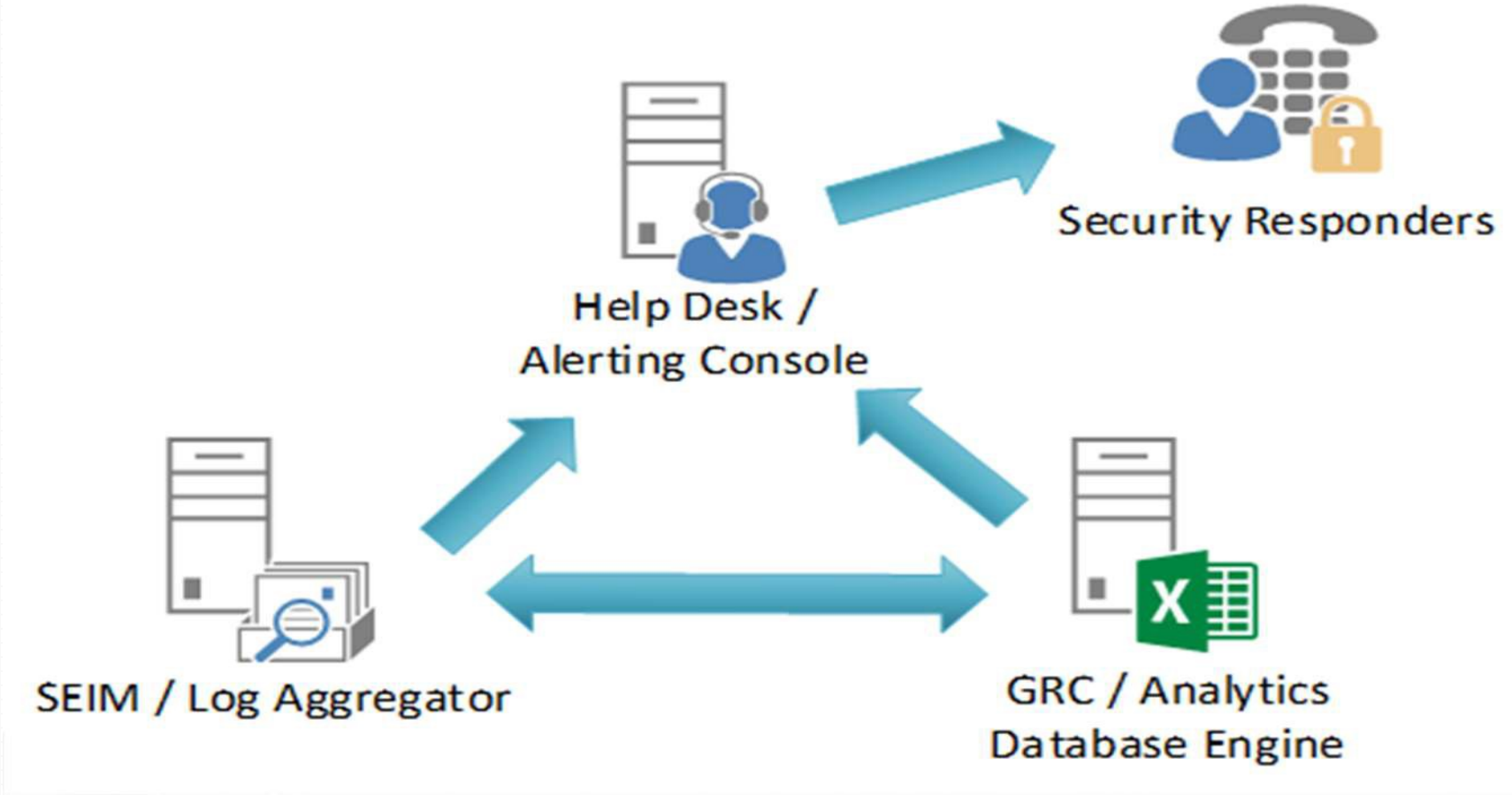
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

VIRGINIA TECH

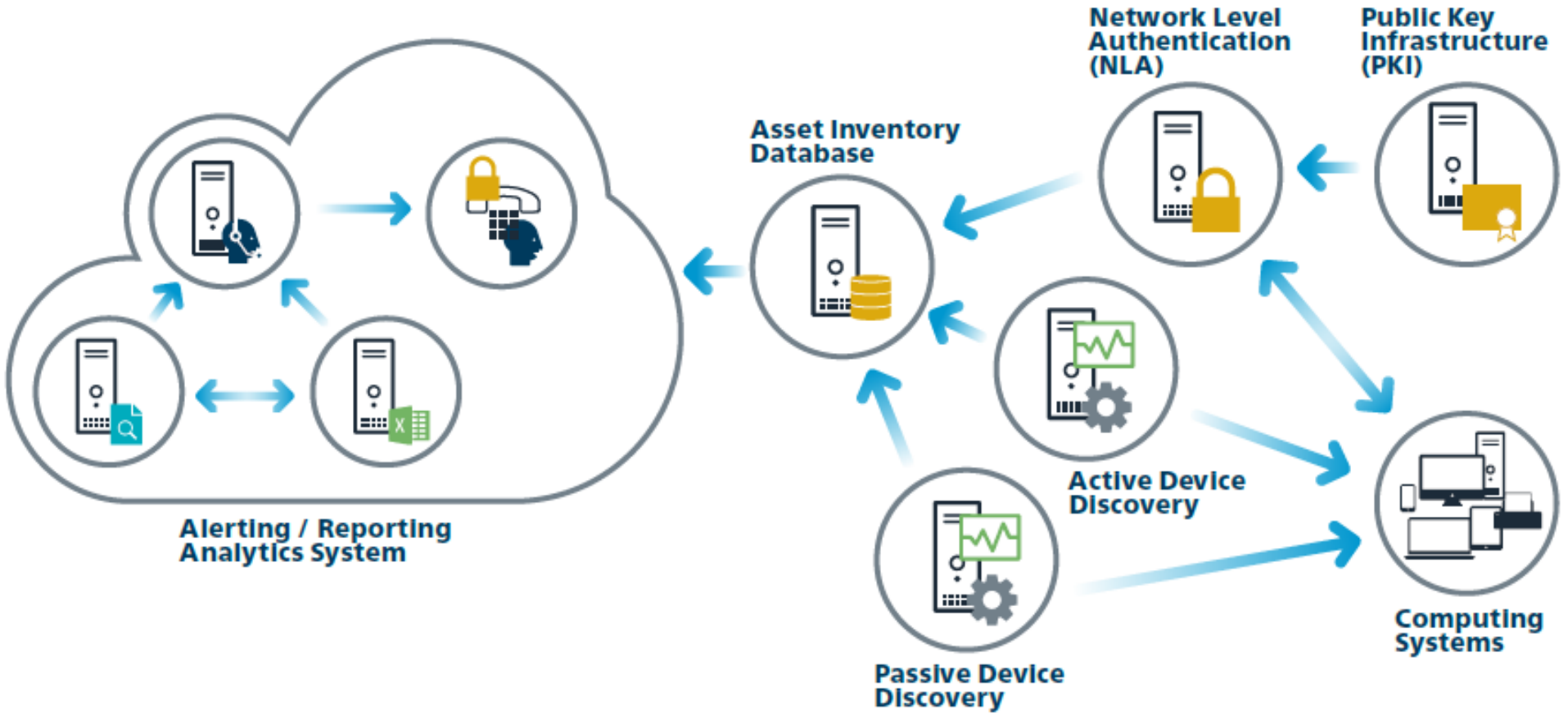
20 CSC Background

- Proven defenses against actual attacks
- Offense informs defense
- Prioritized measures/metrics, continuous diagnostics
- Automation

CSC Alerting/Reporting/Analytics



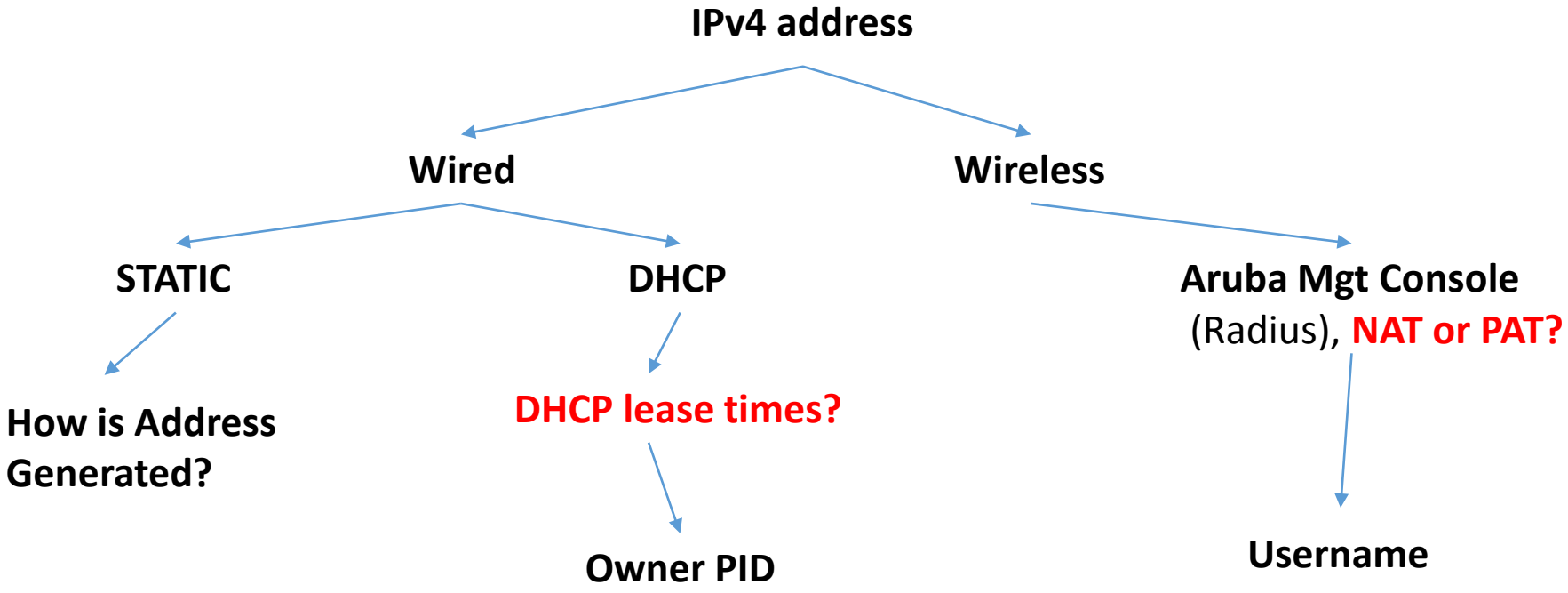
CSC 1 - Inventory & Control of HW Assets



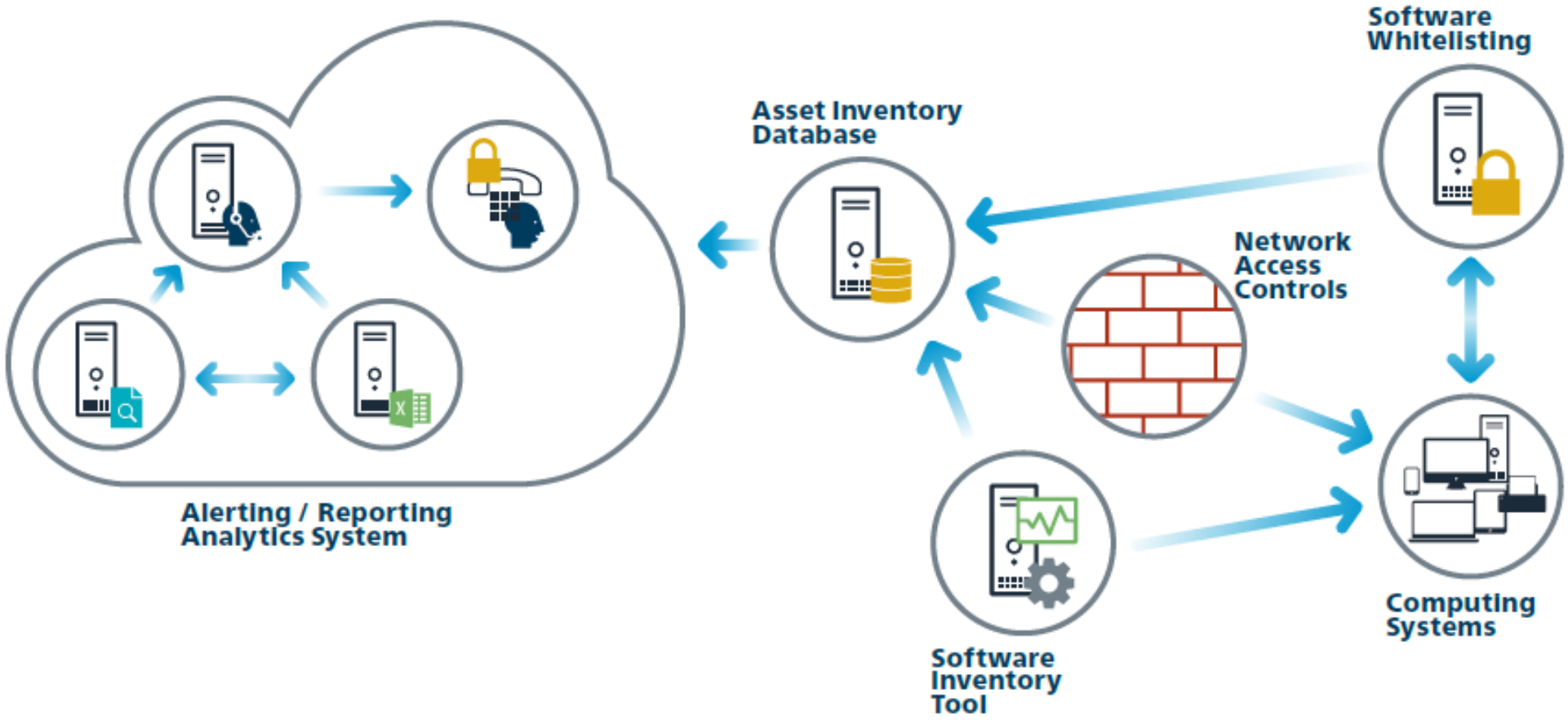
VIRGINIA TECH

Control 1 - Finding Waldo

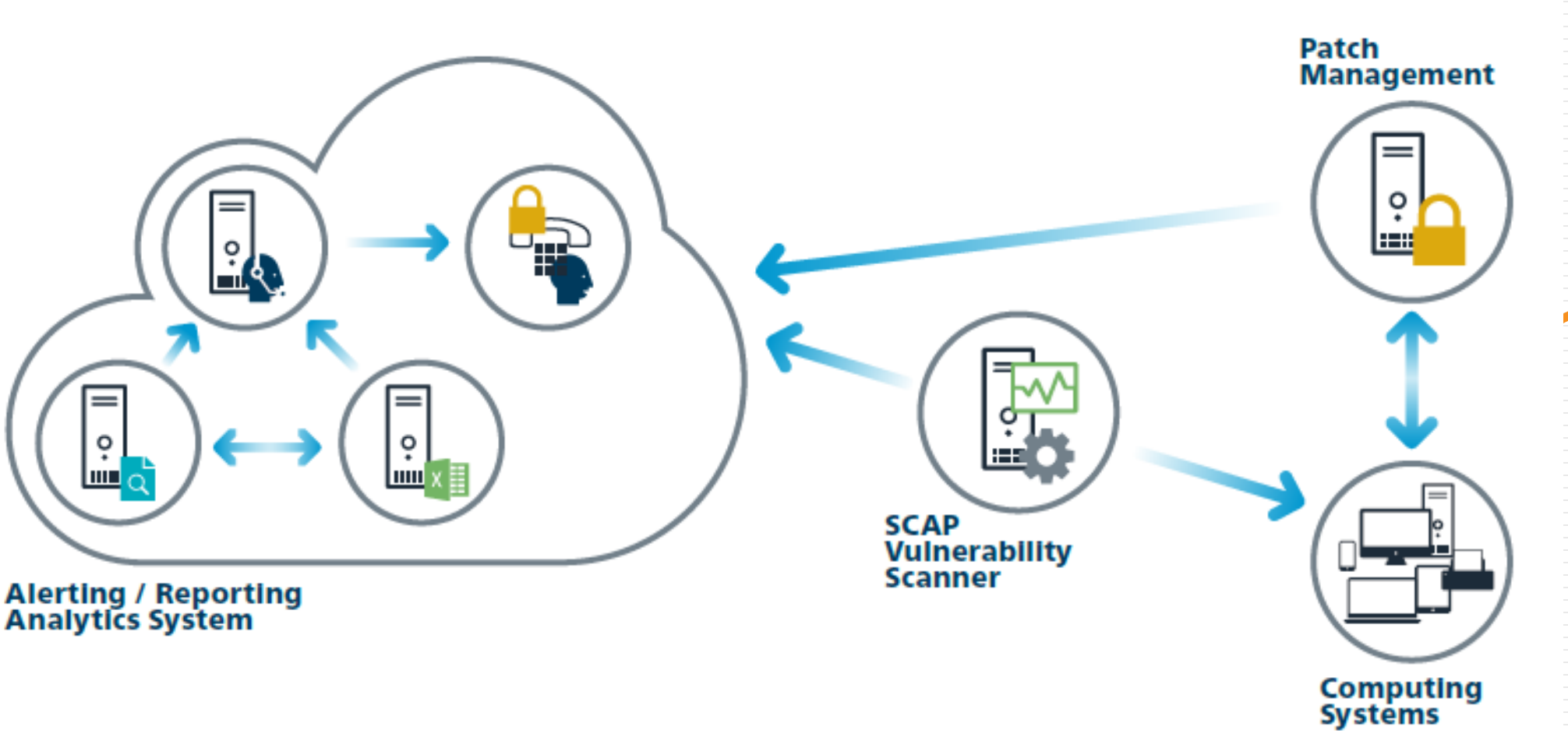
- Given an IP address, can you locate it and find the owner?



CSC 2 - Inventory & Control of SW Assets

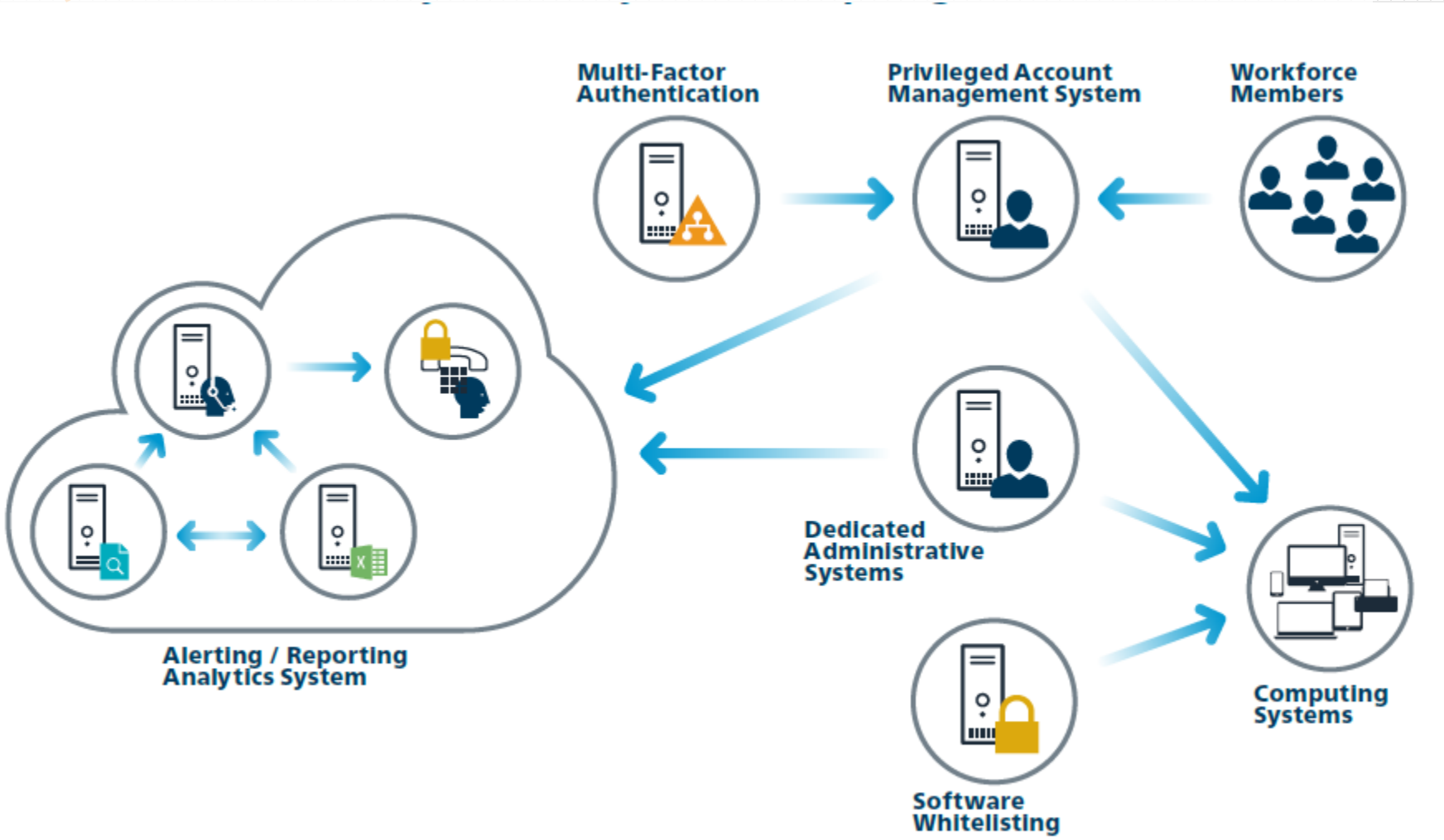


CSC 3 - Continuous Vulnerability Mgt



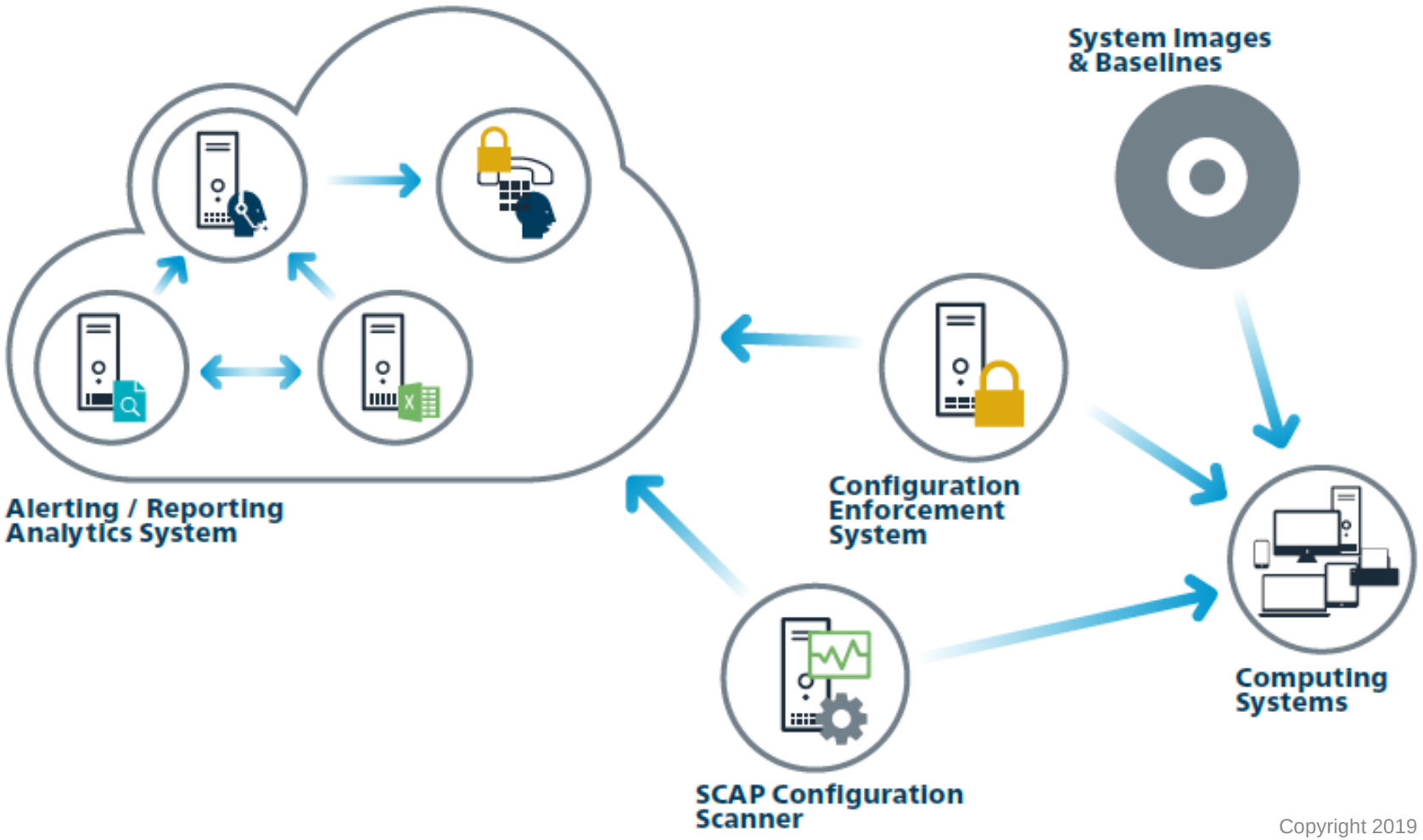
VIRGINIA TECH

CSC 4 - Controlled Use of Admin Privs

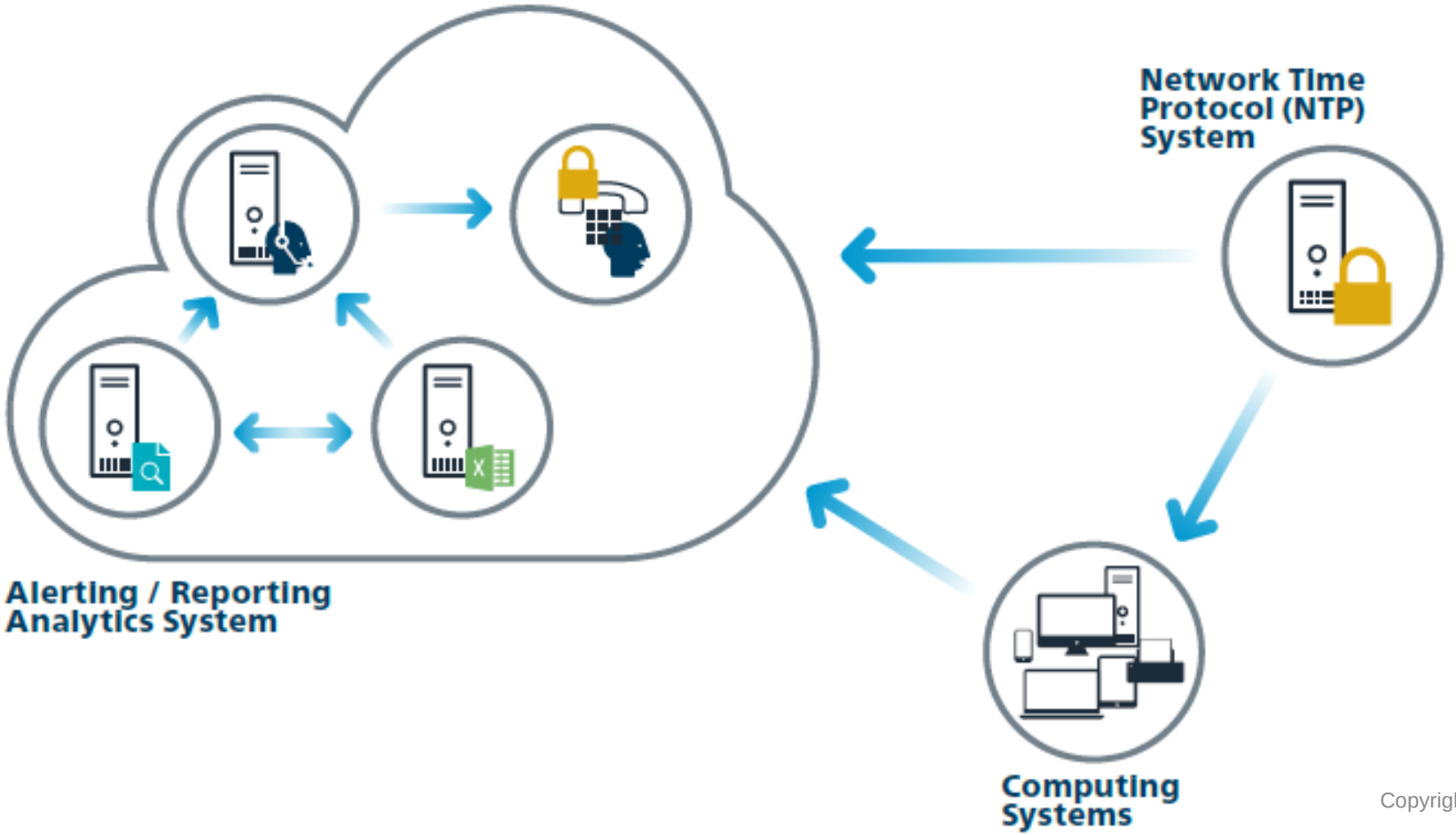


VIRGINIA TECH

CSC 5 - Secure Config for HW, SW



CSC 6 – Maintenance, Monitoring & Analysis of Logs

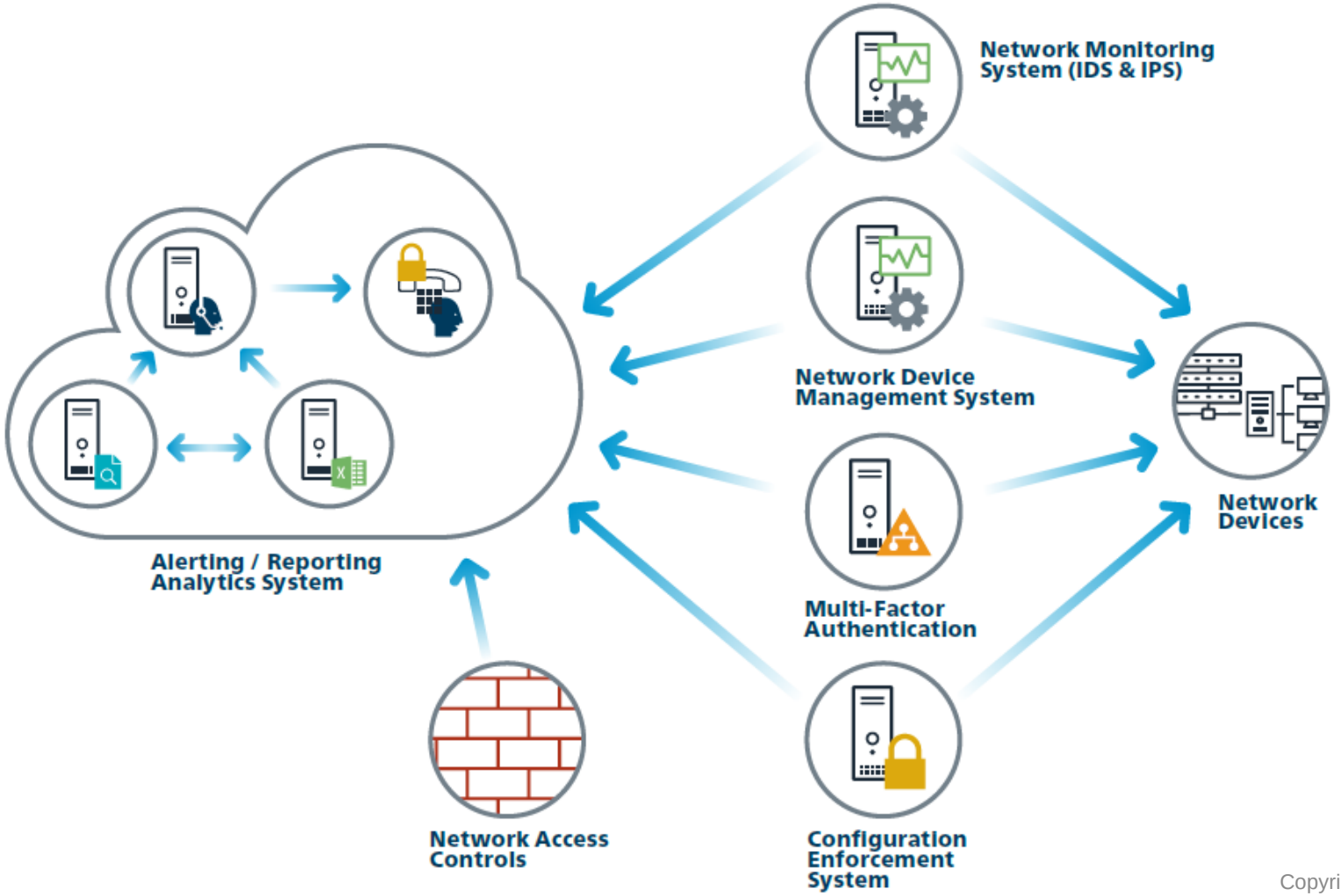


VIRGINIA TECH

Border? What Border?

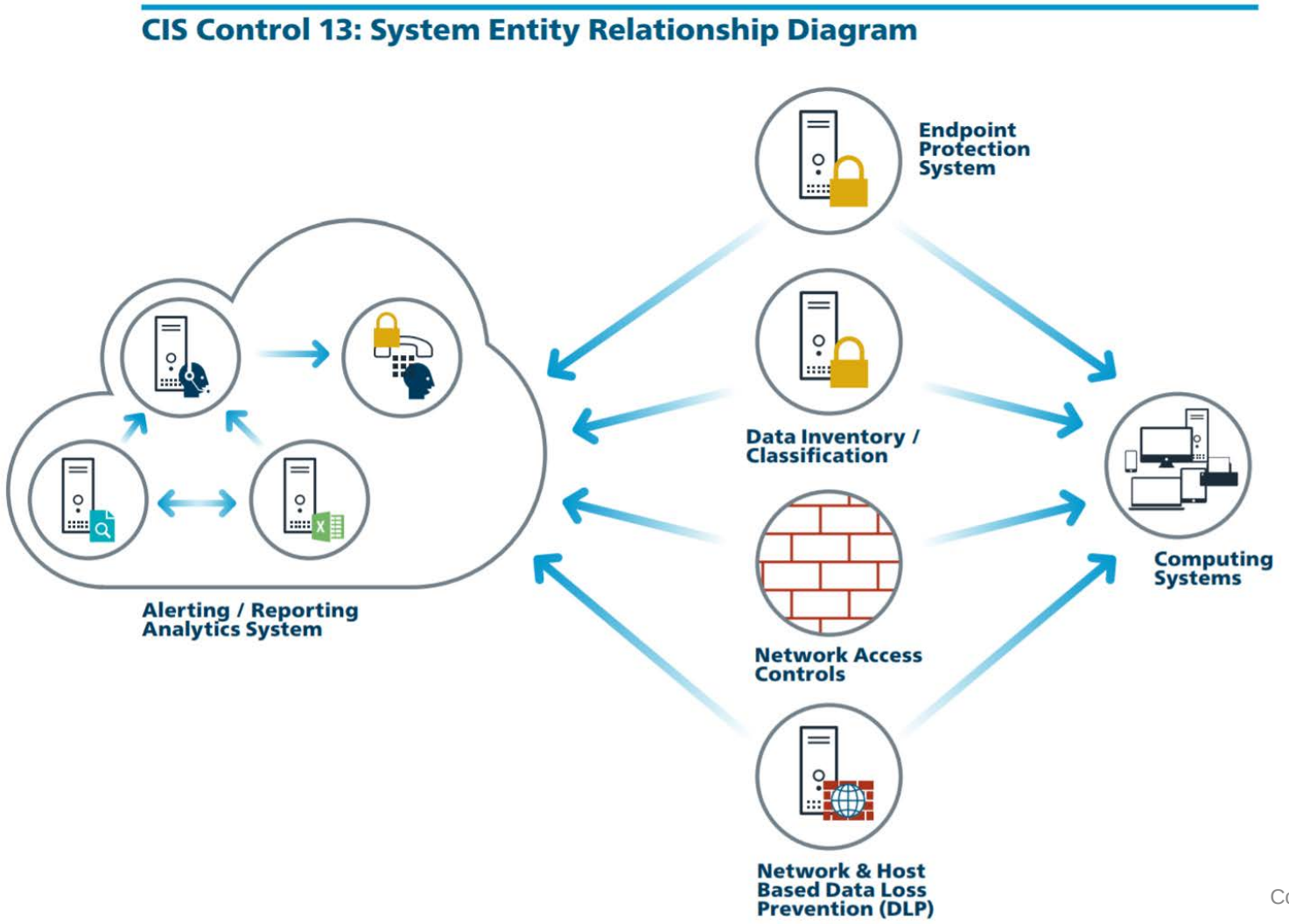
- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- Internet 3.0 – mobile servers (containers, serverless), mobile endpoints (laptops, phones, tablets, IoT, ICS)
- Current security architectures are somewhere between Internet 1.0 and Internet 2.0.
- We need to adapt to Internet 3.0 now.

CSC 12 - Boundary Defense



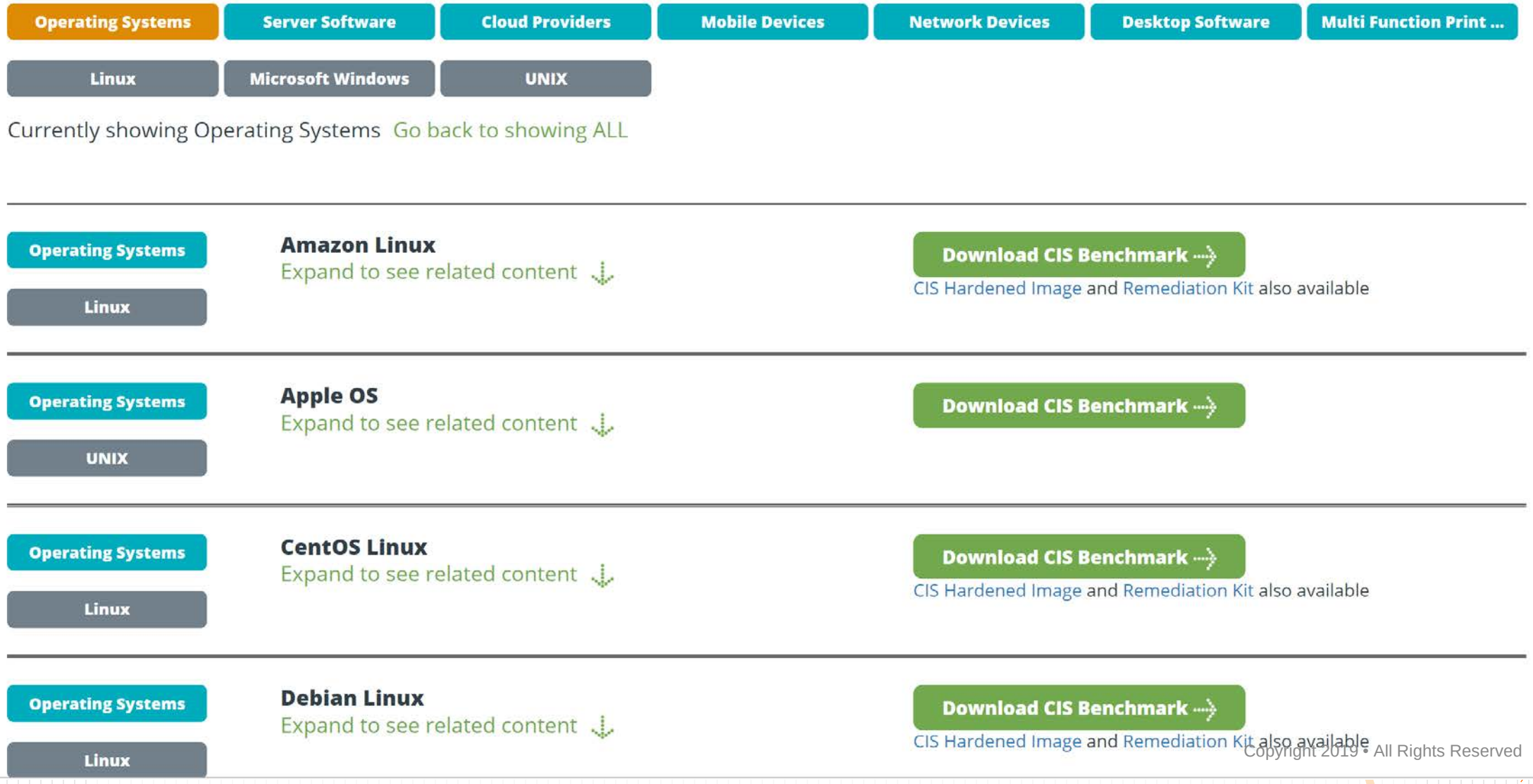
VIRGINIA TECH

CSC 13 – Data Protection



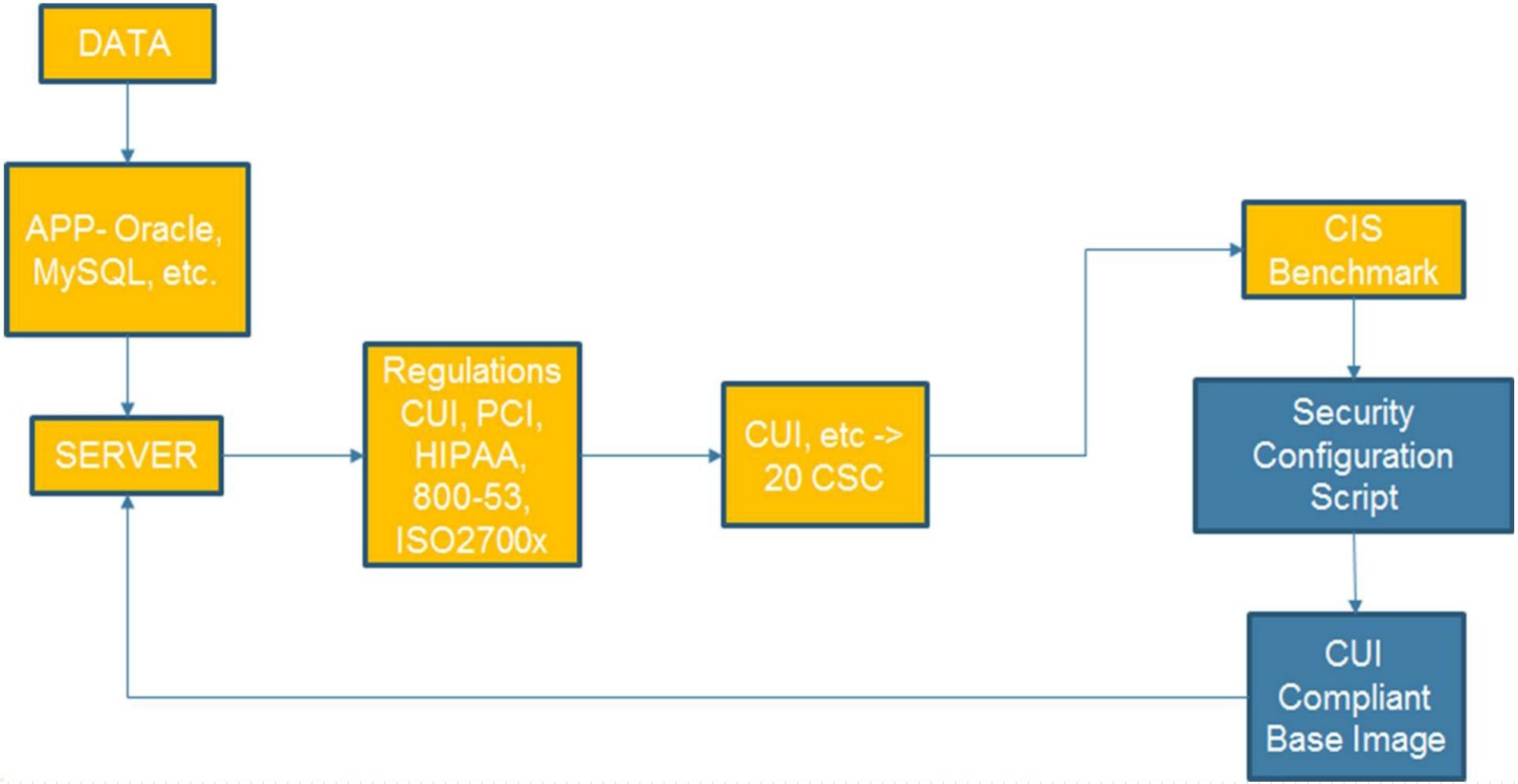
VIRGINIA TECH

CIS Benchmarks



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



VIRGINIA TECH

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.

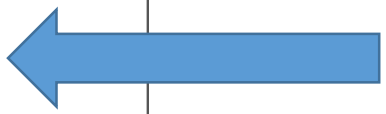
Rationale:

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`:

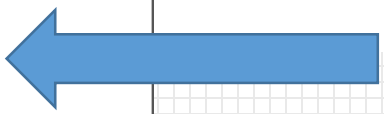
```
# stat /etc/motd
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```



Remediation:

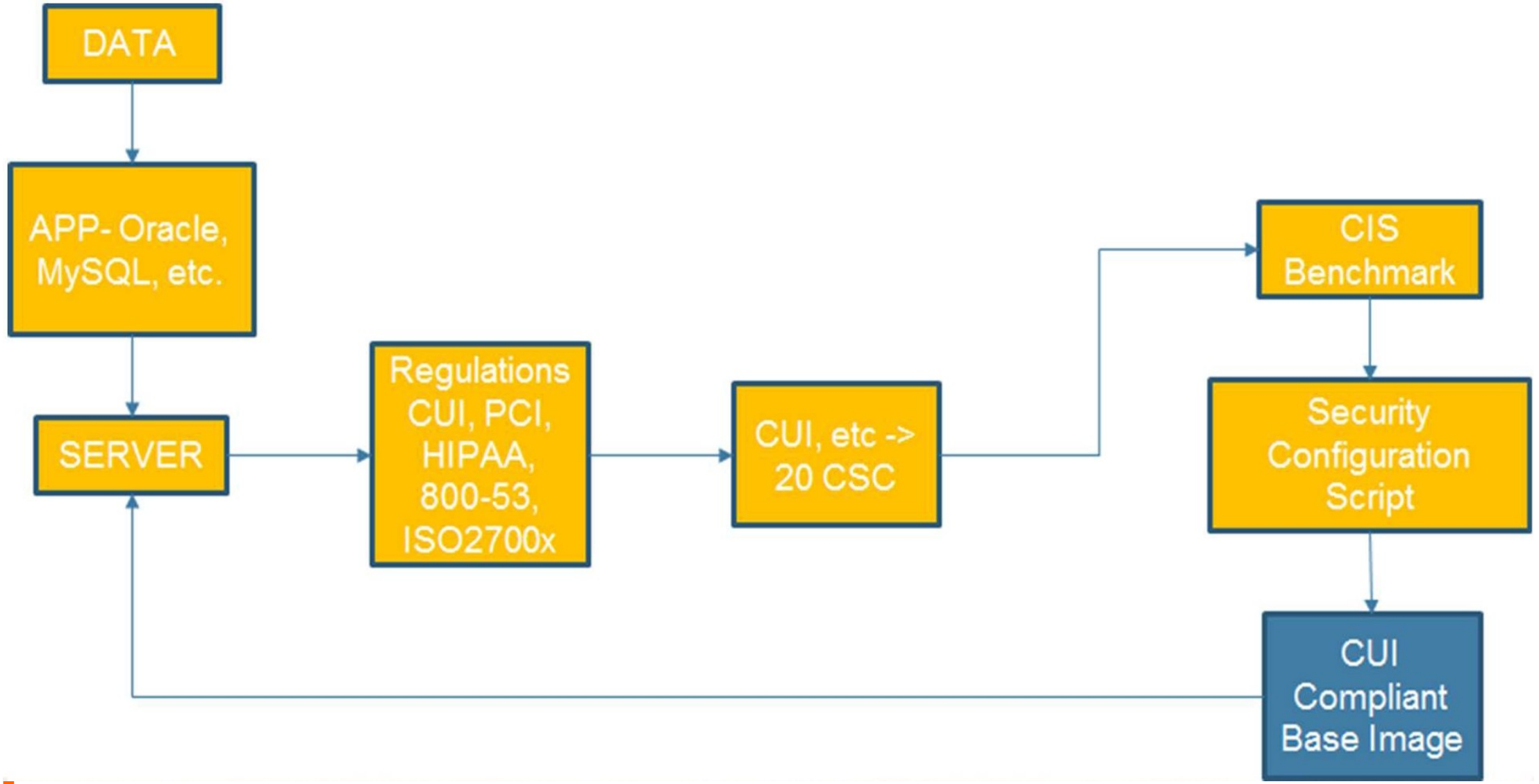
Run the following commands to set permissions on `/etc/motd`:

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

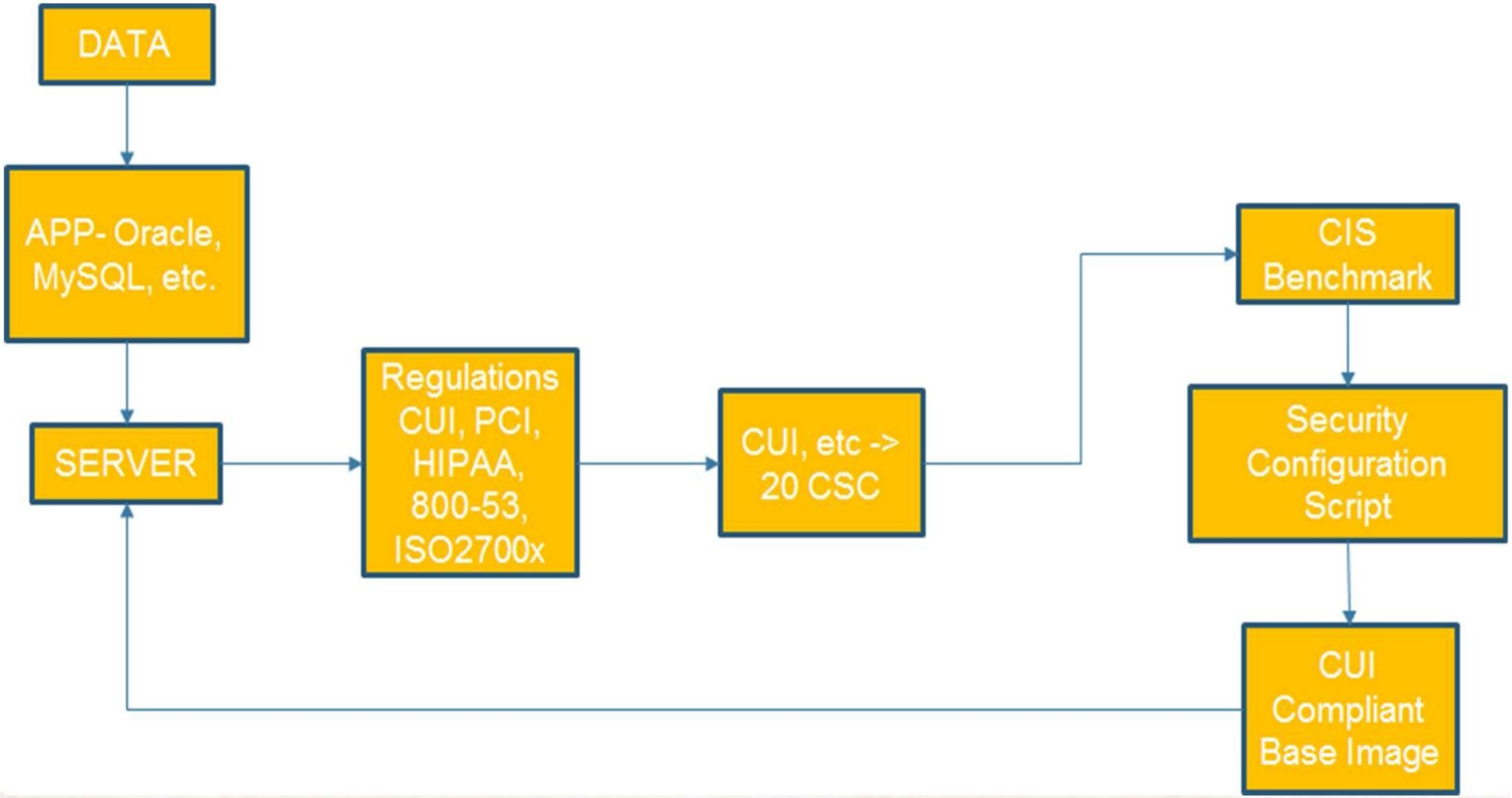


CIS Controls:

VIRGINIA TECH



VIRGINIA TECH



VIRGINIA TECH

ZTN and the 20 Critical Security Controls

- HW Inventory
- SW Inventory
- Continuous Vuln Mgmt
- Controlled use of Admin Priv
- Secure config for devices
- Log Analysis, maintenance
- Email, Browser Security
- Malware Defenses
- Limit Ports, Protocols, Services
- Data Recovery
- Secure config for net device
- Boundary Defense

ZTN and the 20 Critical Security Controls

- Data Protection
- Need to Know
- Wireless Access Control
- Acct Monitoring, Control
- Security Training
- Application Software Security
- Incident Response & Mgmt
- Penetration Testing and Red Team Exericises

Summary

- 20 Critical Security Controls provide a bridge between security frameworks, industry and local standards and operational actions.
- Start with the Basic set

References

- https://www.auditscripts.com/free-resources/critical-security-controls/
- https://cisecurity.org
- https://www.sans.org/course/critical-security-controls-planning-implementing-auditing (SEC440)
- https://www.sans.org/course/implementing-auditing-critical-security-controls (SEC566)