REDSEAL SYSLOG EVENT SPECIFICATION

OVERVIEW

RedSeal can be configured to log key metrics and status that it detects during analysis. The events that are tracked and exported include:

- Host Metrics: Information about every host detected and its risk metrics
- Best Practice Checks: Information about network device checks (refer to RedSeal User Manual (Appendix 10 Configuration Checks) for definitions/specifications
- Model Issues: Anomalies in configuration files including unmapped hosts, duplicate IPs, and others (refer to RedSeal User Manual (Appendix 10 Configuration Checks) for definitions/specifications
- Policy: Details about access that violates policy rules

Refer to the RedSeal User Manual Chapter 7 (UI Tools and Utilities) for details on setting up your logging configurations.

BENEFITS

These events provide additional intelligence to a variety of other solutions:

- SIEM: correlate unique RedSeal risk scores with other data sources (HP ArcSight, Splunk, QRadar, Logrhythm, etc.)
- GRC, Network mapping tools: validate inventory information with RedSeal (LockPath, McAfee ePO, Lumeta, etc.)
- Display/visualization/reporting engines: enable custom reporting/formatting of RedSeal intelligence

Additionally, external solutions with dashboard capabilities, can create custom displays with RedSeal intelligence about overall security posture that can be shared with other IT and management personnel.

EVENT SPECIFICATION SYNTAX

Host Metrics Events

RedSeal Value Name	Value
EventName	HostMetricsEvent
EventAction	RedSeal Network Analysis
EventDate	Date on which event occurred

RedSealServerName	Name of the RedSeal server sending the event
RedSealServerIPAddress	IP address of the RedSeal server sending the event
AnalysisDate	Analysis start time, when the analysis took the snapshot of the Network Model
HostRedSealID	RedSeal internal ID of the host
HostName	Name of the host
PrimaryIp	IP Address of the host
PrimaryService	Primary Service on the host (e.g. http, ftp, etc.)
OperatingSystem	Operating System name and version of the host
AttackDepth	Number of hops taken to access this host from an untrusted source (e.g. -1, 1, 2.. etc.) • -1 = protected • 1 = directly attackable • 2.. etc.
VulnerabilityCount	Number of vulnerabilities present on the host
ServicesCount	Number of services installed on the host
Value	Relative value of the host from 0 - 100
Risk	Calculated Risk value for this host
DownstreamRisk	Cumulative risk values for all hosts reachable from the host
Confidence	Confidence value for the risk calculation
Leapfroggable	Does the host have any vulnerabilities with leapfrog capabilities? (true or false)
AccessibleFromUntrusted	Is there direct access from Untrusted subnets to the host? (true or false)
HasAccessToCritical	Can the host directly access anything in the Critical Assets Group? (true or false)

Example events:

magnesium.lab.redseal.net -EventAction=RedSeal Network Analysis | EventDate=Sep 18, 2015 1:28:06 PM PDT | EventName=HostMetricsEvent | DeviceVendor=RedSeal Networks, Inc. | DeviceProduct=RedSeal Platform | DeviceVersion=8.1.0 | RedSealServerName=magnesium.lab.redseal.net | RedSealServerIPAddress=172.16.16.36 | HostName=172.16.3.247 |

HostRedSealID=2c9090a44fbdb058014fbef9b6d02fee | AnalysisDate=Sep 18, 2015 1:26:40 PM PDT | PrimaryService=ssh | OSVendor=Unknown | OperatingSystem=Unix Variant | AttackDepth=-1 | Exposure=0 | Value=20 | ServicesCount=1 | VulnerabilityCount=0 | Risk=0 | DownstreamRisk=0 | Confidence=1 | Leapfroggable=false | Exploitable=false | PrimaryIp=172.16.3.247 | AccessibleFromUntrusted=false | HasAccessToCritical=false | END RSExternal event
Sep 18 13:21:22 magnesium Sep 18 13:28:06 magnesium.lab.redseal.net -EventAction=RedSeal Network Analysis | EventDate=Sep 18, 2015 1:28:06 PM PDT | EventName=HostMetricsEvent | DeviceVendor=RedSeal Networks, Inc. | DeviceProduct=RedSeal Platform | DeviceVersion=8.1.0 | RedSealServerName=magnesium.lab.redseal.net | RedSealServerIPAddress=172.16.16.36 | HostName=172.16.3.231 | HostRedSealID=2c9090a44fbdb058014fbef9b754303c | AnalysisDate=Sep 18, 2015 1:26:40 PM PDT | PrimaryService=HTTP | OSVendor=Unknown | OperatingSystem=Unix Variant | AttackDepth=1 | Exposure=0.675 | Value=50 | ServicesCount=3 | VulnerabilityCount=2 | Risk=34 | DownstreamRisk=0 | Confidence=1 | Leapfroggable=false | Exploitable=true | PrimaryIp=172.16.3.231 | AccessibleFromUntrusted=false | HasAccessToCritical=false | END RSExternal event

Best Practices Check and Model Issues Events

RedSeal Value Name	Value
EventName	BestPracticesCheckEvent or ModelIssuesEvent
EventAction	Violation
RedSealServerName	Name of the RedSeal server sending the event
RedSealServerIPAddress	IP address of the RedSeal server sending the event
HostName	Name of the device
HostRedSealID	RedSeal internal ID of the device
FirstSeenDate	Date/time the violation was first seen on the device
LastSeenDate	Date/time the violation was last seen on the device
FileLines	File lines in the device configuration file where the violation was found
Message	Short description of the violation

Example events:

Sep 21 10:36:16 mosely Sep 21 10:36:16 mosely.lab.redseal.net -EventAction=Violation | EventDate=Sep 21, 2015 10:36:16 AM PDT | EventName=ModelIssuesEvent | DeviceVendor=RedSeal Networks, Inc. | DeviceProduct=RedSeal Platform | DeviceVersion=8.0.1 | RedSealServerName=mosely.lab.redseal.net | RedSealServerIPAddress=172.16.0.231 | EventSeverity=LOW | HostName=acmeinternet-r1 | HostRedSealID=2c9080674fb83b71014fe1b641977d06 | Message=11 network device(s) and 54 subnet(s) are not in topology groups. | CheckName=Unplaced Objects | RedSealCheckID=MI-12 | FirstSeenDate=Sep 17, 2015 3:26:58 PM PDT | LastSeenDate=Sep 21, 2015 10:36:13 AM PDT |

HelpURL="http://mosely.lab.redseal.net/RSHelp/usr_gde/WebHelp/usr_gde/appdx_nccs/appdx_nccs.htm#TOC_Unplaced_Objects" | END RSExternal event

Sep 20 09:13:32 mosely Sep 20 09:13:32 mosely.lab.redseal.net -EventAction=Violation | EventDate=Sep 20, 2015 9:13:32 AM PDT | EventName=BestPracticesCheckEvent | DeviceVendor=RedSeal Networks, Inc. | DeviceProduct=RedSeal Platform | DeviceVersion=8.0.1 | RedSealServerName=mosely.lab.redseal.net | RedSealServerIPAddress=172.16.0.231 | EventSeverity=LOW | HostName=PA1 | HostRedSealID=2c9080674fb83b71014feb8816d6292a | Message=Management of device by HTTP is enabled on ethernet1/1 | CheckName=HTTP Management Enabled on Interface | RedSealCheckID=RS-102 | FirstSeenDate=Sep 20, 2015 9:13:28 AM PDT | LastSeenDate=Sep 20, 2015 9:13:28 AM PDT | FileLines=PAN-OS:359 | HelpURL="http://mosely.lab.redseal.net/RSHelp/usr_gde/WebHelp/usr_gde/appdx_nccs/appdx_nccs.htm#TOC_HTTP_Management_Enabled_on_Interface" | END RSExternal event

Policy Events

RedSeal Value Name	Value
EventName	PolicyEvent
EventAction	RedSeal Network Analysis
RedSealServerName	Name of the RedSeal server sending the event
RedSealServerIPAddress	IP address of the RedSeal server sending the event
AnalysisDate	Analysis start time, when the analysis took the snapshot of the Network Model
PolicyName	Name of the Policy (e.g. PC Audit)
SourceZone	Name of the policy zone that is the source of the access.
DestinationZone	Name of the policy zone that is the destination of the access.
RuleType	The type of Policy Rule being evaluated (e.g. Access, Firewalls or ZoneOverlap)
ComplianceStatus	Compliance status of the policy Rule (e.g. Pass, Warning, Fail, Fail _Overlap or Deleted)
ChangeStatus	Has the policy status changed for this Rule (e.g. New, Continuing or Change)

Example events:

Feb 23 10:37 dizzy Feb 23 10:37:16 dizzy.lab.redseal.net -EventAction=RedSeal Network Analysis | EventDate=Feb 23, 2015 10:37:16 AM PST | EventName=PolicyEvent | DeviceVendor=RedSeal Networks, Inc. | DeviceProduct=RedSeal Platform | DeviceVersion=7.1.3 | RedSealServerName=dizzy.lab.redseal.net | RedSealServerIPAddress=172.16.0.73 | AnalysisDate=Feb 23, 2015 10:36:04 AM PST | PolicyName=PCI Audit | SourceZone=Wireless | DestinationZone=Cardholder | RuleType=Firewall | ComplianceStatus=Pass | ChangeStatus=Continuing | END RSExternal event