Tanium

Tanium contains 45 modules. These 9 are first modules that you will interact with when you first enter the dashboard.

Interact	Asset	Benchmark
Comply	Deploy	Discover
Patch	Performance	Trends

Interact

"Perform fundamental functions such as asking questions, consuming data, and deploying actions across your enterprise."

Overview

This module is simple and straightforward. This page starts at the first step into a deep dive of information and allows you to choose how to interact with it. It is organized in a filtered manner based what is important to you. By clicking one item these three categories, associated results will appear.

Dashboard

- **Ask a Question**
  You can query your search by machine, OS, IP, etc., that will provide results for

the information you are looking for. Results provided are based on the question asked.

- **Categories**
  This section currently contains 8 categories. It is separated based on IT Asset Management, Security, Operational Efficiency, and Virtualization Management.
  - **IT Asset Management**: Categories like Application License Management and Inventory focus on managing and tracking software licenses and hardware assets within the organization.
  - **Security**: Anti-Virus, Security, and SSL Server Audit categories are centered on maintaining the security posture of the organization, ensuring that systems are protected against threats and vulnerabilities.
  - **Operational Efficiency**: Client Service Hardening and Operations categories aim to improve the performance and reliability of IT services, ensuring that systems are configured correctly and operating optimally.
  - **Virtualization Management**: VMware Guest Info specifically pertains to managing virtualized environments, which is increasingly relevant in modern IT infrastructures.
- **Dashboards**
  Currently there are 42 dashboards are organized around several key themes related to IT management, security, performance monitoring, and compliance. These dashboards provide a comprehensive view of the IT environment, enabling teams to monitor, manage, and secure their assets effectively. Here's how they can be categorized:
  - **Software Management**: Dashboards like Adobe Software, Microsoft Software, and Application Visibility focus on tracking software usage, ensuring compliance with licensing, and monitoring the visibility of applications across the organization.
  - **Application and System Performance**: Dashboards such as Application Usage by Month, Application Usage the Month, and Client Core Health provide insights into application performance and client health, allowing for proactive management of IT resources.

- **Security Monitoring**: Many dashboards, including Proactive Security, Proactive User Security, and Meltdown-Spectre Vulns Status, are dedicated to monitoring security vulnerabilities, ensuring that systems are protected against known threats.
- **Hardware and Inventory Management**: Dashboards like Computer Hardware Health, Hardware Inventory, and Network Hardware Inventory focus on tracking physical assets and their health status, which is crucial for effective IT asset management.
- **Configuration and Compliance**: Dashboards such as Client Configuration, Set Client Directory Permissions, and SSL Server Audit (various versions) are aimed at ensuring that systems are configured correctly and comply with security standards.
- **Virtualization Management**: Dashboards like VMware Guest CPU and Memory, VMware Guest Time Information, and VMware Guest Tools Versions and Upgrades are specifically tailored to manage and monitor virtualized environments.
- **Network Security**: Dashboards such as Proactive Network Security and Wireless Network Security focus on monitoring and managing network security issues.
- **Incident Management**: Dashboards like Crashes and System Crashes provide insights into incidents affecting system performance, allowing for timely troubleshooting and resolution.

- **Saved Questions**
  It started with GET to organize the information before deep diving. This includes OS, Platforms, hardware, etc.

  A question can be saved for future use or easier retrieval. It can be set by:

  - Name
  - Visibility
  - Merge
  - Associated Packages
  - Content Set
  - Reissue
  - Non-Countdown
  - Tag
  - Drill Down
  - Just for you

Asset

“Get a complete view of your enterprise inventory by aggregating live asset data with recent from offline assets.”

Overview

The Assets dashboard in Tanium provides a comprehensive overview of the resources owned by the company, facilitating effective asset management and security monitoring. This dashboard enables users to assess the network's vulnerability and usage patterns, offering insights into the overall health and intensity of network operations. Within the Reports section, assets are categorized into multiple classifications, allowing users to gain deeper insights into their performance and status. Additionally, the Health section, located at the bottom of the dashboard, displays real-time spikes and trends over a specified time period, enabling continuous monitoring of the network's health while Tanium operates in the background to manage monitoring and deployments effectively.

Types of Reports

The types of Tanium Assets Reports you listed can be categorized into several key areas, each focusing on different aspects of asset management and usage within an organization. They are meant to provide a comprehensive view to enable effective IT resource management and strategic decision-making. Here’s a summary of each category:

1. **Asset Age Reports**:
    - **Age of Assets**: Provides insights into the age of various assets within the organization, helping to identify older systems that may require upgrades or replacements.
    - **Age of Assets for Lost Devices**: Focuses on the age of assets that have been marked as lost, which can help in asset recovery efforts.
    - **Age of Assets for New Devices**: Highlights newly acquired devices, assisting in tracking the integration of new assets into the organization.
2. **Software Inventory Reports**:

- **All Adobe Software**: Lists all Adobe products installed across the organization, useful for license management and compliance.
- **All Microsoft Software**: Similar to the Adobe report but focuses on Microsoft products, helping to manage software licenses and usage.
- **All Software**: A comprehensive report that includes all software applications installed, providing a complete view of software assets.
- **All Short-lived Assets**: Identifies assets that have been in use for a short duration, which can indicate temporary deployments or testing environments.

3. **User and Endpoint Reports**:
   - **All Users**: Provides a list of all users within the organization, which can be useful for user management and access control.
   - **Physical Machine Summary**: Summarizes the status and health of physical machines in the organization, helping to monitor hardware performance.
   - **Virtual Machine Summary**: Similar to the physical machine report but focuses on virtual machines, providing insights into the virtual environment.
4. **Software Installation and Usage Reports**:
   - **SIU Endpoints**: Reports on endpoints that have Software Inventory Usage (SIU) enabled, helping to track software usage across devices.
   - **SIU Installed Products**: Lists products installed on SIU-enabled endpoints, assisting in software management.
   - **SIU Product Last Used**: Provides information on when specific products were last used, which can help in identifying unused or underutilized software.
   - **SIU Product Usage**: Offers insights into how frequently different products are used, aiding in software optimization and license management.
5. **Support and Summary Reports**:

- **Tanium Support**: This report likely provides insights into the support status or issues related to Tanium itself, helping in troubleshooting and support management.

Custom Reports

Custom reports based on preference or need can be created based on any existing report. User-based reports from scratch can also be made based on data collected by Asset to show departments, locations, user groups, or other attributes needed.

Benchmark

"Assess the overall risk posture of managed endpoints in your environment, prioritize actions, and remediate issues using the Tanium platform."

Overview

Its purpose is to help organizations understand their security program's state compared to other Tanium Cloud customer, facilitating executive reporting on trends and compliance improvements. In doing so, data is collected to provide benchmark metrics. The metrics are aggregated and anonymized from Tanium Cloud customers, allowing for comparisons against industry benchmarks.

Key Features

1. **Benchmark Metrics**:
    - Metrics are presented as percentile values over time.
    - Percentile Distribution charts show your current percentile against the overall Tanium customer distribution.
    - Percentile Over Time charts illustrate trends in metrics over selected periods.
2. **Risk Score**:
    - Tanium Risk Score 2.0 provides a numerical score (1-1000) indicating overall enterprise risk, with lower scores representing lower risk.
    - Requires Tanium Impact and Tanium Comply for viewing.
    - Scores are categorized into low, medium, high, or critical ranges.

3. **Vulnerability Evaluation**:
    - Evaluates vulnerabilities in the environment, providing impact and priority scores based on CVSS scores and endpoint criticality.
4. **Risk Assessment**:
    - A report detailing operational and security risks, targeted at executives, with options for executive summaries or detailed reports.
    - Can be exported in JSON or HTML formats.
5. **Autonomous Endpoint Management (AEM)**:
    - Provides real-time intelligence and generates notifications related to risk score and benchmark metric changes.
6. **Interoperability**:
    - Works with other Tanium products (Comply, Criticality, Guide, Impact) to enhance risk score calculations and provide comprehensive insights.

To maximize the value delivered by Tanium Benchmark, organizations should focus on four key steps related to governance. First, it is essential to develop a tailored change management process specifically for risk management. This process should align Service Level Agreements (SLAs) with the activities of IT Security, IT Operations, and IT Risk and Compliance. Additionally, organizations need to identify internal and external dependencies that impact their risk management processes, designate maintenance windows for various risk scenarios, and establish a Tanium Steering Group (TSG) to expedite reviews and approvals.

Defining distinct roles and responsibilities is another critical step, which can be achieved through the use of a RACI chart. This chart outlines the responsibilities of IT Security, IT Operations, IT Risk/Compliance teams, and Executives in relation to key tasks such as endpoint coverage, monitoring risk scores, and identifying business-critical endpoints. By clarifying these roles, organizations can ensure effective collaboration and accountability among teams.

Tracking operational maturity is vital for the successful management of a risk management program. Organizations should measure the operational maturity of

their Tanium Benchmark program through four key processes: Usage, Automation, Functional Integration, and Reporting. This approach allows for a comprehensive assessment of how well Tanium Benchmark is being utilized and integrated across various functions.

Cross-functional alignment is crucial for organizations to leverage Tanium as a unified platform. By using Tanium across functional silos, teams can ensure they are acting on a common set of data, which enhances decision-making and improves risk management. Without this alignment, teams may waste time disputing data quality instead of focusing on risk mitigation.

To assess the maturity of the Tanium Benchmark program, organizations can evaluate key metrics, including Executive Metrics, Risk Score, and the percentage of optimal endpoints. These metrics provide insights into the percentage of endpoints with risk metric scores calculated within the last 30 days, the overall risk level of the enterprise, and the proportion of endpoints reporting optimal risk coverage.

Finally, organizations should understand the five levels of maturity for Tanium Benchmark, ranging from Level 1 (Initializing), where no dependent modules are configured, to Level 5 (Optimized), where all modules are configured and endpoint criticality is fully set. Assessing these maturity levels helps organizations identify areas for improvement and ensure they are effectively managing their risk posture. By focusing on risk coverage, lowering risk scores, and maintaining optimal states for endpoints, organizations can gain a comprehensive understanding of their risk landscape and enhance their overall compliance and security posture.

- **Levels of Maturity** (1-5):
  - Level 1: Initializing - No dependent modules configured.
  - Level 2: Progressing - Core content and Comply configured.
  - Level 3: Intermediate - Core content, Comply, and one additional module configured.
  - Level 4: Mature - Core content, Comply, Impact, and Reveal configured.
  - Level 5: Optimized - All modules configured and endpoint criticality set.

Comply

“Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.”

Overview

Comply is a tool designed to assess endpoints for security configuration exposures and software vulnerabilities, adhering to industry standards. It uses SCAP-compliant content to evaluate various operating systems and applications, enhancing security hygiene and simplifying compliance audits.

▼ Key Features

- **Remediation Visibility**: Integrates with Tanium Patch for vulnerability scanning and patching in a unified workflow.
- **Interoperability**: Works with other Tanium products like Tanium Connect, Direct Connect, Discover, and Patch for comprehensive reporting and scanning capabilities.
- **Organizational Governance**: Emphasizes the importance of a dedicated change management process, defining roles, validating cross-functional alignment, and tracking operational maturity through metrics.

▼ Operational Maturity:

- Organizations should measure the effectiveness of Comply through process metrics (usage, automation, integration, reporting) and standards metrics (coverage, vulnerability findings).

▼ Vulnerability Levels:

- High: At least one high vulnerability found.
- Medium: No high vulnerabilities, but at least one medium vulnerability detected.
- Low: No high or medium vulnerabilities, but at least one low vulnerability present.
- Not scanned: Endpoint has not been scanned in the last 30 days.

▼ Maturity Levels:

- Ranges from Level 1 (Initializing) to Level 5 (Optimized), indicating the degree of operationalization and integration of Tanium Comply within an

organization.

What is SCAP?

SCAP, or the Security Content Automation Protocol, is a framework used to enable automated vulnerability management, measurement, and compliance evaluation. In relation to Tanium, SCAP-compliant content is utilized within Tanium Comply to assess endpoints for security configuration and software vulnerabilities. This protocol enhances the functionality of Comply by ensuring that assessments are based on recognized security standards, thereby improving the effectiveness of vulnerability management efforts.

Key points about SCAP in the context of Tanium include:

1. **Standardization**: SCAP provides a standardized approach to security automation, allowing Tanium Comply to evaluate operating systems and applications against widely accepted security standards.
2. **Content Sources**: Tanium Comply leverages SCAP content from recognized organizations such as the Defense Information Systems Administration (DISA) and the Center for Internet Security (CIS) to perform assessments.
3. **Assessment Capabilities**: By using SCAP-compliant checks, Tanium Comply can evaluate various security configurations, such as password policies and file permissions, across multiple operating systems, including Windows, macOS, Linux, AIX, and Solaris.
4. **Compliance and Risk Management**: SCAP helps organizations reduce risk and improve compliance with industry regulations by providing a structured method for identifying security vulnerabilities and configuration issues.

Dashboard

▼ Quick Links

- Assessments
  A comprehensive analysis of endpoints across workstations categorized by operating system (OS) and their viability. The assessments are conducted over a specified timeframe to ensure consistency, following a pre-programmed schedule.

- Compliance Findings
  This page provides insights into the strengths of the network by presenting compliance and vulnerability information, which helps enhance overall network security. Users can filter the results based on their specific needs to gain tailored insights.
    - Compliance
      The compliance page enables users to filter data according to the servers and operating systems in use. Results can be categorized based on compliance status, allowing users to easily distinguish between endpoints that have passed or failed the assessments.
    - Vulnerability
      The Vulnerability Page allows users to filter data based on the server and operating system. The results are categorized by specific issues, such as the need for updates, checks, or removals, and are classified by severity levels ranging from Low to Critical. Additionally, vulnerabilities that fall outside compliance are marked as Unscored.
- Remediations
  Servers with Common Vulnerabilities and Exposures(CVE) identified by unique identifiers for a specific vulnerability, along with a brief description and references to related information. The information included are Knowledge Based articles(KB) which updates and enhancements and support resources, files that are affected, the source of the update files and what lists the patch would fall under. Not all patches are accepted and will be displayed which Block lists they maybe on.
- Reports
  The Reports page features a comprehensive table that categorizes various types of reporting conducted within the network by subject matter. This table presents relevant information clearly and concisely, filtering out unnecessary data to enhance usability. Users can easily access key metrics, trends, and compliance statuses, enabling informed decision-making and effective monitoring of network security. Additionally, the reports can be customized based on user preferences, allowing for tailored insights that align with specific organizational needs.

▼ Summary

- Compliance Exposures
  Displays a graph on the compliance of the endpoints and where improvements are needed.
    - Findings
      Same as Compliance Findings
- Vulnerability Findings
  Same as Vulnerability

▼ Activity

Check and tests made by Tanium throughout a particular time and those results in the form of “Assessments” and “Vulnerability Updates”.

▼ Assessments

Same as Assessments

Deploy

“Install, update, or remove software on a flexible set of targets.”

Overview

The Deploy module is an overview that allows for software management with minimal infrastructure requirements. Applications & maintenance windows can be set to update existing software that are in need of remediation.

Deploy Page

It a summary dashboard of information about the network by operating platform, current software, and health of the endpoints running them. It also contains information on software that has had deployments and its schedule. This software can also be tested prior to ensure safety of the updated software.

Ask a Question

You can query your search by machine, OS, IP, etc., that will provide results for the information you are looking for. Results provided are based on the question asked.

Deploy Action: To enter page to deploy

🚜 Administration > Actions > Actions History > **Deploy Actions**

▼ Deployment Package

1. **Client Configuration and Support**: These packages provide the necessary configurations and support for various operating systems.
    - **AIX, Linux, Solaris, Windows**: Specific configurations tailored to each OS to ensure compatibility and optimal performance.
2. **Client Management**:
    - **Installer Cache**: Stores installation files for quick access during client deployment.
    - **Manifest**: A file that contains metadata about the installed clients and their configurations.
    - **Manifest Installer Cache**: Combines the manifest with cached installer files for efficient deployment.
    - **Upgrade [Non-Windows/Windows]**: Packages that facilitate the upgrade process for Tanium clients across different operating systems.
3. **Deploy**:
    - **Clean up Deploy Files**: Removes unnecessary deployment files to free up space and maintain system cleanliness.
    - **Set Logging Options [Linux/Mac/Windows]**: Configures logging settings for deployment processes across various platforms.
    - **Software Catalog Collection**: Gathers information about software installed on endpoints for inventory management.
    - **Software Package Catalog Icons**: Provides icons for software packages in the catalog for easier identification.
    - **Software Package Gallery**: A visual representation of available software packages that can be deployed.
    - **Unenforce Maintenance Window 1 Group 1 [Mac/Linux]/[Windows]**: Allows for the disabling of maintenance windows for specific groups, providing flexibility in deployment timing.
4. **Direct Connect**:
    - **Open Session- Linux/Mac/Windows**: Facilitates direct connections to endpoints for management and troubleshooting.

5. **End-User Notifications**:
    - **Profile 1 File Cache**: Caches notifications for end-users.
    - **Register Configuration Trigger**: Sets up triggers for configuration updates.
    - **Set Logging Options**: Configures logging for end-user notifications.
6. **Endpoint Configuration**:
    - Various options to enable or disable client extensions, shared process modes, and tools across different operating systems, ensuring that the client operates according to organizational policies.
    - **Reinstall Tool, Reset Components, Restart Client Extensions, Unblock Tool, Uninstall Tool**: Manage the lifecycle and configuration of the Tanium client.
7. **Endpoint Tooling Cache**:
    - **Deploy, Direct Connect, End-User Notifications, Software Management**: Caches tools and configurations necessary for endpoint management.
8. **Endpoint Tooling Data Cache**:
    - Similar to the tooling cache but focuses on data necessary for deployment and management processes.
9. **SPGI Packages**:
    - **RH7 Inplace Upgrade Script Log File Removal from Client**: Manages log files during the upgrade process for Red Hat 7 clients.
    - **RH7 Inplace Upgrade Tattoo File for Client Upgrade to RH8**: Handles tattoo files that are essential for upgrading clients from Red Hat 7 to Red Hat 8.
    - **Update UniversalForwarder Config**: Updates configurations for the Universal Forwarder, which is used to collect and forward log data.

▼ Action Details

- Name

- Description: Describing what the intent of the action is for
    - Best Practice: Summarize key points from the vulnerability report for record keeping

▼ Deployment Schedule

- User input of when the action should take place. It can send at a specific time (**Start At**) or if it is large, over time (**Distribute Over**)

▼ Targeting Criteria

The “Target Question” displays the questions/criteria of computers that meets the conditions. “Show Preview To Continue” lists the affected computers before taking actions.

▼ Deployment Plan

With “Enable Ring Deployment” you can see the progress of the deployment throughout the phases to completion.

> Click “**Deloy Action**” once all steps are complete and to rectify Tanium vulnerabilities

Maintenance

Once the software has been deployed, you can view what operations has been successful by category. This will allow you to view these activities by targeted endpoint. To perform maintenance this will be in the Trend Boards. In the case the Deploy require troubleshoot or changes, that info can be viewed here [Troubleshooting Deploy](#).

Predefined Package Gallery

The Predefined Page Gallery in Tanium provides a comprehensive view of the current software installed on all endpoints, organized by vendor. This functionality includes key attributes such as:

- **Version**: The specific version of the software installed on each endpoint.
- **Eligible Devices**: A list of devices that are eligible for the software installation.

- **Last Installed Date**: The date when the software was last installed on the respective endpoint.

Additionally, the Predefined Page Gallery features various filters that enable users to perform specific searches, ensuring that relevant data can be accessed efficiently.

Predefined package Gallery Entry

🚜 Deploy > Software > **{Entry}**

Upon selecting an entry within the Predefined Package Gallery, users are presented with a detailed summary of the specific software. This summary includes critical information that affects network management, such as package size, architecture, and origin of the program. The Package Size is the total size of the software package, which is important for assessing bandwidth and storage requirements. The architecture of the software (e.g., x86, x64), which is essential for compatibility with endpoint devices. Origin of the Program is Information regarding the source or publisher of the software, aiding in trust and verification processes.

Discover

The Discover page in Tanium Performance provides a comprehensive overview for monitoring, investigating, and remediating performance issues on endpoints managed by the Tanium Client. Users can configure profiles to define specific events for designated computer groups, allowing for effective tracking of critical metrics related to hardware resource consumption, application health, and overall system health.

Key features include:

1. **Event Monitoring**: Users can set event rules to monitor various performance metrics, such as CPU usage, available memory, disk capacity, and application crashes. Events are generated when specific conditions are met, and performance data is collected every 15 seconds for 15 days.
2. **Event Analysis**: The Events page visualizes performance problems across the environment, helping identify common issues and their impact on end-user

productivity. Users can analyze historical and live data to troubleshoot specific endpoints using Tanium Direct Connect.

3. **Performance Scoring**: Performance scores are calculated for each endpoint based on the occurrence of events, providing a percentage score that indicates endpoint health. Scores range from 1 to 100, with higher scores reflecting better performance. Users can customize the weighting of event categories to align with organizational priorities.
4. **Alerts and Interoperability**: Alerts can be enabled for event rules, notifying users when thresholds are met. The Discover page integrates with other Tanium products for enhanced reporting and data export capabilities.

Interfaces

The Discover page provides insights into the manufacturer of devices and assesses whether they are being appropriately managed. In addition to the IP address, devices can be uniquely identified by their MAC address. When a user clicks on a specific result, detailed information is displayed, including the management status of the device and the last time it was online. This functionality allows users to monitor device health and connectivity, ensuring effective management and oversight of all endpoints within the network.

On the Discover page, the results are separated by Metrics and Interfaces.

Activity

Check and tests made by Tanium throughout a particular time and those results through imports, recent & import

Patch

“Minimize critical security vulnerabilities by automating patch delivery”

Overview

The Tanium Patch module is an essential tool for managing operating system patching across enterprises with the speed and scale that Tanium offers. This module provides comprehensive insights into the patches that have been deployed within the network, their current status, and compliance levels—critical factors in mitigating potential vulnerabilities.

With the Patch module, users can quickly identify whether a patch is compliant or not, enabling proactive measures to be taken to safeguard network health. The module supports both Windows and Linux endpoints, allowing for immediate deployment of patches to specific computer groups. Additionally, it facilitates more complex patch management tasks, such as scheduling groups of patches for deployment at designated times, using advanced rule sets and maintenance windows.

Regular scans conducted by Tanium ensure that endpoints remain updated and compliant, providing detailed reports on patch applicability and status. For Windows and Linux systems, the Patch module delivers essential details including severity, release dates, applicable Common Vulnerabilities and Exposures (CVEs), and links to relevant knowledge base articles. For macOS endpoints, updates are managed through Apple MDM commands, ensuring seamless integration and compliance.

The Patch Overview page features summary and health charts that monitor compliance specifically for Windows and Linux endpoints, allowing IT administrators to visualize the patch status across their environment. The module also includes the ability to define custom workflows for patch deployment based on specific rules or exceptions, ensuring that critical patches are consistently applied while managing exceptions for sensitive systems.

In summary, Tanium Patch empowers organizations to maintain a robust patch management strategy, significantly reducing the risk of vulnerabilities and enhancing overall network security.

List of available patches

In the **Configuring Patch,** section “Default Settings” contains a list of available patches by OS that can be imported into Tanium.

Performance

“Monitor, investigate, and remediate endpoint performance issues.”

Overview

The Tanium Performance page is a vital tool for monitoring and analyzing the health of workstations and network performance. It enables users to identify and investigate specific issues such as crashes, high CPU usage, and memory

consumption across managed endpoints. By configuring profiles, users can define event rules that track critical metrics related to hardware and application health, allowing for proactive resolution of performance problems. The Events page provides visual insights into common issues, while the Performance scores offer a comprehensive view of endpoint health, helping to enhance end-user productivity. With Tanium™ Direct Connect, users can access real-time and historical data to troubleshoot individual endpoints effectively, ensuring that any performance concerns are addressed promptly to maintain optimal operational efficiency.

Dashboards

- **Alerts**

  This page allows users to manage alerts generated by performance event rules. When alerts are enabled for each event rule type in a profile, an alert monitor is created. Users can view specific alerts triggered by targeted endpoints that meet the defined thresholds, facilitating timely responses to performance issues.

- **Application Monitoring**

  This section focuses on monitoring the performance of applications running on endpoints. It helps users track application health, detect crashes, and identify resource consumption patterns, allowing for better management of application-related performance issues and enhancing the overall user experience.

- **Boot Time**

  The Boot Time page provides insights into the startup duration of endpoints. It allows users to analyze boot performance, identify devices with prolonged boot times, and troubleshoot potential issues that may be affecting the efficiency of endpoint startups.

- **Direct Connect**

  This feature enables users to connect directly to endpoints to view live and historical process-level data. It is particularly useful for troubleshooting specific performance issues by providing detailed insights into resource usage and application behavior on individual machines.

- **Events**

The Events page visualizes performance issues that have occurred within the environment. Users can see a high-level overview of events and drill down to specific endpoints that experienced issues, such as low memory or high CPU usage, aiding in the identification and resolution of problems.

- **Logon Time**

  This page focuses on monitoring the duration of user logon processes on endpoints. It helps identify slow logon times, allowing IT teams to investigate potential causes and optimize the logon experience for users.

- **Performance Store**

  The Performance Store is a local data repository that collects and stores performance data from endpoints. Data is gathered every 15 seconds and retained for 15 days, providing a historical context for analyzing events and performance trends over time.

- **Profiles**:

  Profiles allow users to define event rules for specified computer groups. Each profile can target specific endpoints and set conditions for when events are generated, enabling tailored monitoring and management of performance metrics relevant to different groups within the organization.

- **Stream**

  The Stream page allows users to configure streams for selected event types to external destinations like Splunk or ELK. This feature enhances reporting capabilities by enabling the integration of performance data with external analytics tools for further analysis and monitoring.

Trends

"Visualize, understand, and communicate trends and correlations of endpoint security and operational health data."

Overview

The Tanium Trends module, which is deprecated as of March 12, 2025, is being replaced by the Tanium Reporting module, prompting users to migrate their Trends boards to take advantage of advanced reporting features. Designed to provide

insights into key security metrics and operational health, Trends enables users to create visualizations of current and historical endpoint data. Key features include the ability to record metrics from saved questions and Tanium solutions, visualize trends by computer groups, display alerts for threshold breaches, and schedule automatic report deliveries to stakeholders. The module operates on core concepts such as sources, which define data origins (including saved question and module sources), panels for visual data representation, and boards that organize collections of panels. Additionally, Trends integrates with other Tanium products for enhanced reporting capabilities and allows exporting of boards through Tanium Connect. For more details on migration and usage, users can refer to the relevant user guides.