Cisco Tetration Analytics and ServiceNow Solution

Deploy real-time analytics across the enterprise stack for agile IT operations management.

Challenge

Many businesses today are determining how to respond to both the threats and opportunities arising from digitization. They are demanding IT departments that can quickly and flexibly offer the services that best equip a modern workforce. With the continued expansion of IT consumerization, cloud, social, and mobility applications, IT departments are facing many challenges in delivering high-quality and agile IT services to keep up with the increasing pace of change:

- Manual service dependency mapping processes that take weeks to months to complete
- Lack of coordination between infrastructure changes and business services context
- Inefficient and slow service problem diagnostics and troubleshooting
- Lack of visibility into cloud, virtual, and physical infrastructure underlying supported business services
- Time-consuming and complex service policy creation and enforcement processes
Cisco Tetration Analytics and ServiceNow solution

The Cisco Tetration Analytics™ platform uses machine learning, behavior analysis, and visualization to deliver real-time IT infrastructure and operational visibility through continuously updated knowledge of application interactions and dependencies. With this platform, IT operations managers can have pervasive visibility across the entire IT infrastructure and perform application dependency mapping (ADM); automated whitelist policy recommendation and enforcement; policy simulation, impact analysis, and compliance management; and service data flow forensics.

ServiceNow provides an enterprise service management suite with applications for service management, business management, and IT operations management (ITOM). ServiceWatch, part of the ServiceNow ITOM suite, provides critical service modeling capabilities, including service and application discovery; service dependency mapping through a configuration management database (CMDB); and visibility into increasingly complex IT infrastructure across server, storage, and network resources.

Application Dependency Mapping Use Case

The solution creates and maintains a single true record of all service configurable items by using continuous two-way updates (Figure 1). Infrastructure constructs specific to the Cisco Tetration Analytics platform are imported into the ServiceNow CMDB, enhancing ServiceNow discovery with ground-truth network insights. This information is correlated with service definitions, creating true visibility into the service infrastructure at the ITOM layer.

In addition, ServiceNow CMDB service definitions are imported into the Cisco Tetration Analytics configuration data, synchronizing Cisco Tetration Analytics application dependency mappings with ServiceWatch service dependency mappings and building Cisco Tetration Analytics mappings using ServiceNow mappings as the starting point (Figure 2).
The solution provides complete stack service dependency mapping: from the application to the infrastructure, network, and host. This feature allows IT operations staff to start with a business service and accurately identify the network constructs that enable this specific business service. The Cisco Tetration Analytics platform notifies ServiceNow about high-quality infrastructure events with correlated service context for fast troubleshooting and resolution of performance problems. Through closed-loop machine-learning algorithms and automated behavior analysis provided by the Cisco® platform, the solution tracks baseline business service flows in compliance with policies and detects locations where any deviations from the baseline occur, providing automated policy enforcement.

ServiceNow provides its prebuilt dashboards and user interface elements within the Cisco Tetration Analytics user interface. This approach enhances the Cisco Tetration Analytics user interface with better context information for machine learning and event data: services mappings, change history, etc. At the same time, IT operations staff can access through the ServiceNow user interface all prebuilt Cisco Tetration Analytics dashboards and reports for visibility into network insights (Figure 3).

**Endpoint Visibility and Service Discovery Use Case**

Using this Service discovery feature, all the endpoints discovered by Tetration Analytics Cluster are pulled into ServiceNow and mapped to the CI table, if the endpoints are not already discovered and stored in ServiceNow. This process enriches the ServiceNow CMDB. This feature also helps customers, by giving them visibility to the entire infrastructure, viewed as a single source of truth for all the endpoints in the data center from within ServiceNow.

Cisco Tetration Analytics uses a representational state transfer (REST) API to import CMDB user-defined information. It uses this information to provide annotated tags to make discovery and search operations user friendly, with a natural-language feel.

![Cisco Tetration Analytics Dashboard within the ServiceNow Dashboard](image)
Security and Monitoring Use Case

By using ServiceWatch ITOM software from ServiceNow, IT and security operations teams can trigger automatic patching and configuration changes for security infrastructure as well as other standard workflows to contain and fix security incidents and vulnerabilities.

For IT operations, the Cisco Tetration Analytics platform first establishes a baseline behavior for applications across all computing, storage, and networking tiers that make up business services. It then alerts ServiceWatch in real time for dashboard reporting and remediation for any service behavior deviations and anomalies detected. Cisco Tetration Analytics detection of application anomalies that may affect business enables fast and accurate root-cause analysis and efficient change management through ServiceWatch.

In addition, security operations teams can automatically add Cisco Tetration Analytics threat and anomaly intelligence to ServiceNow security incidents to accelerate remediation of security breaches and reduce the amount of time spent on basic tasks with orchestration tools. The solution enables teams to view the current security posture with customizable dashboards and reports backed by quantitative data. This solution also improves processes and team performance through metrics and post-incident reviews, accessed by double-clicking the actionable insights identified by the Cisco Tetration Analytics platform.

Benefits

Cisco Tetration Analytics and ServiceNow together provide these benefits:

- Enhanced service definitions and dependencies with ground-truth network insights across the entire IT infrastructure: physical, virtual, and cloud
- Accurate service-aware view of application communications, interdependencies, and service-affecting anomalies in infrastructure
- Advanced event management and fast troubleshooting through pervasive continuous infrastructure monitoring, proactive service health tracking, and malicious service flow detection
- Increased operational efficiency through automated dynamic service dependency mapping and automated business-context-sensitive policy design and enforcement
- Better service-level agreement (SLA) guarantees through intelligent service workload placement, business service impact assessment, and on-demand policy simulation
- Integrated single-pane ServiceNow user interface for IT operations, with access to all prebuilt Cisco Tetration Analytics dashboards and reports for enhanced visibility and network insights
For More Information

If you are interested in a joint Cisco Tetration Analytics and ServiceNow solution, please contact a representative:

- For more information about ServiceNow, visit http://www.servicenow.com.
- For more information about Cisco Application Centric Infrastructure (Cisco ACI™), visit https://www.cisco.com/go/aci.