Security Log Format Revision for A858P1S1

Proposal for Structured Data

Timo Warns

08 December 2021

Reminder: Proposed Status To-Be

- Define security log format in terms of Structured Data (as replacement or, at least, as an alternative format)
- *If current MSG format is kept, complete the scheme on delimiter escaping.*
- *At least for SD format, allow for flexibility in terms of parameters (i.e. enable implementation-specific additions)*
  - *Define a standard set of parameters to choose from*
  - *Give guidance on how to add further parameters*

IPS MSG format vs. Structured Data

```
<169>1 2021-09-15T10:11:12.000Z IPS.F-WWCF.airbus.com
ConfigSvc - ID03
BOM
1,
,
2,
0,
[::1],
10,
4,
"Chain FORWARD (policy DENY) Port(*): TCP(0),UDP(1), ALL
Chain FORWARD (policy ACCEPT) port 5908
Chain FORWARD (policy ACCEPT) port 5909
Chain FORWARD (policy ACCEPT) port 5910
Chain FORWARD (policy ACCEPT) port 5913
Chain FORWARD (policy ACCEPT) port 5914
Chain FORWARD (policy ACCEPT) port 5915
Chain FORWARD (policy ACCEPT) port 5916
Chain FORWARD (policy ACCEPT) port 5917
target prot opt source destination LOG UDP — ::00/0
::00/FFFF REJECT UDP — ::00/0 ::00/FFFF UDP
reject-with icmp”,
52,
4,
0042000004200000004I900002290000911
```

```
<169>1 2021-09-15T10:11:12.000Z IPS.F-WWCF.airbus.com ConfigSvc -
ID03
[
      ips@54680
      SERVICE=”ConfigSvc”
      EVENT=”Firewall Configuration Change”
      SRC=”[::1]”
      PAYLOAD=”0042000004200000004I900002290000911”
]
BOM
Chain FORWARD (policy DENY) Port(*): TCP(0),UDP(1), ALL
Chain FORWARD (policy ACCEPT) port 5908
Chain FORWARD (policy ACCEPT) port 5909
Chain FORWARD (policy ACCEPT) port 5910
Chain FORWARD (policy ACCEPT) port 5913
Chain FORWARD (policy ACCEPT) port 5914
Chain FORWARD (policy ACCEPT) port 5915
Chain FORWARD (policy ACCEPT) port 5916
Chain FORWARD (policy ACCEPT) port 5917
target prot opt source destination LOG UDP — ::00/0 ::00/FFFF
REJECT UDP — ::00/0 ::00/FFFF UDP
reject-with icmp
```

Security Logging Format Options

Option	Pros	Cons
MSG format	● More efficient representation of log entries in terms of space needed	● Current definition has very limited support for implementation-specific refinements / extensions ● Same fields for all types of log entries ● Need for IPS-specific parser ● No field for log integrity values in current format
Structured Data	● Support for implementation-specific refinements and extensions ● Context-specific parameter sets ● Human-readable / interpretable ● Support by COTS SIEMs	● Less efficient representation of log entries in terms of space needed

Recommendations:

- Support Structured Data format for log entries
- Decide whether to support both formats or only Structured Data format

Thank you