



# DOING SIMPLE AT SCALE

HOW TO IMPLEMENT THE CIS TOP 20 USING OPEN SOURCE, FREE SOFTWARE, AND SELF BUILT TOOLS





# Micah K Brown

- Twitter: @MicahKBrown
- Munich Re: IT Security Engineer II
- GitHub: <https://github.com/micahkbrown>
  - DLP Demystified (2018 talk)
  - Star Wars: How an ineffective Data Governance Program Destroyed the Galactic Empire (2019 talk)
  - How to cook a Five Star Meal from the Convenience of Your Hotel Room (Derby Con 2019)
  - Doing simple at scale (2020 talk)
- Vice President of Greater Cincinnati ISSA Chapter
- CISSP
- Served 45 pounds of free Pulled Pork to @DerbyCon 2019!
- Real Corp 2018 goal: "Learn to Cook Brisket Like a Texan."
- Real Corp 2019 goal: "Continue to Cook Brisket Like a Texan."
- On most Fridays, find me smoking both an old fashioned and pizza!

\*Thoughts and view are my own and do not reflect that of my employer.

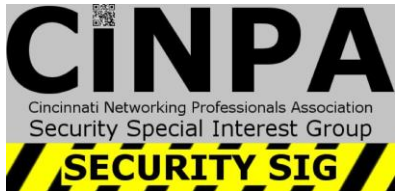
## Greater Cincinnati IT Security groups



<http://www.cincy-issa.org/>



<https://sites.google.com/view/cincysmba>



<https://www.meetup.com/TechLife-Cincinnati/events/>



<https://www.infosecincy.org/>



**“One of the hardest things I do, as an enterprise is  
the ‘simple at scale’”  
— Micah K Brown**

# CONTROL I:

INVENTORY AND CONTROL OF HARDWARE ASSETS



# I: INVENTORY AND CONTROL OF HARDWARE 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

# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Step I: Define your environment

1. **Bring 'Procurement' / 'Purchasing' into the conversation early.**
2. **Active Discovery for servers, network devices, appliances, cloud**
  - i. **Define scope: look at your core router's routing table**
  - ii. **Use a 'discovery' scan on all server, network, and appliance VLANs.**
3. **For client systems define active discovery. (AD, malware, client discovery tool)**
4. **For mobile systems audit your billing from authorized telcom**
5. **For BYOD, audit system enrollment**
6. **Document results in CMDB**

# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Step 2: Inventory of Authorized and Unauthorized Devices on server, network, appliance VLANs:

- nmap is free and open source (in almost every base image of Linux)
  - Can do a lot of investigating and fingerprinting
- Zenmap is **GUI friendly scanner** based on nmap
  - Great tool to start with, even gives you the actual nmap command it is using so you can level up
  - Built into Kali!
- Alienvault **OSSIM** \*\*\*
- OpenAudit \*\*\*
- OpenNSM \*\*\*

# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Step 3: Automate system discovery

- Audit AD client system activity (last login attribute)
- Audit anti-malware clients (often baked into client images)
- DHCP
  - Windows DHCP Servers Audit Event tools (free)
    - Good for auditing client user VLANs
    - <http://blogs.technet.com/b/teamdhcp/archive/2009/03/20/tool-to-read-dhcp-server-events-for-windows-server-2008-r2.aspx>
  - Linux DHCP Server Config and Logging
    - [https://www.centos.org/docs/5/html/Deployment\\_Guide-en-US/s1-dhcp-configuring-server.html](https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-dhcp-configuring-server.html)



# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Step 3: automate system discovery (continued)

- 802.1x is the default open protocol that allows network devices to grant / revoke network access based on centralized user / device identity.
  - **Windows NPS server role**
    - [https://technet.microsoft.com/en-us/library/Cc732256\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Cc732256(v=WS.10).aspx)
  - FreeRADIUS & 802.1x
    - [http://tldp.org/HOWTO/html\\_single/8021X-HOWTO/](http://tldp.org/HOWTO/html_single/8021X-HOWTO/)
- Many open source NACs exist but make sure to test extensively
  - OpenNAC
  - FreeNAC
  - PacketFence
- Ensure strong key management and PKI infrastructure exist

# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Step 4 and 5: Mobile and BYOD

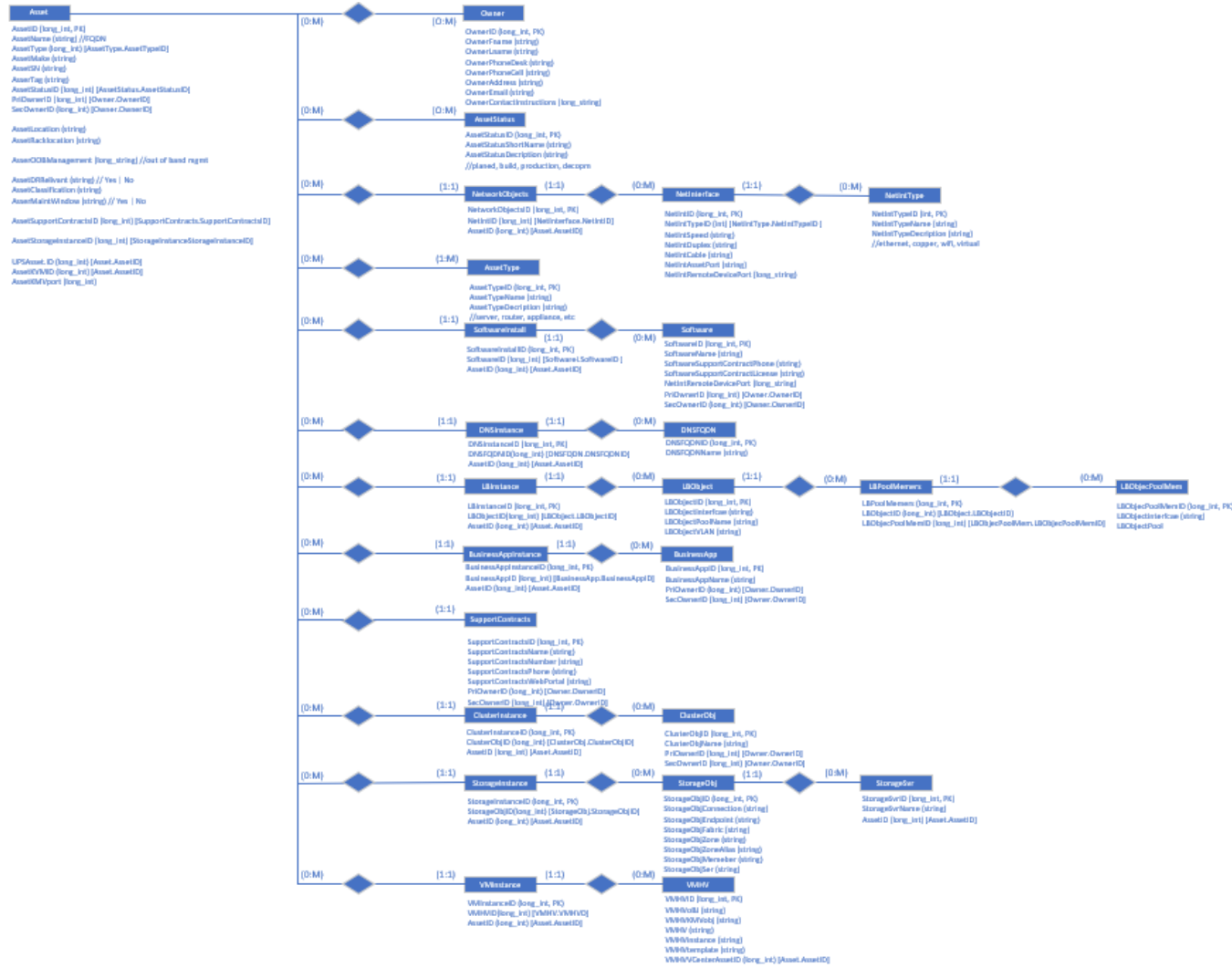
- Controls differ on control suite but you should:
  - Report on devices user enrolls
  - Report when user accesses authorized container
  - Block and Alert company data from leaving authorized container
  - Discover company data in authorized container
  - Remote wipe any company data from authorized container
  - For company own devices allow company to do full wipe
  - For BYOD allow user to explicitly request company to do full wipe on their behalf

# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Step 6: build and **MAINTAIN** a **CMDB**:

- For small shops with limited IT, building your own might be possible
- Services like Spiceworks will give you a free tool that is monetized through targeted adds. Do you really want your environment blueprint residing on other peoples servers?
- Most ticketing systems have a decent **CMDB** functionality.
- When you build your own; it is a custom fit (with all + and -)

# BENEFITS OF DEFINING YOUR IDEAL CMDB



## Assets contain

- Owners (Pri, Sec)
- Status
- Asset Type
- Support Contract
- Software Install
- Business App Instance
- Network Obj
- DNS Obj
- Cluster instance
- Storage instance
- VM / Hypervisor / Container

**“To do anything well you must have the humility to bumble around a bit, to follow your nose, to get lost, to goof. Have the courage to try an undertaking and possibly do it poorly. Unremarkable lives are marked by the fear of not looking capable when trying to do something new”  
— Epictetus, The Art of Living**

## CONTROL 2:

INVENTORY AND CONTROL OF SOFTWARE ASSETS

# I: INVENTORY AND CONTROL OF HARDWARE ASSETS

## Main Points:

- 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.

## 2: INVENTORY AND CONTROL OF SOFTWARE ASSETS

### Step one: Define authorized software

- Bring 'Procurement' / 'Purchasing' into the conversation early
  - They can tell you what we pay for which may or may not be what we use
  - They are responsible for 'true-up' and licensing adjustments
  - They might have 'asset' tags
  - Support Contracts can help you build a what 'should be here'

## 2: INVENTORY AND CONTROL OF SOFTWARE ASSETS

### Step two: Inventory installed software

- **Powershell is amazing**
  - `Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize > C:\temp\InstalledPrograms-PS.txt`
- This can also be done various ways depending on the linux distribution
- Alienvault OSSIM - TBD
- Spiceworks - TBD
- Nessus Community – TBD
- OpenVAS - TBD
  
- This should be run and audited on a regular basis



## 2: INVENTORY AND CONTROL OF SOFTWARE ASSETS

### Step three: prevent install of unauthorized software

- Remove users admin rights\* (unless business justification exists)
- Block access to popular portable apps
- GPO to restrict execution of code in popular locations (and subfolders):
  - <https://blog.brankovucinec.com/2014/10/24/use-software-restriction-policies-to-block-viruses-and-malware/>
  - %AppData% (and subfolders)
  - %LocalAppData% (and subfolders)
  - %Downloads% (and subfolders)
  - **Restrict code running on extracted 7zip, WinRAR, WinZIP, windows ZIP**
- Output of step two can be used as justification for application white listing
  - Microsoft AppLocker is built into windows <https://github.com/nsacyber/AppLocker-Guidance>
  - Appsamvid (free Windows) <https://www.thewindowsclub.com/appsamvid-application-whitelisting-software>
    - Lacking in centralized management



**“If you know the enemy and know yourself, you  
need not fear the result of a hundred battles.”  
— Sun Tzu, The Art of War**

## CONTROL 3:

CONTINUOUS VULNERABILITY MANAGEMENT



## 3: CONTINUOUS VULNERABILITY MANAGEMENT

### 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.

# 3: CONTINUOUS VULNERABILITY MANAGEMENT

- General full stack
  - OpenVAS (kali)
  - Nexpose Community (rapid7)
    - <https://www.rapid7.com/info/nexpose-community/> (1 year,)
  - Nessus Essentials (Tenable scan 16 devices)
    - <https://www.tenable.com/products/nessus/nessus-essentials>
  - Metasploit
  - Retina CS (256 assets)
- Web Server
  - BurpSuite free
  - Nikto (web server scanner)
  - OWASP ZAP
- Database
  - SQLMap



**“Many are harmed by fear itself, and many may  
have to come to their fate while dreading fate”  
— Seneca, Oedipus**

## CONTROL 4:

CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES



## 4: CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

### Main Points:

- Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
- Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.


## 4: CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

1. Leverage an enterprise wide naming convention for user accounts
  - Normal user, normal contractor, admin, domain controller, service account, etc. . .
2. Leverage strong credential management for sensitive credentials, keys, and identities
  - 'Password Protected' files
  - Keepass – fails if multiple people need to work in the file at the same time
    - Keepass Pro – addresses the multi-user need
  - TeamPass – install your own server or stand up docker instance
    - <https://teampass.net/>
  - Psono – integrates with <https://haveibeenpwned.com> database
    - <https://gitlab.com/psono>
  - Bitwarden – while enterprise plans exist, you *can* host yourself as sever or docker!
    - <https://bitwarden.com/>

## 4: CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

1. **Work with application owners / server owners to understand what logs are created when admin access is added and removed.**
  - a. **Define normal use (log)**
  - b. **Define abnormal use (alert)**
  - c. **Define forbidden use (alert high priority)**
2. **Define critical use cases you care about**
  - a. **Install software, service, share, and patches**
  - b. **Creation of drive map**
  - c. **Network config changes**
  - d. **Add new admin access**
3. **Audit high priority alert / report with admin activities on regular basis**
4. **Repeat this process on regular basis**





**"Zeno would also say that nothing is more hostile  
to a firm grasp on knowledge than self deception"  
— Diogenes Laertius, Lives of the Eminent  
Philosophers**

## CONTROL 5:

SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS,  
WORKSTATIONS AND SERVERS



## 5: SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS AND SERVERS

### Main Points:


- Maintain documented, standard security configuration standards for all authorized operating systems and software.
- Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

<https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/>

## 5: SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS AND SERVERS

This can often be easier in the cloud environment as many popular cloud providers have build hardened templates that meet **CIS, NIST**, and other security frameworks

- CIS hardened images
  - <https://learn.cisecurity.org/benchmarks>
  - <https://www.cisecurity.org/cis-hardened-images/>
- NIST Hardening guides
  - <https://nvd.nist.gov/ncp/repository>
- Microsoft Windows Security Baseline
  - Security Compliance Toolkit (SCT)
  - <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>



**"If anyone can prove and show to me that I think and act in error, I will gladly change it - for I seek the truth, by which no one has ever been harmed. The one who is harmed is the one who abides in deceit and ignorance" - Marcus Aurelius, Meditations**

## CONTROL 6:

MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS



## 6: MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

### Main Points:

- Ensure that local logging has been enabled on all systems and networking devices.
- Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

## 6: MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

### Step 1) Define Logging Standard

- Microsoft has Best Practices for Windows
  - <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>
- NIST
  - <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>
- Many Pay-for-Play SIEMS will make their logging documentation free and publicly available
- Most Hardware / Software has logging best practices so no need to recreate the wheel
- Consider different levels of logging for different areas of your network
  - Cisco Traditional Datacenter Model: Core, Distribution, Access
  - Cloud vs on prem
  - Networks bound by rules, laws, regulations, contractual agreements

## 6: MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

### Step 2) centralized log management

- ELK stack (built into default securityonion image as well as HELK!)
- Greylog (freemium model for all features)
- Solarwinds Event Log Consolidator
- Kiwi syslog
- Splunk free (limited for 500 mb a day)
- Others exist

### Step 3) Audit for logging

- Create alerts if a resource stops logging for 48 hours
- Manual audit for device logging status on repeated basis
  - For a device to be good it must be discoverable, have an entry in CMDB, and be logging

## 6: MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

### Step 4) Supercharge your alerts / reports

- Talk to app / system owners as to what logs / events they care about
- Use the Miter ATT&CK Framework to detect common offensive techniques
  - <https://attack.mitre.org/>
- Sigma helps deploy common open source rules to many popular SIEMs
  - <https://github.com/Neo23x0/sigma>
- Purple Team Test methodology to create custom rules based on controlled attacks



## 6: MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

### Step 4) Supercharge your alerts / reports (continued)

- Make allies with Audit by helping automate their job
- Create a report that you can update daily that will search the previous X days of logs (time to execute search is your limitation) for an malicious IPs listed in open source intel feed(s) of your choice. Look for any successful connection entering and exiting your gateway.
  - Cisco: Talos Intelligence
  - SANS: Internet Storm Center
  - Department of Homeland Security: Automated Indicator Sharing
  - FBI: InfraGard Portal
  - VirusTotal: VirusTotal