Tripwire State Analyzer Report Catalog

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Tripwire® State Analyzer automates change alerts. It works in tandem with Tripwire Enterprise and Tripwire IP360™ to provide smart alerting and automation in critical security areas that are not manageable by traditional system state monitoring approaches.

Originally developed for customers with high security requirements in the electric generation and transmission utilities industry, its high adoption rate now spans multiple industries that face similar monitoring challenges.

Tripwire State Analyzer is scalable, flexible, and easy to maintain. This document highlights available reports.

Users and Passwords

In the solution for local users, multiple aspects of user accounts are reported on.

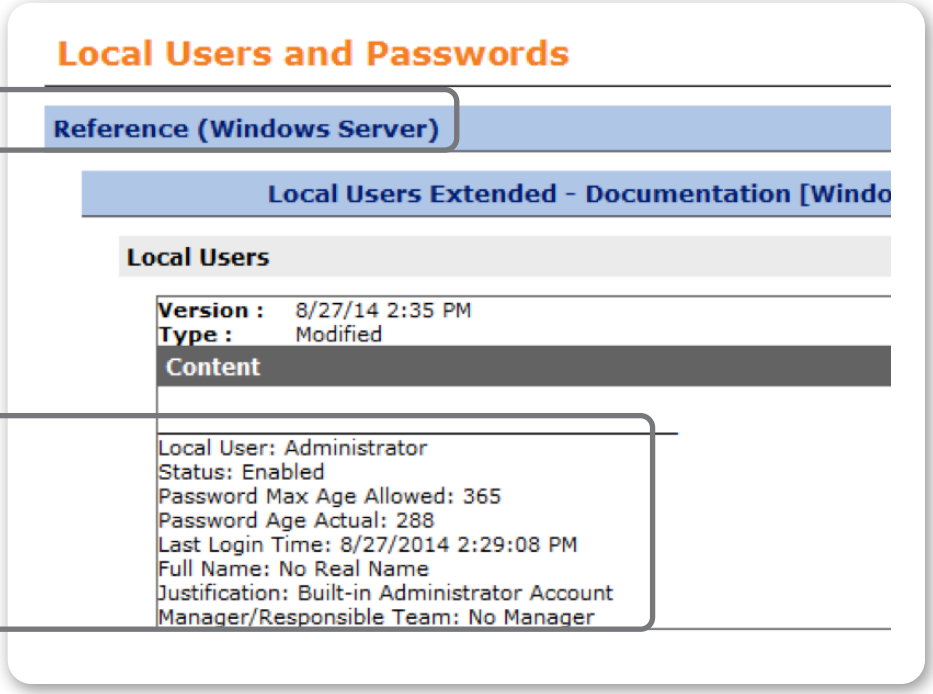
The solution has built-in options which allow for:

- Addition of custom fields
- Option of readable output, or CSV output
- Alerting on password over allowed age limit
- Alerting on passwords nearing allowed age limit

Evidence Reporting

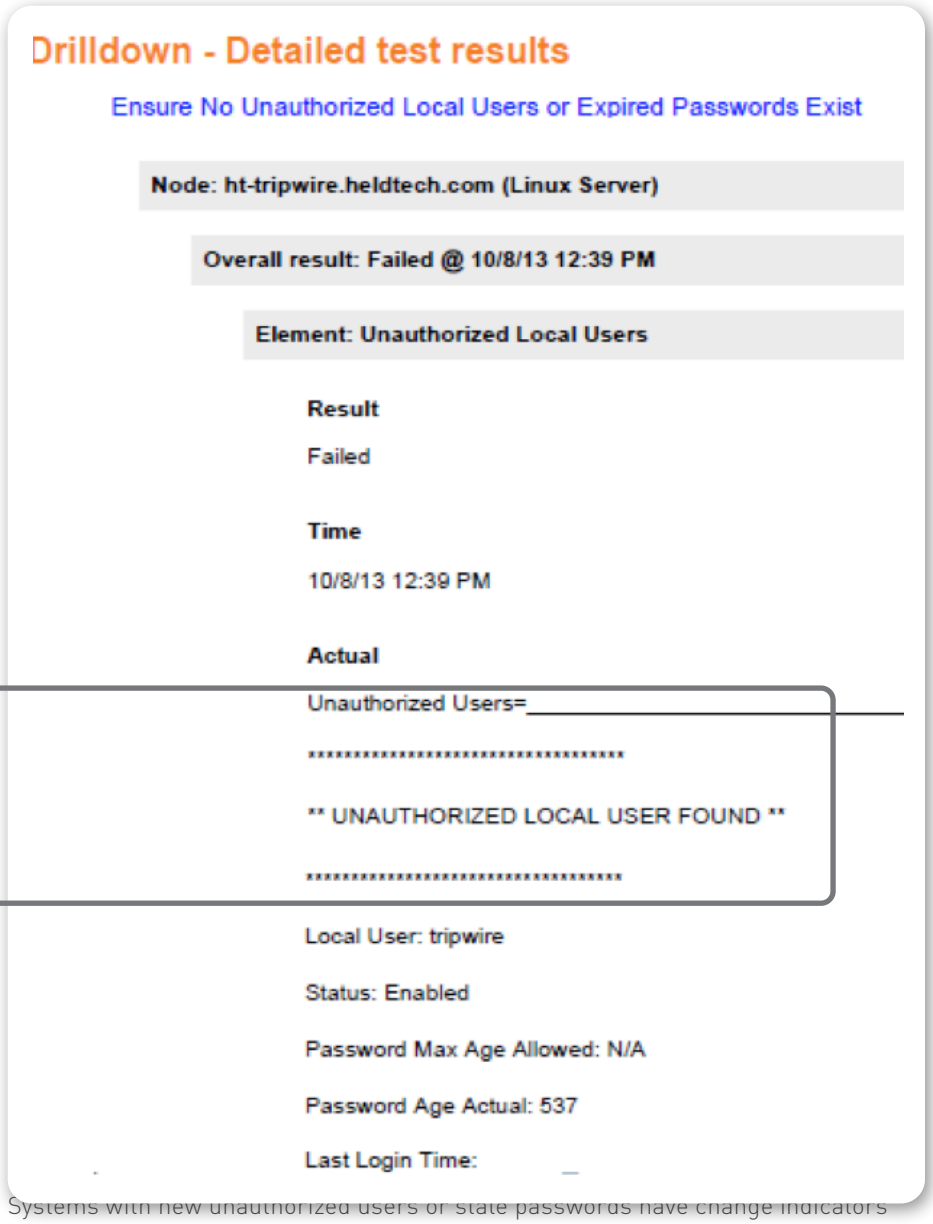
Report by asset

Reporting includes Justification and password age analysis



Example user account not allowlisted

Security Alerting



An account found that needs to be allowlisted or removed from the system

Systems with new unauthorized users or state passwords have change indicators from green to red. This example shows a detailed report of just the exceptions that a System Administrator should attend to.

Support and Requirements

This solution is supported on:

» Windows

» RHEL

Ports

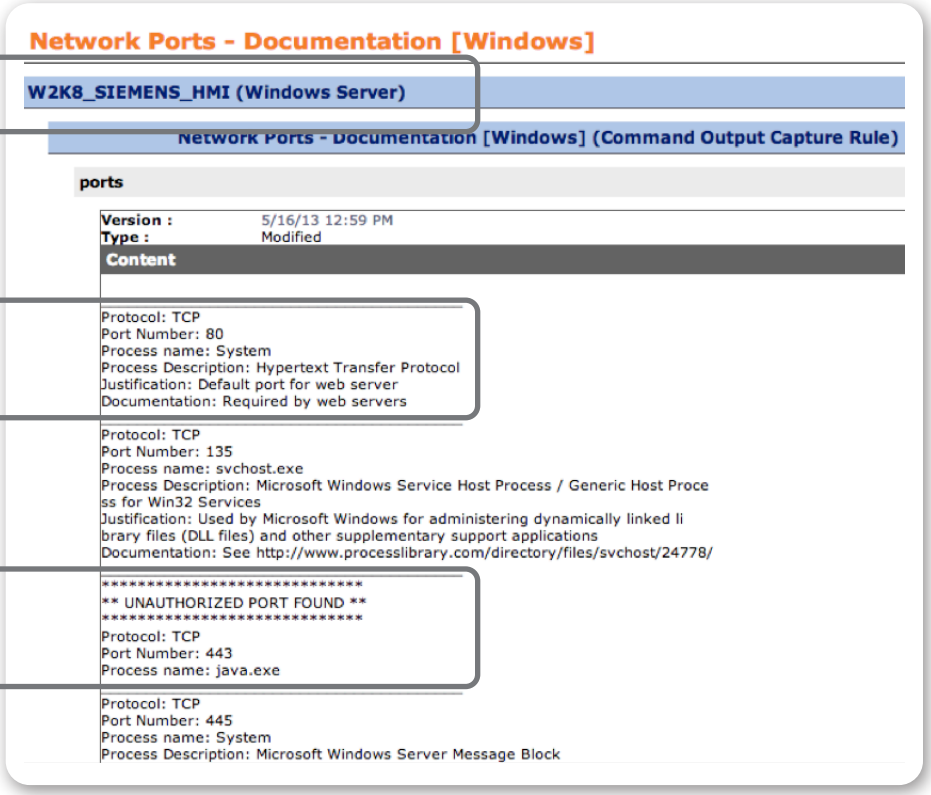
Reports are generated to support two use cases: evidence reporting and alerting for daily maintenance of compliance. Report generation is automated once the solution is fully implemented, and allows for scanning as often as is desired.

Evidence Reporting

Report by Asset

Justification for each allowed port

Ports lacking justification called out



The solution has built-in options which allow for:

- Ephemeral ports
- Port ranges
- TCP and UDP
- Digest data from nmap or IP360
- Matching ports to process
- Addition of custom fields to reports

Support and Requirements

This solution is supported on:

- Agent-based, internal scanning:
  - Windows
  - RHEL
  - AIX
  - Solaris
- Agentless, external scanning for an IP device

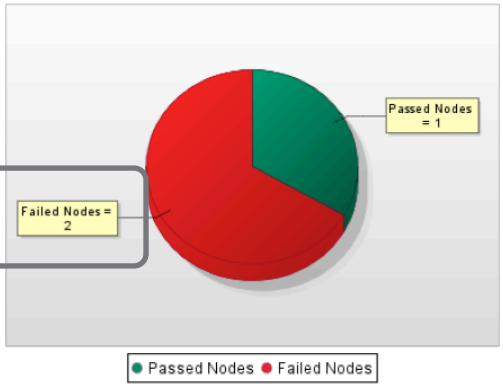
Compliance Alerting

Immediate indication if an unexpected port is detected

Drill-down on an asset to show details of unexpected ports

Return to a compliant state by closing or justifying the port

Unauthorized Ports on Windows



Ensure No Unauthorized Listening Ports Exist

The Responsible Entity shall enable only those ports and services required for normal and emergency operations

Node	Passed Tests	Failed Tests	Percent Compliant
JTI-NERC-XP	1	0	100%
Server2008r2Ent	0	1	0%
W2K_SIEMENS_HMI	0	1	0%

Detailed Test Results Template

Ensure No Unauthorized Listening Ports Exist

The Responsible Entity shall enable only those ports and servi

Node: W2K_SIEMENS_HMI (Windows Server)

Overall result: Failed @ 5/20/13 7:17 PM

Element: Unauthorized Network Ports

Result

Failed

Time

12/18/14 2:55 PM

Actual

Unauthorized ports=

****
** UNAUTHORIZED PORT FOUND **
****
Protocol: TCP
Port Number: 17500
Process name: Dropbox.exe

****
** UNAUTHORIZED PORT FOUND **
****
Protocol: UDP
Port Number: 17500
Process name: Dropbox.exe

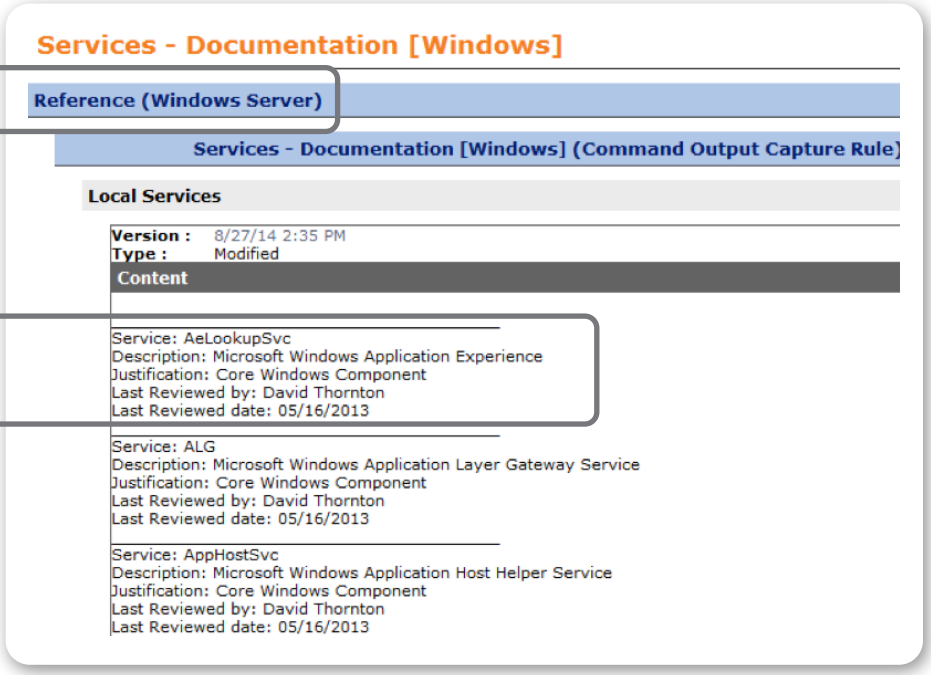
Services

Once the user has supplied information about normal or expected services on a system or class of systems, Tripwire will alert on new, unexpected ports. Report generation is automated once the solution is fully implemented, and allows for reporting as often as is desired.

Evidence Reporting

Report by asset

Justification for each allowed service



The solution has built-in options which allow for:

- Specifying justification by individual servers or by server role
- Custom fields

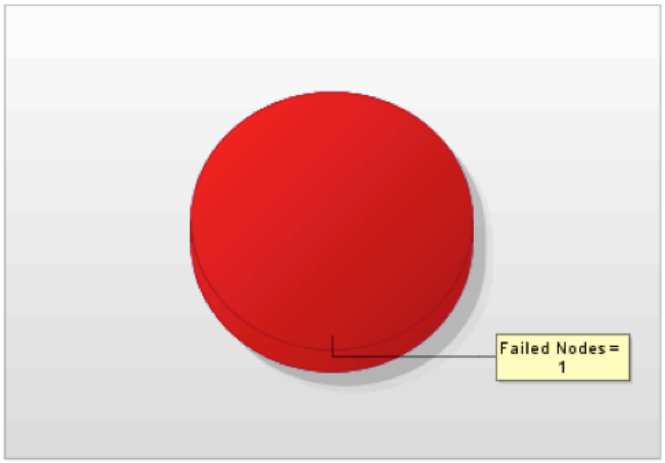
Support and Requirements

This solution is supported on:

- Windows
- RHEL
- AIX
- Solaris

Compliance Alerting

Services



Ensure No Unauthorized Services Are Running [Windows]

Node	Passed Tests	Failed Tests	Percent Compliant
Reference	0	1	0%

Drill-down on an asset to show details of unexpected services

Drilldown - Detailed Test Results

Ensure No Unauthorized Services Are Running [Windows]

The Responsible Entity shall enable only those ports and service

Node: Reference (Windows Server)

Overall result: Failed @ 9/18/14 6:21 PM

Element: Unauthorized Local Services

Result

Failed

Time

9/18/14 6:21 PM

Actual

Unauthorized services=

****
** UNAUTHORIZED SERVICE FOUND **
****
Service: gupdate

****
** UNAUTHORIZED SERVICE FOUND **
****
Service: gupdatem

Return to a compliant state by stopping or justifying the service

PLATFORM COVERAGE AND REQUIREMENTS

All solution areas listed in the chart below are based on Tripwire Enterprise. All server platforms require Tripwire Enterprise v8.0 or later and a Tripwire Enterprise agent installed on the server.

	SOLUTION AREA							
PLATFORM	PORT	SERVICES	USERS	USERS & PASSWORDS	GROUPS	SOFTWARE	SHARES	ROUTES
Windows[1]	X	X	X	X	X	X	X	X
RHEL[2]	X	X	X	X		X		X
AIX 5.3[3]	X	X	X			X		
AIX 6.1[3]	X	X	X			X		
Solaris 10[3, 4]	X	X	X			X		
NMAP Scans[5]	X							

Additional platforms can be supported through a custom engagement with Tripwire Professional Services.

1 Windows XP, 7, 8, 2000, 2003, 2008, 2008 R2 & 2012

2 Requires WGET or CURL

3 Requires LSOF and WGET

4 Global Zone only

5 Requires NMAP capable host with TE Agent to act as initiator

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

TSARC1a 2106