How to Tell if Base Services are Configured and Operating as Designed?

Mr. Ariel Garcia

August 2018

UNCLASSIFIED

Overview

- **The Why, What, and How of Enterprise Configuration and Change Management**
- **IT Auditing Requirements**
- **What is SCORE?**
- **What to do on SCORE?**
- **Way Ahead**

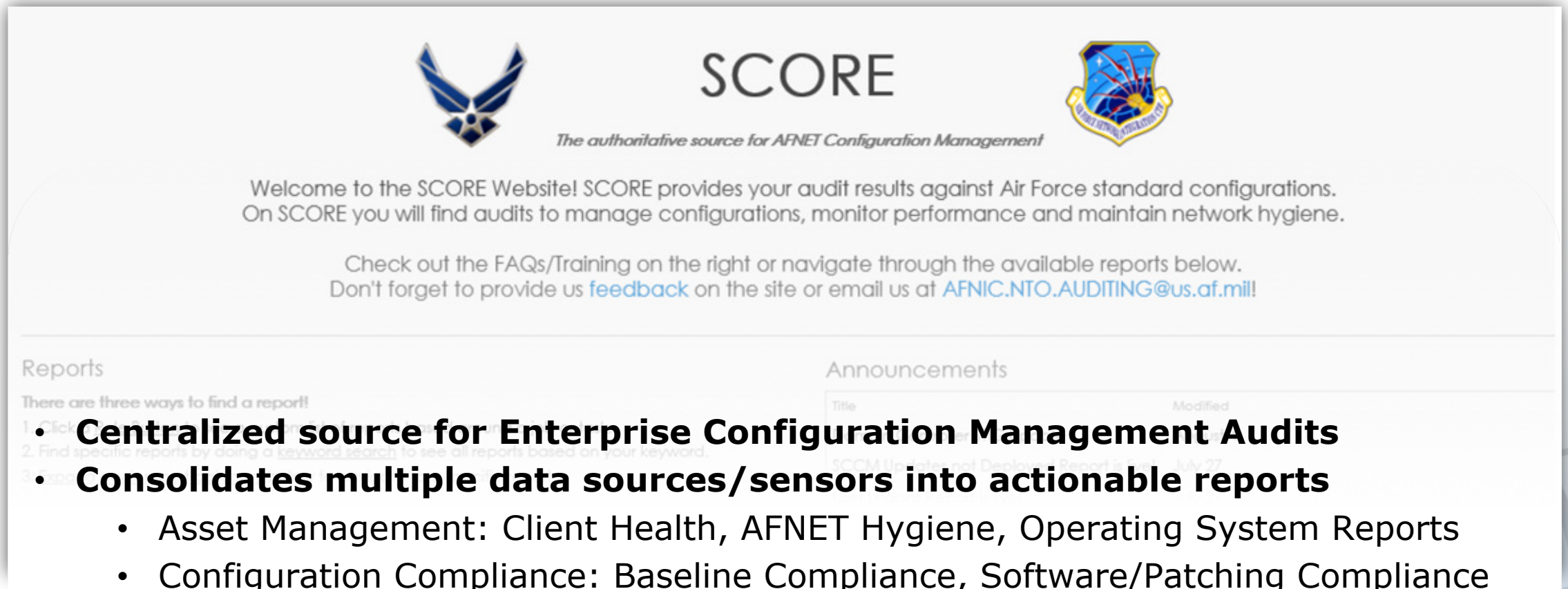
The Why, What & How of Enterprise Configuration Management

- **WHY: Control of performance & configuration baselines**
  - Problem: Root cause analyses frequently identify poor Config/Change Management
  - Fix: Must strengthen Enterprise Config/Change Management capabilities/processes
- **WHAT: Establish/Enforce Enterprise Standardization**
  - Fielding organizations establish baselines from industry best practices, functional specifications, technical orders, and security requirements (e.g., STIGs)
  - All organizations follow Change/Configuration Management processes
    - TO 00-33A-1101, AFNET Asset and Configuration Management Process
    - TO 00-33A-1100, AFNET Operational Change Management Process
  - AFNIC conducts baseline audits using SCORE Website
  - Network Operators monitor & remediate baseline deviations
- **HOW: Enterprise Configuration Management Auditing**
  - Provide actionable Configuration Management audits
  - Identify previously unknown enterprise-level issues
  - Involve all levels of AFNET operations

IT Auditing Requirements

- **Why must we audit?**
  - **"**Auditing helps **ensure compliance between the last known authorized operational baseline (should be) and the current operational baseline (as-is)**. Audits are **conducted on a regular and random basis** to ensure the integrity and currency of the CMS, in addition to auditing prior to and after major changes and releases.**" – MPTO 00-33A-1101**
- **What needs to be audited? Per MTPO 00-33A-1101…**
  - Server Baselines
  - Desktop/Laptop/Tablet Baselines
  - Weapon System Baselines
  - Infrastructure Baselines
  - AFNET Hygiene
    - Active Directory Service Accounts
    - HBSS rules
    - Proxy settings (base and gateway level)
    - Group Policy Objects (GPO)
    - User/System permissions
    - Ports, Protocols, and Services (PPS) use

What is SCORE?



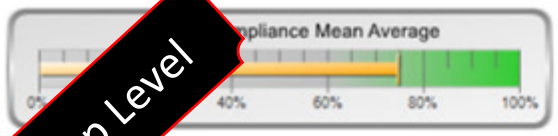
- **Centralized source for Enterprise Configuration Management Audits**
- **Consolidates multiple data sources/sensors into actionable reports**
  - Asset Management: Client Health, AFNET Hygiene, Operating System Reports
  - Configuration Compliance: Baseline Compliance, Software/Patching Compliance
  - Performance Monitoring: Virtual Environment, Core Enterprise Services
- **PMO-specific audits account for documented Air Force deviations/exceptions**

SCORE Website: https://cs.eis.af.mil/sites/10026

Configuration Compliance Report by Finding

- Configuration compliance for a specific baseline, broken out by finding
- Most useful to verify compliance across all system-specific machines

Top Level



The Compliance Overview report lists compliance by Configuration Item for a selected Baseline. Compliance results can be further refined by AD site. This report is useful for determining general compliance and is meant for an overview of compliance health. To get a detailed list of resources by Configuration Item, click on the individual compliance numbers.

Click for Chart View
Top 50 Non-Compliant

Configuration Item	Compliant	Non-Compliant	Error	Total	Percentage Compliant
Exchange Client Access Server STIG - CAT II - V-33559 - Exchange Servers - Exch-1-002	110	3		113	97.35%
Exchange Client Access Server STIG - CAT II - V-33562 - Exchange Servers - Exch-1-005	112	1	0	113	99.12%
Exchange Client Access Server STIG - CAT II - V-33570 - Exchange Servers - Exch-1-008	112	1	0	113	99.12%
Exchange Client Access Server STIG - CAT II - V-33584 - Exchange Servers - Exch-1-202	113	0	0	113	100.00%
				113	97.35%

CLICK

Second Lvl

Comm...me	Operating System	Time (UTC)	AD Site
	Microsoft Windows Server	1/24/2018 9:53:57 PM	Aviano
D05	Microsoft Windows Server	1/19/2018 4:51:55 PM	SCOTT
D02	Microsoft Windows Server	1/31/2018	Yokota

CLICK

Parameters

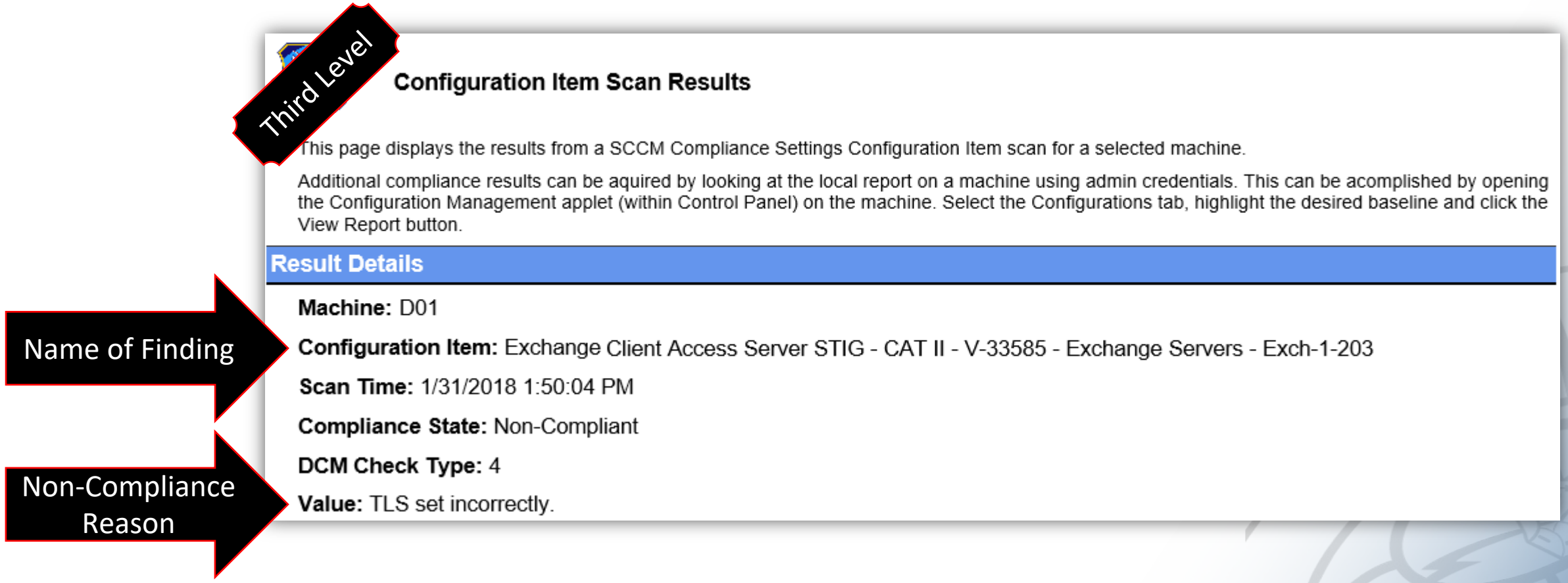
DCM Baseline: Exchange

Collection: Exchange

AD Site: All Sites

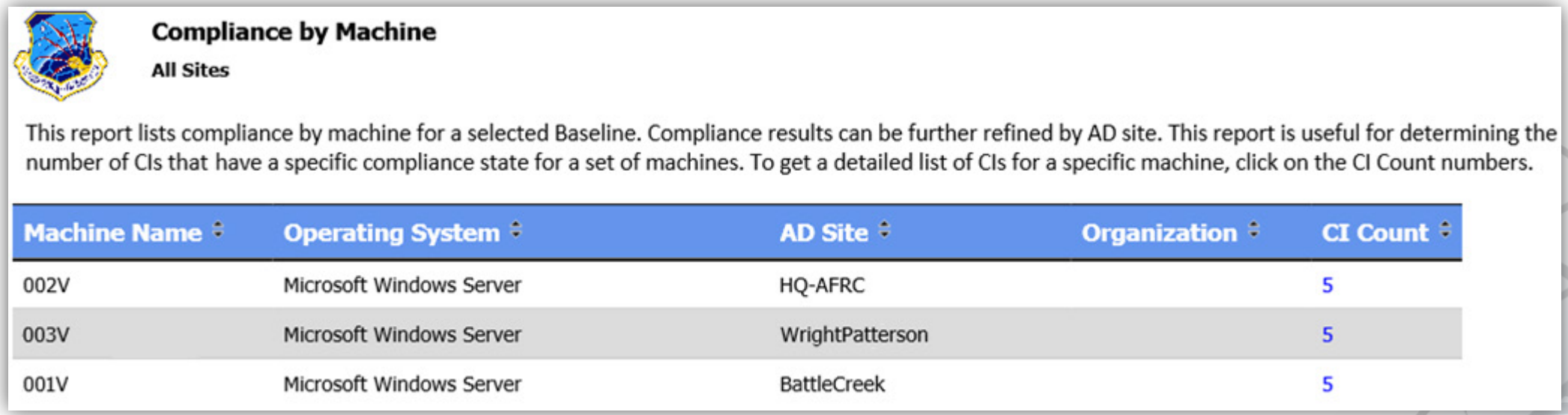
What to do on SCORE?
Check Config Baseline Compliance By Finding (cont.)

- Third level report most useful for researching non-compliance root cause
- Shows results of audit to include explanation of non-compliance
- Important to note name of finding: <Source_Doc> - <(E/D/C/T####)> - <Friendly Name>



Configuration Compliance Report by Machine

- Data presented by machine with most non-compliant machines listed at top of report
- Locates most non-compliant machines for a particular configuration baseline
- Sub-report lists all non-compliant finding on the specified machine
- Third-level report shows finding details

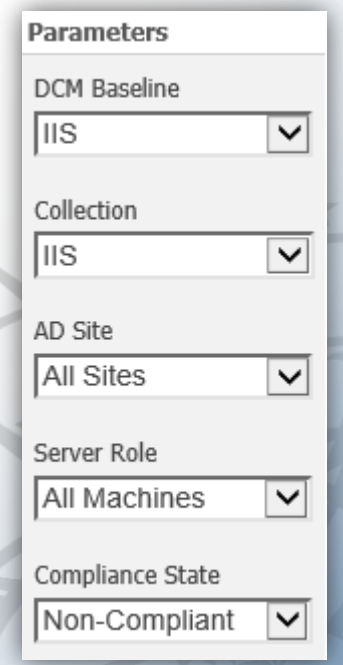


Compliance by Machine

All Sites

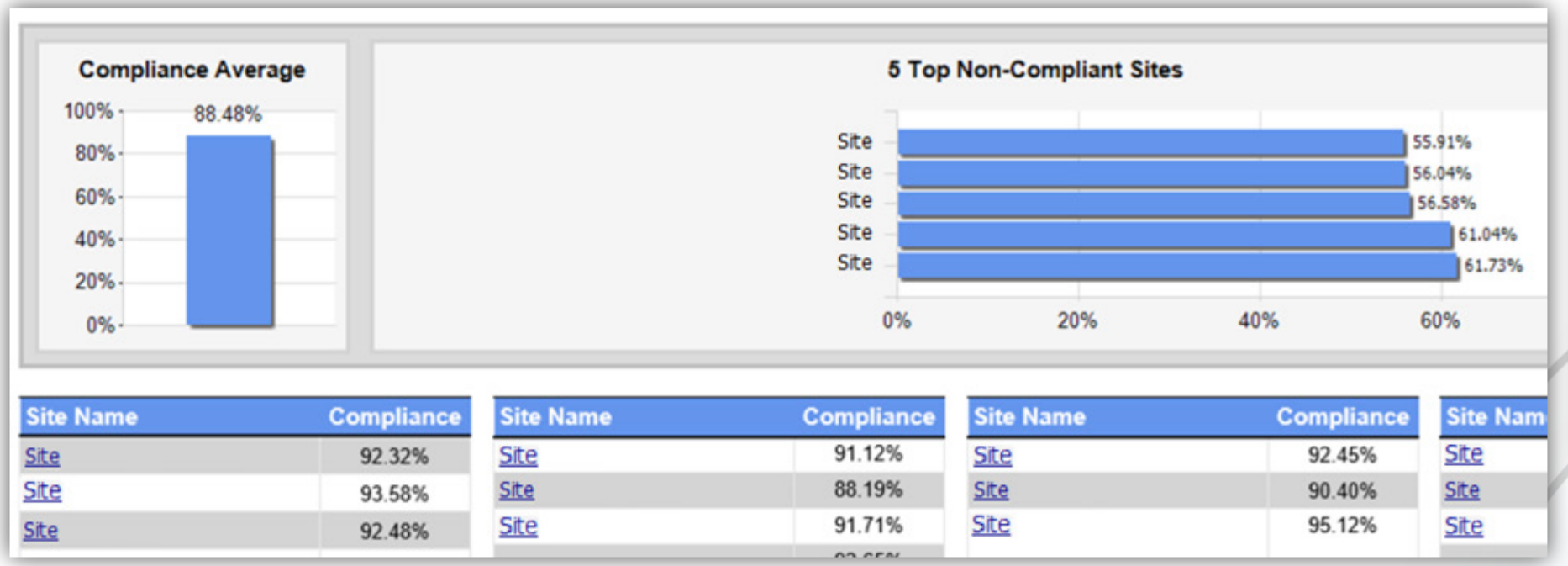
This report lists compliance by machine for a selected Baseline. Compliance results can be further refined by AD site. This report is useful for determining the number of CIs that have a specific compliance state for a set of machines. To get a detailed list of CIs for a specific machine, click on the CI Count numbers.

Machine Name	Operating System	AD Site	Organization	CI Count
002V	Microsoft Windows Server	HQ-AFRC		5
003V	Microsoft Windows Server	WrightPatterson		5
001V	Microsoft Windows Server	BattleCreek		5



Software Update Compliance Report

- Click on base for detailed view of non-compliant machines
- **Note:** Only shows patches pushed through SCCM's built-in patch management process. If patch is pushed via SCCM package or other external mechanism, it will not show up on report.
- Most helpful for checking patch status at specific locations and select patch categories

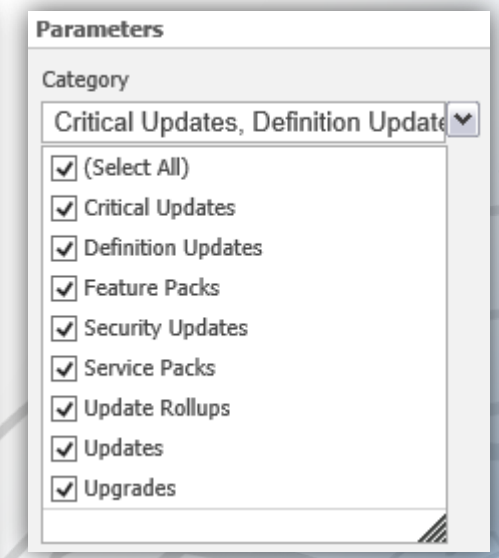


Site Name	Compliance
Site	92.32%
Site	93.58%
Site	92.48%

Site Name	Compliance
Site	91.12%
Site	88.19%
Site	91.71%

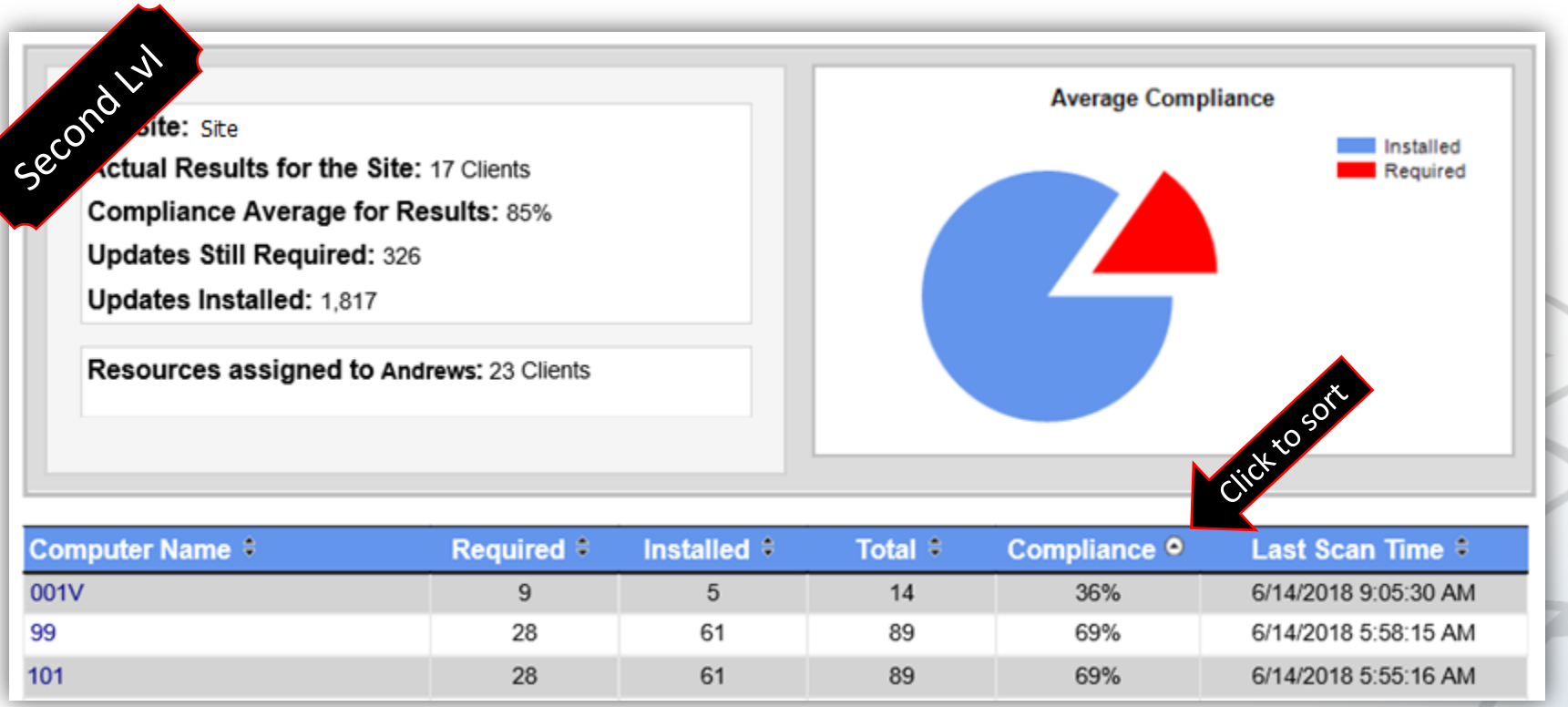
Site Name	Compliance
Site	92.45%
Site	90.40%
Site	95.12%

Site Nam
Site
Site
Site



What to do on SCORE?
Check End Point Patching Health (cont.)

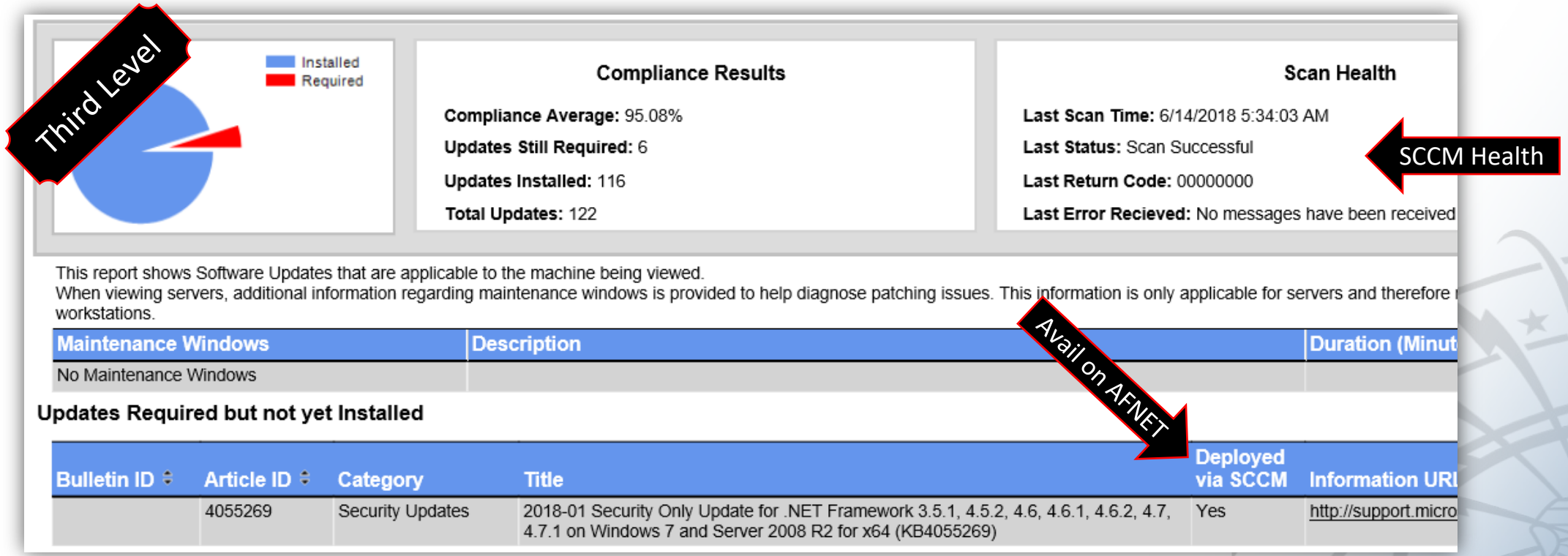
- Second-level report shows required, installed, total patches on machines
- Use the arrows next to column headers to sort – clicking the arrows next to "Compliance" shows the most non-compliant machines first!
- Click a machine name for third-level report



Computer Name	Required	Installed	Total	Compliance	Last Scan Time
001V	9	5	14	36%	6/14/2018 9:05:30 AM
99	28	61	89	69%	6/14/2018 5:58:15 AM
101	28	61	89	69%	6/14/2018 5:55:16 AM

What to do on SCORE?
Check End Point Patching Health (cont.)

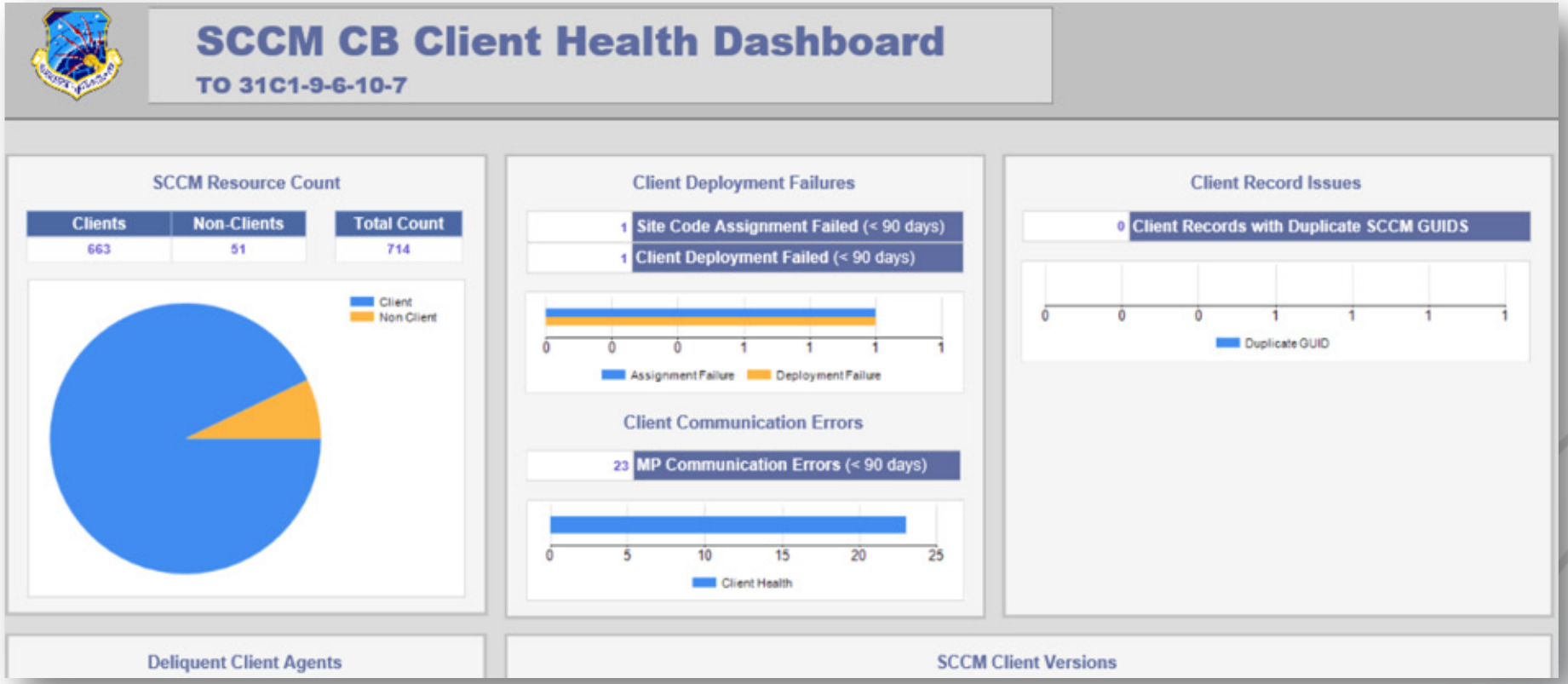
- Third-level report shows installed patches and assigned maintenance windows
- "Scan Health" identifies potential SCCM client problems
- "Deployed via SCCM" column indicates a required patch is currently advertised and available for download

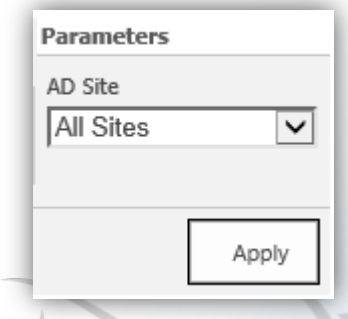


What to do on SCORE?
Check End Point Patching Health (cont.)

SCCM Client Health Dashboard

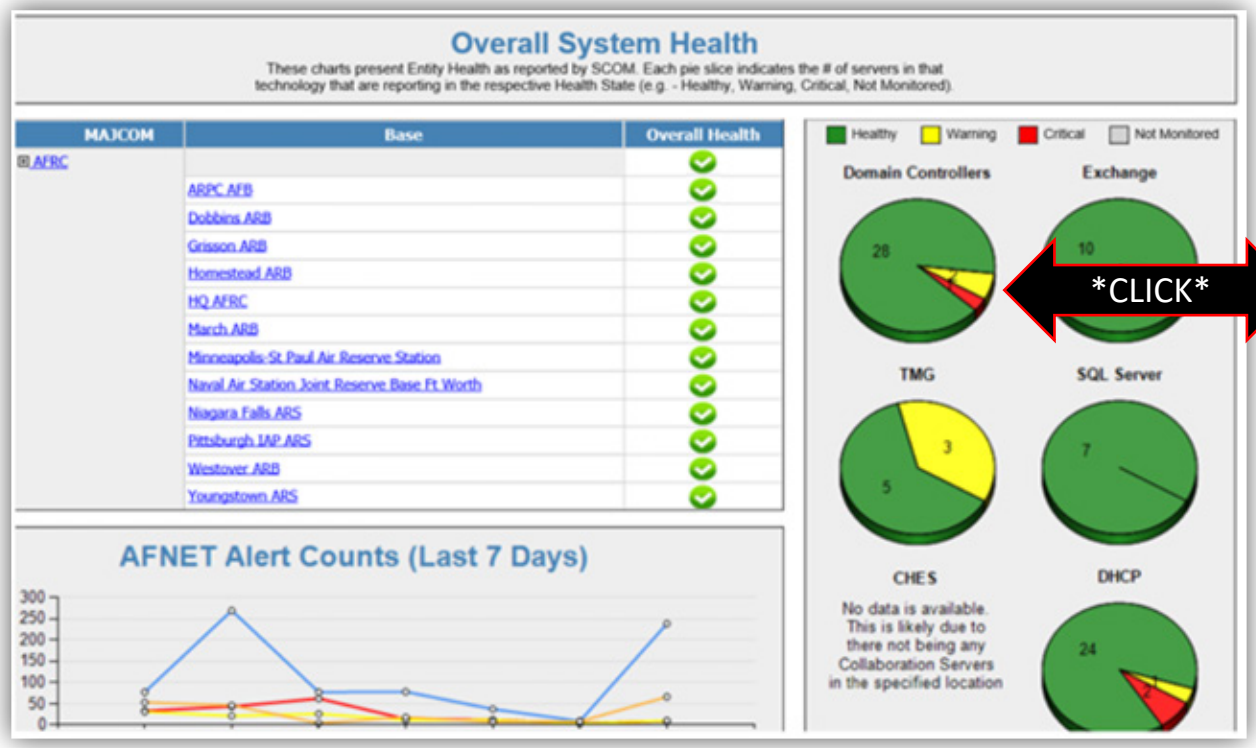
- Enterprise-wide SCCM Client Health data or target specific sites
- Presents actionable data for base-level technicians to remediate
- Detailed machine-level view of each data-set is available by clicking any of the numbers in the dashboard

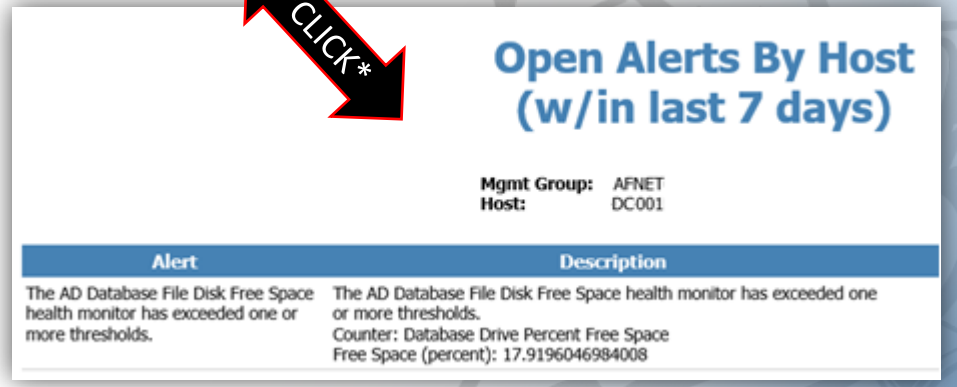




Core Services – System Health Dashboard

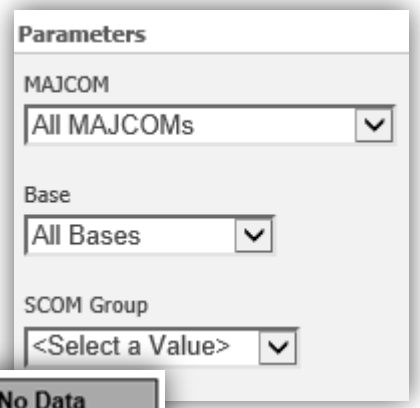
- Shows system health for core services servers
- Used at base level for performance alerts from base-level core servers (e.g. DCs, DHCP servers)



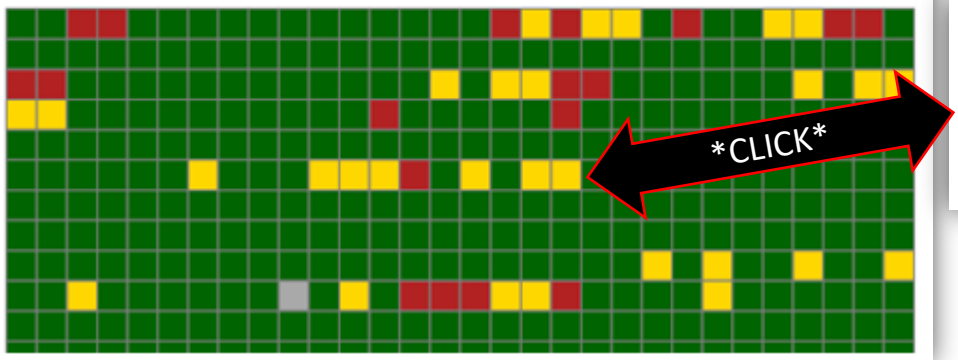


Core Services – Virtual Environment Health Dashboard

- Shows virtual environment health for core services
- Click pie charts/heat maps to load sub-reports for details on individual machines



Good	Average	Bad	No Data
0.00% - 10.00%	10.01% - 20.00%	20.01% - 100.00%	N/A
379	30	20	1



MAJCOM:	AFSPC
Base:	Base
Server:	002
vROps Resource Id:	17
Stat Key:	CPU Contention %
Value:	13.00

What to do on SCORE? Network Hygiene

AD – Dormant and Stale Users Report

- Shows enterprise-wide dormant and stale users accounts
- Used at base-level to clean up 'dead' active directory accounts
- Identifies breakdowns of specific organization out-processing processes

MAJCOM	Base	Total Count	Dormant Count	Stale Count
⊞ ACC		10,000	250	250
⊟ AETC		10,000	250	250
	Altus AFB	1,000	50	50
	Columbus AFB	1,000	50	50
	Goodfellow AFB	1,000	50	50
	JBSA-Randolph - Joint Base San Antonio	1,000	50	50
	Joint Base San Antonio	1,000	50	50

Click

Click

User Base Name	CN	Display Name	EDIPI	Org	Last Logon	Dormant	Stale
Altus AFB	DOE.JOHN.CTR	DOE, JOHN CTR USAF AETC 123 AW	123456789	123 AW	1/1/0001 00:00	Yes	
Altus AFB	DOE.JANE.CTR	DOE, JANE CTR USAF AETC 123 AW	123456789	123 AW	1/1/0001 00:00	Yes	
Altus AFB	SNUFFY.BOB.CIV	SNUFFY, BOB CIV USAF AETC 123 AW	123456789	123 AW	5/24/2017 05:50	Yes	Yes

AD – Administrator Account Report

- Shows enterprise-wide administrator accounts
- Identifies whether mandatory attributes correctly configured
- Used at base-level to verify continued need & use of administrator accounts

MAJCOM	Base	ADM User Count	User Count	ADM User Count Ratio
⊞ ACC		100	10,000	1:10
⊟ AETC		50	10,000	1:5
	Altus AFB	10	1,000	1:10
	Columbus AFB	10	1,000	1:10
	Goodfellow AFB	10	1,000	1:10
	JBSA-Randolph - Joint Base San Antonio	10	1,000	1:10
	Joint Base San Antonio	10	1,000	1:10

What to do on SCORE? Network Hygiene (cont.)

AD – Service Account Report

- Shows enterprise-wide service accounts and compliance against network standards
- Used to detect poor service account maintenance, required attributes

MAJCOM	Base Name	Total Count	Compliant Count	Non-Compliant Count
⊞ ACC		100	100	-
⊟ AETC		100	81	19
	Altus AFB	9	5	4
	Columbus AFB	15	15	-
	Goodfellow AFB	19	17	2
	JBSA-Randolph - Joint Base San Antonio	13	13	-
	Joint Base San Antonio	44	44	-

Operating System Count Report by MAJCOM & Base

- Shows OS counts at the Enterprise, MAJCOM, and Base-level
- Sub-report correlates asset data with network data for robust picture of networked machines

MAJCOM & Base Operating System Counts

Virtual Machines: Exclude
Dormant Machines: Exclude (60+ Days)
Disabled Machines: Exclude
Operating Systems: Microsoft Windows 10 Enterprise

MAJCOM	Base Name	Operating System	Count
⊞ ACC			10,000
⊞ AETC			10,000
⊟ AFDW			10,000
	⊞ Fort Detrick AFB		100
	⊟ Fort Meade		100
		Microsoft Windows 10 Enterprise	100

What to do on SCORE? Save Lots of Time & Money

Save Millions of Dollars!

- Cloud hosted email costs the AF $$ for every account
- Dormant/Stale report identified accounts that should not be migrated
- Initial scrub saved AF $4 million in cloud license costs

Save Thousands of Hours!

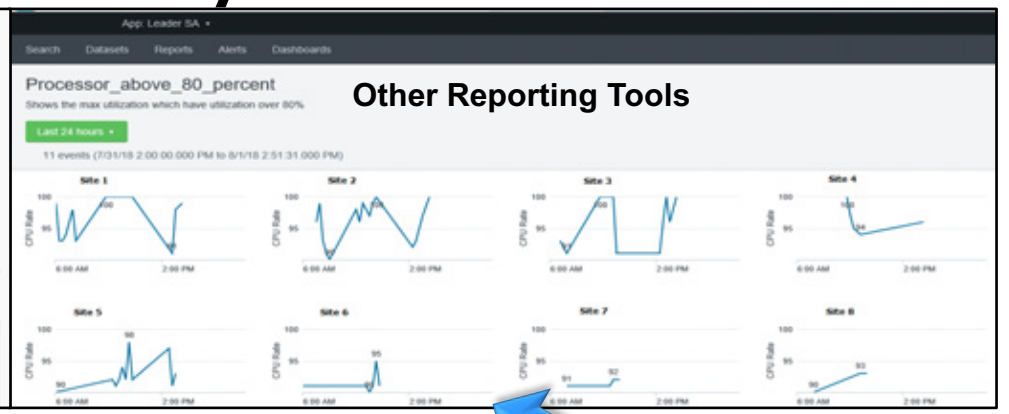
- Ops-identified Domain Controller (DC) preventative maintenance inspection (PMI) checks take ~55 hrs/week
- DC baseline audit includes automated PMI checks
- Reviewing results on SCORE reduces 55 hrs/week to minutes

Save Hundreds of Steps!

- AF recently completed migration to Windows 10
- SCORE provided base-by-base migration status; showed locations needing hardware refresh
- Reporting allowed focused efforts vice visiting every desktop
- Future reports will identify end of life machines requiring replacement/upgrade

SCORE Next Generation Leveraging Artificial Intelligence

Presentation Layer



The road to the future…

- **Standardize**
- **Automate Remediation**
- **Predictive Analytics**

SCORE DATA WAREHOUSE

ANALYTICS ENGINES
ex: R, Python

EXTRACT, TRANSFORM & LOAD

AUTHORITATIVE DATA SOURCE

SCCM

CMDB

CONFIGURATION FILES

PERFORMANCE LOGS

In Summary…

- **Configuration Management Auditing is good!**
  - Baselines audits in place
  - Network Hygiene reports are available
- **Take action!**
  - Review reports and remediate
  - Identify deviations to incorporate into audits
  - Provide feedback on how to improve reports
- **More to come!**
  - More data sources!
  - More baseline audits!
  - More analytics!

The key to success: managing, maintaining, and updating baselines as authorized changes occur.

SERVITIO *75 Years* **DEDICATI**