Príloha č. 1

Opis predmetu zákazky :

Systém pre ukladanie a koreláciu logov v sieti, Systém pre centrálnu automatizáciu a správu zariadení fortinet - FortiGate, FortiSwitch, FortiAP

1x Systém pre ukladanie a koreláciu logov v sieti obstarávateľa a nasadenie do IKT infraštruktúry

- Systém musí byť plne kompatibilný riešeniami pre NGFW/UTM FortiGate 1200D, FortiMail-VM02, FortiAnalyzer 400E
- Prevedenie HW appliance do racku s veľkosťou maximálne 1RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu
- Schopnosť spracovávať logy v objeme GB/deň - min. 100 GB za deň
- Schopnosť spracovávať logy - konštantná rýchlosť správ, ktorú môže platforma udržiavať minimálne 48 hodín bez zníženia výkonu databázy a systému (logs/sec) - 1900
- Počet sieťových rozhraní - min. 4x GE RJ45
- Možnosť škálovateľného navýšenia objemu spracovávaných logov pomocou licencií
- Kapacita diskového priestoru - min. 4 TB v Raid zapojení (2x 4TB)
- Možnosť škálovateľného navýšenia diskovej kapacity pomocou licencií
- Podpora SYSLOG, podpora šifrovaného prenosu dát/logov
- Riešenie musí obsahovať konfigurovateľné prehľady s drill down funkcionalitou
- Filtrovanie správ/logov na základe rôznych parametrov, ich kombinácií. Podpora AND, OR logiky pri vytváraní filtrov
- Možnosť ukladania definícií filtrov pre rýchle opätovné použitie
- Možnosť prehliadania logov v historickom alebo realtime režime
- Možnosť zobrazovania logov v RAW alebo štruktúrovanom formáte
- Korelácia logov
- Možnosť automatického vytvárania incidentov
- Možnosť automatického vyšetrovania incidentov pomocou definovateľných playbookov
- Podpora Indication of Compromise - Systém musí obsahovať reputačné databázy nebezpečných IP/URL adries a musí vykonávať spätné prehľadávanie historických logov pri update reputačných DB za účelom detekcie napadnutia systémov a koncových staníc - min. 7 dní do minulosti
- Podpora vytvárania reportov v formátoch PDF, HTML, CSV, XML
- Možnosť generovania reportov v pravidelných intervaloch
- Možnosť vytvárania vlastných požiadaviek voči databáze a ich použitie ako zdroj dát v reportoch
- Podpora SNMP
- Podpora REST API

- GUI a CLI administračné rozhranie dostupné pomocou HTTPS a SSH protokolov

- Podpora LDAP, RADIUS, Tacacs+ pre administrátorské účty

1x Systém pre centrálnu automatizáciu a správu zariadení fortinet - FortiGate, FortiSwitch, FortiAP a nasadenie do IKT infraštruktúry

- Prevedenie HW appliance do racku s veľkosťou maximálne 2RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu
- Počet spravovaných zariadení/VDOM - min. 135
- Schopnosť spracovávať/prijímať logy zo spravovaných zariadení v objeme GB/deň - min. 2 GB za deň
- Požadovaná disková kapacita - min. 30TB
- Požadovaná podpora RAID - RAID 0/1,1s/5,5s/6,6s/10/50/60

- Požadovaná disková kapacita pri konfigurácii RAID 50 - min. 24TB

- Počet sieťových rozhraní - min. 4x GE RJ45 a 2x GE SFP

- Prevedenie HDD - Odnímateľné HDD z prednej strany apliance

- Požiadavky na napájanie - 2x 100–240V AC, 50-60 Hz
- Požiadavky na rozsah prevádzkových teplôt - 32°–104°F (0°–40°C)

- Požiadavky na chladenie - predná strana nasávanie, vyfukovanie dozadu

Licenčné a záručné požiadavky

Platnosť licencie 1 rok od dátumu akceptácie , záruka min. 3 roky od dátumu akceptácie. Podpora výrobcu v režime 24x7. Vlastníctvo Supportného kontraktu a licencií priamo objednávateľom. Prístup na supportný portál vo vlastníctve objednávateľa, otváranie, správa supportných ticketov priamo objednávateľom.