Distribúcia SPP
Plátennícka 2, 821 09 Bratislava

Akciová spoločnosť

Akciová spoločnosť je zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel Sa, vložka číslo 3481/B.

Všetkým známym záujemcom

Váš list číslo / zo dňa	*Naše číslo*	*Vybavuje / linka*	*Bratislava*
	KR-NZ-0370-25	*Mgr. Cehlár*	*13.05.2026*

Vec: **Odpoveď na žiadosť o vysvetlenie**

Obstarávateľ: **SPP - distribúcia, a.s.**, so sídlom: Plátennícka 2, 821 09 Bratislava, IČO: 35 910 739 (ďalej len ako *„Obstarávateľ“*) v súvislosti s verejným obstarávaním na zákazku*: Služba SOC - dohľadové centrum pre bezpečnosť IT v SPP-D,* vyhlásenú na základe Oznámenia o vyhlásení verejného obstarávania zverejneného v Úradnom vestníku Európskej únie S 46/2026, číslo uverejnenia oznámenia: 163266-2026 dňa 09.03.2026 a vo Vestníku verejného obstarávania č. 48/2026 pod č. 3558 - MRS dňa 10.03.2026 (ďalej len *„zákazka“* alebo *„súťaž“*), obdržal v zmysle § 48 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len *„ZVO“*) od záujemcu/ov **požiadavku/y na vysvetlenie informácií potrebných na vypracovanie ponuky, návrhu a na preukázanie splnenia podmienok účasti**, konkrétne:

Otázka č. 2

Vykonal obstarávateľ internú analýzu logovacích schopností koncových OT zariadení (RTU, plynomery, prepočítavače, a pod.) ?

1. Čo v prípade, keď OT zariadenia nepodporujú logovanie a negenerujú žiadne bezpečnostné logy podľa **štandardizovaných protokolov** cez bežne akceptované rozhrania, ako sú **Syslog** (definovaný v RFC 5424)?

Odpoveď č. 2

Víťazný uchádzač ako poskytovateľ SOC (ďalej aj len ako „dodávateľ“) nebude zodpovedný za kompatibilitu zariadení monitorovaných v SIEM obstarávateľa. Technické detaily a návrhy na spôsoby monitorovania zo strany dodávateľa SOC budú riešené v analytickej fáze, ktorú predpokladá a bližšie je opísaná v rámci prílohy č. 7 Súťažných podkladov *Opis predmetu zákazky (Technické zadanie)*, ako aj v rámci prílohy č. 7 Súťažných podkladov *Zmluva a jej prílohy* (ďalej len ako „analytická fáza“).

OT zariadenia, pokiaľ nebudú priamo monitorovateľné, búdu monitorované v SIEM, napr. cez analýzu netflow získaného zo vstupného routra/firewallu.

Otázka č. 3

V prípade, že koncové OT zariadenia nepodporujú **Syslog**, je možné vykonávať analýzu udalostí pomocou kompenzačných riešení v podobe pasívnych **(Network Security Monitoring - NSM)** alebo tiež známych ako OT IDS?

Odpoveď č. 3

Dodávateľ SOC nebude zodpovedný za kompatibilitu zariadení monitorovaných v SIEM obstarávateľa. Technické detaily a návrhy na spôsoby monitorovania zo strany dodávateľa SOC budú riešené v analytickej fáze.

Otázka č. 4

Vie obstarávateľ poslať presné modely a typové označenia (RTU, plynomery, prepočítavače, a pod.) OT zariadení v predmete monitoringu?

Odpoveď č. 4

Dodávateľ SOC nebude zodpovedný za kompatibilitu zariadení monitorovaných v SIEM obstarávateľa. Technické detaily a návrhy na spôsoby monitorovania zo strany dodávateľa SOC budú riešené v analytickej fáze.

Otázka č. 5

Aké sú požiadavky na rozsah zaznamenávaných udalostí z koncových OT zariadení (RTU, plynomery, prepočítavače, a pod.) (Čo logovať**)** ? Vie obstarávateľ presne zadefinovať kategórie **bezpečnostných udalosti ako napríklad:**

1. Úspešné aj neúspešné pokusy o prihlásenie,
2. Odhlásenia,
3. Vytváranie a odstraňovanie účtov
4. Firmware upload/download
5. RTU CPU STOP/START
6. Zmeny konfigurácie a logiky (zmena set pointov, úpravy riadiacej logiky)

Odpoveď č. 5

Technické detaily a návrhy na spôsoby monitorovania zo strany dodávateľa SOC budú riešené v analytickej fáze. Analytická fáza je na to aby, dodávateľ SOC dal tieto odporúčania a podieľal sa na ich implementácii.

Otázka č. 6

Aké sú architektonické požiadavky na zber, agregáciu a bezpečnosť logov z OT do IT prostredia ?

1. Niektoré staršie plynomery a prepočítavače (Purdue Level 0) zvyčajne nemajú TCP/IP konektivitu a schopnosť generovať Syslog. Komunikujú so systémom cez sériové linky (Modbus RTU, M-Bus). Sú sériové zariadenia požadované monitorovať ?
2. Má obstarávateľ definované zóny podľa Purdue Model IEC 62443 v OT sieti? Existuje OT DMZ 3,5 ?
3. Je nasadený firewall na IT / OT perimetri?
4. Je nasadený OT firewall na úrovni Level 2 alebo Level 3 Purdue Modelu? (Medzi OT zariadeniami v predmete monitoringu a IT/OT firewallom)
5. Akceptuje obstarávateľ dvojstupňový zabezpečený zber logov z OT zariadení a to najprv nasadením OT syslogu, ktorý bude cez jednosmernú dátovú diódu preposieť logy do IT SIEMu Splunk?

Odpoveď č. 6

Technické detaily a návrhy na spôsoby monitorovania zo strany dodávateľa SOC budú riešené v analytickej fáze.

Otázka č. 7

Má obstarávateľ inštalovaný Splunk OT add-on pre kontextualizáciu OT zariadení https://splunkbase.splunk.com/app/5151

Odpoveď č. 7

V tomto momente nie je addon inštalovaný.

S úctou

JUDr. Marián Uhrík
predseda komisie na vyhodnotenie ponúk
SPP - distribúcia, a.s.