Better Together:

Driving Even Greater ROI From ServiceNow With Tanium

One of the questions we hear all the time from Chuco clients is, **"Can you help us with integration between ServiceNow and Tanium?"**

The benefits of integrating ServiceNow with Tanium are so clear, we can't think of a reason you wouldn't want to do it. Relying on siloed data sources increases the risk of inaccurate inventories, visibility gaps, and delays in response times.

Through integration, workflows created in ServiceNow can access accurate, real-time endpoint data from Tanium — regardless of whether the endpoints are physical, virtual, cloud-based, or in the IoT. Better information means more efficient and more effective automation.

So if you're asking whether Chuco can help make this integration a reality in a way that works within a specific timeline and budget, the answer is a resounding **"Yes, absolutely!"**

We'll share an example of how we worked with a Chuco client in improving their ROI from ServiceNow by using Tanium as a unified platform for IT security and operations. We'll also discuss several use cases for integrating Tanium with ServiceNow.

There are several compelling use cases including:

- Enhancing your configuration management database (CMDB) in ServiceNow through real-time updates from Tanium
- Optimizing IT and software asset management
- Further streamlining and automating patch management and compliance
- Implementing security orchestration, automation and response (SOAR)

Self-Service Patching

In a recent client engagement, we worked with a large multinational company that was using legacy tools for patching server operating systems.

Replacing its legacy patching tools with Tanium, and integrating with the ServiceNow CMDB, allowed the organization to automate patch scheduling across all servers.

The integration also allowed the IT organization to standardize patch schedule options across the enterprise, automatically enroll new servers into default schedules, and enable authorized users to manage their own patch schedules as needed.

Server owners are now able to manage their own patching configurations. The "self-service" model means that they can easily choose the relevant servers, as well as when and where to patch them.

Once their requests are saved, the workflow automatically updates tables in ServiceNow and makes bulk updates directly into Tanium.

Admins no longer have to move data back and forth. Where admins had to handle thousands of requests previously, they now only have to deal with approximately 20 requests for the same amount of data.

The validation system tracks all requests and detects when Tanium and ServiceNow are in sync, and flags instances where they are not. The system can also be configured to trigger a custom reboot process, which notifies users at specified intervals.

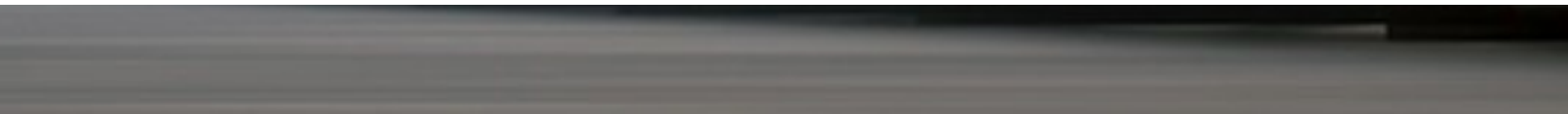
The system can also be configured so that only servers with the correct tags are patched. Every machine can have a tag and can be more than one-dimensional. For example, in addition to their status (production, QA, test, etc.), they can be grouped by location within separate columns (building, room, city/state, zip code).

Other Use Cases

Another use case clients often ask about is security incident creation.

When the Tanium Endpoint Security platform is integrated with the ServiceNow Security Incident Response (SIR) product, SecOps analysts can run queries about their assets in the Tanium console based on security event information found in SIR.

After your environment is scanned and potential cyber threats and compromises are identified, a security incident is created, already populated with the enriched configuration item (CI) data that has been gathered. These processes can be triggered automatically, based on profiles you have created in the Now Platform instance containing Tanium



capabilities. The net result is an efficient and effective strategy for endpoint detection and response (EDR) and protecting your assets.

Looking beyond the CMDB, which pulls technical information about each machine, integration between Tanium and ServiceNow Asset Management allows you to consolidate financial information about licenses and warranties for every endpoint in your global IT estate.

Next Steps

Here are additional links to Tanium content on ServiceNow integration, including a recent case study with Honeywell which Chuco also contributed to.

As discussed, there are many opportunities to get more out of ServiceNow and Tanium through integration. We're happy to share other use cases, and are also happy to talk through various strategies for which aspects make sense to prioritize for your particular IT and business environment.

- How Honeywell automates server patching ServiceNow + Tanium: https://www.tanium.com/resources/honeywell-automates-server-patching-with-servicenow-and-tanium

- Security incident creation – Tanium integration v2: https://docs.servicenow.com/en-US/bundle/sandiego-security-management/page/product/secops-integration-taniumv2/concept/taniumv2-overview.html

Ready to Learn More?

Please feel free to get in touch to learn how Chuco can help you integrate Tanium and ServiceNow at your organization: info@chuco.com.