TANIUM 7.X ON TANOS SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

18 November 2022

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

The Tanium 7.x on TanOS 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, Tanium SQL Database, and TanOS.

Tanium 7.x is a scalable endpoint security and management system. Its foundation is the Tanium Core, which includes basic asset inventory, control, and utilization monitoring capabilities, as well as connectors for integrating with third-party systems.

Tanium uses a linear peer-to-peer architecture specifically designed for fault tolerance, transient endpoints, and 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

Department of Defense Instruction (DoDI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that 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 [National Security Agency/Central Security Service], 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 must 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

Category	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 DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.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 Controlled Unclassified Information (CUI) will be available for 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 AO. 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 DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable 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). Department of Defense 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 in accordance with (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) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DoDI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Tanium Implemented Controls Specific to DOD and Federal Systems

The Tanium Server's web-based Console must be configured to allow access only via CAC smartcard authentication. It also requires syncing the Console user accounts with Active Directory (AD) so 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 identified by the respective AD security group.

With Tanium 7.1 and later versions, role-based access control (RBAC) was introduced. RBAC enables the creation of more fine-grained availability functions for Tanium users through the Tanium Console. With RBAC, the AD computer group management still determines which computers a Tanium user can interact with, but RBAC determines which content is available to the user for those interactions.

RBAC also allows further restrictions on sets of questions and actions a user can issue. A fine-grained permissions framework ensures a least-privilege framework.

The 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 Functionality

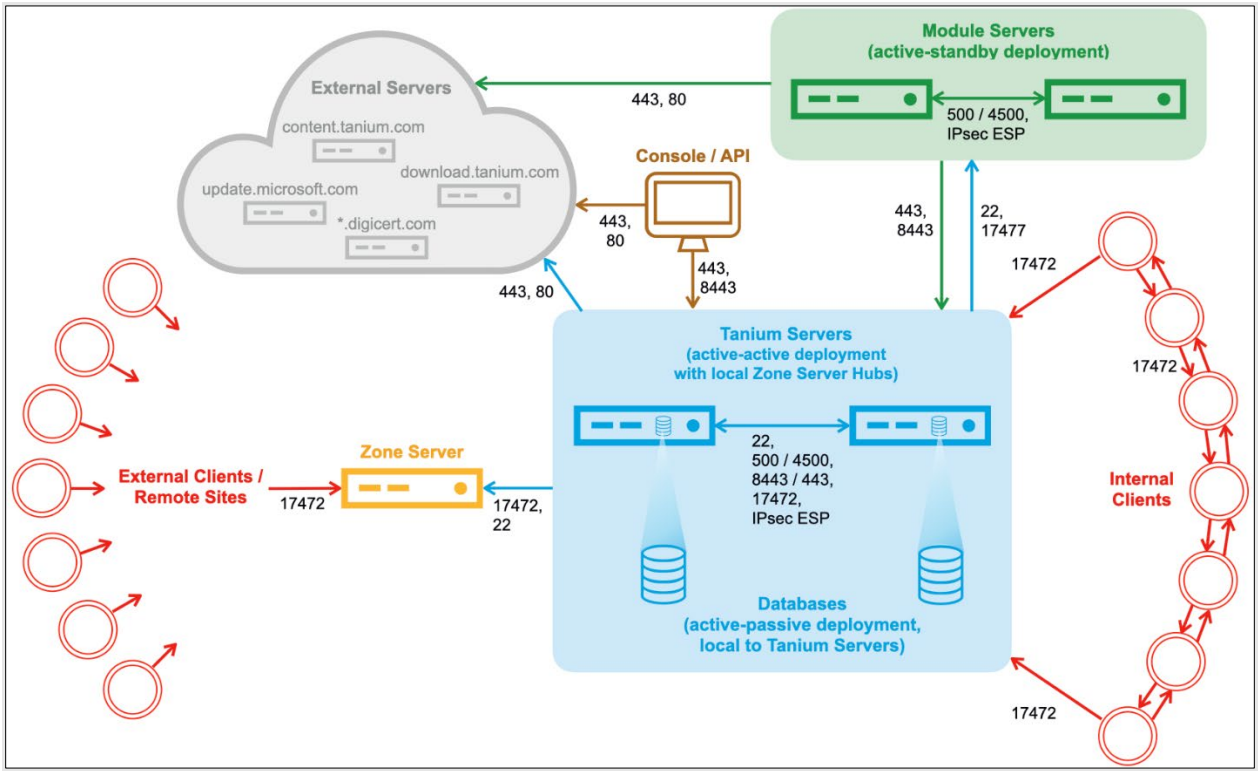
The Tanium Core Platform allows information to be collected from and actions deployed on all the endpoints in the environment. Install and configure the component servers, Tanium Console, Tanium Client, and Tanium modules, and then ask questions, consume data, deploy actions, and administer the endpoints.

Tanium Server: The core server that communicates with clients. The Tanium Server also 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 solutions. The Tanium Server depends on a database server that is installed when the Tanium Server role is installed.

Tanium Module Server: A dedicated server to run application services and store files for Tanium solution modules. It is installed on a separate Tanium Appliance 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 Product Topology



Tanium Console is the graphical user interface used to manage the Tanium Core Platform and access Tanium modules (such as Tanium Interact) and Tanium shared services. The Tanium Console is a web application installed with the Tanium Server that does not require separate licensing. Use the Tanium Console to perform the following key tasks:

- Import and use Tanium modules, shared services, and content packs.
- Manage content, including sensors, packages, saved questions, and filter groups.
- Manage actions.
- Manage RBAC configurations for users, user groups, roles, computer groups, personas, and content sets.
- Configure global settings that affect the behavior of the Tanium Console, Tanium Server, Tanium Zone Server, Tanium Zone Server Hub, and Tanium Clients.

Tanium Client discovers both static and dynamic real-time data pertaining to the endpoint and reports within seconds. This data can include the following information:

- Hardware and software inventory.
- Software configuration.
- Local or domain user details.
- Installed application or services, startup programs, and running processes.
- Existence of Windows registry keys and 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 Client, with similar speed, can execute commands, actions, scripts, or other executable programs, as if an authorized administrator were taking actions from the command line on the target endpoint. For example, send the Tanium Client an instruction to do the following:

- Install or uninstall applications or services.
- Update or patch installed applications, services, hardware drivers, or firmware.
- Manage installed applications or services.
- Add, remove, or modify the Windows Registry settings or other configuration stores.
- Add, remove, or modify files or the contents of files.
- Start or stop services.

3.1.1 Tanium Modules

Tanium Interact issues questions to managed endpoints, analyzes their answers, and deploys actions to the endpoints based on the answers. Although it is licensed as part of the Tanium Core platform, Interact is a Tanium module that can be updated separately from the Tanium Console and Tanium Server.

Tanium Asset can obtain a complete and up-to-date view of the enterprise inventory. An asset is any endpoint, such as a computer, server, or virtual machine, that is managed by a Tanium Client. The inventory is an aggregation of live asset data with the most recent data from offline assets. Build reports to show an overview of all assets or drill down into specific endpoints or users.

Tanium Comply evaluates endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks. Complete results on demand and comprehensive, enterprise-wide results can help reduce an organization's overall risk, improve security hygiene, and simplify preparation for industry compliance audits such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX). Comply uses Security Content Automation Protocol-compliant content, such as standards published by DISA or the Center for Internet Security (CIS), to evaluate operating systems and applications for configuration of password policies, file permissions, and other components. Comply supports Windows, macOS, Linux, AIX, and Solaris endpoints.

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. Connect includes templates for many common SIEM tools, file, log, and email formats. Use these templates to integrate with configuration management databases, trouble ticketing systems, and proprietary IT systems.

Tanium Deploy is a software management module that can rapidly install, update, and remove software across large organizations with minimal infrastructure requirements. Create deployments to run during a maintenance window that is convenient for the organization’s IT operations, or deploy applications or a group of applications to a flexible set of targets, including computer groups, user groups, departments, locations, individual computers, and individual users. Update existing software installation to the latest available versions, and create custom packages to install, update, and remove applications.

Tanium Discover finds and maintains an inventory of interfaces. Install the Tanium Client on the organization’s endpoints to actively scan and monitor the local subnet or other defined network segments, detecting unmanaged interfaces. Interfaces are unique media access control (MAC) addresses. An endpoint with multiple network interface controllers displays as multiple interfaces in Discover. “Managed interfaces” are on endpoints that have the Tanium Client running and are managed by Tanium. “Unmanaged interfaces” are on the network but do not have the Tanium Client running. Discover provides real-time information about unmanaged interfaces on the network.

Tanium Enforce enables unified endpoint management and security by providing centralized policy management across operating system, application, and security for Windows, Linux, and macOS environments regardless of the device location—on-premise, remote, or cloud. Use Impact to understand administrative rights in the AD environment for the organization and the potential impact if a compromise occurs. Manage lateral movement impact by identifying,

prioritizing, and remediating access rights and dependencies to reduce attack surface, prioritize actions, and scope incidents.

Tanium Integrity Monitor simplifies regulatory compliance by consolidating tools and accomplishing the following tasks:

- Continuously monitor critical operating system, application, and log files, as well as critical Windows registry paths.
- Deploy continuous monitoring for common or new attack vectors to any dynamic group of computers or across the enterprise.
- Go from alert to active investigation using other modules on the Tanium platform. Automatically send emails to open incidents for suspicious events in incident response systems with Tanium Connect.
- Automatically identify approved events based on change requests or tasks by integrating with ServiceNow Change Management.
- Automatically send events to SIEM solutions; Security Orchestration, Automation and Response (SOAR) solutions; and other data lakes or log solutions for analysis and auditing with Connect.

Tanium Map identifies the components of applications and services and provides a view of relationships between the applications and the endpoints on which they are running. With this knowledge, organizations can make applications more resilient and know the impact before taking endpoints down for maintenance.

Tanium Patch manages operating system patching across the enterprise at the speed and scale of Tanium. Deploy a single patch to a computer group immediately or perform more complex tasks, such as using advanced rule sets and maintenance windows to deliver groups of patches across the environment at specified times. Define custom workflows and schedule patches based on rules or exceptions built around patch lists, block lists, and maintenance windows. For example, the organization might always apply critical Microsoft patches to all machines except for datacenter servers, always exclude .NET patches, or install patches during nonworking hours. Patch generates in-depth reports and returns current patch applicability results from every endpoint. For any patch or patch list deployment, the following details are provided:

- The patch details, such as severity, release date, applicable common vulnerabilities and exposures (CVE), files, and links to knowledge base articles.
- The status of the patch, split out by computer group.
- The assigned patch lists or block lists for the patch.

Tanium Performance monitors, investigates, and remediates endpoint performance problems. Configure profiles to define events for specified computer groups. Define event rules to monitor critical metrics related to hardware resource consumption, application health, and system health. Visualize the problems that have occurred across the environment and the commonalities between them on the Events page. Proactively resolving these problems can improve end-user productivity. To troubleshoot an issue with a single endpoint, use Tanium Direct Connect, which

provides live and historical process-level data from a single endpoint. Use this data to troubleshoot or understand the impact of software and hardware changes on performance.

Tanium Reveal detects sensitive unstructured data at rest on endpoints across an entire IT environment. Use Reveal to continuously monitor for artifacts that match patterns. When sensitive content that matches a pattern is discovered, label the files where the content exists and further analyze or act on them to address regulatory compliance, information security, or data privacy issues.

Tanium Risk provides real-time data, automation, and intelligence to facilitate faster informed decision making with a comprehensive assessment of endpoint risk. Use this data to prioritize actions with intelligent risk scoring based on operational and security metrics. Risk provides reports to communicate key trends, improvements and industry benchmarks for executive and board-level reporting. Using Risk to continuously monitor endpoints can improve compliance and risk posture.

Tanium Threat Response expedites incident response actions from hours or days to minutes. Detect, react, and recover quickly from attacks and the resulting business disruptions.

- **Detection**: Threat Response monitors activity in real time and generates alerts when potential malicious behavior is detected. Configure threat intelligence from a variety of reputable sources and then use this information to search endpoints for known indicators of compromise and perform reputation analysis. The reputation data that Threat Response uses constantly compares activity, such as all processes run, autorun-related files, and loaded modules, against known malicious hashes defined by user hash lists or other services such as Palo Alto Wildfire, VirusTotal, and ReversingLabs.
- **Investigation**: Threat Response continuously records key system activity for forensic and historical analysis. Look for specific activity across every endpoint in an enterprise and drill down into process and user activity on individual systems in both real-time and historical views.
- **Containment**: Threat Response includes sensors and packages that provide endpoint visibility and remediation. With the sensors, search endpoint data quickly for evidence of compromise. Upon discovery of compromised endpoints, use Threat Response packages to isolate incidents and prevent additional compromise, data leakage, and lateral movement.

Tanium Trends allows users to visualize, understand, and communicate trends and correlations of endpoint security and operational health data. Trends gives visibility into the history of key pieces of information about the enterprise IT estate, coordination with real-time status for those indicators, and the ability to close the loop by deploying necessary action on any endpoint—all without leaving the Tanium Console session.

4. GENERAL SECURITY REQUIREMENTS

4.1 Security Posture of Tanium Platform

Because every implementation of Tanium will have its own nuances, this 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 platforms. The appropriate STIGs must be applied for the browser, 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, it does not outline how to package an update and deploy it to the clients. However, it does 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 and clients, many of the client requirements can be accomplished on the Tanium server itself, via the console, by asking questions of the clients.