APSolute Vision Reporter (AVR) je monitorovací nástroj k bezpečnostnímu řešení Radware DefensePro, který poskytuje okamžitý přehled o výkonu a bezpečnostním stavu vaší infrastruktury a sítě.

Z adresy **avr-dp@master.cz** systém zasílá upozornění na jakékoli aktivity a změny. V tomto článku najdete vysvětlení jednotlivých položek, které e-maily obsahují.

Ukázka alert e-mailu:

Time : 03/24/2021 04:36:22

Alert Name : –

Alert Description : New action –

Alert Events:See below for list of events that triggered this alert

#START :0:0

1 OLF6 AVR 1.1 date=03/24/2021 04:33:04 0 devtype=0 et=0 devid=ff8080813d1fccea013d1fd4f456002e hostip=- hostname=172.16.22.20 pport=1 dir=0 proto=UDP act=3 attackname=Memcached-Server-Reflect attackipsid=66747-1613645708 attackid=18286 sip=188.240.208.80 dip=Multiple dport=N/A rule=36804 nthreatcat=6 attackrisk=3 starttime=03/24/2021 04:33:04 laststamp=03/24/2021 04:33:17 vlantag=1349 mpls=N/A pktcnt=0 pktbw=0 duration=Less than 1 min alertrule=New Rule1

Význam jednotlivých polí:

Sekvence pole	Pole	Popis	Příklad nebo statická hodnota
1	Číslo řady	Číslo řady v upozornění.	1

2	Formát	Open Log Format (OLF) verze 6. Formát, který AVR používá k ukládání a shromažďování dat ze zařízení.	OLF6
3	Kód produktu	APSolute Vision Reporter	AVR
4	Typ události zařízení	Typ události na zařízení. Hodnoty: • 1.1 – z DefensePro nebo DefenseFlow • 1.2.1 – z APSolute Vision	1.1
5	Datum	Datum a čas události	date=02/28/2021 15:59:08 0
6	Typ zařízení	Hodnoty: • 0 – Device • 1 – Host (protože APSolute Vision Reporter shromažďuje data pouze z aplikací DefensePro a DefenseFlow a AppWall, bude mít toto pole vždy hodnotu 0	devtype=0
7	Typ události	Hodnoty: • -1 – provoz • 0 – útok	et=-1
8	ID zařízení	Identifikátor zařízení Radware	devid=ff8080813d1fccea013d1fd4f456002e
9	IP adresa hosta	IP adresa zařízení Radware	hostip=-
10	Název hosta	Jméno zařízení Radware	hostname=172.16.22.20

11	Směr	Hodnoty: • 0 – příchozí • 1 – odchozí • -1 – neznámý	dir=0
12	Protokol	Protokol spojený s událostí	proto=UDP
13	Akce	Hodnoty: • 0 – modified • 1 – forward • 2 – proxy • 3 – drop • 4 – source reset • 5 – destination reset • 6 – source and destination reset • 7 – bypass • 8 – challenge • 9 – quarantine • 10 – drop and quarantine Pro ostatní hodnoty je defaultní „zamítnuto“ (Denied)	act=0
14	Jméno typu útoku		attackname
15	ID útoku		attackipsid
16	ID typu útoku		attackid
17	Zdroj útoku	Zdrojové IP útoku	sip
18	Cíl útoku	Cílové IP útoku	dip
19	Cílový port		dport=N/A
20	Číslo služby		rule

21	Číslo kategorie útoku		nthreatcat
22	Závažnost útoku	Ohodnocení závažnosti útoku	attackrisk
23	Začátek útoku		starttime
24	Poslední čas, kdy byl útoku detekován		lateststamp
25	Číslo vlan		vlantag
26	MPLS	Multiprotokolové přepojování podle návěští (Multiprotocol Label Switching)	mpls=N/A
27	Počet paketů		pktcnt=0
28	Šířka pásma paketů	Šířka pásma paketů v kilobitech (kb)	pktbw=0
29	Pravidlo výstrahy	Pravidlo, které spustilo výstrahu.	alertrule=New Rule1