

FOUNDATIONAL CYBERSECURITY

WITHOUT BREAKING YOUR BUDGET

STARTING AT LEVEL 1

- Do NOT plan to do everything at once
- You will need cooperation from other teams
 - Form a committee
- Set deadlines
 - These are VERY easy to procrastinate
- Start reporting to management from level 0
 - You will be able to show progress immediately



INVENTORY AND CONTROL OF ASSETS

- **You have to know what you have in order to protect it**
- Manual - Not fun but it's a start
- Automation is key
- 802.1x
- Have a plan for unknown devices
- Solution:
 - PacketFence
 - Opensource NAC
 - Spiceworks IP Scanner
 - PRTG Network Monitor
 - Windows DHCP Logging



INVENTORY AND CONTROL OF SOFTWARE ASSETS

- **Know what software is installed on all machines**
- Application whitelisting
 - Control what is allowed to run
- Solutions:
 - Applocker
 - Spiceworks
 - Can scan for software
 - ManageEngine / PDQ / ThreatLocker
 - Can scan for and update software (base OS and 3rd party)
 - More expensive than the previous two



SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

- **Create a golden config/template for the OS and apps**
- **Solutions:**
 - Hardening Guides
 - CIS, NSA IAD, DISA STIGs
 - Microsoft Security Compliance Toolkit
 - Policy Analyzer is helpful



MALWARE DEFENSES AND MONITORING

- **GET AN EDR!**

- Detection and Response
- Machine Learning
- <https://attackevals.mitre-engenuity.org/enterprise>

- Don't forget Network monitoring

- Security Onion
- RITA
- ADHD
- Ntopng



LOGGING

- **3 Essentials - Log, Monitor, Audit.**
- Sysmon
 - Swiftonsecurity's configuration
- <https://what2log.com/>
- Logging for AD
 - GPO for audit settings
- Syslog for linux servers
 - Auditd, Kiwi
 - Learn the logging levels and facility codes
- Centralized Storage
 - ElasticStack



PATCHING!

- **You've heard. Do it.**
- Create an AUTOMATED method to regularly patch your systems
- Solutions:
 - WSUS
 - Windows only
 - Linux
 - Cron job to check the repos
 - Automation
 - Puppet, Ansible, ManageEngine



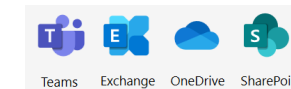
OS PROTECTION FEATURES

- **Ground-up security starts at the operating system!**
- AppArmor/SELinux
 - Access control and policies for Linux machines
- Windows AMSI
 - Sits on an API layer
- Bitlocker
 - Encrypts the hard drive in the machine
 - Relies on TPM chips in the computer
 - Can store the keys in AD

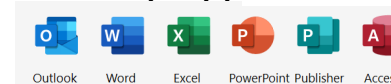


MS 365 SUITE

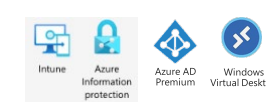
- **And now for some good news!**
- Microsoft 365 has features to address your foundational security.
- Includes:
 - InTune/AutoPilot
 - DLP tracking/reporting
 - Windows Defender for Business
 - Phishing protection



Desktop Apps



Next-level Security



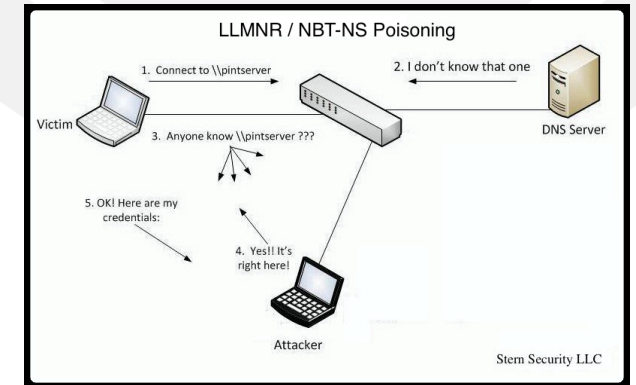
CONFIGURATION ITEMS TO START WITH (ENDPOINT)

- Implement MFA
- Remove local admin rights from users
 - LUA Buglight to work with programs that 'require' admin access
- Limit USB access (Group Policy)
 - Autoplay is not your friend
- Enable LAPS
 - Passwords are stored in AD
 - Can also use PowerShell scripts
 - Even for servers



CONFIGURATION ITEMS TO START WITH (DOMAIN)

- **Audit your service accounts!**
- LLMNR
 - Turn it off. Why do the hackers work for them?
- MDNS
 - Used by Chromecast/Bonjour/etc
 - Use a firewall rule to block 5353/udp on host machines
- NETBIOS
 - A legacy protocol that should have died long ago
- WPAD
 - For proxy configurations



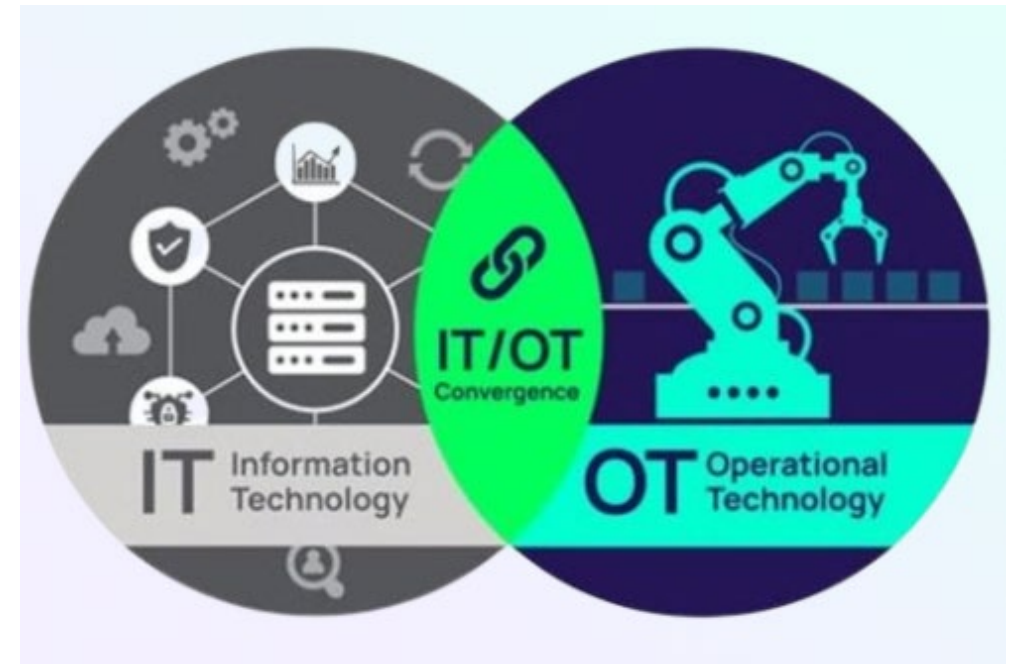
CONFIGURATION ITEMS TO START WITH (SERVICES)

- Use the latest version of SMB, NTLM
- Enable SMB signing
- Use Kerberos instead of NTLM if possible
 - Legacy apps may get in the way here
- Shut down FTP, etc. on printers if not needed
- Use SFTP, SCP, and other SSH related protocols if possible
- Turn off unnecessary services (print spooler, for example)



CONFIGURATION ITEMS TO START WITH (OT TECHNOLOGY)

- Change default passwords
- Check default services
- Ask vendors about more advanced configurations
 - Encrypted configuration
- Separate the IT and OT networks
 - Monitor direct Internet Access
- Look into mitigation strategies
 - HMI, Operator workstations
 - Extra monitoring
- Always keep in mind availability is key



SO YOU THINK YOU'RE SECURE?

- **Test that theory, Buckwheat!**
- Bloodhound
 - Searches for lateral movement paths
- Purple Knight
 - AD Domain
- Atomic red team
 - A lot of attacks packaged into one program
 - Choose your own adventure
 - Focus on one at a time
- JPCert
 - Lists IOCs for common tools (like above)



GENERALLY GOOD TOOLS

- Active Countermeasures Suite
 - <https://www.activecountermeasures.com/>
- DeepBlueCLI
- Wireshark
- Log parsers (Linux/Windows/Mac/etc.)
- Learn PowerShell



WHY USE A MODEL?

- **Using a framework is easier than starting from scratch**
- Ensures you have a methodology
- Helps prioritize tasks
- ACSC
- CIS 18
- NIST CSF



ACSC

- **Australian Cyber Security Centre**
 - Essential 8
 - Split into maturity levels
 - Easy place to start
 - Has a section for MS Office
-
- <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>



CIS 18

- **Center for Internet Security**
 - 18 main controls
 - Split into implementation groups
 - Stick with IG 1 when starting
-
- <https://www.cisecurity.org/controls/cis-controls-list>

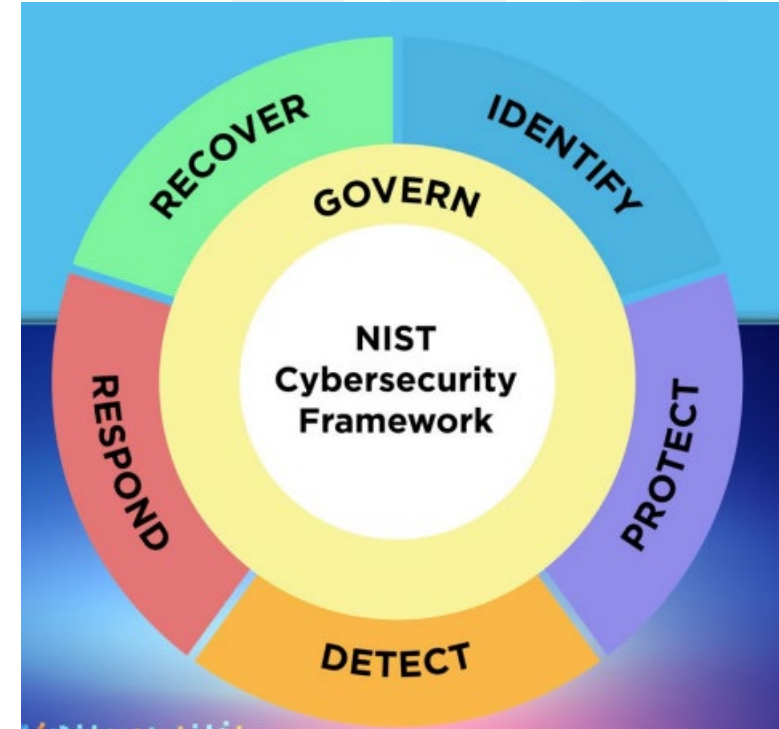


NIST CSF 2.0

- **NIST Cybersecurity Framework**

- 6 main controls

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover



- <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

COMMON THEMES

- Take care of the low hanging fruit first!
- Patching
- Restrict administrator privileges
- Asset management
- Identity management
- Application control/hardening
- Backups
- **Rinse. Repeat. Security never sleeps!**



TECHNOLOGY SEMINAR SERIES

- Nov 11-12
 - Management and Leadership for Cyber and IT Practitioners
 - Hands-on activities for 2 days
- <http://ninestarconnect.com/techseminar>



TECHNOLOGY
SEMINAR SERIES

QUESTIONS?



Sdankner@ninestarconnect.com