



GLOSSARY

#

5-tuple (Quintuple) The five pieces of data found within all IP-based network packets: source IP address, source port, destination IP address, destination port, and protocol. You can define inspection rules, queries, and reports using the data found in the 5-tuple.

A

(\)

Access IP Address This is the IP address that MARS uses to connect to the device and to get its configuration information. MARS needs this address for NAT-related session correlation, attack path calculation, and mitigation enter access information.

Activate Making changes or edits known to the MARS after submitting changes.

D

Devices The hosts and reporting devices present in the system.

Discovery The act of identifying, either automatically or manually, devices in networks.

Dynamic Vulnerability Scanning The MARS STM probes selected networks, and their components, for vulnerabilities.

E

Event A security event reported to the MARS STM appliance. Events have: types, sources, destinations, reporting devices, etc.

Event Types Groups of similar security events. An event type is the normalized signature from a reporting device.

F

False Positive An event that resembles a valid security threat, but is not.

Firing Events An event that contributed to a rule firing.

I

Incident	Incidents are collections of events and sessions that meet the criteria for a rule, having helped to cause it to fire.
Incident Instances	An instance of an incident.

M

MI B	management information base
mitigate	To stop a detected attack or anomaly. The method of mitigation varies based on network composition and configuration.

O

Offset	The offset of a firing event is the line number of the rule criteria that this firing event matches.
---------------	--

P

Pre NAT Source Address	Session endpoints.
Post NAT Source Address	The source as appearing at the destination.
Post NAT Destination Address	Session endpoints.
Pre NAT Destination Address	The destination as appearing at the source.

Q

Query	A user-defined request to the database for information.
--------------	---

R

Report	A user-defined request to the database on an automatic or on-demand basis.
Reporting Device	A discovered device that reports information – usually in the form of logs – to a MARS STM appliance.

Reporting IP Address This is the IP address as it appears to MARS. This address is where the logs (syslog, SNMP traps, LEA) come from.

Rule The sub-set of events that contributed to the incidents of the specified rules firing.

S

Service A protocol and range of IP addresses.

Session A session is a collection of events that all share a common source and destination, which were reported within a given time window. For example, usually the events in a session map well to the events generated between the opening and closing of a TCP/IP connection.

Sessionize Combining event data from multiple reporting devices to reconstruct the occurrence of a session. Sessionizing takes two forms: reconstructing a session-oriented protocol, such as TCP, where the initial handshake and the session tear down and reconstructing a sessionless protocol, such as UDP, where the initial start and session end times are defined more based on first and last packets tracked within a restricted time period. In other words, packets that fall outside of the time period are considered part of different sessions.

T

True Positive A valid security threat.

U

Unreported device A device from which the MARS Appliance receives events, such as syslog messages, SNMP notifications, or NetFlow events, but the device is not defined in the appliance. Without a definition, MARS is unable to correlate events correctly as it needs to know which message format to use in parsing.

T

True Positive A valid security threat.

