TANIUM 7.0
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

11 December 2017

Developed by Tanium and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

This Tanium 7.0 Security Technical Implementation Guide (STIG) is intended to provide security guidelines for the protection of the Tanium Application and its components, including but not limited to the Tanium Application, Tanium Console, Tanium Module Server, Tanium Clients, and Tanium SQL Database.

Tanium 7.0 is a scalable Endpoint Security and Management system. Its foundation is the Tanium Core. Tanium Core includes basic asset inventory, control and utilization monitoring capabilities, and connectors for integrating with third-party systems.

Tanium uses a linear peer-to-peer architecture specifically designed for fault tolerance, transient endpoints, and the global Wide Area Network (WAN) segments. It is not a typical peer-to-peer application; only other Tanium endpoints can communicate over the peer-to-peer architecture. The clients communicate with each other over a specific Transmission Control Protocol (TCP) port.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing

Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

2.1.1 Tanium Implemented Controls Specific to DoD and Federal Systems

The Tanium Server's web-based Console must be configured to allow access only via Common Access Card (CAC) smartcard authentication. It also requires the syncing of the Console user accounts with Active Directory (AD) so that roles and delegation of functions can be segregated by AD security groups. These AD security groups sync to Tanium as user roles. The CAC authentication will use the AD account for access to the Console and will provide the Tanium Role as is identified by the respective AD security group.

The actual syncing of the Tanium Console to the AD is configured in the Module Server via the Connection Manager.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

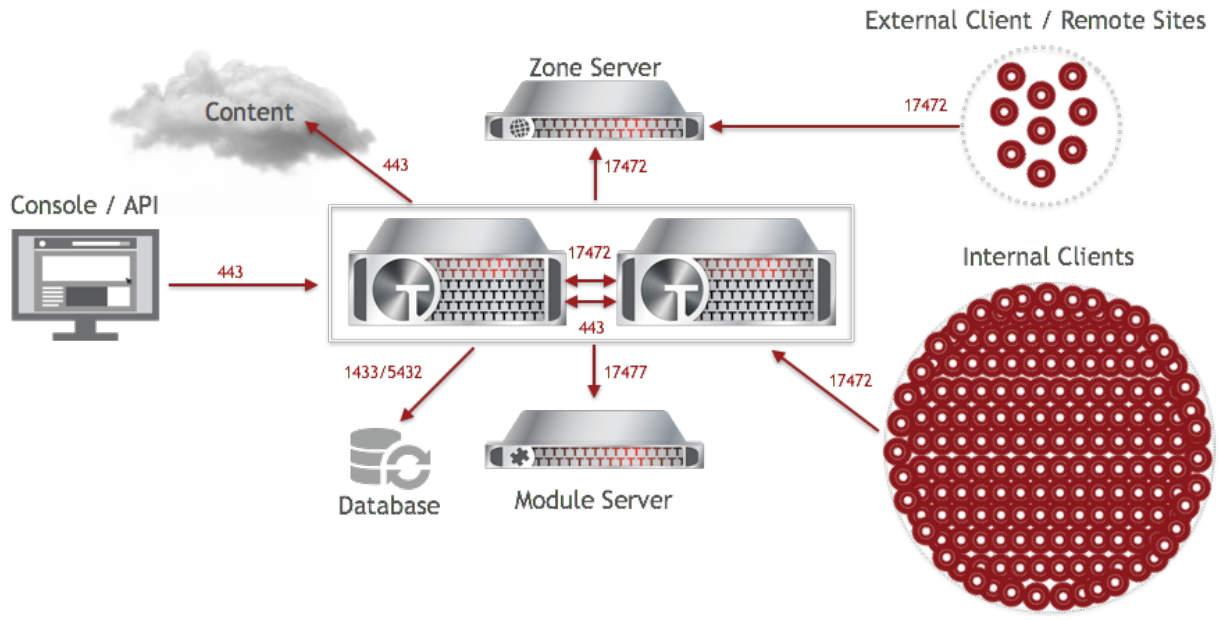
3.1 Tanium 7.0 Functionality

The Tanium Core Platform allows for information to be collected from and actions deployed on all the endpoints in the environment. Install and configure the component servers, the Tanium Console, Tanium Client, Tanium Interact, Tanium Authoring, and Tanium Connect. Then ask questions, consume data, deploy actions, and administer the endpoints.

Tanium Core Platform component servers:

- **Tanium Server**: The core platform server that communicates with clients. The Tanium Server runs the UI console and API services and communicates with all other platform and solution components, as well as the content.tanium.com servers that host Tanium content packs and Tanium solution import packages. The Tanium Server includes web server features and functions. The web server component is a custom-built web server; all of the applicable configuration settings are managed by the Tanium product.
- **Tanium Module Server**: A dedicated server to run application services and store files for Tanium solution modules. It is installed on a separate host machine to prevent intentional or accidental scripts from having a direct impact on the Tanium Server.
- **Tanium Zone Server**: A server typically deployed in an enterprise DMZ network to proxy traffic between Tanium Clients that reside on limited-access networks and a Tanium Server that resides on the trusted core network.

Figure 3-1: Tanium Production Topology



Tanium Console is the graphical user interface that is used to manage the Tanium Core Platform and use Tanium solution modules. Tanium Console key tasks include:

- Importing Tanium solutions
- Importing Tanium content
- Managing actions
- Creating and managing sensors, packages, and saved questions
- Administering console and platform settings, such as users, user roles and rights, user groups, and computer groups
- Administering global settings that affect Tanium Server and Tanium Client behavior

Tanium Client is a service installed on endpoint computers. In response to questions, it discovers and reports within seconds both static and dynamic real-time data pertaining to the endpoint, including:

- Hardware and software inventory
- Software configuration
- Local or domain user details
- Installed application or services, startup programs, and running processes
- Existence of registry keys and their values
- Windows Management Instrumentation (WMI) data elements
- File system details, including identification of files by hash or contents
- Event log results
- Network configuration settings and state

Tanium Interact performs basic functions such as asking questions, consuming data, and deploying actions across the Tanium enterprise. Interact is installed automatically during the Tanium Server installation. Although it is licensed as part of the core platform, Interact is a Tanium solution module, so it can be updated separately from the Tanium Console and the Tanium Server.

Tanium Comply supports continuous compliance goals by proactively performing security checks on operating systems, password permissions, files, and more. Tanium Comply allows for the support of enterprise compliance goals at Tanium speed. Comply is primarily used for operating system-level checks and scales using the Tanium architecture. It features the following benefits:

- Evaluates benchmarks and vulnerabilities against operating systems, network configuration, password policy, file permissions, and other components
- Supports Windows, Linux, and macOS platforms
- Supports Center for Internet Security (CIS) content
- Enables custom checks and result mapping

Tanium Connect integrates Tanium with security information and event management (SIEM), log analytics tools, threat feeds, or send email notifications. Tanium Connect is the link between a *connection source* and a *connection destination.* These connections can be run on a schedule at determined times/days.

- Examples of connection destinations include:
  - ArcSight
  - elastic
  - LogRhythm
  - McAfee
  - Palo Alto
  - Splunk
  - SQL Server
  - Tanium email notifications
  - Tanium file destination
  - Tanium SIEM destination
- Examples of connection sources include:
  - Action history
  - Audit log
  - Tanium Event
  - Palo Alto Wildfire
  - Question Log
  - Reputation service
  - Saved question
  - Server information
  - System status
  - VirusTotal process

Tanium Discover finds and maintains an inventory of assets in the Tanium environment. Installing the Tanium Client on endpoints enables active monitoring of the local subnet, detecting unmanaged assets, and reporting the assets to Discover. The following tasks can then be performed:

- Block unmanaged assets from network access.
- Deploy Tanium Client to bring assets under management.
- Get real-time information about unmanaged assets on the network.

Tanium-managed endpoints scan for or detect unmanaged assets at configurable intervals that depend on the discovery method. Discover queries endpoints for updated detection data every few minutes. New information is immediately available. The detection process provides continuous scanning without impact to network operations.

Discover is integrated with a collection of sensors, packages, and actions. This tool set provides the ability to bring network assets under management within minutes of detection.

Tanium IOC Detect provides indicator of compromise (IOC) detection and YARA rule matching for management and analysis capabilities to enable real-time responses to intrusions. IOC Detect also provides a REST API that allows for integration between IOC Detect and other parts of the security network.

Tanium Incident Response is a solution to scan and hunt for incidents, examine forensic artifacts, and collect system data for analysis across every endpoint.

Tanium Integrity Monitor simplifies regulatory compliance and makes file integrity monitoring more effective enterprise-wide by consolidating tools while taking full advantage of the benefits of the Tanium platform.

Tanium Patch is used to manage Windows operating system patching across the enterprise at the speed and scale of Tanium. A single patch can be deployed to a computer group immediately. This also allows for more complex tasks, such as using advanced rule sets and maintenance windows to deliver groups of patches across the environment at specified times.

Tanium Protect delivers proactive protection to block malicious attacks on endpoints using native operating system and third-party controls at the speed and scale of Tanium across the environment.

Tanium Trace is used to directly investigate key forensic and security events on Linux and Windows endpoints across the network. Trace provides a live and historical view of critical events including process execution, logon history, network connections, and file and registry changes. The Trace solution is composed of three parts:

- The Trace event recorder that monitors event data on the endpoint
- The Trace interface where you can explore and manage endpoint Trace data
- The sensors for issuing searches across the entire enterprise for Trace data

Tanium Trends gives visibility into the history of key pieces of information about the enterprise IT estate, coordination with real-time status for those same indicators, and the ability to close the loop by deploying necessary action on any endpoint—all without leaving the Tanium Console session.

3.2 Tanium 7.0 Infrastructure

Tanium is not built on a hierarchical server infrastructure to provide data collection, aggregation, and distribution functionality. Instead, Tanium uses a linear peer-to-peer architecture specifically designed for fault tolerance, transient endpoints, and the global Wide Area Network (WAN) segments. It is not a typical peer-to-peer application; only other Tanium endpoints can communicate over the peer-to-peer architecture. The clients communicate with each other over a specific Transmission Control Protocol (TCP) port.

The following highlights these key architectural differences:

- Traditional Communications Flow
  - Server propagates request to all relay servers.
  - Relay server collects individual responses from its clients.
  - Relay server sends series of individual responses back to server.
- Tanium Communications Flow
  - Tanium Server contacts a few clients.
  - Client contacts peer client and passes aggregated response over LAN.
  - Last client sends final aggregated response to server.

4. GENERAL SECURITY REQUIREMENTS

4.1 Security Posture of Tanium Platform

Because every implementation of Tanium will have its own nuances, this STIG is not an all-encompassing STIG intended to provide complete end-to-end guidance for the Tanium architecture. Instead, it is intended to secure the areas where compromise could occur.

The security posture of the Tanium components requires the full configuration of all platform STIGs, including the operating system, browser, SQL database, antivirus, web, and any other feature installed on any of the components for which a STIG exists.

This STIG does not provide operational guidance for the multiple Tanium functionalities. For instance, this STIG does not outline how to package an update and deploy to the clients. It will, however, provide specific configuration guidance if a function of Tanium could impact the security posture of the Tanium platform.

Although the requirements for this STIG might span across different Tanium servers, the clients, or the SQL database server, many of the client requirements can be accomplished on the Tanium server itself, via the console, by asking questions of the clients.