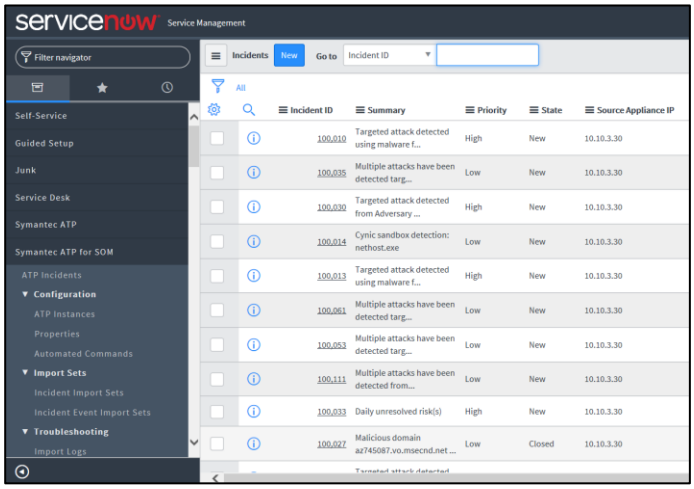
Symantec™ Advanced Threat Protection Integration with ServiceNow®

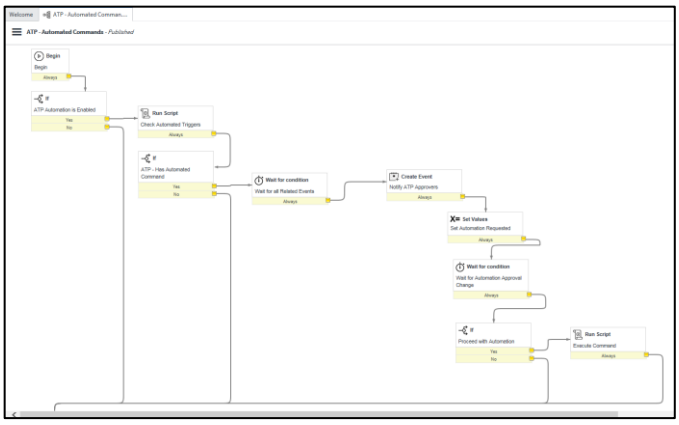
Overview

Customers have invested in numerous security products. They often have existing workflow or ticketing system for incident response and security monitoring. It is important that these security products and systems are integrated, so that security incidents can be easily tracked, investigated, and managed. In the end, they should work together for security analysts to close the loop and complete post incident activities. Public API included in Symantec™ Advanced Threat Protection (ATP) is the foundation of both inbound and outbound communication among different systems.

ServiceNow Integration



Free Symantec ATP app is now available on ServiceNow™ app store. The Symantec ATP app allows customers to view Symantec Advanced Threat Protection incidents in the ServiceNow console. They can also leverage the ticketing and workflow capabilities of ServiceNow to monitor and investigate possible threats in their organization. The integration replicates Symantec ATP incidents and related events data from the ATP appliances into the ServiceNow console. It also enables admins to see and integrate ATP incidents with their own processes and take advantage of the ticketing and workflow strength that ServiceNow has. Customers can drill down into granular details of every ATP incident, even the events associated with that incident, and can create notification to route based on the routing rules set within the ServiceNow app.



Responding to Incidents More Efficiently

With ServiceNow Security Operation app, Symantec ATP customers can take multiple actions directly from the ServiceNow interface. They can search for a file hash, delete malicious files across all endpoints, or quarantine compromised endpoints for further investigation without the need to switch from one management console to another. Customers can also automate and customize their incident response flow. For example, when a file has been identified as suspicious by Symantec ATP, any endpoint with this file should be isolated from corporate network, and the file should be added to the blacklist immediately. Any incident response flow can be set as one-time request or be automated for every occurrence. In addition, Symantec ATP prioritizes what matters the most and highlights targeted attacks that require immediate attention. Security analyst now has rich threat intelligence from Symantec ATP and be more efficient and confident when responding to advance threats.