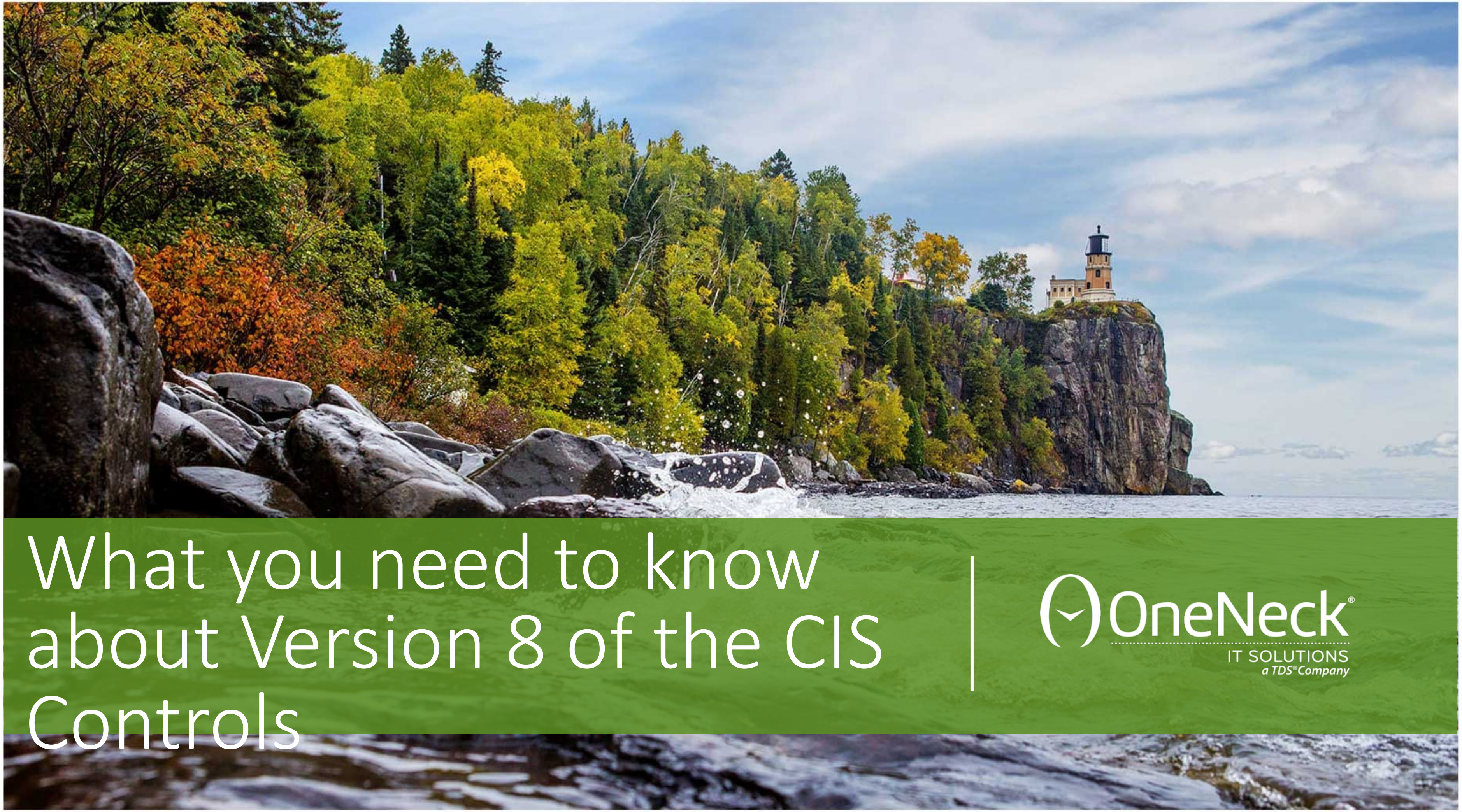


What you need to know about Version 8 of the CIS Controls

OneNeck®
IT SOLUTIONS
a TDS® Company

Andres Torrado

Security Architect/Sr. Security Consultant

OneNeck®
IT SOLUTIONS
a TDS® Company

My Background

- Worked in IT for 20 years
- Started at help desk position
- Network Engineer
- Security Engineer
- CISO
- Security Architect
- Sr. Security Consultant

OneNeck® IT SOLUTIONS a TDS® Company

What is a Security Framework?

- A method of implementing security controls, processes, and policies in an organization to improve security.
- Some Frameworks are followed for compliance
- What types are there?
  - NIST 800-53
  - ISO
  - PCI
  - CIS Controls

What to Choose

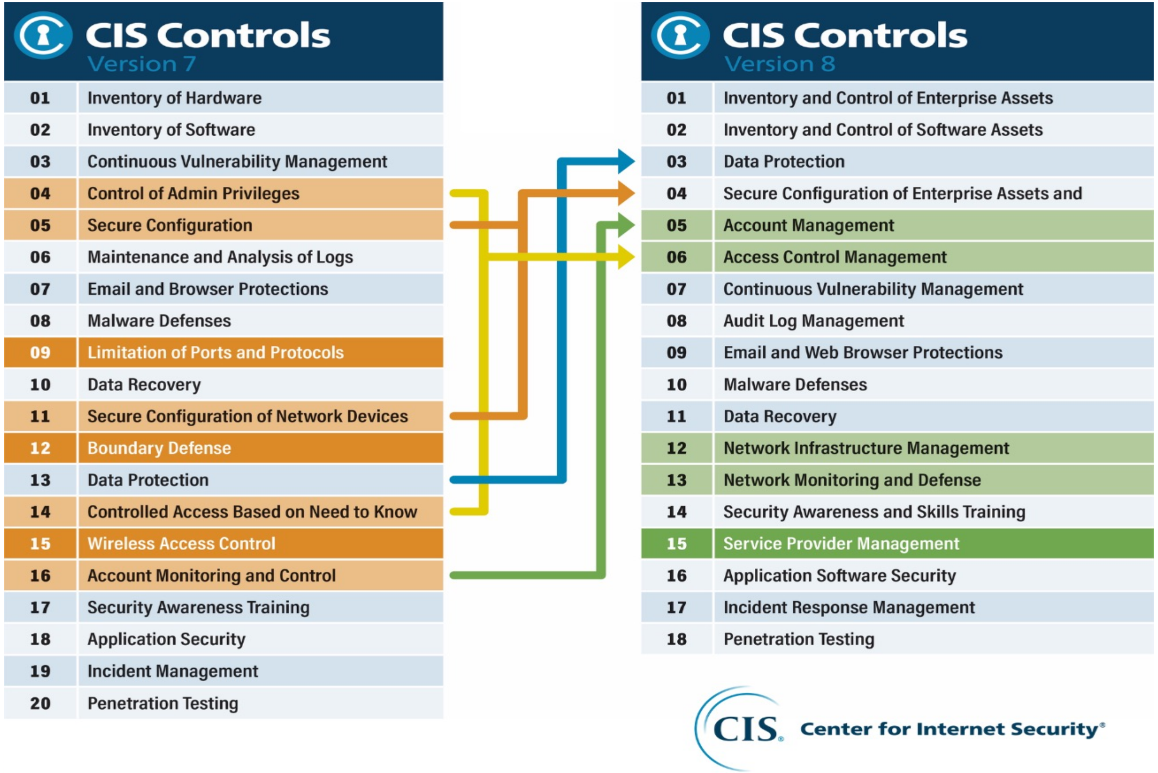
- Can you do both?
  - Yes or No

CIS Controls

- Formally known as the SANS top 20
- Priority
- Easier to implement
- Customizable to each environment
- New Versions version 8 now

OneNeck® IT SOLUTIONS a TDS® Company

Version 7 vs Version 8



CIS Controls
Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

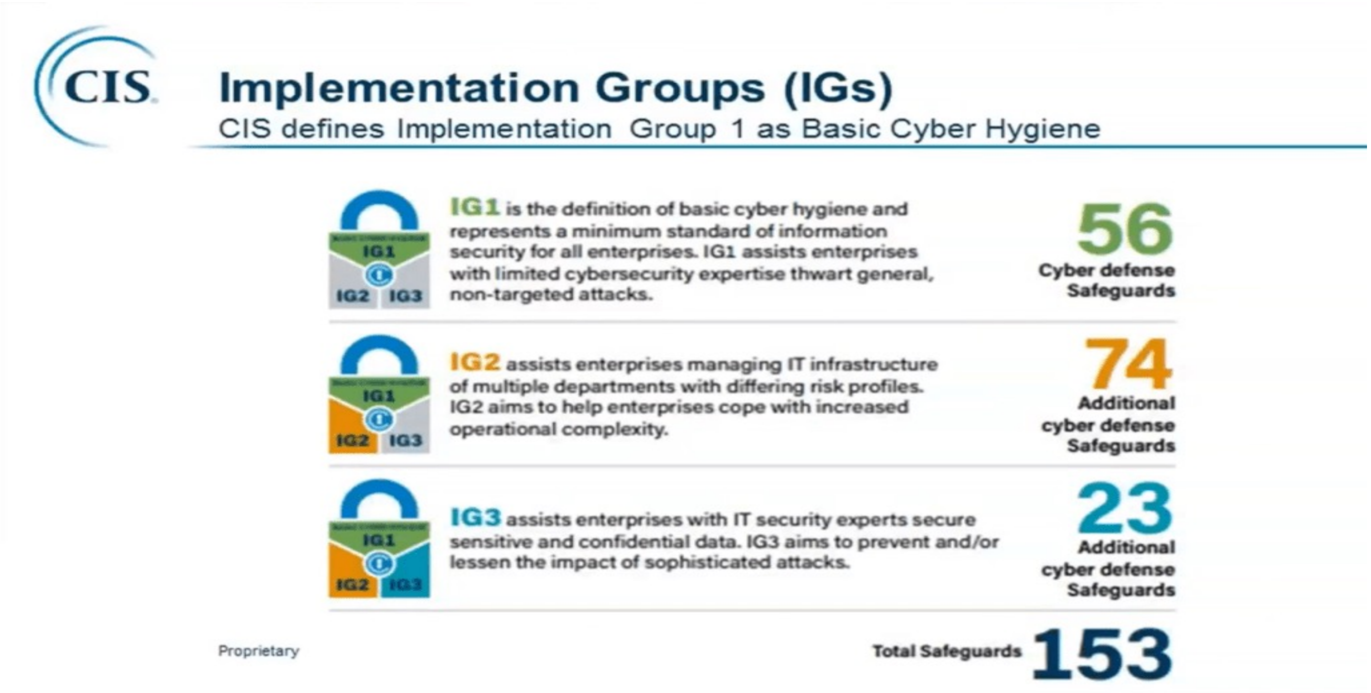
CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS Center for Internet Security®

OneNeck®
IT SOLUTIONS
a TDS®Company

Implementation Groups are still around



CIS Implementation Groups (IGs)

CIS defines Implementation Group 1 as Basic Cyber Hygiene

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Proprietary

Total Safeguards **153**

Safeguards

- Each control has an audit metric
- Do as many safeguards as needed to meet the metric
- You might not have to do all of them

Why the changes

- Analyze real world attacks using Data from MS-ISAC, Verizon DBIR, and MITRE ATT&CK
- Ransomware (Data Protection)
- Technology Changes (work from home, cloud computing, virtualization)
- Help enterprises better prioritize security efforts

Some of the Biggest Changes

- Data Protection
  - 14 Safeguards
  - Data everywhere
- Account Management
- Service Provider Management

Build a Strategy

- Do an assessment (self or paid)
- Build a timeline and strategy for implementation
- Where do you want to get to in 3 years
- Find tools do you need to help you get there

Start Small

- Get support from leadership
- Work the IG1 safeguards
- Look to the top of the Control list
- Show improvements
- Focus on easy wins

Work the Strategy

- Work on the next controls or control group
- Test yourself on what you did

Free Tools

Control 1

- Inventory and Control of Hardware Assets
  - NMAP
  - Automation (Dev OPS)

Free Tools

Control 7

- Continuous vulnerability management
  - OpenVAS
  - SIEM integration

OneNeck IT SOLUTIONS a TDS® Company

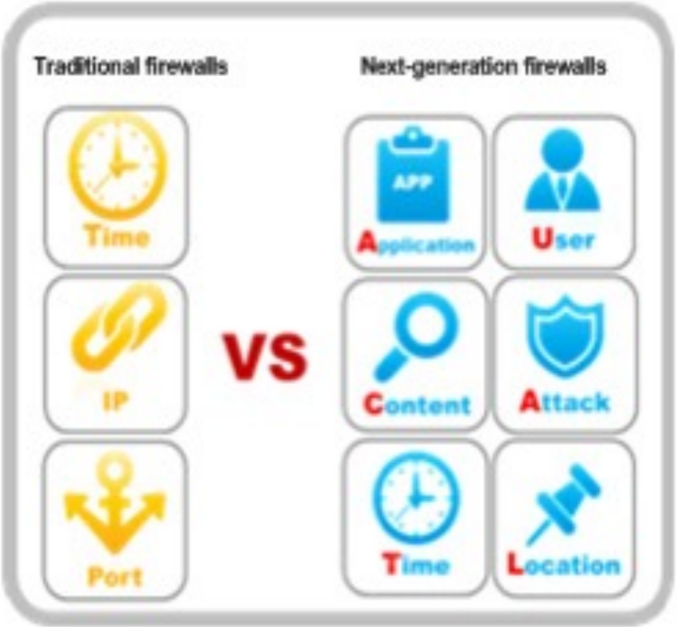
Free Tools

Control 13

- Network Monitoring and Defense
  - SNORT
  - IDS then IPS

NGFWs

- A lot of vendors are strong in this space
- Features
  - Application aware
  - Integrated inspection
    - IPS/IDS
    - Malware
    - Web inspection



Resources

- https://www.iso.org/isoiec-27001-information-security.html
- https://www.cisecurity.org/controls/
- https://nvd.nist.gov/800-53/Rev4/
- https://www.shodan.io/
- https://www.cisecurity.org/controls/implementation-groups/

Questions?

OneNeck®
IT SOLUTIONS
a TDS® Company

Thank you

OneNeck®
IT SOLUTIONS
a TDS® Company