Case Study: Symantec ATP Apps for Splunk

Symantec ATP app provides various visualizations for Network, Endpoint and Email threat protection using Splunk

Splunk Infrastructure Details:

App and Add-on supported on Standalone, Distributed and Clustered Splunk deployments

Distributed Splunk Architecture:

- App supported on Splunk Search Heads
- Add-on supported on Splunk Search Heads, Indexers and Forwarders

Customer Challenge

Symantec Advanced Threat Protection (ATP) helps you to uncover, prioritize, investigate and remediate complex attacks across endpoint, network, web and email domains by providing various means to collect data from Symantec Endpoint Security, Web security.cloud and Email security.cloud. To efficiently protect the organization from these threats it is very important to correlate all the data and provide a deep insight on security threats as well as some preventive measures to protect from these threats.

The CREST Difference in 90 Days

Crest developed Splunk Symantec ATP app provides prebuilt dashboards and panels along with other UI elements tailored for an ATP user. These dashboards helps the ATP users to get an overview as the app contains aggregated as well as individual visualizations which correlates data collected from Symantec ATP and Symantec Email Security.cloud. It also provides Splunk Adaptive Response for Splunk Enterprise Security Suite (ES) app which allows us to isolate affected endpoints or delete affected files right from within Splunk. ATP users can also correlate the ATP data in Splunk with the data collected from other data center technologies in Splunk.

Crest Data Systems is a leading App Development, Professional Services, and Managed Services Partner of Splunk. Crest has built 200+ Splunk Apps & Technology Add-ons (TA) for customers ranging from Global Fortune 500 companies to Silicon Valley Startups in IT Ops, Security, and IoT domains. With a dedicated team of Splunk-certified Administrators, Engineers, and Consultants across the US and India, Crest provides Professional Services & 24x7 Managed Support Services to Splunk Enterprise & Cloud to customers across US, Europe, and APAC.

USA
2107 N. 1st Street, #205
San Jose CA 95131

INDIA
First Floor, Bhaskar House
SG Road, Ahmedabad 380 015

+1 (408) 909-9161
info@crestdatasys.com
http://www.crestdatasys.com/