SOLUTION BRIEF

SentinelOne

SentinelOne Splunk App

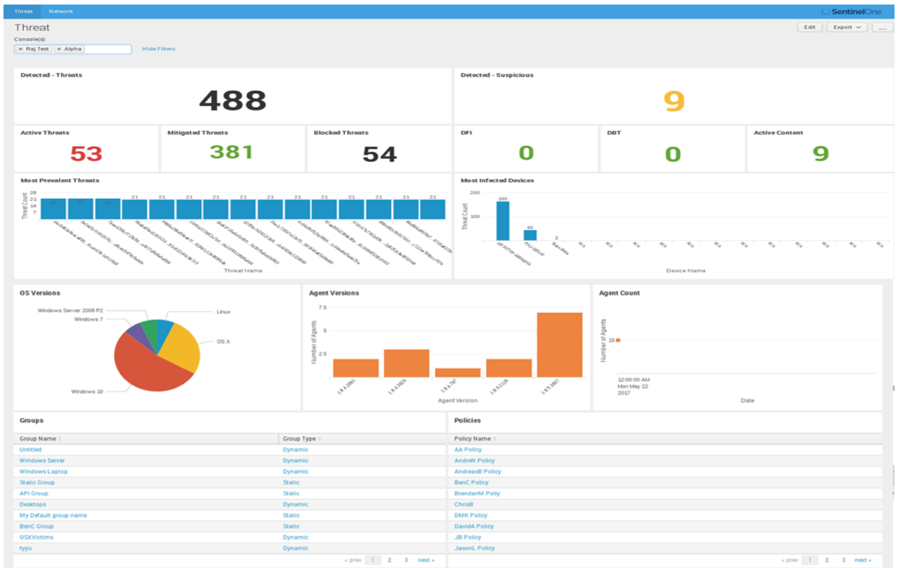
Today's organizations are complex environments combined with the speed and variety of threats and the business impact of breaches necessitates near real-time detection-to-response. Shrinking the time to effective protection requires visibility into the key areas of the network, real-time correlation of critical events to identify threats and automation of workflows with cross-platform integration to accelerate time-to-response.

SentinelOne is a pioneer in autonomous security for the endpoint, datacenter and cloud. The SentinelOne Endpoint Protection Platform (EPP) enables rich visibility into the events, files and processes at the endpoint, powers threat detection with static and behavioral artificial intelligence (AI), and automates the response workflow to help organizations achieve real-time security with speed and simplicity.

SentinelOne Splunk App

The SentinelOne Splunk App empowers organizations to combine the strengths of their Splunk deployments to collect, monitor, analyze and visualize massive streams of machine data with deep visibility, detection, response, remediation and forensics capabilities of SentinelOne EPP.

The solution uses the SentinelOne REST APIs to fetch information about threats, devices, policies and other objects from the SentinelOne console and indexes them within Splunk. The information is synchronized every 15 minutes by default, but can be done at a greater frequency. Default dashboards use saved searches to provide threat and operational summaries.



Threat

Console(s): Raj Test, Alpha

Detected - Threats: 488

Active Threats: 53

Mitigated Threats: 381

Blocked Threats: 54

Detected - Suspicious: 9

DFI: 0

DBT: 0

Active Content: 9

Most Prevalent Threats

Most Infected Devices

OS Versions

Agent Versions

Agent Count

Groups

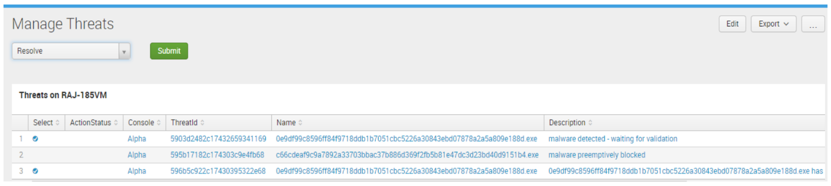
Group Name	Group Type
Untitled	Dynamic
Windows Server	Dynamic
Windows Laptop	Dynamic
Static Group	Static
API Group	Static
Desktops	Dynamic
My Default group name	Static
BenC Group	Static
OSXVictims	Dynamic
tyyu	Dynamic

Policies

Policy Name
AA Policy
AndreN Policy
AndreasB Policy
BenC Policy
BrendanM Polly
ChrisB
DMK Policy
DavidA Policy
JB Policy
JasonL Policy

Figure 1: SentinelOne Splunk App Console

The SentinelOne Splunk App can connect with multiple SentinelOne consoles, which could include a combination of on-prem and cloud-consoles, to let administrators get a roll-up view across all the consoles, while also allowing the flexibility to limit monitoring a specific console. Additionally, the SentinelOne Splunk App lets customers take direct actions from within Splunk, such as resolving threats, upgrading agents, and disconnecting infected devices from the network. This is especially useful to simplify management and monitoring workflows for large enterprise deployments with console-hopping causes administrative overheads and reduces efficacy and timeliness of response.



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

Figure 2: SentinelOne Splunk App Response Integration

Benefits

- Power real-time threat prevention, detection and investigation with visibility extending to the endpoints deployed on- and off-network
- Automate incident response with workflow integration powered within a single pane of glass
- Streamline multi-console deployments with integrated analysis and management
- Understand network-wide trends and behavioral patterns to make more informed decisions through custom searches and reports
- Simplify deployment complexity and operational overheads with an integrated console for monitoring and management
- Gain rich forensics insights to power the security operations workflows

SentinelOne is a certified AV replacement for Windows and MacOS.

OPSWAT 04 / 25 / 2017 BRONZE CERTIFIED ANTIMALWARE

HIPAA

PCI

APPROVED CORPORATE ENDPOINT PROTECTION

AV TEST av-test.org 02/2016 CERTIFIED MACOS SIERRA

SentinelOne

For more information about the SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, **please visit: sentinelone.com**