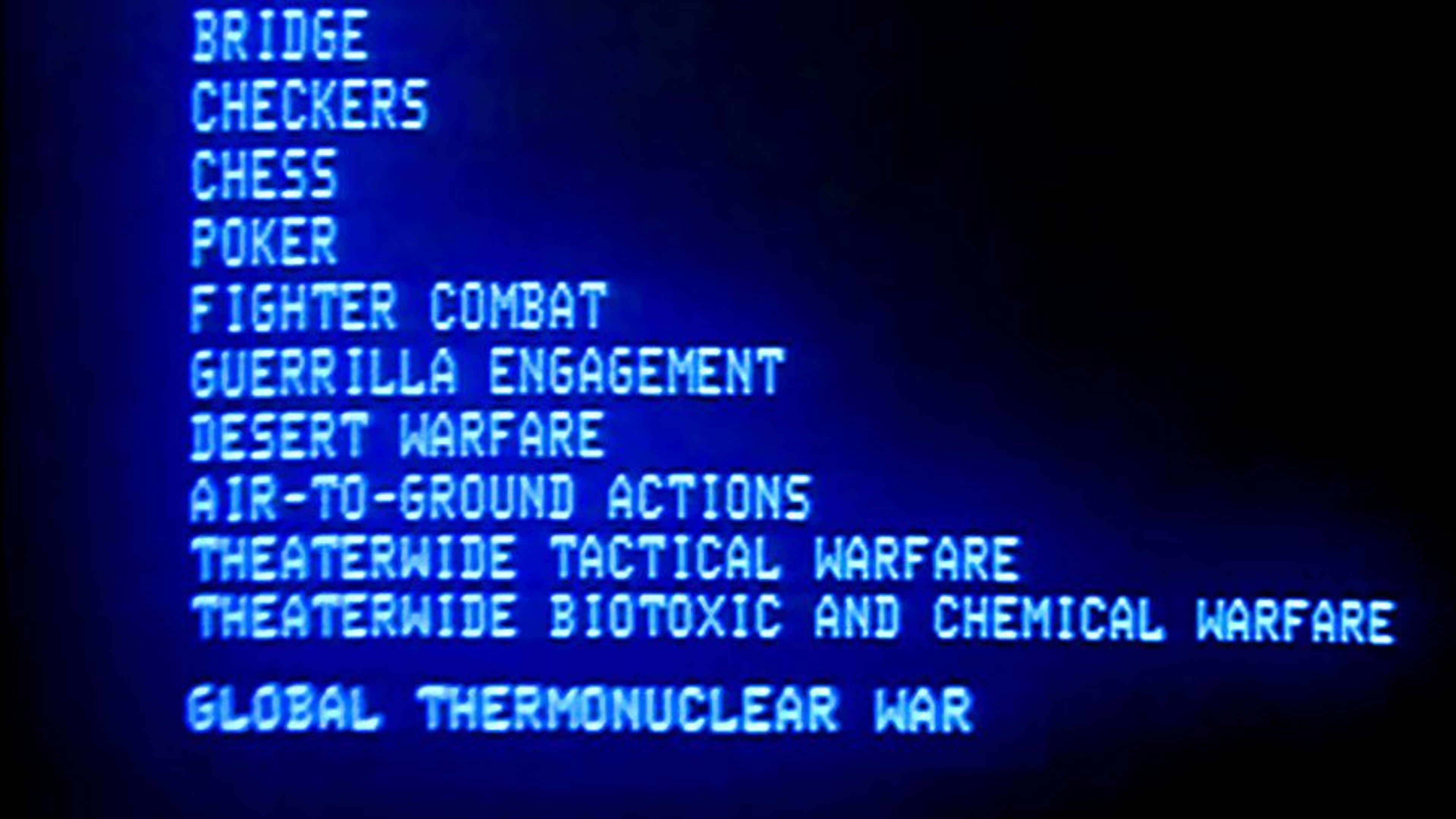
Robotics Security Kickstart

Don't let your robots be the source of a breach

Sid Faber, sid.faber@canonical.com

CANONICAL ubuntu



```
BRIDGE
CHECKERS
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE

GLOBAL THERMONUCLEAR WAR
```

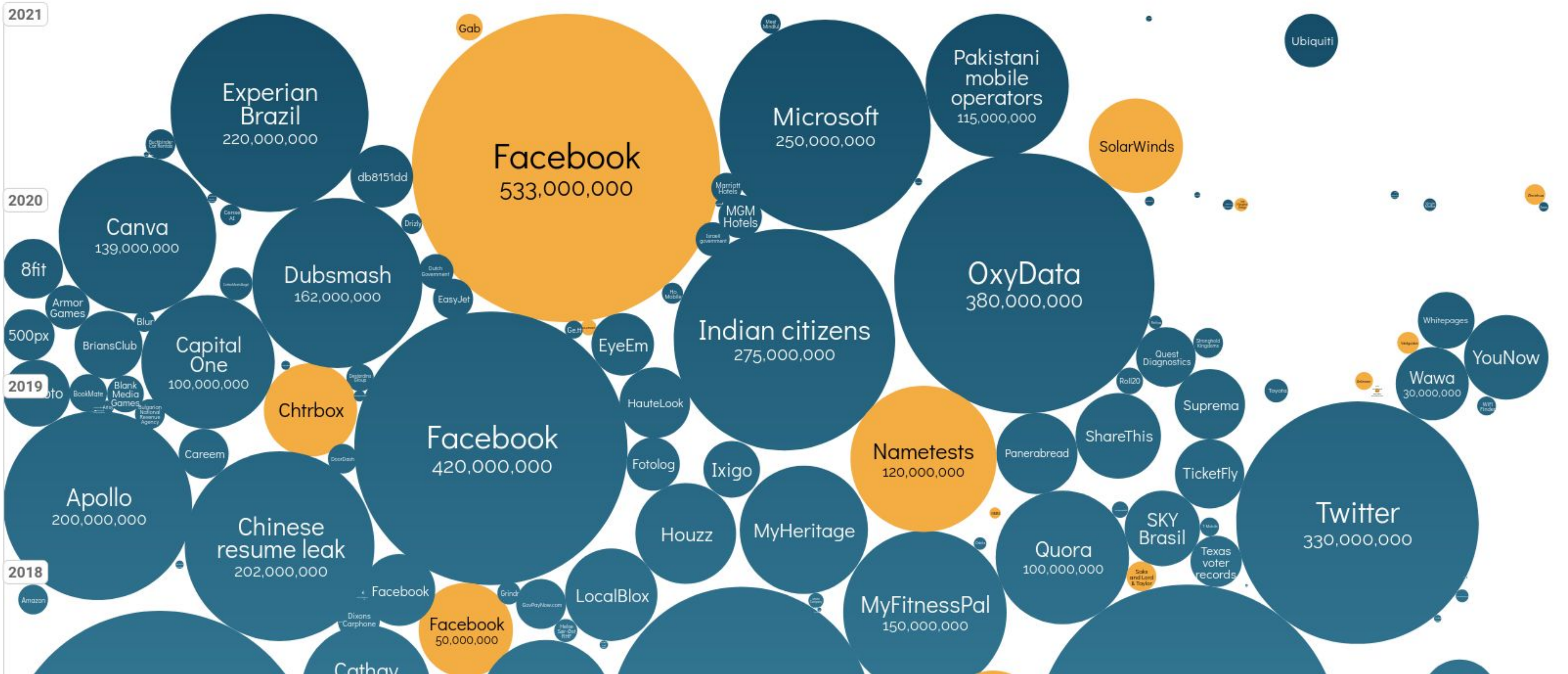
World's Biggest Data Breaches & Hacks

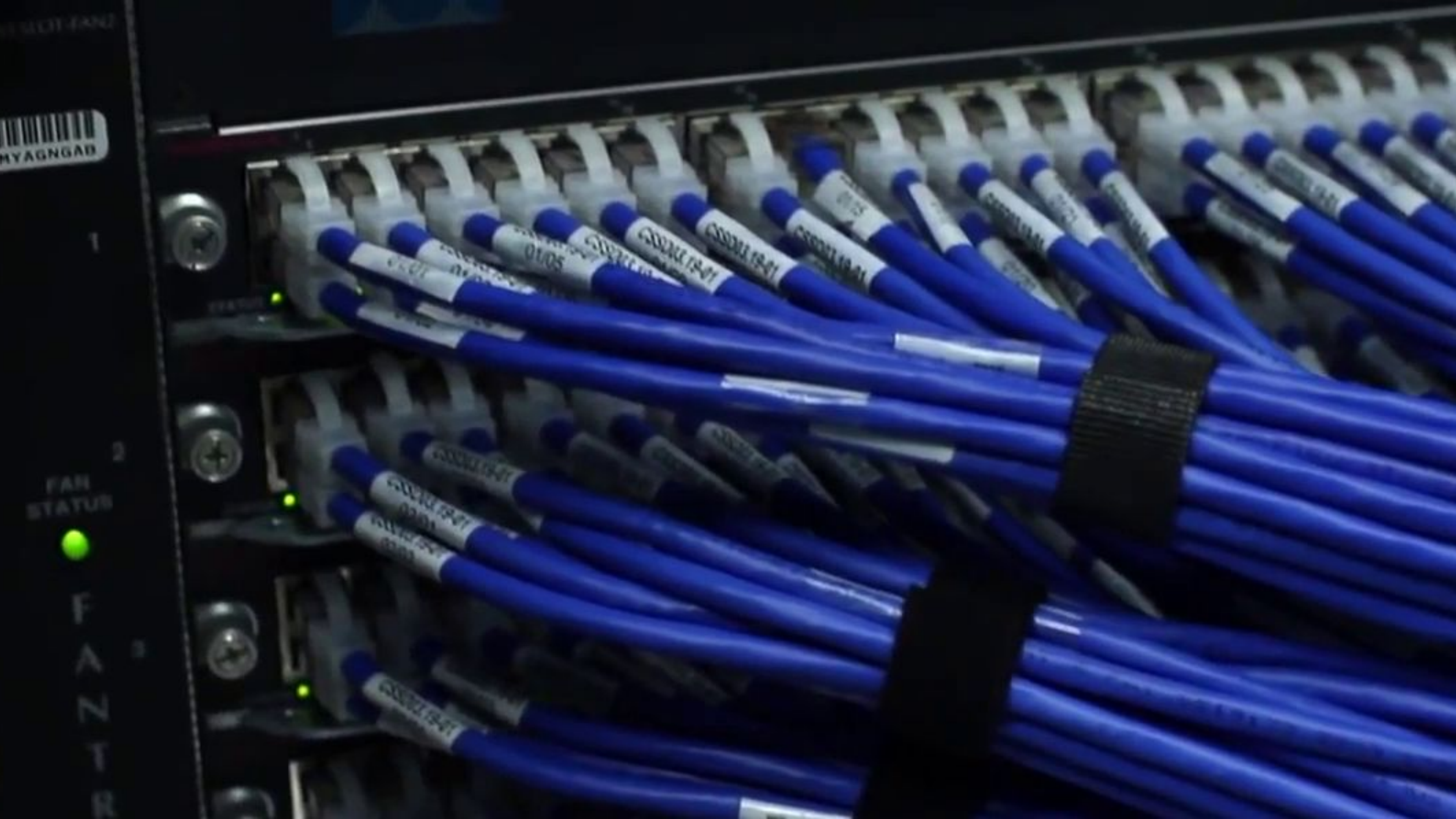
Selected events over 30,000 records

UPDATED: Apr 2021

size: records lost | filter

interesting story

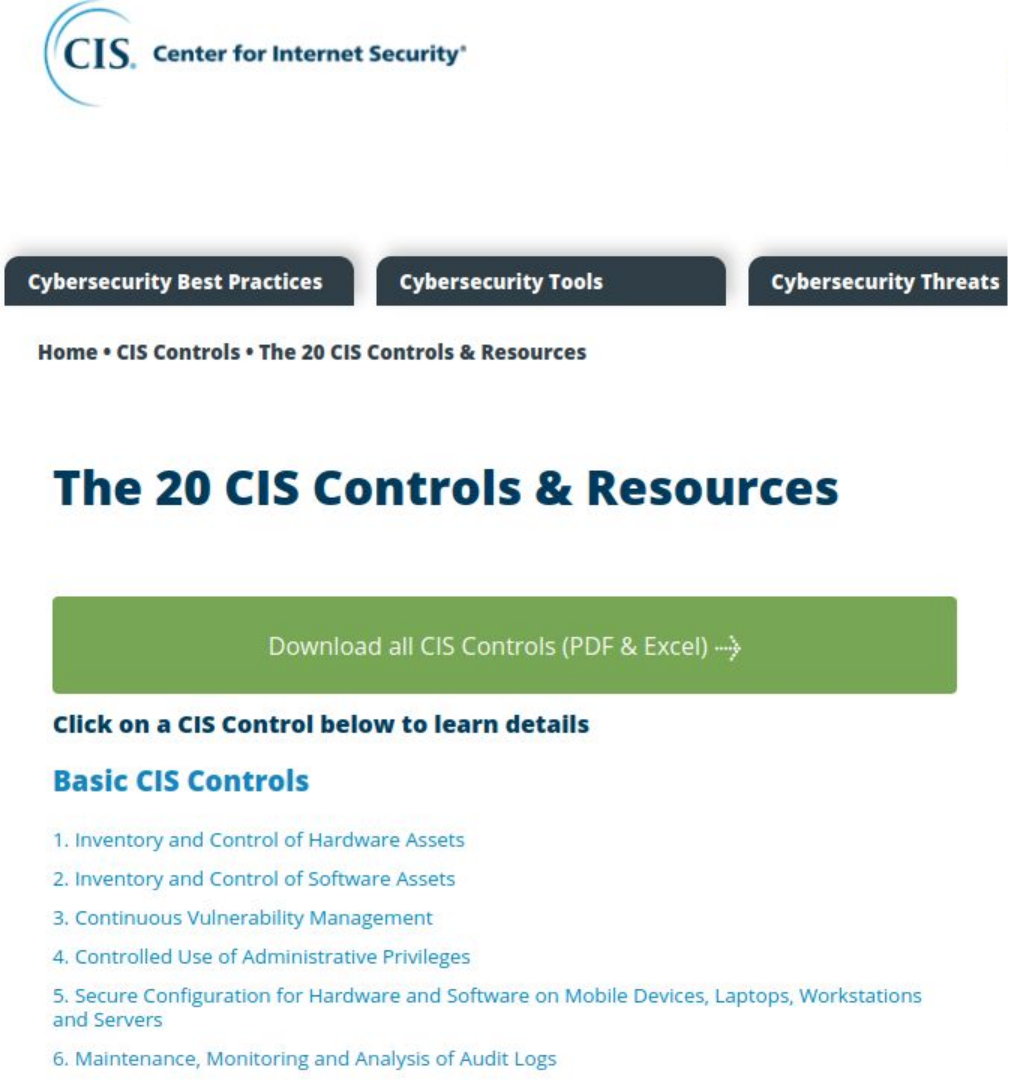




MYAGNGAD
1
2
FAN STATUS
FANTR

The CIS Top 20

https://www.cisecurity.org/



CIS. Center for Internet Security®
Cybersecurity Best Practices
Cybersecurity Tools
Cybersecurity Threats
Home • CIS Controls • The 20 CIS Controls & Resources

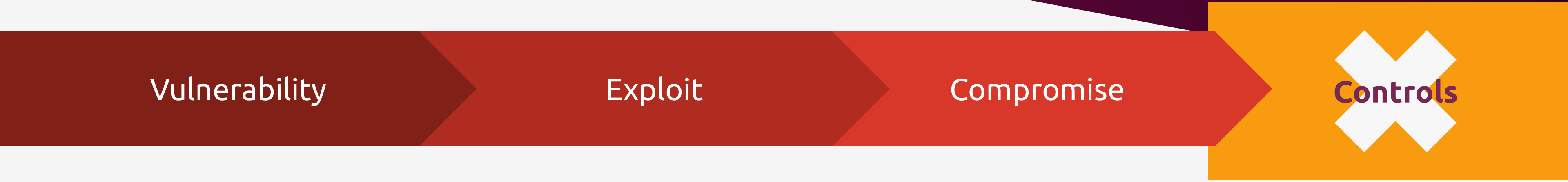
The 20 CIS Controls & Resources

Download all CIS Controls (PDF & Excel)

Click on a CIS Control below to learn details

Basic CIS Controls

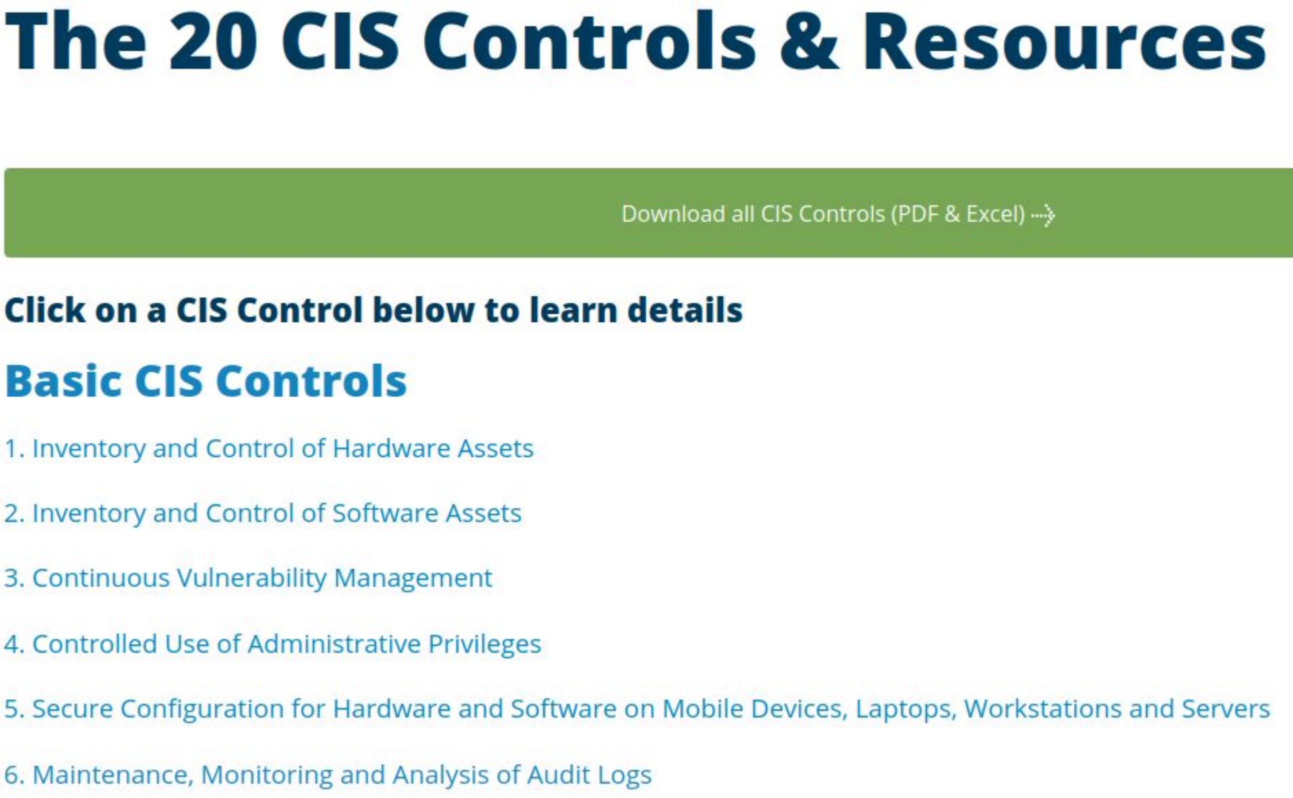
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs



Vulnerability	Exploit	Compromise	Controls
A weakness in the security system	The ability to use a vulnerability to gain an advantage	Loss of value - could be monetary, personal, replacement cost, time-related, etc.	Prevent or detect compromise

The CIS Top 20

https://www.cisecurity.org/



The 20 CIS Controls & Resources

Download all CIS Controls (PDF & Excel)

Click on a CIS Control below to learn details

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

Controls 1 and 2: Inventory and Control of Hardware & Software Assets

Main Points:

- Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
- Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
- Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
- Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

Controls 3:

Main Points:

- Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
- Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

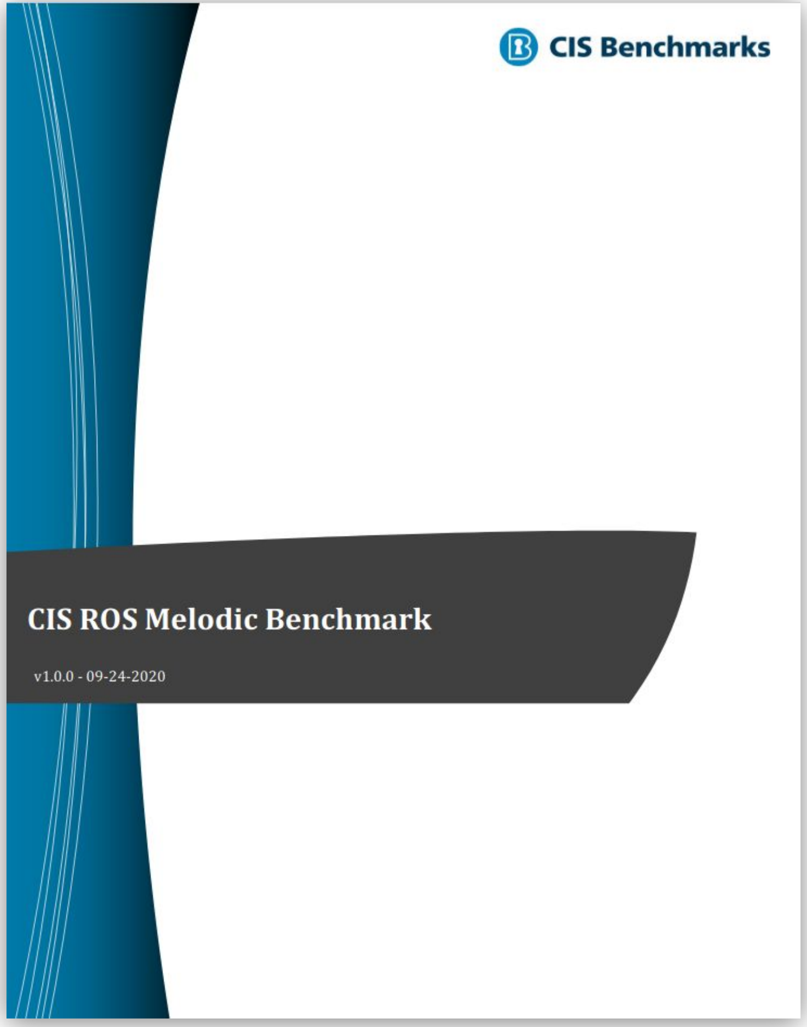
ESM for ROS

Support and security updates for ROS and Ubuntu

- Backported security updates, CVE and bug fixes for ROS.
- Extended Security Maintenance for a number of packages in the Ubuntu Main and Universe Repositories.

The ROS Benchmark

https://www.cisecurity.org/



CIS Benchmarks

CIS ROS Melodic Benchmark

v1.0.0 - 09-24-2020

Thank you