Symantec™ Advanced Threat Protection Integration with Splunk & ServiceNow

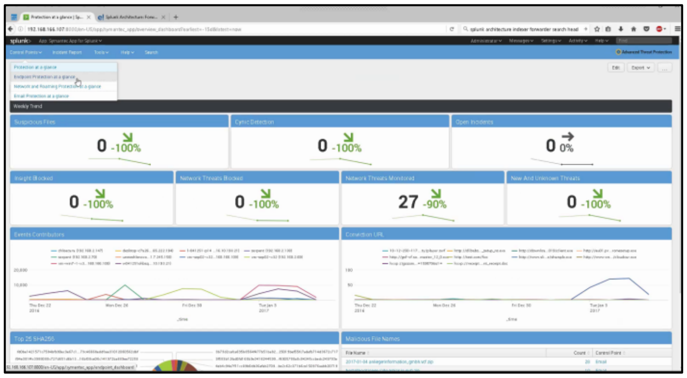
Symantec.

Overview

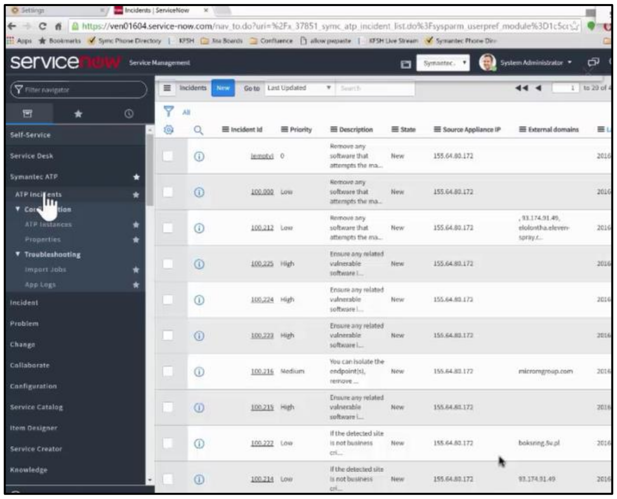
Customers have invested in numerous security products. They often have existing workflow or ticketing system for incident response and security monitoring. It is important that these security products and systems are integrated, so that security incidents can be easily tracked, investigated, and managed. 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.

Splunk Integration

Symantec ATP allows customers to export threat events to Splunk® directly by providing a connector that can replicate event data generated by Symantec ATP. Free ATP app is now available on Splunk app store. This functionality correlates threat data from Symantec ATP with other events collected in Splunk, providing a broader visibility into your environment. Customers can create and customize a security dashboard in Splunk easily by leveraging the rich threat data from Symantec ATP. For example, you can create a dashboard to show the top 10 suspicious files with top 20 malicious files. You can also drill down to see if there's any particular file hash related to specific event or incident. With Symantec ATP, you can now do ad hoc queries via Splunk; for instance, show the top file hashes seen in a certain period of time. If you have multiple Symantec ATP modules, you may also filter ATP events via Splunk console by different search fields, such as endpoint, network, email, or roaming events. In addition, the Symantec ATP Adaptive Response Add-on for Splunk would allow enterprise security users to blacklist or remediate malicious files and isolate compromised endpoints directly from the Splunk management console.



ServiceNow Integration



Incident Id	Priority	Description	State	Source Appliance IP	External domains	L
(empty)	0	Remove any software that attempts the ma...	New	155.64.80.172		2016
100.000	Low	Remove any software that attempts the ma...	New	155.64.80.172		2016
100.212	Low	Remove any software that attempts the ma...	New	155.64.80.172	, 93.174.91.49, elolontha.eleven-spray.r...	2016
100.225	High	Ensure any related vulnerable software i...	New	155.64.80.172		2016
100.224	High	Ensure any related vulnerable software i...	New	155.64.80.172		2016
100.223	High	Ensure any related vulnerable software i...	New	155.64.80.172		2016
100.216	Medium	You can isolate the endpoint(s), remove ...	New	155.64.80.172	micromgroup.com	2016
100.215	High	Ensure any related vulnerable software i...	New	155.64.80.172		2016
100.222	Low	If the detected site is not business cri...	New	155.64.80.172	boksning.5v.pl	2016
100.214	Low	If the detected site is not business cri...	New	155.64.80.172	93.174.91.49	2016

Free Symantec ATP app is also now available on ServiceNow™ app store. The Symantec ATP app allows customers to 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.