In Partnership with

TANIUM

Improve Visibility and Respond to Security Incidents Faster with Tanium and ServiceNow

The Challenge

As networks continue to grow and expand, visibility becomes increasingly difficult. When responding to threats, up-to-the minute status is necessary. But with a growing number of endpoints, getting the latest information can be a laborious task, requiring the time and effort of multiple people. When investigating an alert, a security analyst often needs to know what processes are running or whether specific files exist on the affected endpoint to determine the presence of malware or possible damage.

ServiceNow has partnered with Tanium to improve visibility and control of endpoints, enabling this valuable information to be collected automatically. Respond to threats quickly by using Tanium's endpoint visibility and control with ServiceNow workflows, automation, and orchestration. Visibility and automation combine to make security response faster and more efficient.

Use Case One

ServiceNow Security Operations receives an alert about possible malware on an endpoint from one of several connected security products, including Tanium. The alert is matched against the ServiceNow configuration management database (CMDB) to provide beneficial context to determine priority of the alert based on business criticality and ownership of the asset.

The alert affects an endpoint that has been classified as a critical asset, so Security Operations automatically creates a security incident. The incident is automatically assigned to responders based on its type and the affected asset. In parallel, it also triggers a workflow that will gather additional information to assist the analyst with remediation. As part of this automated research, a request is sent to Tanium Incident Response to retrieve detailed artifacts from the affected endpoint.

Tanium Incident Response can search for hash values of processes, mutexes, application logs, DLLs, open ports/connections, running services, registry values, and even files "at rest" that are anywhere on disk. The search can be done by name, hash, path, or contents to allow the security analyst to identify and respond to issues faster. This information is collected in seconds and added to the incident record in Security Operations, eliminating the need to switch between multiple applications.

ServiceNow Security Operations also compares observables from the alert, including the source IP address and file hash, against threat intelligence feeds to determine whether the alert is related to known malware. The result populates the Threat Intelligence tab in the incident record, showing the analyst that the observables are related to a recent Trojan. With the necessary information now available in one location, the security analyst can easily see what the malware has done and take steps to contain and eradicate it.

Once the malware has been remediated and the incident closed, a post-incident review with a timeline of all actions is automatically generated. Because ServiceNow tracks all response tasks, data from this incident and others can be used to create reports and dashboards to demonstrate the effectiveness of the security organization.

Running Processes

1 to 100 of 156

Name ▲	Configuration item	Owner	Owner domain	Path	Hash	Source	Created
baretail.exe	wepos01.s043.s-mart.com	Administrator	SECOPS	C:\\Users\\Administrator\\Downloads\\bar...	160D6A3BDC9D64677643376F82E559EB4112289E...	Retrieve Running Processes	2017-01-19 14:14:38
baretail.exe	Tanium-A	Administrator	SECOPS	C:\\Users\\Administrator\\Downloads\\bar...	160D6A3BDC9D64677643376F82E559EB4112289E...	Retrieve Running Processes	2017-01-19 14:25:13
chrome.exe	Tanium-A					Retrieve Running Processes	2017-01-19 14:25:24
cmd.exe	wepos01.s043.s-mart.com	SYSTEM	NT AUTHORITY	C:\\Windows\\SYSTEM32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:14:38
cmd.exe	wepos01.s043.s-mart.com	SYSTEM	NT AUTHORITY	C:\\Windows\\SYSTEM32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:14:38
cmd.exe	Tanium-A	Administrator	SECOPS	C:\\Windows\\system32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:25:13
cmd.exe	wepos01.s043.s-mart.com	SYSTEM	NT AUTHORITY	C:\\Windows\\SYSTEM32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:14:38
cmd.exe	Tanium-A	SYSTEM	NT AUTHORITY	C:\\Windows\\SYSTEM32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:25:13
cmd.exe	wepos01.s043.s-mart.com	SYSTEM	NT AUTHORITY	C:\\Windows\\SYSTEM32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:14:38
cmd.exe	Tanium-A	SYSTEM	NT AUTHORITY	C:\\Windows\\SYSTEM32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:25:13
cmd.exe	wepos01.s043.s-mart.com	Administrator	SECOPS	C:\\Windows\\system32\\cmd.exe	6F88FB88FFB0F1D5465C2826E5B4F523598B1B83...	Retrieve Running Processes	2017-01-19 14:14:38
conhost.exe	wepos01.s043.s-mart.com	SYSTEM	NT AUTHORITY	C:\\Windows\\system32\\conhost.exe	6BD1F5AB9250206AB3836529299055E272ECAA35...	Retrieve Running Processes	2017-01-19 14:14:38

Running processes from Tanium Incident Response are displayed in ServiceNow Security Operations within the security incident for easy reference and action.

Use Case Two

Tanium and ServiceNow have integrated to ease IT remediation in a second way as well. Any saved question or notification within Tanium can be used to generate a new incident within ServiceNow. For instance, if Tanium IOC Detect finds a threat or if a new local administrator account is added on a database server, Tanium could trigger a ServiceNow incident.

Customers are currently using this integration to generate ServiceNow incidents to collect disk utilization on laptops in a specific department and notify IT when an unapproved application has been installed by a user with administrative privileges. Tanium is more than a data collection tool. It can also be used for hunting and communicating with ServiceNow about any action that operations or security teams would need an automated workflow process to address.

Summary

Integrating Tanium and ServiceNow means security analysts can get valuable endpoint data without changing consoles. Incident research can be completed in seconds through a combination of Tanium's immediate visibility and ServiceNow automation. This leads to significant time savings for security analysts, allowing them to focus on analysis and remediation, instead of data collection and administrative tasks. Security response becomes faster and more efficient.

About Tanium

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control, and manage millions of endpoints across the enterprise within seconds. Serving as the "central nervous system" for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current and historical state and execute change as necessary, all within seconds. With the unprecedented speed, scale, and simplicity of Tanium, organizations now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations. Visit us at www.tanium.com or follow us on Twitter at @Tanium.

About ServiceNow

ServiceNow is changing the way people work. With a service-orientation toward the activities, tasks and processes that make up day-to-day work life, we help the modern enterprise operate faster and be more scalable than ever before. Customers use our service model to define, structure, and automate the flow of work, removing dependencies on email and spreadsheets to transform the delivery and management of services for the enterprise. ServiceNow enables service management for every department in the enterprise including IT, human resources, facilities, field service, and more. We deliver a "lights-out, lightspeed" experience through our enterprise cloud – built to manage everything as a service. To find out how, visit www.servicenow.com.