macOS Sierra

Enterprise Security

Disclaimer:

I am not responsible if a Macintosh is broken due to following these steps

What will be discussed:

- Firmware Password
- Installer Images & First Boot
- Admin & Standard Accounts
- Hybernation ~vs~ Sleep
- Firewall
- Services & Daemons
- Spotlight Suggestions
- Homebrew
- DNS
- Captive Portal
- Certificate Authorities
- OpenSSL, Curl & Privoxy
- Browsers
- PGP & GPG
- OTR, Tor & VPN
- Viruses & Malware
- System Integrity Protection
- Gatekeeper & XProtect
- Password Management
- Backups
- Wi-Fi
- SSH
- Physical Access
- System Monitoring
- Binary Whitelisting
- Profile Manager
- Audit & Forensics
- Additional Resources

Firmware Password

- Prevents your Mac from starting up from alternate storage

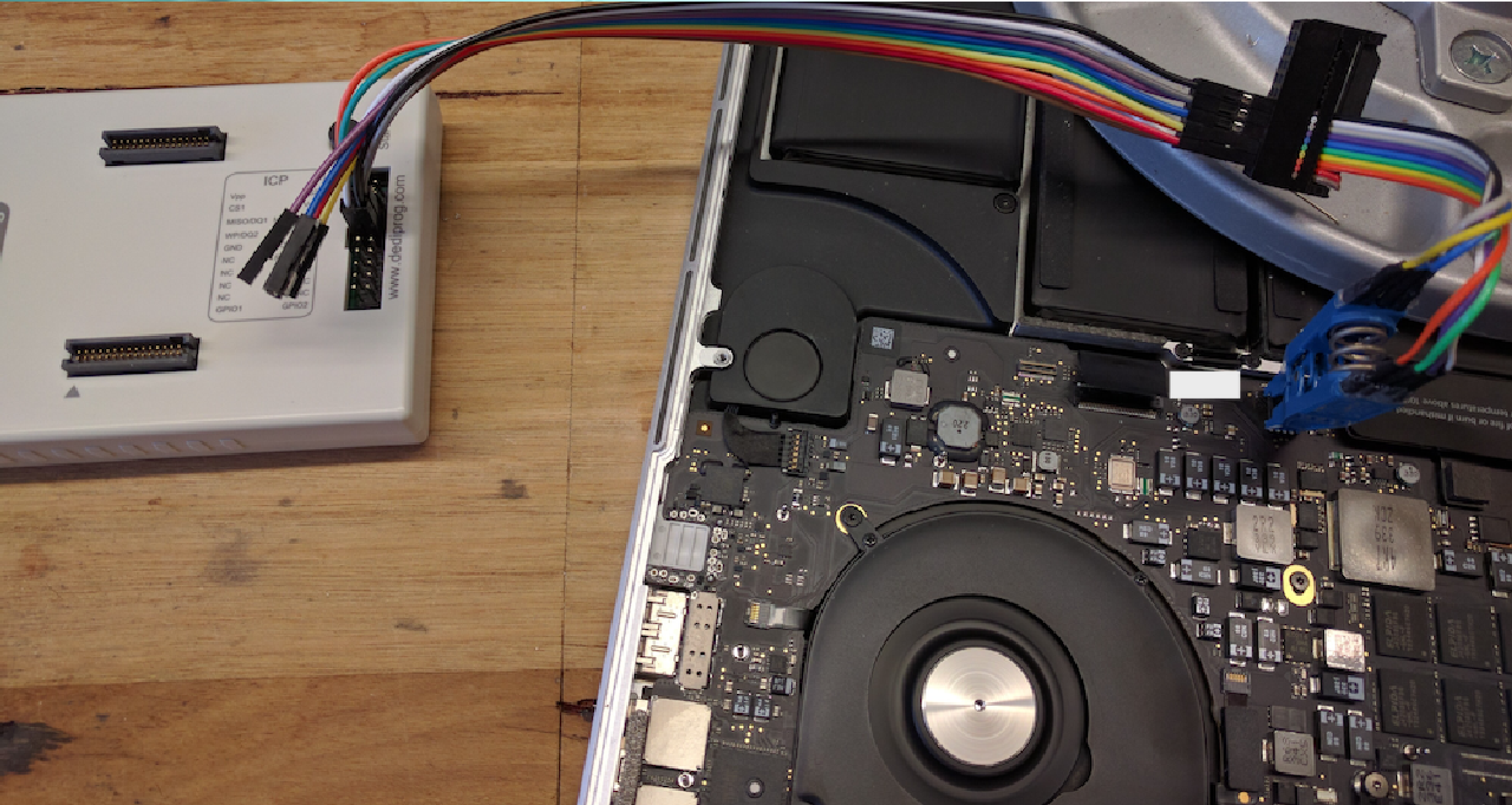
- Can be reset in Apple store with proof of ownership

- Alternatively managed with ‘firmwarepasswd’ utility

- May be set to be required at every boot

Firmware Password

Using a Dediprog SF600 to dump and flash SPI chip



Installer Images & First Boot

- Installing from Recover Mode reveals the system’s serial number over the network in plain text when communicating with Apple

- Server app includes the System Image utility and NetBoot service

- Custom restorable images can contain pre/post-install scripts

- Additional software can be automatically installed at 1st boot

- Macs can be installed/restored using target disk mode & USB

- Recovery partitions are optional and customizable

Installer Images & First Boot

- Post-install scripts can also be managed with Chilcote Outset
[https://github.com/chilcote/outset/] (written in python)

- Use Outset to process packages, profiles, and/or scripts at every boot/logon/logoff/on-demand

- AutoDMG is an alternative install image tool
[https://github.com/MagerValp/AutoDMG/]

- The computer/host names can be set using 'scutil'
eg: $ sudo scutil --set ComputerName your_computer_name

Admin & Standard Accounts

- Every system must have at least one Admin account

- Hide the admin account's home folder and login window ID, and disable admin's ability to disable file vault

- Standard users have no access to some preference panes, console, sudo, or modifying system folder or applications

Hybernation ~vs~ Sleep

- Sleep leaves the contents of memory in place

- Sleep uses EFI memory to store the FileVault master key

- Hybernate removes contents from RAM and EFI memory

- The ‘pmset’ utility is used to manage sleep/hybernate/keys

Firewall

- Application firewall (socketfilter) blocks incoming connections

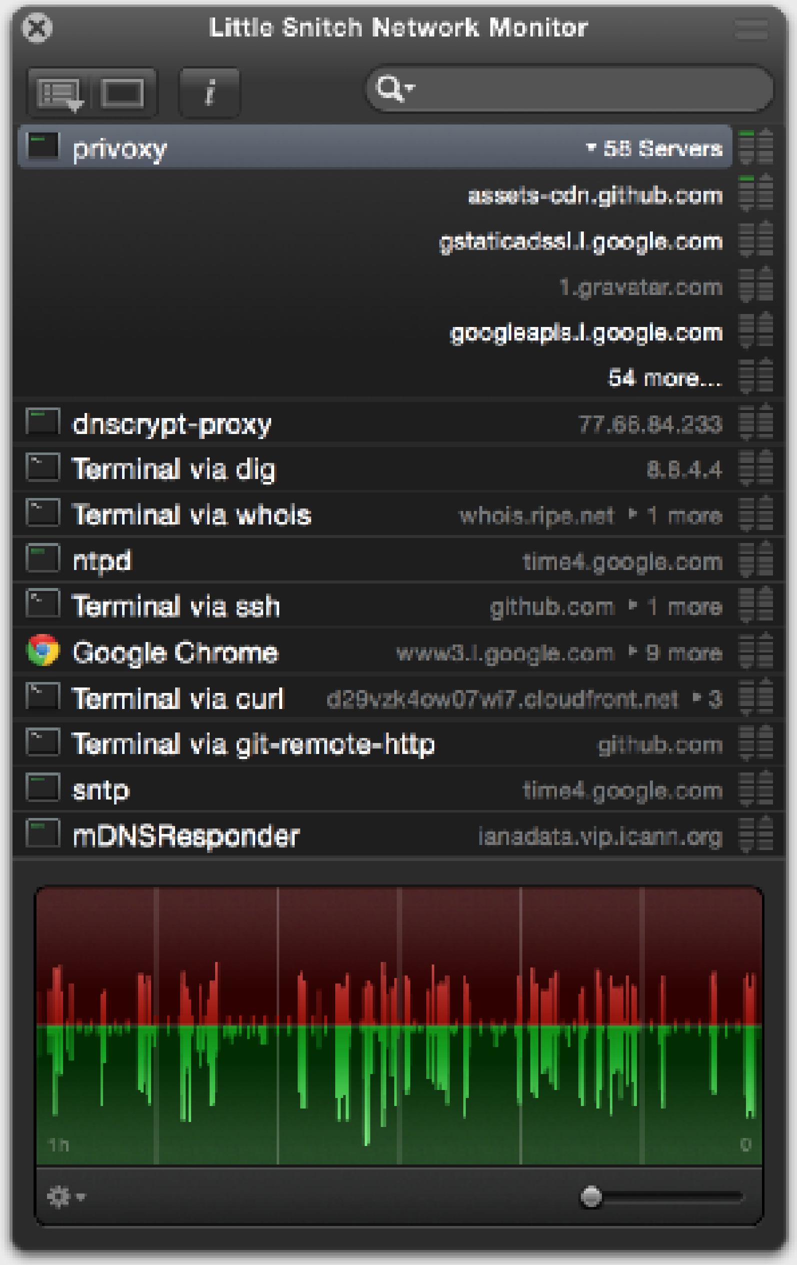
- Stealth mode prevents responses to ICMP and on closed ports

- Built-in and Code-Signed software whitelists by default

- Little Snitch, Hands Off, Radio Silence and Security Growler: provides ability to monitor &block outbound traffic at a granular level

- pf as the kernel level system firewall [Murus]

- pf has the ability to audit phone-home behavior [https://github.com/fix-macosx/net-monitor]



Little Snitch Network Monitor

privoxy	▾ 58 Servers
	assets-cdn.github.com
	gstaticadssl.l.google.com
	1.gravatar.com
	googleapis.l.google.com
	54 more...
dnscrypt-proxy	77.66.84.233
Terminal via dig	8.8.4.4
Terminal via whois	whois.ripe.net ▸ 1 more
ntpd	time4.google.com
Terminal via ssh	github.com ▸ 1 more
Google Chrome	www3.l.google.com ▸ 9 more
Terminal via curl	d29vzk4ow07wi7.cloudfront.net ▸ 3
Terminal via git-remote-http	github.com
sntp	time4.google.com
mDNSResponder	ianadata.vip.icann.org

Services & Daemons

- Disable services which home, perform other useless functions
  [https://github.com/karek314/macOS-home-call-drop]

- Review damons, agents and services for the system and users
  [http://launchd.info] “LaunchControl”
  [https://githum.com/synack/knockknock]

- Manage security services (wireshark, audit/security scripts, etc)

Spotlight Suggestions

- Spotlight is by default chatty with Microsoft, Google, etc...

- Disable spotlight suggestions in System Preferences and Safari

- Change the default search engine to DuckDuckGo

- Modify spotlight settings to exclude servers

- Disable spotlight from searching undesired locations, files

- Disabel spotlight from indexing text

- See also: fix-macosx.com & fix10.isleaked.com

Homebrew

- Makes software installations easier to manage

- The missing repository

- Replaces Fink Commander, others from earlier OSX

- Make cron script to periodically update/upgrade

- Remember to opt-out of homebrew analytics

- Be mindful of installing at a system/user level

- Enable additional homebrew security options

DNS

- Use the hosts file to block known undesirable domains
  [https://github.com/StevenBlack/hosts/]

- Use internal FQDN servers and monitor queries separately

- dnsmasq can cache replies to reduce traffic, prevent problems

- Ensure the system is in a DNSSEC protected zone

- Defined search domains can be useful on departmental basis

- Best to manually set DNS servers, do not use DHCP

- dnscrypt can wrap your dns client/server traffic in a condom

Captive Portal

- When macOS connects to a SHITTY network, the probe it sends out will signal positive for a (malware ridden) captive portal (F U!!)

- This happens often at established organizations (rouge IT)

- Vulnerable to hijacking attack, known as wispr request

- DISABLE THIS CRAP IMMEDIATELY

- ‘sudo defaults write /Library/Preferences/SystemConfiguration/com.apple.captive.control Active -bool false’

Certificate Authorities

- macOS has >200 root authority certificates installed

- Risk of a man in the middle attack in which a coerced or compromised CA trusted by the system issues a fake/rouge SSL

- This is a growing problem today

- Use an internal CA which handles requests for all third parties

- Manage the internal CA separately, disable trust in ALL on macOS

OpenSSL, CURL & Privoxy

- The version of OpenSSL in Sierra is 0.9.8zh, which is not current
- Apple declares OpenSSL deprecated, distributes custom patches
- Use homebrew to install the latest OpenSSL ‘brew install openssl’
- curl uses Secure Transport for SSL/TLS validation
- Most prefer OpenSSL, replace curl ‘brew install curl --with-openssl’
- privoxy provides convenient local web traffic filtering
- Set system-wide proxy settings to point to it, make custom rules

Browsers

- Firefox and Chrome are preferred (not at default configuration)

- Disable flash in Chrome. Never install Java, Flash or Silverlight!!!!!

- Use PrivacyFox, NoScript, Ghostery and tie into management

- Use separate profiles for browsing Trusted, iffy, and risky sites

- Disable WebRTC with uBlock Origin

- Safari looks nice, but is a disaster at the code level.

- Safari can be blocked from use in user profiles on macOS Server

PGP & GPG

- PGP used for encrypting email end-to-end

- GPG used to verifying signatures of software, and encrypting symmetrically and asymmetrically files and text

- Modify the GPG default configuration

- Trust the local GPG keyservers (should be safe)

- Mail integration is available as a gnu applicaiton

OTR, TOR & VPN

- The most popular chat program for macOS is Adium

- profanity is a decent console based chat application

- tor messenger is a great one for anonymity

- tor browser garuntees anonymity, difficult to do in browser+tor

- local tor relays are acceptible alternatives, may not always work

- Viscosity adds OpenVPN as menu item, works great with pfSense

- Possible to configure pf to only allow VPN traffic, block otherwise

Viruses & Malware

- Macs are NOT immune to Malware, but hold up better than most

- Winderz sees... ~1.3 million new signatures each day, mac: .017

- 3rd party anti-virus for mac increases attack surface

- The best program is a user-supperted “CommonSense2016"

- This is a powerful unix system, more powerful than 3rd parties

- NEVER bolt on security, integrate into the system’s architecture

System Integrity Protection

- SIP enabled by default beginning in macOS 10.11

- Must be disabled for modifying some CA’s or launch daemons

- csrutil is used to check the status, modifying done in recovery

- Applies to every running process, including privilaged code and sandboxed applications

- Prevents code injection and runtime atttachments on file systems

- Enables the “rootless” feature in unix
[https://apple.stackexchange.com/questions/193368/]

Gatekeeper & XProtect

- Gatekeeper prevents unsigned programs and files from opening

- XProtect prevents the execution of known bad files and outdated plugin versions, but does nothing to cleanup existing malware

- macOS attaches metadata (HFS+ extended attributes) to files

Password Management

- Strong passwords generated with OpenSSL, GPG, /dev/urandom, or keychain tools

- Keychain provides system-wide password/cert management

- Keychain is encrypted with a PBKDF2 derived key
[juusosalonen.com/post/30923743427/breaking-into-the-osx-keychain]

- Keychain does not encrypt names of corresponding passwords

- GnuPG also provides sufficient alternative password management

- ALWAYS use two factor where available, reconsider where not

- Yubikey is a great hardware two-factor solution

Backups

- Always encrypt sensitive data before backing it up

```
[ tar zcvf - ~/Downloads | gpg -c > ~/Desktop/pr0n.tar.gz.gpg ]
```

- Always encrypt time machine backups

- Other useful programs: SpiderOak, Arq, Espionage, and restic

Wi-Fi

- Option+Click the WiFi menu item for additional info/tools

- Apple devices tend to broadcast all remembered network names

- Maintain the list of remembered wifi via policies
[/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist]

- Enable WPA2-Enterprise and leave the rest restricted from users

- Maintaining a regularly randomly spoofed mac address helps with privacy when allowing users to connect to foreign networks

- Disable WEP, unencrypted connections in policy management

SSH

- For outgoing SSH connections, use hardware or password protected keys (NOT THE TRADITIONAL METHOD IN BASH)

- Modify the default ssh client configuration files to meet policies

- Works great with privoxy to encapsulate tunneled traffic

- iTerm is a terriffic alternative to Terminal (in Technicolor)

Physical Access

- usbkill can be used to shut down the system upon changes

- Volume encryption

- Policies for lock, screensaver, passwords, etc...

System Monitoring

- OpenBSM audit built into macOS

- Monitors process execution, network activity, and much more

- DTrace built-in system-wide for convenient process audits

- Includes iosnoop, opensnoop, execsnoop, errinfo, & dtruss

- ps, lsof, netstat are included by default

- Wireshark runs great natively on macOS

- also see: [https://github.com/BonzaiThePenguin/Loading/]

Binary Whitelisting

- Santa is a security software developed for Google's Mac Fleet
[https://github.com/google/santa/]

- Santa uses Kernel Authorization API to monitor and allow/disallow binaries from executing in the kernel.

- Binaries can be white/black listed by unique hash or dev cert

- bash, python and other interpreters are whitelisted (since they are signed by Apple's dev cert), so Santa will be unable to block such scripts from executing. Such scripts can disable Santa.

Profile Manager

- Can perform Macintosh and Mobile Device Management

- Can enforce boot, login, logout, and other custom scripts

- Configures various parts of the system effortlessly across domain

- Can be used to install/maintain/block third party software

- Full remote management down to the updates, proxies, etc...

Audit & Forensics

- OSquery: used to retrieve low level system information
[https://github.com/facebook/osquery/]

- grr: incident response framework focused on remote forensics
[https://github.com/google/grr/]

- osxcollector: forensic evidence collection & analysis toolkit
[https://github.com/yelp/osxcollector/]

- OSXAuditor: analyzes artifacts on a running system, such as quarantined files, Safari, Chrom and Firefox history, downloads, HTML5 databases and localstore, social media and email accounts, WiFi...
[https://github.com/jipegit/OSXAuditor/]

Additional Resources

This will be included with the final published slides

found on:

dc214.org