SentinelOne blog

GET A DEMO

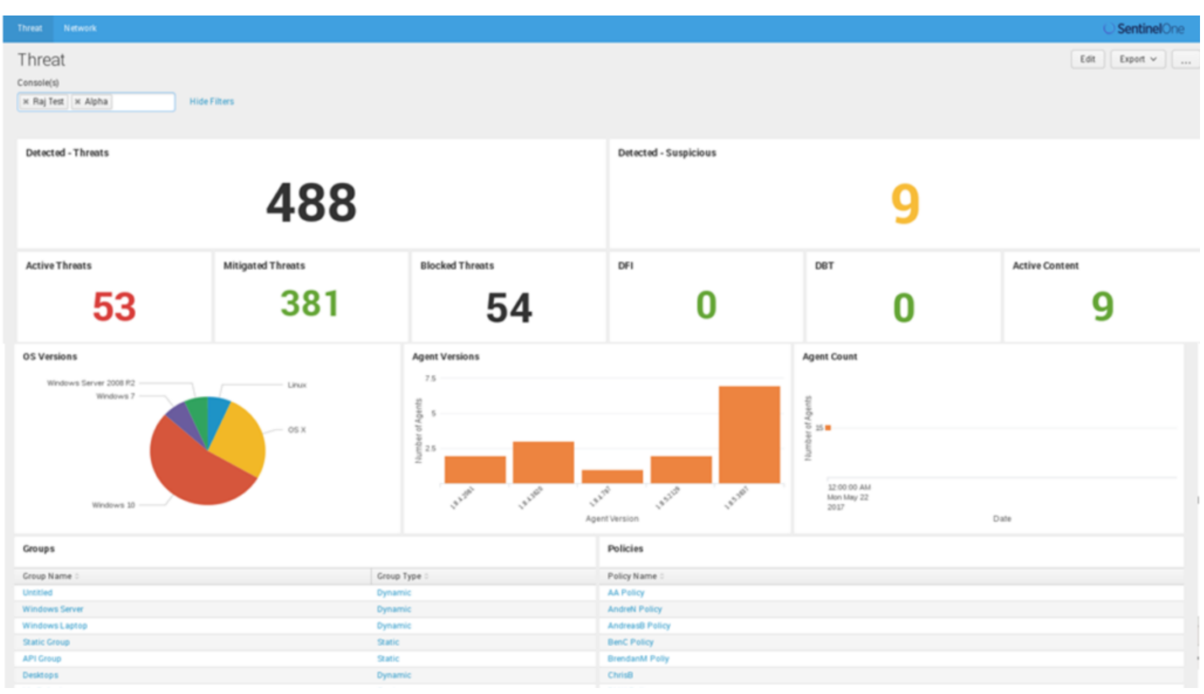
The SentinelOne Splunk App

September 25, 2017
by Raj Rajamani

Today, we are pleased to announce the availability of the SentinelOne Tech Add-On and App for Splunk. Splunk is one of the most widely deployed tools used by our customers to monitor and analyze massive streams of data. The SentinelOne App provides pre-built dashboards, lets you search SentinelOne data, and even lets you take actions from the Splunk console. Here are some of the key use cases where you can leverage the SentinelOne Splunk App.

Threat Summarization

The SentinelOne App uses SentinelOne REST APIs to fetch information about threats, devices, policies, activities and other objects from the SentinelOne console and indexes them in Splunk. Default dashboards use saved searches to provide threat and operational summaries.



Threat

Console(s)

× Raj Test × Alpha

Detected - Threats	Detected - Suspicious
488	9

Active Threats	Mitigated Threats	Blocked Threats	DFI	DBT	Active Content
53	381	54	0	0	9

OS Versions

Agent Versions

Agent Count

Groups

Group Name	Group Type
Untitled	Dynamic
Windows Server	Dynamic
Windows Laptop	Dynamic
Static Group	Static
API Group	Static
Desktops	Dynamic

Policies

Policy Name
AA Policy
AndrewN Policy
AndreasB Policy
BenC Policy
BrendanM Poly
ChrisB

Search

The SentinelOne app creates a SentinelOne index with distinct source types for all the objects it fetches from SentinelOne. This lets the admin perform queries to gain further insights into endpoint policies and threats.

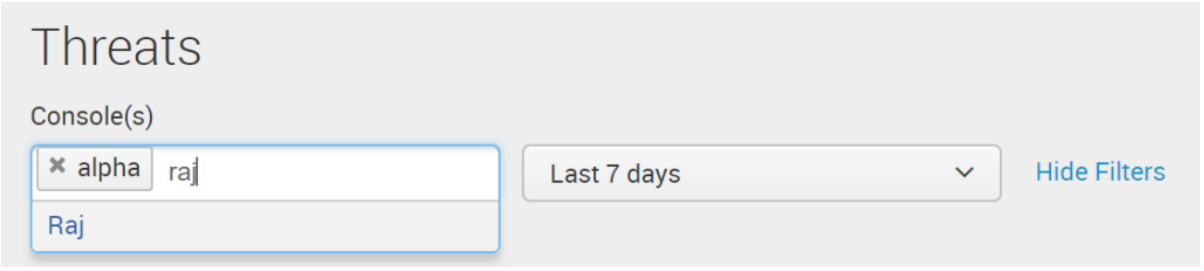
index=sentinelone sourcetype=agent agent_version="1.8.5.3834"

index=sentinelone sourcetype=threat classifier_name=STATIC

index=sentinelone sourcetype=group subdomain=tango

Roll-up Reporting

Some large enterprises deploy multiple consoles, sometimes regionally, to comply with local data privacy laws. Others have hybrid deployments where air-gapped networks are managed by an on-prem console and other devices by a console in the SentinelOne cloud. The SentinelOne Splunk App can connect with multiple consoles to let admins get a roll-up view across these consoles. Searches can also be limited to specific consoles using the *console* field.



Threats

Console(s)

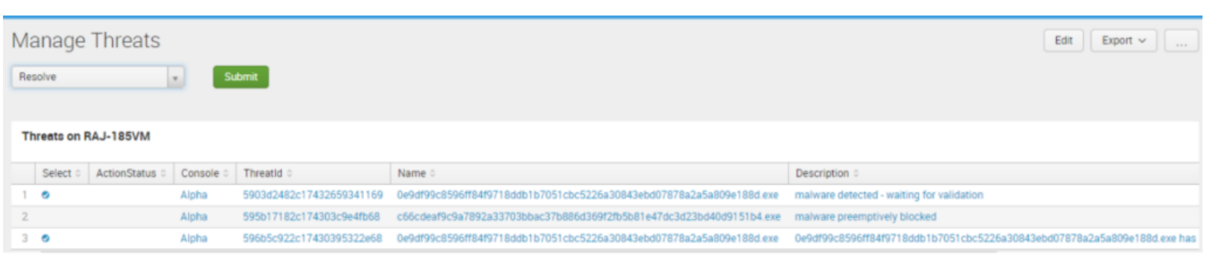
✖ alpha raj

Raj

index=sentinelone console="alpha" sourcetype=agent agent_version="1.8.5.3834"

Actions

The SentinelOne app lets you take actions from within Splunk, such as resolving threats, upgrading agents, and disconnecting infected devices from the network from within the Splunk interface. This is especially useful in SOCs and other large enterprise setups.



Manage Threats

Resolve

Threats on RAJ-185VM

	Select	ActionStatus	Console	ThreatId	Name	Description
1	●		Alpha	5903d2482c17432659341169	0e9df99c8596ff84f9718ddb1b7051cbc5226a30843ebd07878a2a5a809e188d.exe	malware detected - waiting for validation
2			Alpha	595b17182c174303c9e4fb68	c66cdeaf9c9a7892a33703bbac37b886d369f2fb5b81e47dc3d23bd40d9151b4.exe	malware preemptively blocked
3	●		Alpha	596b5c922c17430395322e68	0e9df99c8596ff84f9718ddb1b7051cbc5226a30843ebd07878a2a5a809e188d.exe	0e9df99c8596ff84f9718ddb1b7051cbc5226a30843ebd07878a2a5a809e188d.exe has

After months of beta deployments and enhancements, we are now excited to make the app available on Splunkbase. Also take a look at the solution brief for more insights. From all of us at SentinelOne, enjoy and Happy Splunking!

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Introducing the SentinelOne Excel Plugin
- PowerQuery Brings New Data Analytics Capabilities to Singularity XDR
- Rapid Response with XDR One-Click Remediations
- Feature Spotlight | Introducing Singularity Dark Mode
- Introducing the New Singularity XDR Process Graph
- Feature Spotlight | Combating Email Threats Through AI-Driven Defenses with Armorblox Integration