# One-Man Shop

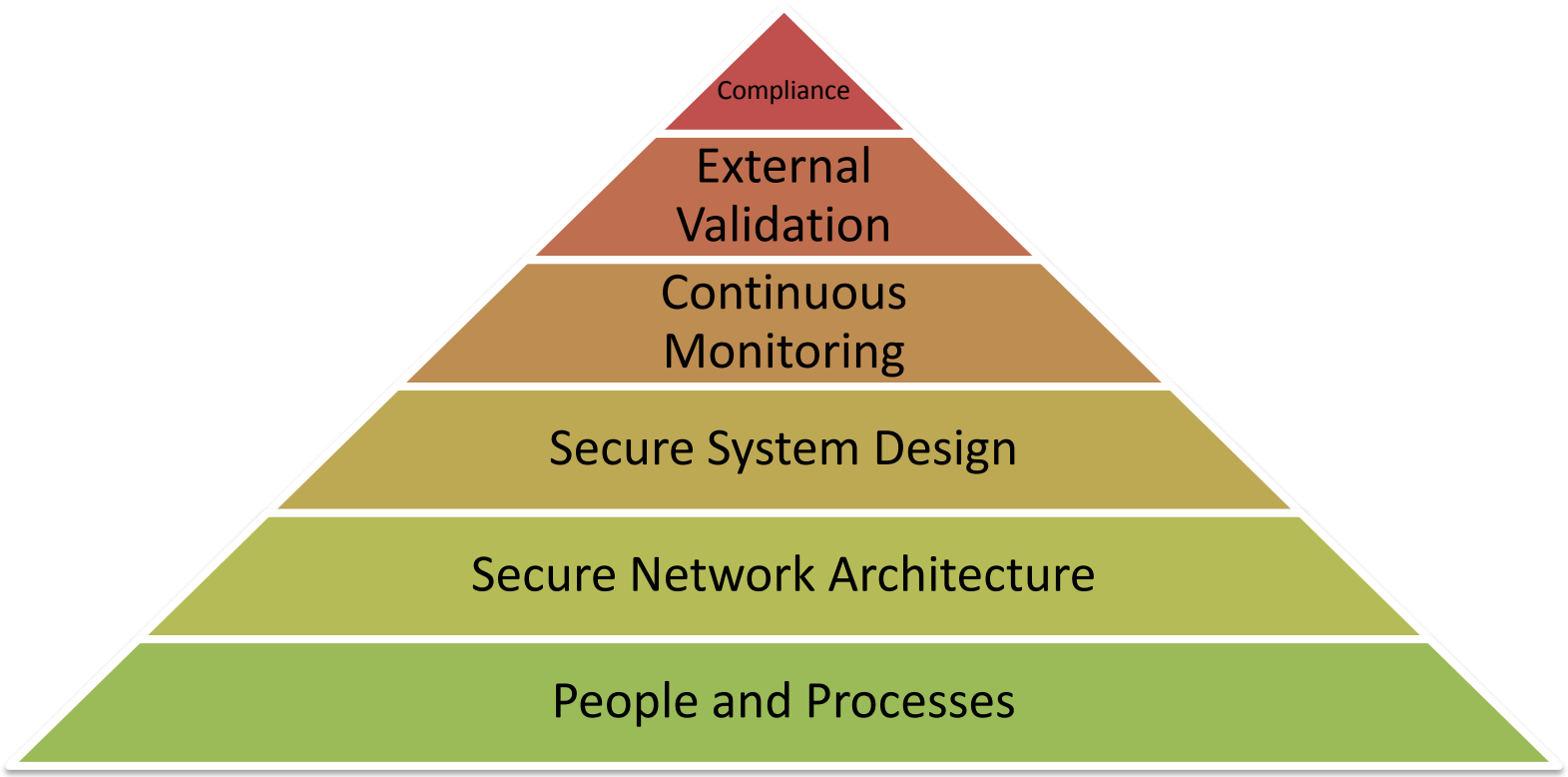
How to build a functional security program with limited resources

**DEF CON 22**

# One-Man Shop – Agenda

- Caveats & Considerations
- People and Processes
- Network Architecture
- System Design
- Continuous Monitoring
- External Validation
- Compliance

# Security Program Hierarchy of Needs

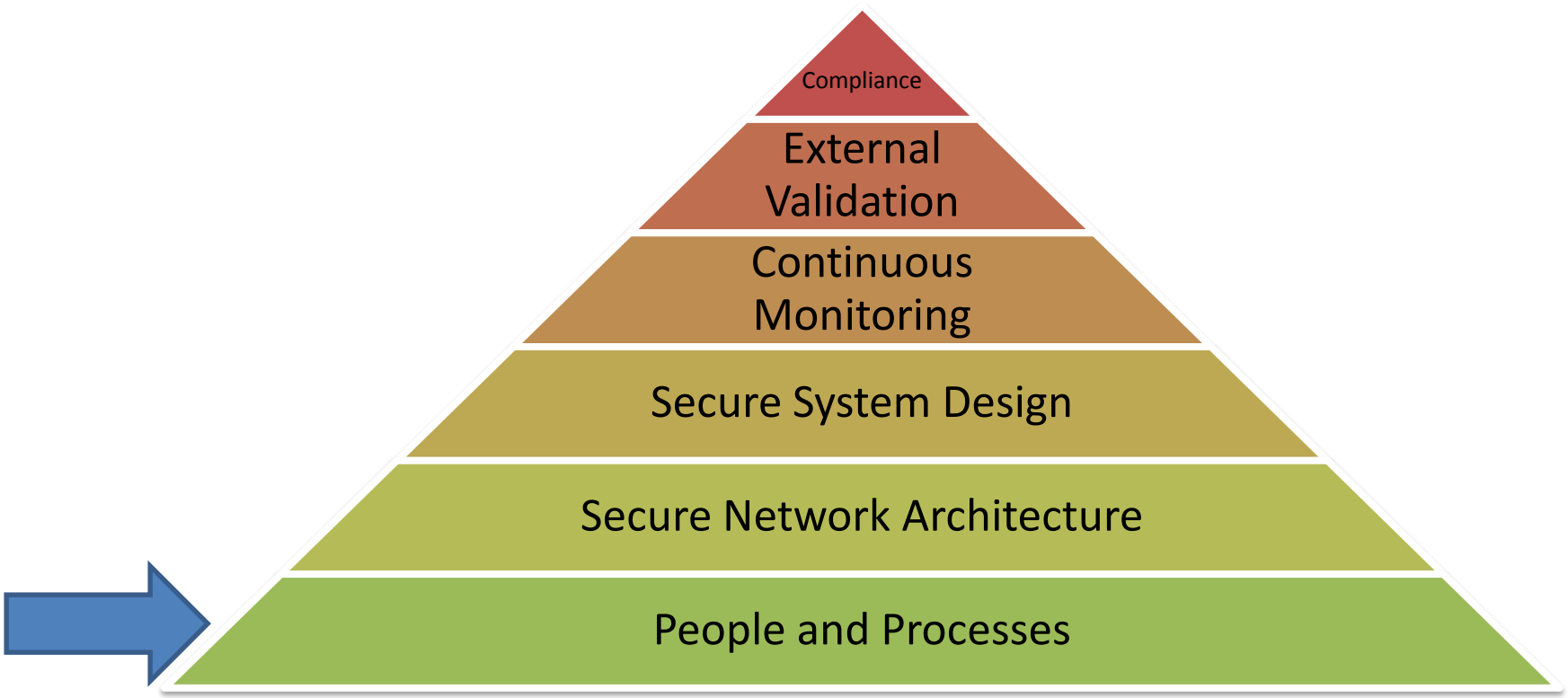


# Caveats and Considerations

- This is going to take Organizational Support
- Security still answers to “The Business”
- Security cannot mature past the Organization

- Be realistic. The sky isn’t falling.
- Schedule time to stop firefighting
- Just do the “right” thing

# Security Program Hierarchy of Needs



# **People** and Processes

- People – within the organization
  - Identify who they are and what roles they play
    - Negotiate sole ownership of systems and processes
    - even better - RACI Matrix
  - Most people take accountability seriously
  - Set and communicate expectations
- "The Business"
  - owns the data
  - owns compliance
  - will get the fines and have charges pressed

# **People** and Processes

- People – within IT
  - Recruit help. Make them aware of your plans
  - A good sysadmin or network person will make a good security liason. That may be you. ☺

# People and **Processes**

- "Security needs to be embedded."
- "Security is (part of) a process"

- Consistency through Automation...
- and Security through Consistency

- Here's where your help comes in...

# People and **Processes**

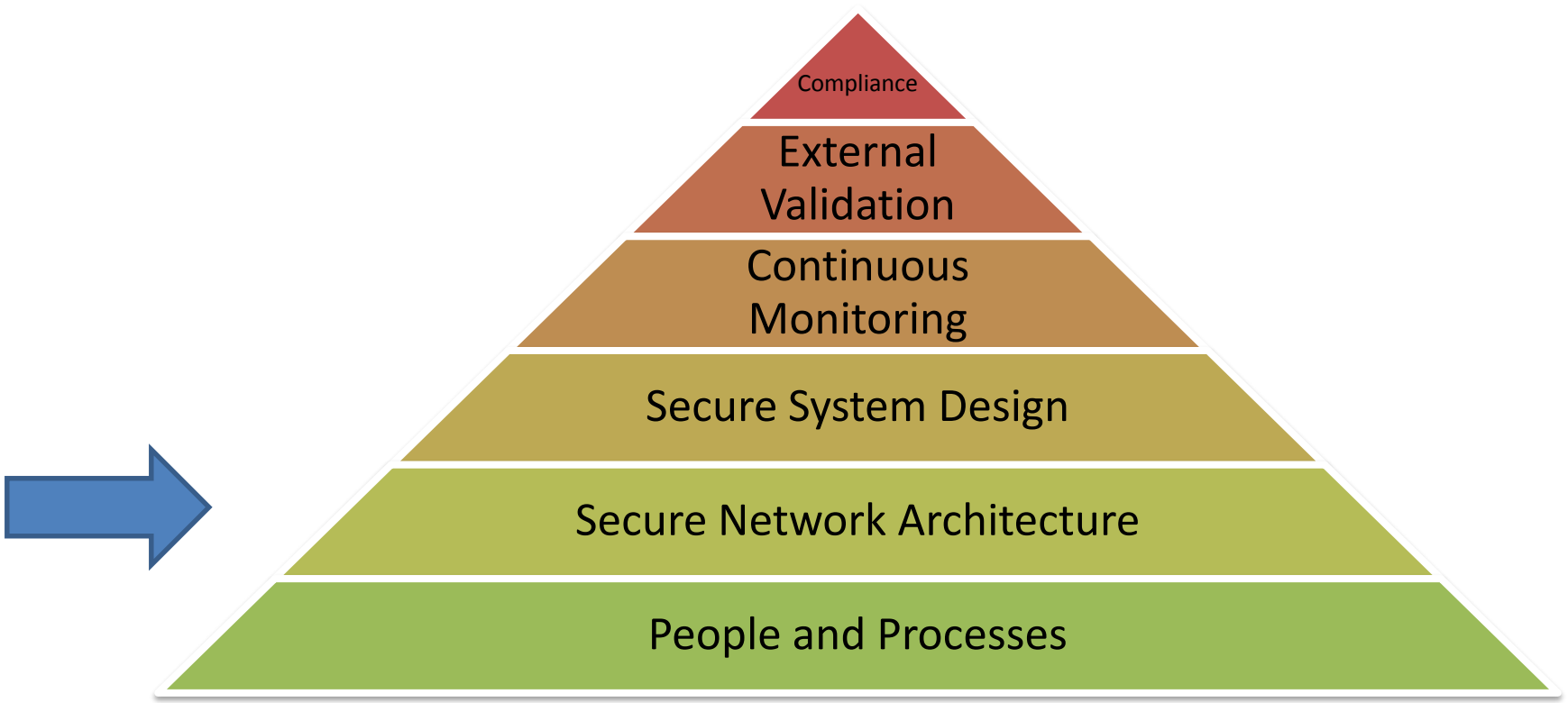
- Identify and document processes
  - As simple as a check list
  - "Swim lanes" flow chart to show handoffs
  - Identify where security can fit in best
    - Doesn't necessarily require security staff review
    - Can be a checklist or guideline for department
- Examples:
  - Purchasing Standardized Equipment
  - Server and Workstation Management
  - Inventory

# People and **Processes**

- Speaking of Inventory: **KNOW YOUR ENVIRONMENT**
  - Identify devices on your network and what roles they play
  - Make network maps
    - This means physical and logical network
  - Endpoints and their uses.
    - Servers, Workstations, Phones, Printers, etc
  - Users and their business functions
  - Sensitive data and where business processes occur

- Automate inventory and alert on differences

# Security Program Hierarchy of Needs



# Secure Network Architecture

1. Divide network endpoints into groups based on roles, risks, exposures, trust level, etc.
2. Create network zones based on roles
3. Identify risks each zone faces
4. Deny all traffic by default
5. Place security controls at zone boundaries for traffic that can’t be denied

# Secure Network Architecture

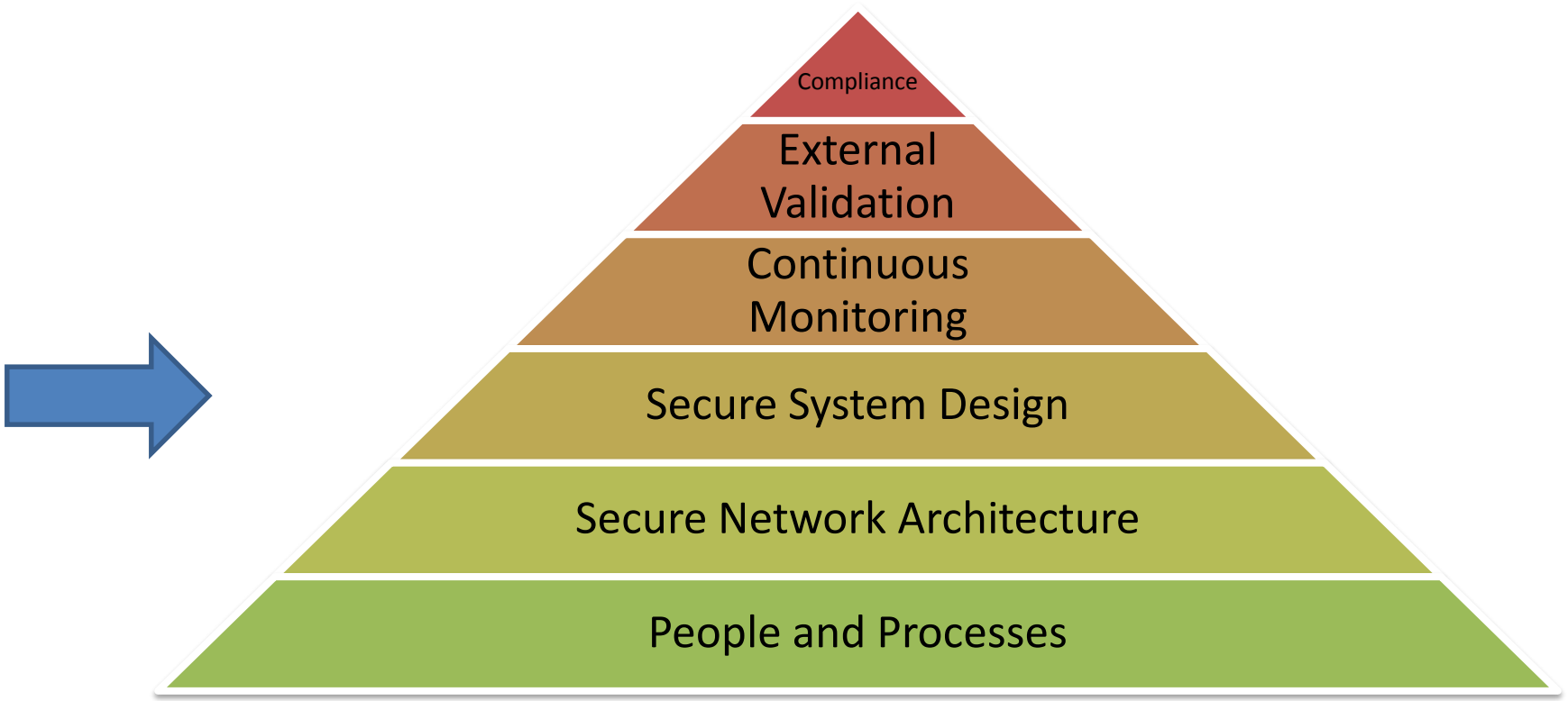
- *Deny all traffic by default
- All traffic should pass through a control
- Allow only what’s necessary for proper function
- Deep Packet Inspect everything you can't deny
- Log everything you can't inspect

- exceptions should be approved and documented

# Secure Network Architecture

- Possible Security Controls depending on risks
  - Firewalls
  - Protocol Enforcement
  - IDS/IPS
  - Netflow Information
  - Deep Packet Inspection
  - File Extraction and Analysis
- Log all alerts centrally for easy correlation

# Security Program Hierarchy of Needs



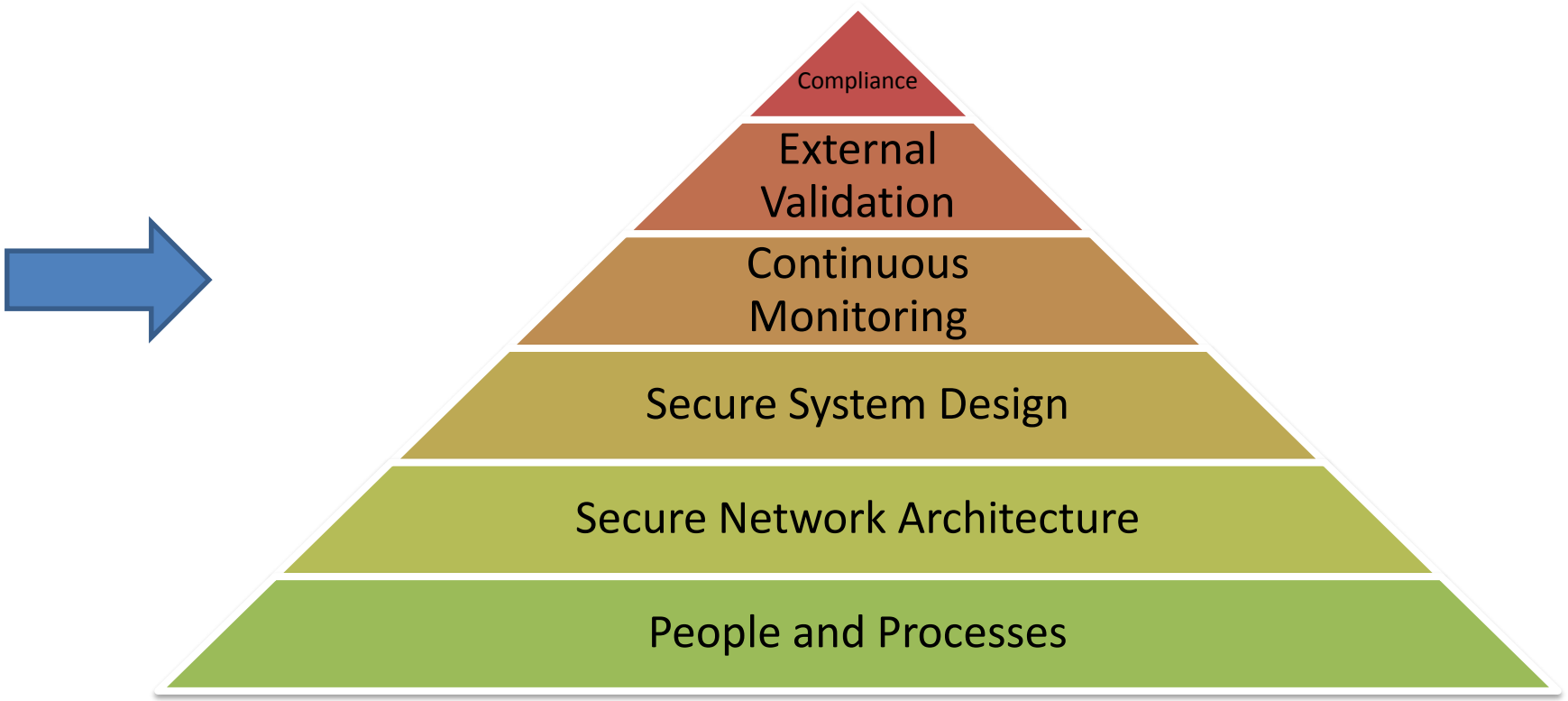
# Secure System Design for Servers

- Systems should cross as few security zones as necessary
- Traffic within a security zone should be as segmented as possible (Host Based Firewalls)
- Centralized Logging
- Backups! Virtualized? Take Snapshots
- Automate Account Provisioning
- Aim for Single Sign On
  - Disable Once, Disable Everywhere
  - Allows for centralized Auth and Access Control

# Secure System Design for Workstations

- Design a standardized desktop image
- Least Privilege. No local admins
- Centralize workstation administration
- Enable Automatic Updates
  - OS Killing patches are rare
- AV is dead, but its still a layer of protection
- EMET for additional defense
- MAC filtering at switchports

# Security Program Hierarchy of Needs



# Continuous Monitoring

- Host Monitoring
  - Periodic IP/Port Scans
  - Periodic Vulnerability Scans
  - Automated Log Review
    - VPN Access by IP/Region
    - Dropped Packets sourced from DMZ
    - Event logs of privileged accounts
    - New users and group memberships
  - Netflow anomalies

# Continuous Monitoring

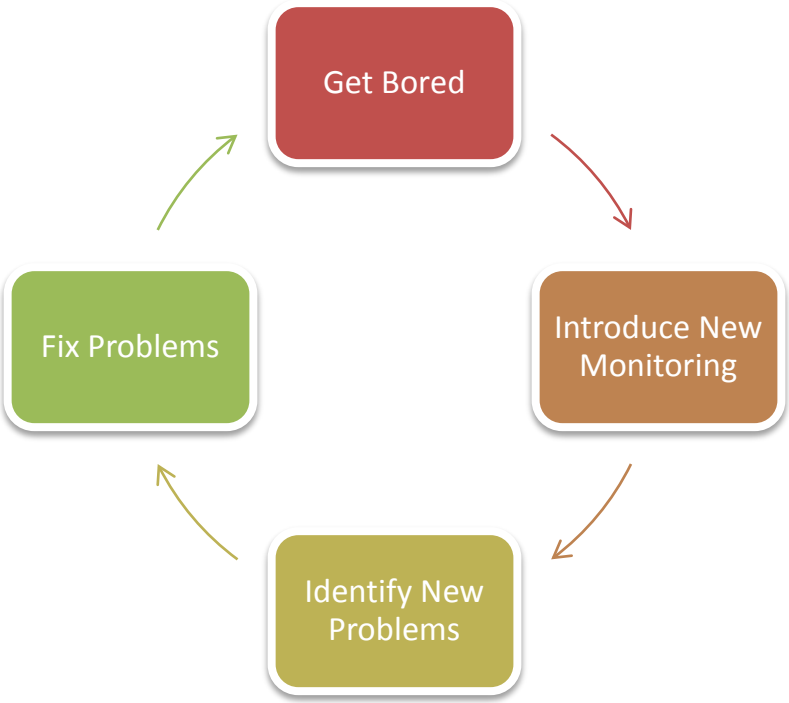
- Forensics and Incident Response
  - Snort with ETPro ruleset for IDS
  - urlsnarf from the dsniff suite
  - tcpdump internal span ports for DNS traffic
  - execap for capturing windows binaries off the wire
  - Cuckoo Sandbox for analysis
  - Immunity's El Jefe for process monitoring

# Continuous Monitoring

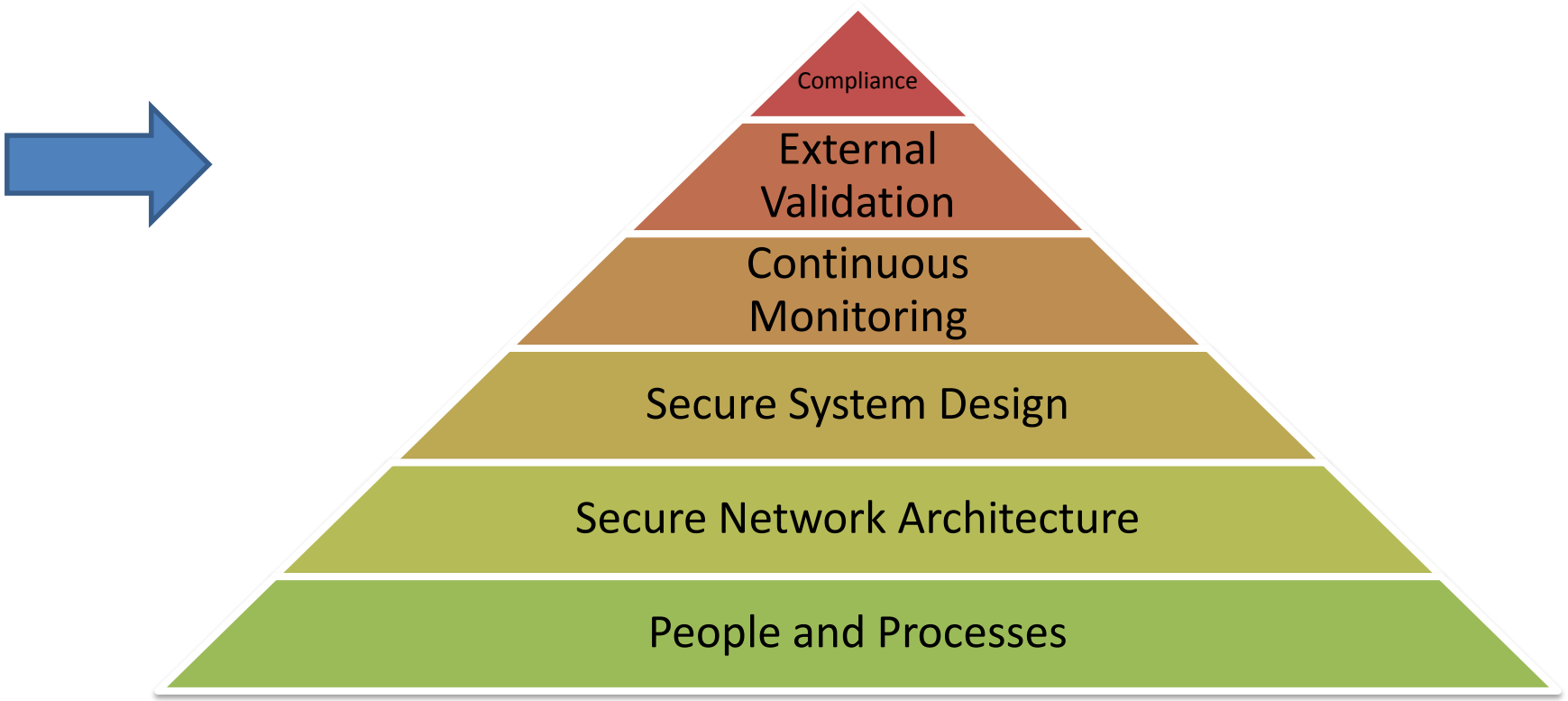
- Forensics and Incident Response
  - If a user isn't admin, process hiding is hard
  - Most malware contained to user's profile
  - Use WMI for Remote Windows IR
    - wmic /node: x.x.x.x process get commandline
    - wmic /node: x.x.x.x process where name = "winlogon.exe" delete
    - wmic /node: x.x.x.x process call create "process.exe"
  - Free / Open Source DFIR Tools
    - Mandiant Redline, FTK Imager, Autopsy

# Continuous Monitoring

- Just when you think you're bored…
  - Introduce a new monitoring tool.  You'll find new problems that need to be fixed.



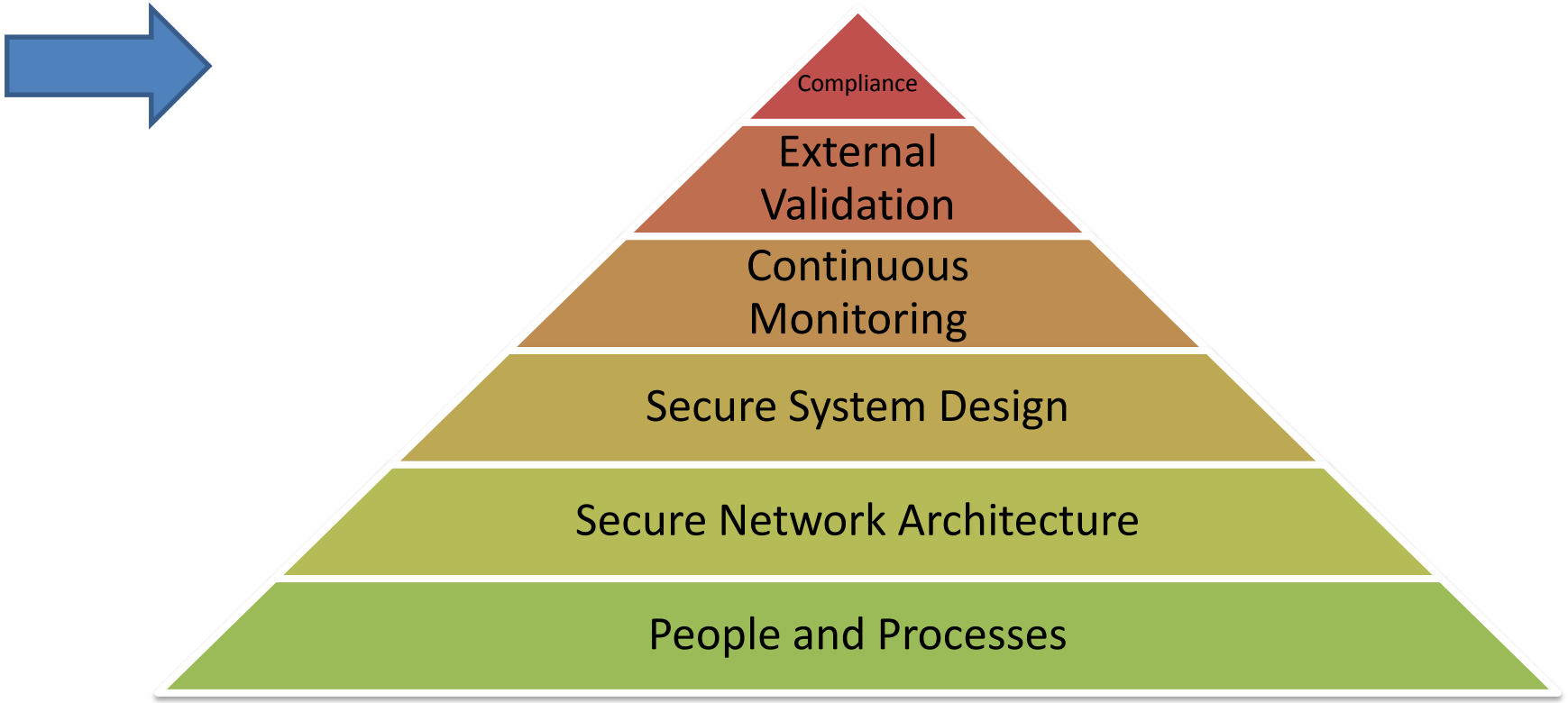
# Security Program Hierarchy of Needs



# External Validation

- Consider an external auditor to review your environment
- At least verify against others in your industry
- Consider external penetration testing

# Security Program Hierarchy of Needs



# Compliance

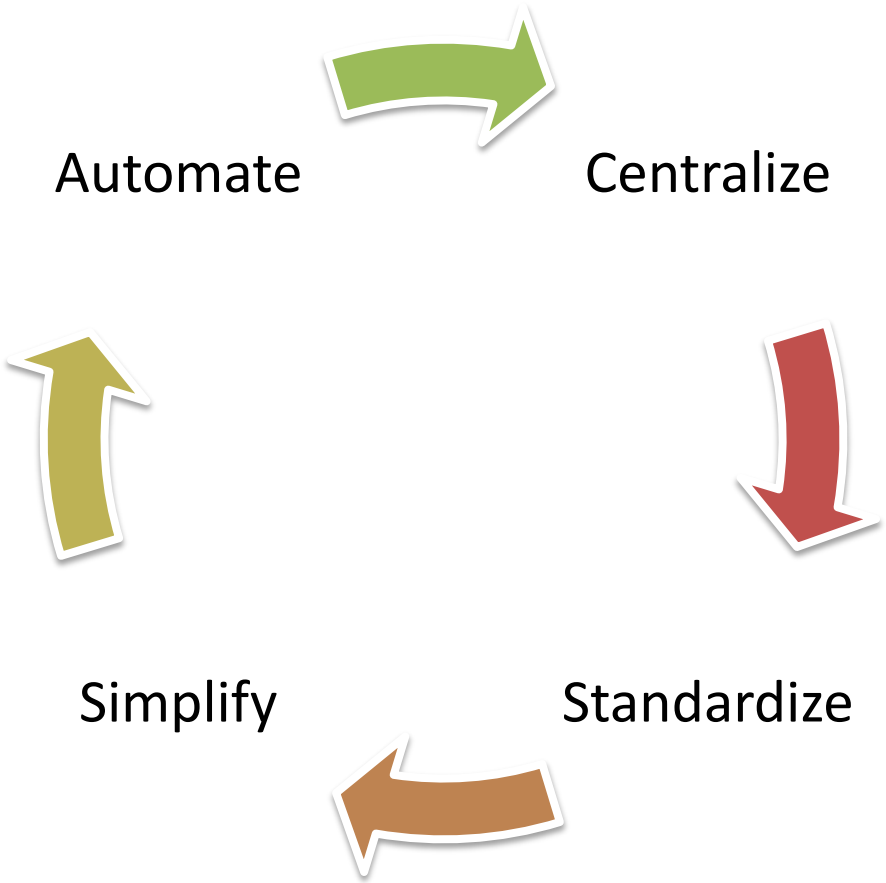
- To be honest, It's…
  - not worth talking about
  - shouldn't be a driver
  - a byproduct of a good security program

- Most auditors will accept a remediation plan, even if it takes multiple years
- Slow progress is still progress

# Let’s compare to SANS Top 20

| | |
|---|---|
| 1. Device Inventory | 11. Account Monitoring and Control |
| 2. Software Inventory | 12. Malware Defenses |
| 3. Secure Hardware and Software Configs | 13. Limitation of Network Ports, Protocols |
| 4. Secure Network Device Config | 14. Wireless Device Control |
| 5. Boundary Defense | 15. Data Loss Prevention |
| 6. Security Audit Log Analysis | 16. Secure Network Engineering |
| 7. Application Software Security | 17. Penetration Test and Red Team |
| 8. Controlled use of Admin Privs | 18. Incident Response Capability |
| 9. “Need to Know” Data Access | 19. Data Recovery Capability |
| 10. Continuous Vulnerability Assessment | 20. Security Skills Assessment and Training |

# Questions?



# Contact Information


- **Tim McGuffin**
- **tim@mcguffin.org**


- **Updated slides available at**

  **http://tinyurl.com/one-man-shop**