How to enhance protection using SmartEvent policies

Shlomi Feldman

SCADA/ICS sales

19/09/17

Hi Everyone,

Wanted to bring to your attention, the important capabilities of our SmartEven which significantly enhance protection for SCADA systems.

SCADA systems operational behavior can be understood by the SCADA communication protocol commands traffic. Transactions back and forth with the field equipment (PLCs/RTUs) can be used to create a baseline pattern to indicate normal operational behavior of the system.

For example we have a system with 1500 registers on a PLC. 300 of those registers get write commands from the SCADA server each 2 minutes.

* Creating the traffic baseline:
we will use our application control blade to create applications and policies to monitor the write commands to the PLC. Each time the Gateway will recognize a write command to the PLC, it will log the event.






* Learning the normal behavior pattern:
after allowing the gateway to log events for a sufficient time, ensuring that no special events occurred during this period. The SmartEvent will be able to provide us understanding of the normal behavior pattern, viewing the quantity and frequency of each and every event.


* How this feature helps us to enhance protection?
A Denial-of-service (DoS) attack on the PLC will include large number of write commands in short period of time, with intention to flood the PLC, making it to slow down and event to stop.
SmartEvent allows the user to prevent such attacks. As the user already aware of his normal operational pattern, especially the write commands frequency to the PLC.
He can create a SmartEvent policy which will alert or events block traffic, in case events frequency is larger than the normal behavior required pattern. 