

Continuous Monitoring and its Effect on Change Control

Dr. Nathaniel Evans

Dr. William Horsthemke

Nathan Rinsema

Matthew Scialabba

Argonne National Laboratory

Agenda

- Introduction
- Goals
- Overview of continuous monitoring
- Overview of paper-driven Certification and Authority (C&A) process
- Overview of paper-driven Change Control Board (CCB) process
- How continuous monitoring affects C&A process
- How continuous monitoring affects CCB process
- A technical example we have implemented
- Conclusion

Goals

- To show the positive effect that continuous monitoring will have on a variety of traditional security exercises, including the C&A process and the CCB process, which are generally paper based.
- As a note, the majority of our experience is in the Department of Homeland Security (DHS) world. The Department of Energy (DOE) may be slightly different, but we plan to speak in generics as much as possible.

Continuous Monitoring

There are three parts to a continuous monitoring system:

1. Continuous audit
 - Inventory and patch management
2. Continuous controls monitoring
 - Configuration management
3. Continuous transaction inspection
 - Scanning, network-level monitoring, tracking, and alerting

Certification and Authorization Process

- At intervals of several years, facilities must undergo a C&A process to confirm that:
 - All machines are patched
 - All configurations are set up and documented
 - The network architecture makes sense
- This is normally done through a paperwork exercise consisting of the following:
 - Site Security Plan (SSP)
 - Requirements Traceability Matrix (RTM)
 - Security Testing and Evaluation (ST&E)
 - Contingency Plan (CP) and Test (CPT)
 - Risk Assessment (RA)
 - Security Assessment Report (SAR)

Change Control Board Process

Documentation-driven

- If change requires editing documentation, the Change Request must be approved by the CCB
- Change Requests are written and illustrated. They require pre-approval before submittal to CCB. After submittal, they are
 - Reviewed by CCB
 - Discussed with CCB
 - Approved or rejected by CCB
- CCB can consists of a variety of individuals who have authority over certain aspects of the systems. These may include the following:
 - Enterprise architecture
 - Security
 - Program management

Continuous Monitoring Affects Certification and Authority (Your Authority to Operate)

- SSP – needed once; update accordingly
 - Inventory – monitored continuously, so no longer needed
 - Configurations – monitored continuously, so no longer needed
- RTM – **no longer needed**; controlled through change management and verified through change control software
- Contingency Plan – updated and performed annually
- ST&E – done continuously to evaluate against controls, so document is no longer needed
- Risk Assessment and SAR – **no longer needed**; scans are done continuously and risk is analyzed during change control

Continuous monitoring has allowed us to theoretically eliminate two documents and reduce the need to continually update and get approval on the other two



Continuous Monitoring Affects CCB

- Approval required for changes in kind, not in scale
 - Addition of new types of systems, networks, services, or external interconnections
 - **New** = types not already approved for use
- Approval not required for addition of technologies similar to those already approved
- Approval required for substantial changes to architecture
 - Re-organization of multiple systems or networks
 - Changes that alter the ability to observe the change
- Change in access control policy or types of user
 - Policy changes in general are difficult to monitor or track



Now for the technical stuff...

An Example



Controls Monitoring – Configuration Management

Network gear

- Record history of configuration
 - Full configuration files
 - Initial (a previous)
 - Current
 - All modifications since initial
- Record notification of configuration changes
 - Simple Network Management Protocol (SNMP) Inform trap
 - Correlate change with on-device change log history if necessary
- Record configuration changes
 - Difference (*diff*) between *new* and *current* configuration files
 - Replace *current* with *new*
 - Retain all differences (option to purge if excessive)

Audit – Inventory Management

All approved devices are members of Authorized-Devices Database

- Certified and Accredited Devices $\{C\&A\} \in \{Authorized\ Devices\}$

Device discovery

- Alert if not approved — *Mac Address* $\notin \{Authorized\ Devices\}$
 - Ease database update if approved by authorized administrator

Verify complete inventory for continuous monitoring tasks

$\{Task\ Inventory\} \subseteq \{C\&A\}$ and $\{C\&A\} \subseteq \{Task\ Inventory\}$

- {Availability and Performance Monitoring}
- {Vulnerability Assessment}
- {Property}
- {Patch Management}

Transaction Inspection – Network-Level Monitoring

Network infrastructure and configuration

- SNMP Get (*periodic query*)

Event-level information from network gear

- SNMP Informs (*traps with acknowledgement*)

Information

- Device (MAC)
 - {*Switch, Port, VLAN, IP address*}
- Interface
 - {*Attached-devices, status (up/down, admin)*}
- Configuration of network gear
 - Capabilities (*port count*) and settings

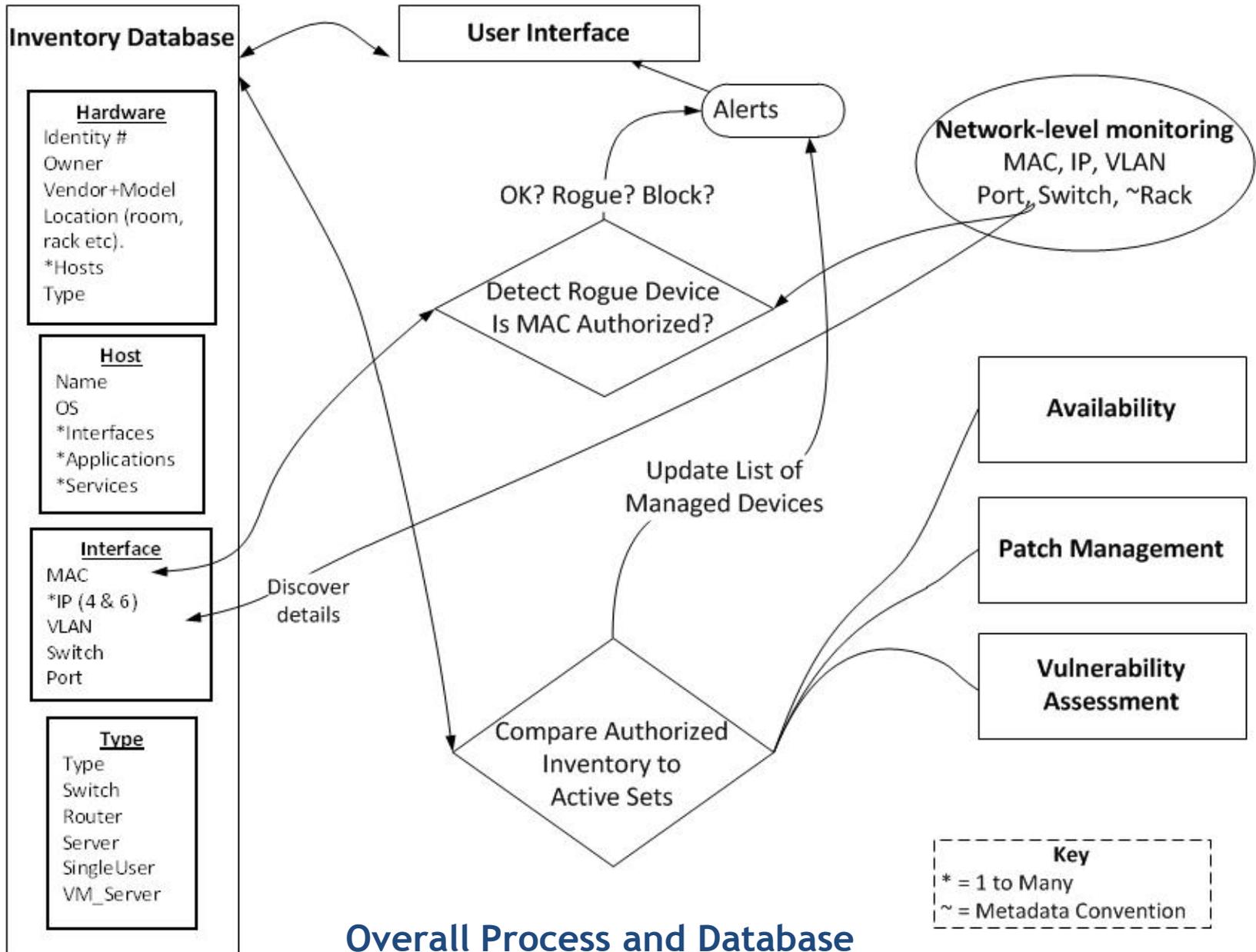
Transaction Inspection – Tracking and Alerts

MAC, Interface, ARP History

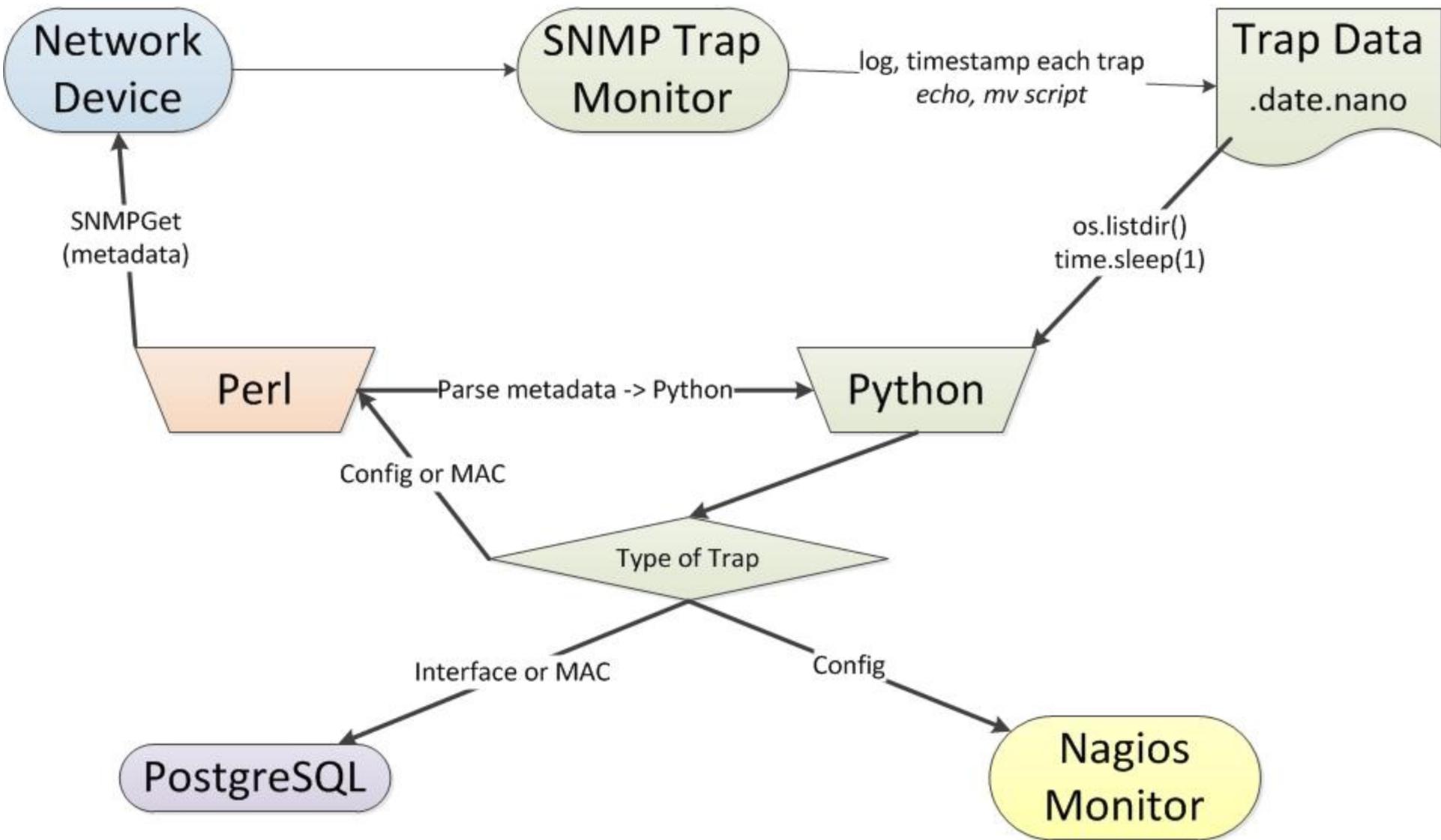
- Device (MAC) discovery
 - Alert if not approved – *Mac Address* \notin *{Authorized Devices}*

- Device History
 - Δ {Port, Switch, VLAN, IP Address} \Rightarrow Alert-able
 - Δ Physical Host of Virtual Machine (VM)
 - Alert if VM outside approved VM cluster (Administrative move of VM)

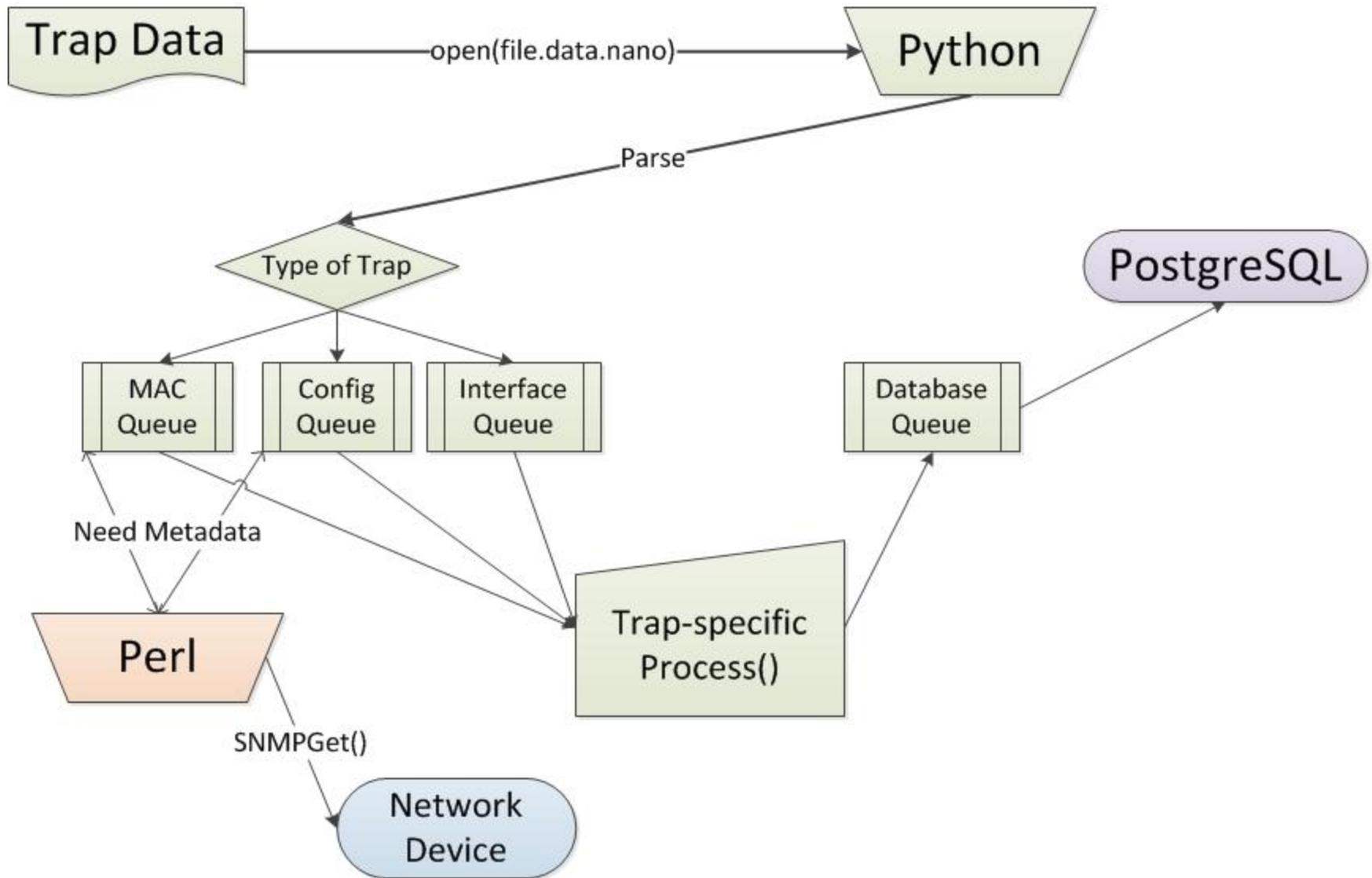
- Interface Modification
 - External (connect/disconnect)
 - Internal configuration change (admin up/down)



Overall Process and Database



Trap Processing



System Configuration

Server Software Configuration:

- snmptrapd listening on port 162
- Specific SNMP inform user created
- User granted log and execute permissions
- Default trap handle calls trap.sh

Network Hardware Configuration:

- SNMPv3 inform user
 - MAC address add, remove, or change
 - Configuration change
 - Interface status change: up, down, administratively down

Global Configuration Assumptions:

- Using SNMPv3
 - A fully privileged database user and password
 - *The database does NOT need to be listening on the network if run locally*
 - Dummy ASA user and password
 - ASA authorization limiting a dummy ASA user to defined commands

System Specifications

Software Versions:

- CentOS 5.8 x86_64 Kernel 2.6.18-308.1.1.el5

- Python Version python-2.4.3-46.el5
 - python-pgsql-0.9.7-1.el5

- Perl Version perl-5.8.8-38.el5
 - perl-DBI-1.52-2.el5
 - perl-Net-SNMP-5.2.0-1.el5.1

- Net-SNMP Version net-snmp-5.3.2.2-17.el5

- Network hardware:
 - Cisco 2960(G) IOS Version 12.2(53)SE1
 - Cisco 6000 IOS Version 12.2(33)SX13
 - Cisco 4900 IOS Version 12.2(50)SG1
 - Cisco ASA 55xx IOS Version *does not update continuously to network_monitor.py



Goal and Objective

Validate the sensitivity of a continuous monitoring methodology

Detects all substantial changes

- Inventory
- Services
- Connectivity

Verifies status

- Vulnerability
- Patch

Objective: Create trustworthy signature for security of C&A system

That's it...

Questions??

