Continuous Monitoring
Federal Information Systems

Earnest Neal – Atlantic Systems Group, Inc.
Steve Johnston – Tripwire, Inc.

7th Annual IT Security Automation Conference

Continuous Monitoring is…

…more than just watching data

Agenda

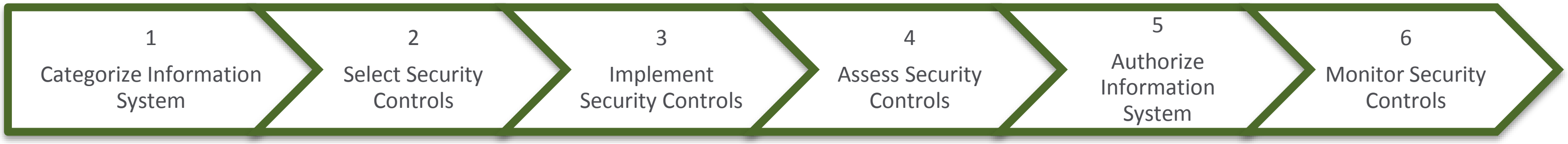
- Overview of Continuous Monitoring Basics
- CAESARS architecture and SP 800-137
- Case Study Automated vs. Manual
- ASG and Tripwire Continuous Monitoring Solution
  - Finding the Events of Interest
  - Maintaining a Secure Configuration State
  - Providing actionable results

Continuous Monitoring Basic Overview

- Technical and business process development to support a Agency
  - Technical development follows the Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESAR) Reference Architecture
  - Process development follows NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- Strategy Development
  - Clear understanding of Agencies' risk tolerance helping to identify priorities
  - Meaningful metrics illustrating security posture
  - Continuous evaluation of the effectiveness of security controls
  - Compliance validation
  - Security status visible to all organizations to maintain vigilance
  - Awareness of threats and vulnerabilities

Continuous Monitoring Basic Overview

- Establishing Agency’s Information Security Continuous Monitoring (ISCM)
  - Define Agency-ISCM strategy
  - Establish the Agency-ISCM program
  - Develop the Agency-ISCM Reference Architecture
  - Analyze data and report findings
  - Respond to findings
  - Review and update the Agency-ISCM strategy and program



1 Categorize Information System

2 Select Security Controls

3 Implement Security Controls

4 Assess Security Controls

5 Authorize Information System

6 Monitor Security Controls

Benefits of Continuous Monitoring

- Moves the focus back to Security
- Provides staff (management/operational) access to real-time security information
- Leads to improved security posture
- Creates better awareness of threats and vulnerabilities
- Automates manual processes wherever possible
- Enables prioritization of remediation
- Remediation costs move to daily operations

Continuous Monitoring Challenges

- Identifying existing capabilities
  - Prevent unnecessary work in areas already developing
  - Increase effort to leverage those capabilities
- Participation
  - Ensure sufficient involvement to create a Agency-wide view of CM to capture the organizations core missions and business functions
- Developing the risk thresholds/tolerance levels
  - Capturing information and facilitating data driven management decisions
- Automation development
  - Engineering components of sub-systems not already in-place

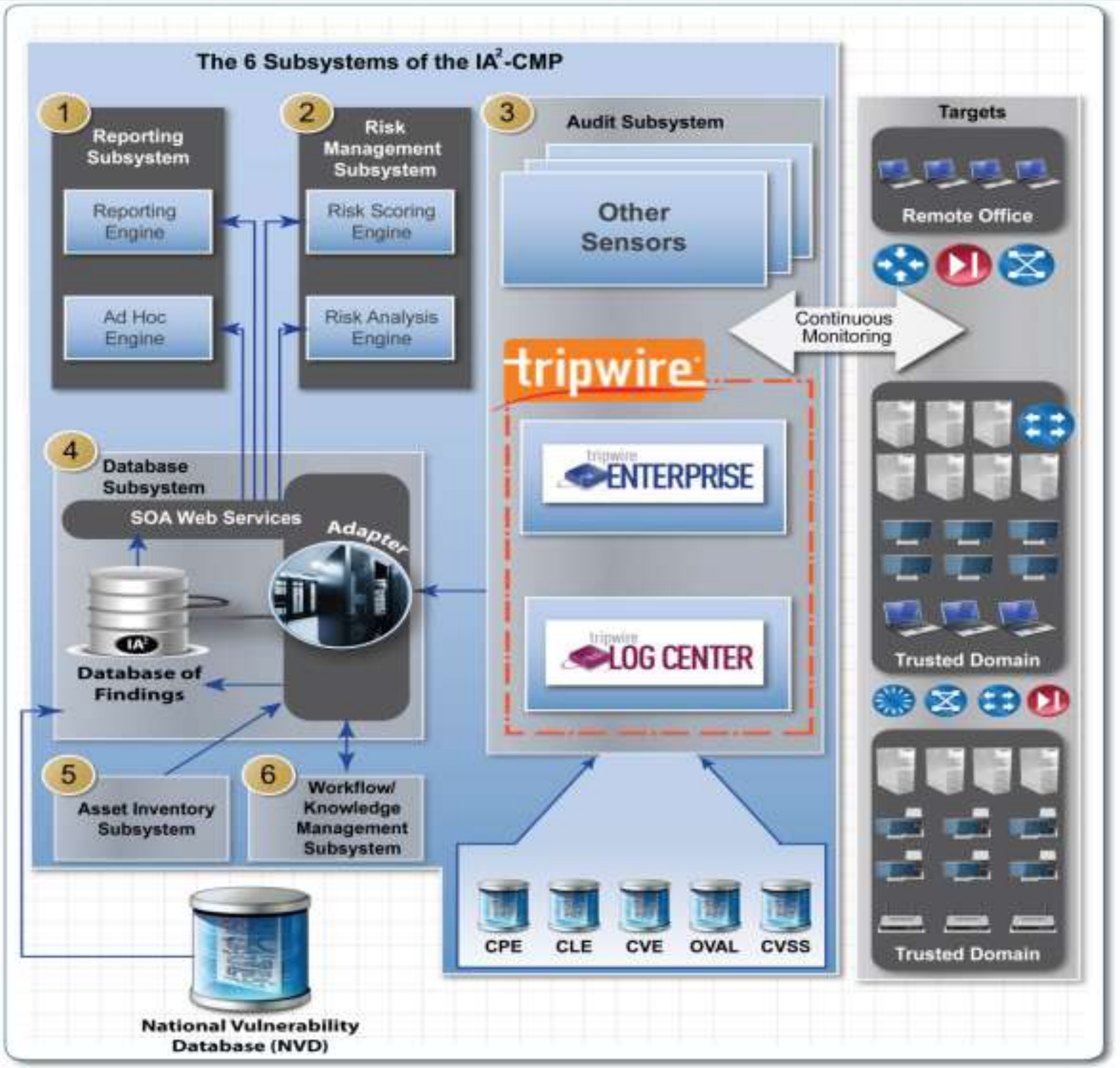
Case Study

- VA
  - In 2005 300 systems were assessed with the average reporting time of 200 hours per system. In 2007 all 650+ systems were assessed, over 5 million individual tests, and the average reporting time was reduced to 4 hours… for QA review.

Year	Hours	Cost	Total
2005	200	$125.00	$25,000.00
2007	4	$125.00	$500.00

- Legislative Branch Auditing Organization
  - 2009/10 this organization needed to meet aggressive C&A deadlines that were costing millions. They had Limited Resources, Budget Constraints, Outsourcing C&A processes were too costly
  - Saved 600K within first year and an estimated 1.8 million through the current C&A Period

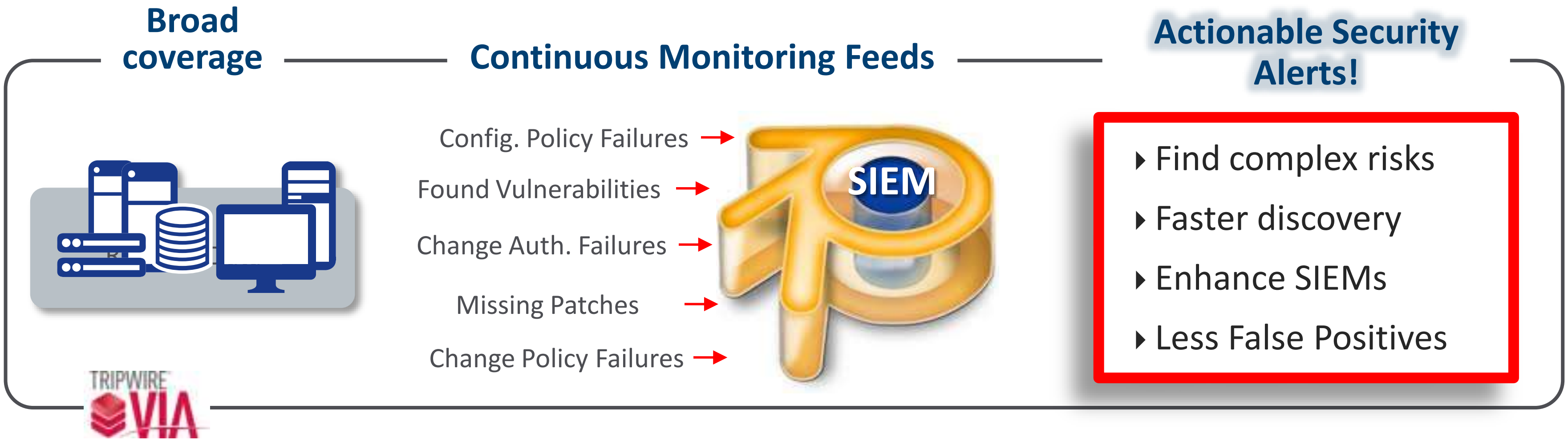
Continuous Monitoring – Reference Architecture



Atlantic Systems Group, Inc.
Service-Disabled Veteran-Owned Small Business

tripwire TAKE CONTROL.

Continuous Monitoring Security Alerts



Broad coverage

Continuous Monitoring Feeds

Config. Policy Failures →

Found Vulnerabilities →

Change Auth. Failures →

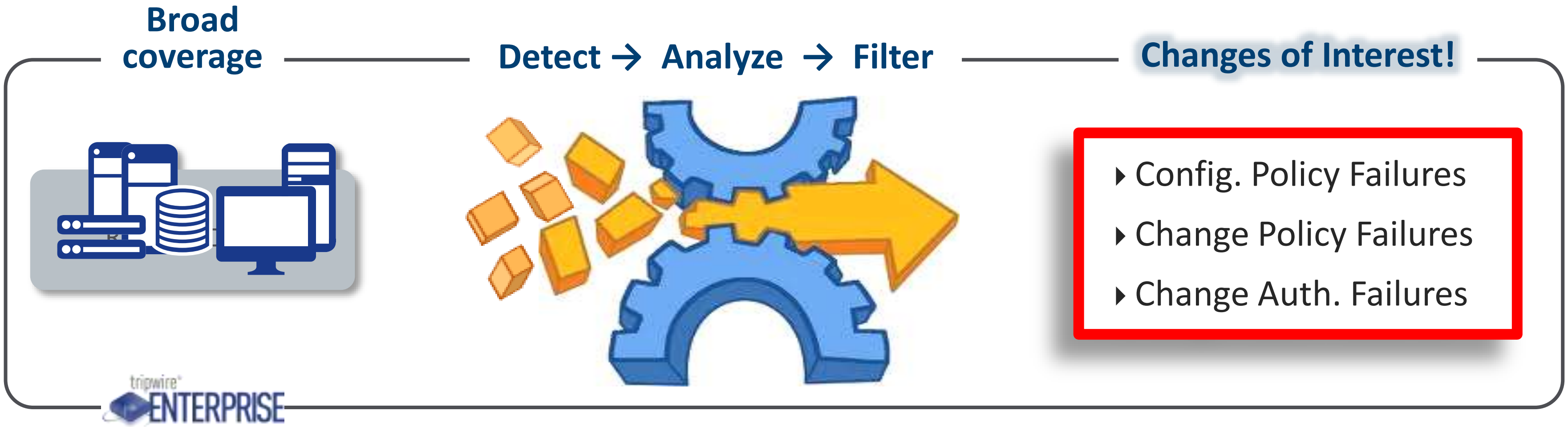
Missing Patches →

Change Policy Failures →

Actionable Security Alerts!

- Find complex risks
- Faster discovery
- Enhance SIEMs
- Less False Positives

Configuration Changes of Interest: Analyze / Filter Change



Broad coverage

Detect → Analyze → Filter

Changes of Interest!

- Config. Policy Failures
- Change Policy Failures
- Change Auth. Failures

The Worst Problems Are Often Most Difficult To Discover

⚠ Logging turned off

⚠ FTP event to foreign IP

⚠ New user added

⚠ Login successful

⚠ FTP enabled

⚠ 10 failed logins

⚠ DLL modified by new user

Atlantic Systems Group, Inc.
Service-Disabled Veteran-Owned Small Business

tripwire
TAKE CONTROL.

Detecting configuration modifications Alone IS Not Enough

- ⚠ **Logging turned off**
- ⚠ **New user added**
- ⚠ **FTP enabled**
- ⚠ **DLL modified by new user**

Vulnerability, Change and Configuration Assessment **cannot** make these types alerts. **Change intelligence is required**.

Detecting Log Security Events Alone IS Not Enough

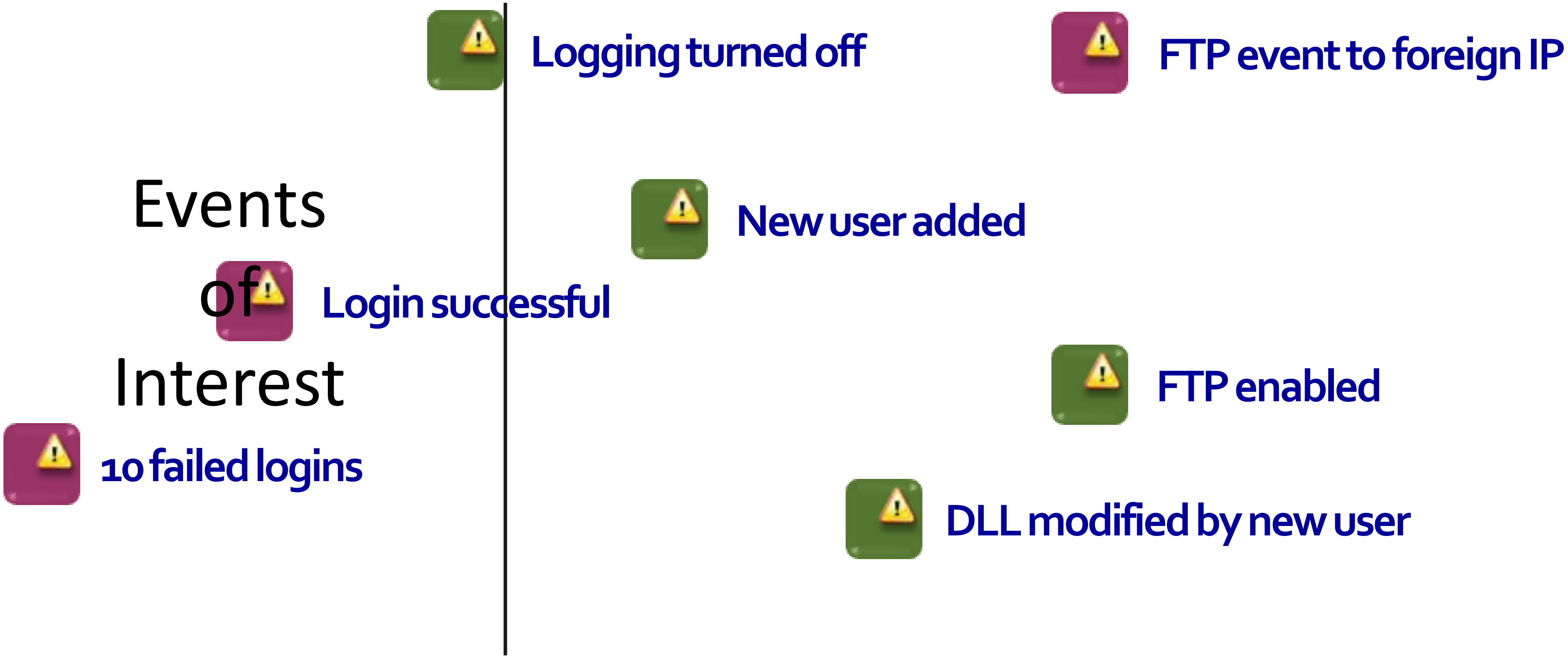
⚠ FTP event to foreign IP

⚠ Login successful

⚠ 10 failed logins

Log management alone **cannot** alert on these events—**SIEM is required**.

Relating Configuration Modification to Log Events Is Required



Events of Interest

10 failed logins

Login successful

Logging turned off

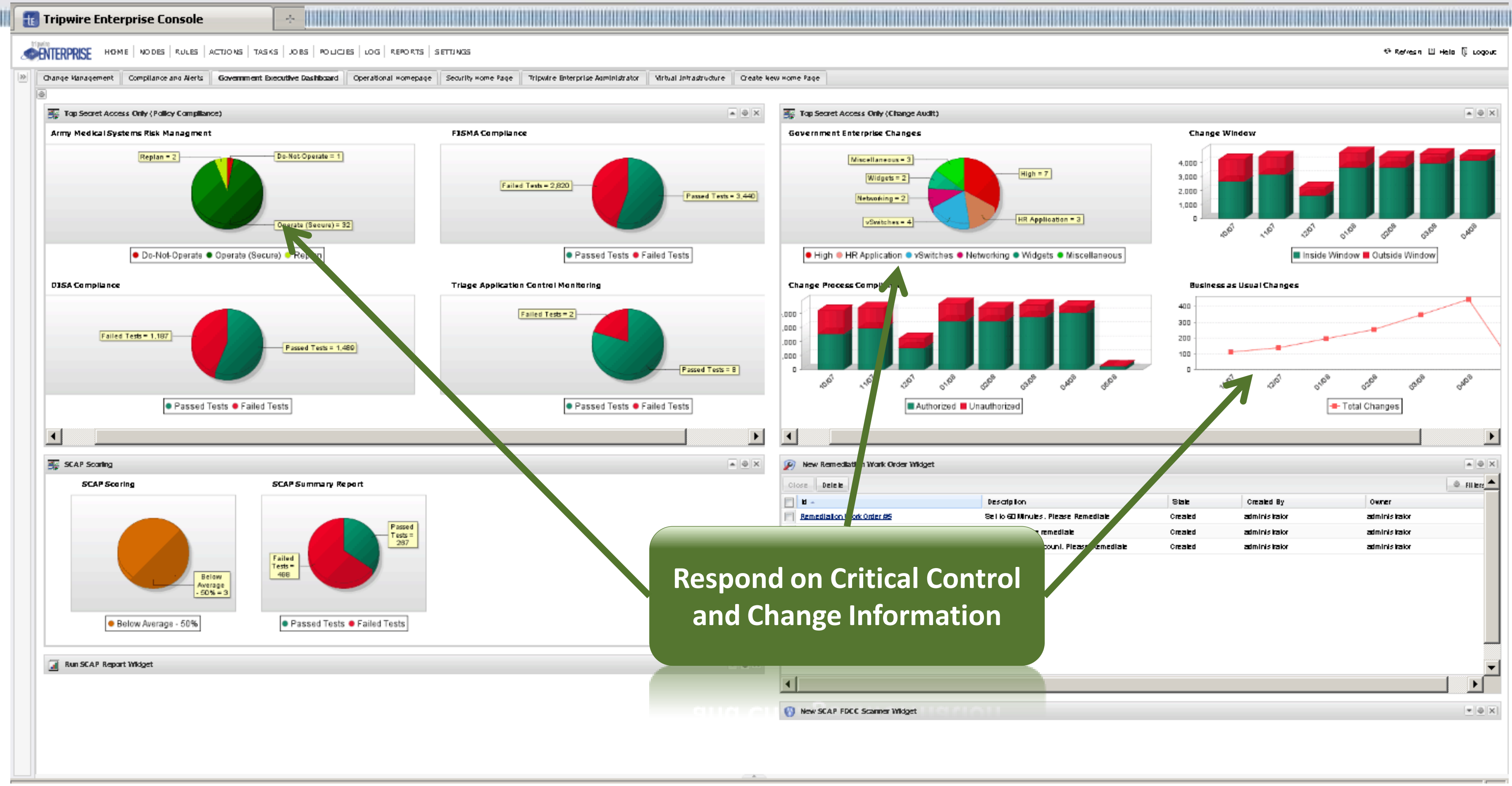
New user added

DLL modified by new user

FTP enabled

FTP event to foreign IP

Example Feedback to the Authorized Official

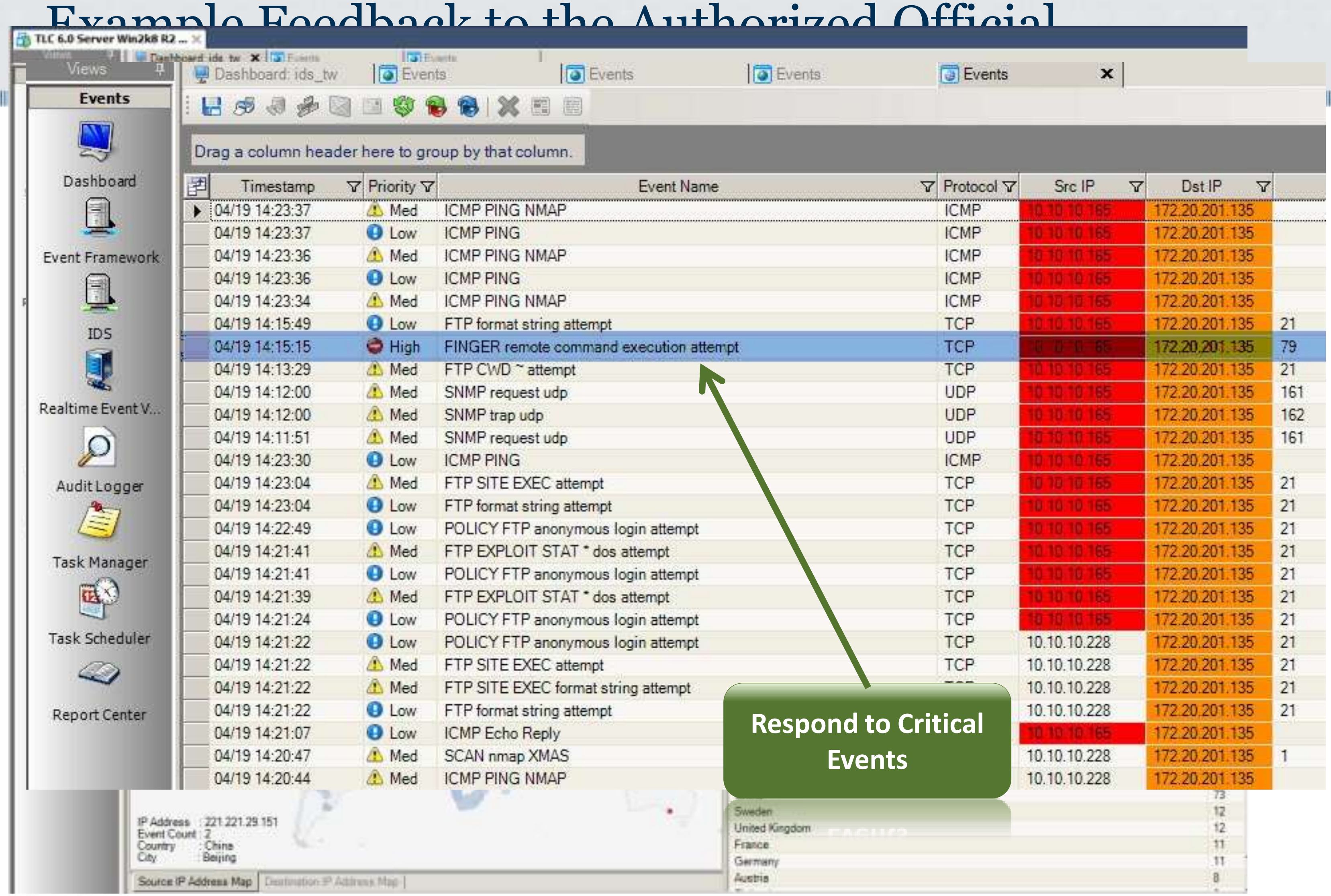


Tripwire Enterprise Console
ENTERPRISE
HOME | NODES | RULES | ACTIONS | TASKS | JOBS | POLICIES | LOG | REPORTS | SETTINGS
Refresh | Help | Logout
Change Management | Compliance and Alerts | Government Executive Dashboard | Operational Homepage | Security Home Page | Tripwire Enterprise Administrator | Virtual Infrastructure | Create New Home Page
Top Secret Access Only (Policy Compliance)
Army Medical Systems Risk Managment
Replan = 2
Do-Not-Operate = 1
Operate (Secure) = 32
● Do-Not-Operate ● Operate (Secure) ● Replan
FISMA Compliance
Failed Tests = 2,820
Passed Tests = 3,440
● Passed Tests ● Failed Tests
DISA Compliance
Failed Tests = 1,187
Passed Tests = 1,489
● Passed Tests ● Failed Tests
Triage Application Control Monitoring
Failed Tests = 2
Passed Tests = 8
● Passed Tests ● Failed Tests
Top Secret Access Only (Change Audit)
Government Enterprise Changes
Miscellaneous = 3
Widgets = 2
Networking = 2
vSwitches = 4
High = 7
HR Application = 3
● High ● HR Application ● vSwitches ● Networking ● Widgets ● Miscellaneous
Change Window
4,000
3,000
2,000
1,000
0
10/07 11/07 12/07 01/08 02/08 03/08 04/08
■ Inside Window ■ Outside Window
Change Process Compliance
■ Authorized ■ Unauthorized
Business as Usual Changes
400
300
200
100
0
12/07 01/08 02/08 03/08 04/08
Total Changes
SCAP Scoring
SCAP Scoring
Below Average - 50% = 3
● Below Average - 50%
SCAP Summary Report
Passed Tests = 287
Failed Tests = 488
● Passed Tests ● Failed Tests
Run SCAP Report Widget
New Remediation Work Order Widget
Close | Delete
Filters
Id | Description | State | Created By | Owner
Remediation Work Order #5 | Set to 60 Minutes. Please Remediate | Created | administrator | administrator
remediate | Created | administrator | administrator
count. Please remediate | Created | administrator | administrator
New SCAP FDCC Scanner Widget

Respond on Critical Control and Change Information

Continuous Monitoring

Example Feedback to the Authorized Official



Timestamp	Priority	Event Name	Protocol	Src IP	Dst IP	
04/19 14:23:37	⚠ Med	ICMP PING NMAP	ICMP	10.10.10.165	172.20.201.135	
04/19 14:23:37	ℹ Low	ICMP PING	ICMP	10.10.10.165	172.20.201.135	
04/19 14:23:36	⚠ Med	ICMP PING NMAP	ICMP	10.10.10.165	172.20.201.135	
04/19 14:23:36	ℹ Low	ICMP PING	ICMP	10.10.10.165	172.20.201.135	
04/19 14:23:34	⚠ Med	ICMP PING NMAP	ICMP	10.10.10.165	172.20.201.135	
04/19 14:15:49	ℹ Low	FTP format string attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:15:15	⛔ High	FINGER remote command execution attempt	TCP	10.10.10.165	172.20.201.135	79
04/19 14:13:29	⚠ Med	FTP CWD ~ attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:12:00	⚠ Med	SNMP request udp	UDP	10.10.10.165	172.20.201.135	161
04/19 14:12:00	⚠ Med	SNMP trap udp	UDP	10.10.10.165	172.20.201.135	162
04/19 14:11:51	⚠ Med	SNMP request udp	UDP	10.10.10.165	172.20.201.135	161
04/19 14:23:30	ℹ Low	ICMP PING	ICMP	10.10.10.165	172.20.201.135	
04/19 14:23:04	⚠ Med	FTP SITE EXEC attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:23:04	ℹ Low	FTP format string attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:22:49	ℹ Low	POLICY FTP anonymous login attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:21:41	⚠ Med	FTP EXPLOIT STAT * dos attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:21:41	ℹ Low	POLICY FTP anonymous login attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:21:39	⚠ Med	FTP EXPLOIT STAT * dos attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:21:24	ℹ Low	POLICY FTP anonymous login attempt	TCP	10.10.10.165	172.20.201.135	21
04/19 14:21:22	ℹ Low	POLICY FTP anonymous login attempt	TCP	10.10.10.228	172.20.201.135	21
04/19 14:21:22	⚠ Med	FTP SITE EXEC attempt	TCP	10.10.10.228	172.20.201.135	21
04/19 14:21:22	⚠ Med	FTP SITE EXEC format string attempt	TCP	10.10.10.228	172.20.201.135	21
04/19 14:21:22	ℹ Low	FTP format string attempt		10.10.10.228	172.20.201.135	21
04/19 14:21:07	ℹ Low	ICMP Echo Reply		10.10.10.165	172.20.201.135	
04/19 14:20:47	⚠ Med	SCAN nmap XMAS		10.10.10.228	172.20.201.135	1
04/19 14:20:44	⚠ Med	ICMP PING NMAP		10.10.10.228	172.20.201.135	

IP Address : 221.221.29.151
Event Count : 2
Country : China
City : Beijing

Source IP Address Map | Destination IP Address Map

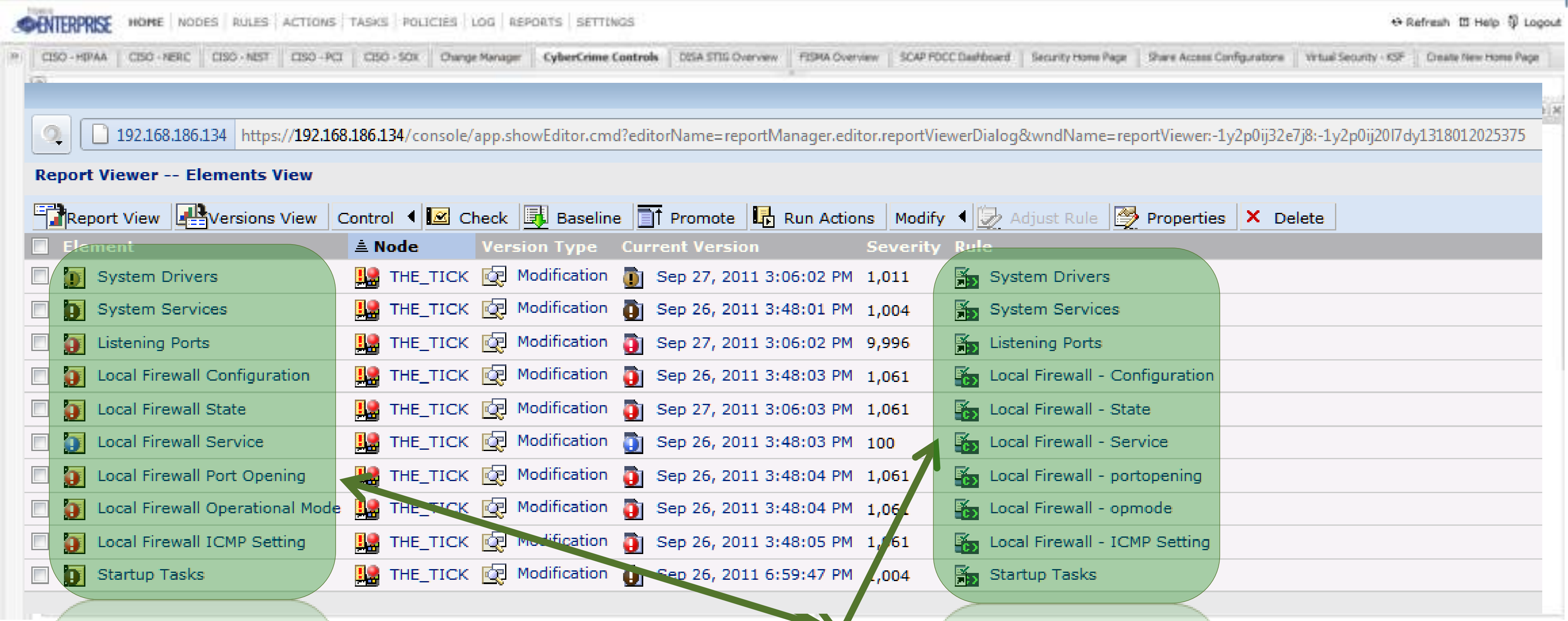
	73
Sweden	12
United Kingdom	12
France	11
Germany	11
Austria	8

Respond to Critical Events

Atlantic Systems Group, Inc.
Service-Disabled Veteran-Owned Small Business

tripwire™
TAKE CONTROL.

Get visibility into Cyber Threats



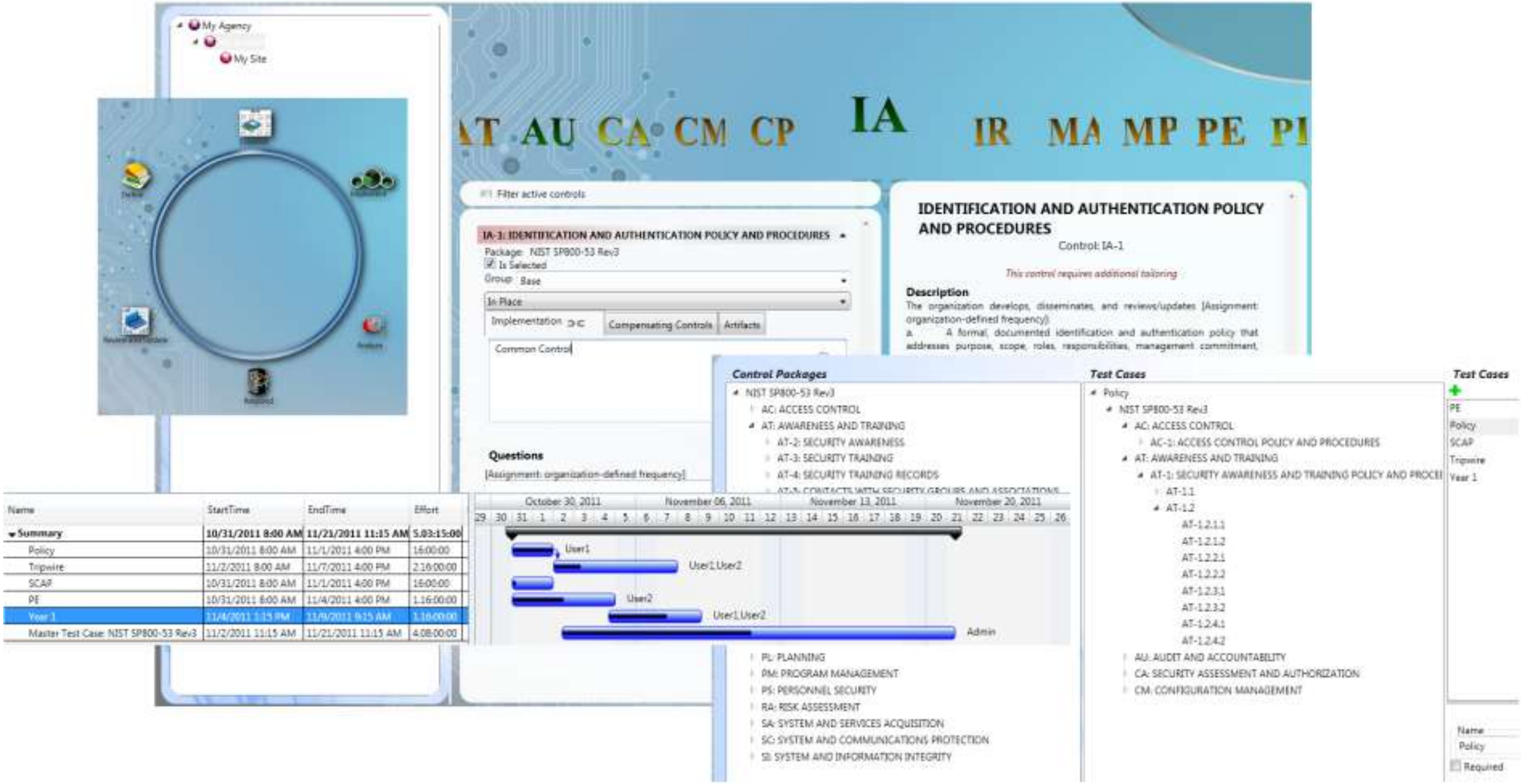
192.168.186.134 https://192.168.186.134/console/app.showEditor.cmd?editorName=reportManager.editor.reportViewerDialog&wndName=reportViewer:-1y2p0ij32e7j8:-1y2p0ij20l7dy1318012025375

Report Viewer -- Elements View

□	Element	Node	Version Type	Current Version	Severity	Rule
□	System Drivers	THE_TICK	Modification	Sep 27, 2011 3:06:02 PM	1,011	System Drivers
□	System Services	THE_TICK	Modification	Sep 26, 2011 3:48:01 PM	1,004	System Services
□	Listening Ports	THE_TICK	Modification	Sep 27, 2011 3:06:02 PM	9,996	Listening Ports
□	Local Firewall Configuration	THE_TICK	Modification	Sep 26, 2011 3:48:03 PM	1,061	Local Firewall - Configuration
□	Local Firewall State	THE_TICK	Modification	Sep 27, 2011 3:06:03 PM	1,061	Local Firewall - State
□	Local Firewall Service	THE_TICK	Modification	Sep 26, 2011 3:48:03 PM	100	Local Firewall - Service
□	Local Firewall Port Opening	THE_TICK	Modification	Sep 26, 2011 3:48:04 PM	1,061	Local Firewall - portopening
□	Local Firewall Operational Mode	THE_TICK	Modification	Sep 26, 2011 3:48:04 PM	1,061	Local Firewall - opmode
□	Local Firewall ICMP Setting	THE_TICK	Modification	Sep 26, 2011 3:48:05 PM	1,061	Local Firewall - ICMP Setting
□	Startup Tasks	THE_TICK	Modification	Sep 26, 2011 6:59:47 PM	1,004	Startup Tasks

Know the system settings that need to be secured

IA² - Continuous Monitoring Program (CMP)



IA-1: IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Package: NIST SP800-53 Rev3

☑ Is Selected

Group: Base

In Place

Implementation | Compensating Controls | Artifacts

Common Control

Questions

[Assignment: organization-defined frequency]

IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: IA-1

This control requires additional tailoring

Description

The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:

a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment,

Name	StartTime	EndTime	Effort
Summary	**10/31/2011 8:00 AM**	**11/21/2011 11:15 AM**	**5.03:15:00**
Policy	10/31/2011 8:00 AM	11/1/2011 4:00 PM	16:00:00
Tripwire	11/2/2011 8:00 AM	11/7/2011 4:00 PM	2.16:00:00
SCAP	10/31/2011 8:00 AM	11/1/2011 4:00 PM	16:00:00
PE	10/31/2011 8:00 AM	11/4/2011 4:00 PM	1.16:00:00
Year 1	11/4/2011 1:15 PM	11/9/2011 9:15 AM	1.16:00:00
Master Test Case: NIST SP800-53 Rev3	11/2/2011 11:15 AM	11/21/2011 11:15 AM	4.08:00:00

Control Packages

- NIST SP800-53 Rev3
  - AC: ACCESS CONTROL
  - AT: AWARENESS AND TRAINING
    - AT-2: SECURITY AWARENESS
    - AT-3: SECURITY TRAINING
    - AT-4: SECURITY TRAINING RECORDS
    - AT-5: CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
  - PL: PLANNING
  - PM: PROGRAM MANAGEMENT
  - PS: PERSONNEL SECURITY
  - RA: RISK ASSESSMENT
  - SA: SYSTEM AND SERVICES ACQUISITION
  - SC: SYSTEM AND COMMUNICATIONS PROTECTION
  - SI: SYSTEM AND INFORMATION INTEGRITY

Test Cases

- Policy
  - NIST SP800-53 Rev3
    - AC: ACCESS CONTROL
      - AC-1: ACCESS CONTROL POLICY AND PROCEDURES
    - AT: AWARENESS AND TRAINING
      - AT-1: SECURITY AWARENESS AND TRAINING POLICY AND PROCE
        - AT-1.1
        - AT-1.2
          - AT-1.2.1.1
          - AT-1.2.1.2
          - AT-1.2.2.1
          - AT-1.2.2.2
          - AT-1.2.3.1
          - AT-1.2.3.2
          - AT-1.2.4.1
          - AT-1.2.4.2
    - AU: AUDIT AND ACCOUNTABILITY
    - CA: SECURITY ASSESSMENT AND AUTHORIZATION
    - CM: CONFIGURATION MANAGEMENT

Test Cases

PE
Policy
SCAP
Tripwire
Year 1

Name: Policy

□ Required

Questions and Answers

Complete Security & Compliance Solution

Tripwire Solution	Benefits
Security Intelligence	• Arm CISOs with the data they need • Have business context (risk) to help prioritize & make better decisions • Improve analytics
Security Hardening	• Reduce attack surface • Harden systems through secure configurations • Understand the security and risk posture
Continuous Monitoring	• Make cost-effective, risk based decisions • Continuous controls-based visibility of state, policy & events • Meet NIST 800-137 guidelines and go beyond the compliance checkbox
Threat Response	• Detect real-time evidence of potential data compromise, misuse, tampering • Reduce the breach-to-detection time gap
Operationalize Security	• Quick deployments of new datacenters, infrastructure and business services • Find and fix security breaches & weaknesses in defenses • Manage planned and unplanned changes to production systems
Forensics/Investigation	• Quickly extract actionable information from critical systems • Quickly identify root cause of incident & problem management • Have historical proof to simplify compliance
Continuous Compliance	• Satisfy compliance requirements for security assurance • Make compliance a by-product of being secure continuously • Be compliant at lowest cost
Compliance Auditing	• Avoid fines, audit failures and penalties • Proactively manage compliance • Easily prove compliance on-demand at lowest possible cost