



PONUDNIK: _____

ŠTEVILKA PONUDBE IN DATUM: _____

PREDMET NAROČILA: Sistem SIEM

z.š.	količina	em	Naziv blaga / storitve	cena/em	Cena skupaj brez DDV
1.	1	kpl	Sistem SIEM		
2.	1	kpl	Namestitev in konfiguracija sistema SIEM		

CENA SKUPAJ (brez DDV) _____
_____ % DDV**Osnovne tehnične zahteve za sistem SIEM:**

- Rešitev mora podpirati spremljanje/zbiranje, shranjevanje, analizo in korelacijo zapisov dogodkov in tokov v približno realnem času (near real time).
- Rešitev mora podpirati možnost nadaljnje izboljšave z dodajanjem licenc in/ali novih komponent brez potrebe po popolni zamenjavi in zavrnitvi te (ponujene) instance, kot sledi:
 - vertikalni in/ali horizontalni tip širitve,
 - implementacija načina visoke razpoložljivosti (high-availability),
 - upravljanje ranljivosti (vulnerability management) z uvozom rezultatov skeniranja iz drugih orodij,
 - spremljanje omrežnih tokov na omrežnem nivoju 7,
 - uvedba/izboljšanje integrirane forenzike varnostnih incidentov,
 - spremljanje konfiguracij omrežnih naprav, topologije omrežja in povezanih omrežnih tveganj.
- Rešitev mora podpirati možnost implementacije načina visoke razpoložljivosti brez uporabe dodatne strojne opreme ali programske opreme drugih proizvajalcev.
- Rešitev mora podpirati uporabo ene same konzole za vse implementirane funkcionalnosti.
- Rešitev mora podpirati dostop do centralne upravljalne konzole prek standardnega spletnega brskalnika in preko šifriranega protokola HTTPS.
- Rešitev mora podpirati zbiranje dnevnikov iz naprav, ki praviloma poteka brez agentov (agentless), oziroma s pomočjo agentov na napravah, če je potrebno.
- Rešitev mora podpirati možnost definiranja različnih obdobij hrambe dnevnikov po definiranih kriterijih, za posamezne skupine dnevnikov.
- Rešitev mora podpirati možnost izdelave varnostnih/arhivskih kopij zbranih podatkov in po potrebi uvoza arhiviranih zapisov dnevnika.
- Rešitev mora podpirati shranjevanje zbranih dnevniških zapisov tako v izvorni obliki (raw format) kot tudi v normalizirani obliki, z možnostjo ohranjanja celovitosti podatkov (preprečevanje neopaženih sprememb dnevniških zapisov v sistemu).
- Rešitev mora podpirati možnost prikrivanja (*obfuscation*), tj. šifriranje občutljivih podatkovnih modelov v dnevnikih zapisih, z uporabo zasebnih/javnih ključev.



11. Rešitev mora izvesti normalizacijo, korelacijo in analizo dnevnikov.
12. Rešitev mora normalizirati skupna polja v dnevniških zapisih, ki jih prejmejo od različnih naprav (npr. uporabniško ime, IP naslov, ime gostitelja).
13. Rešitev mora podpirati skupno klasifikacijo dogodkov. Dogodke je potrebno razvrstiti glede na tip – npr. preverjanje pristnosti (*authentification*), dostop (*access*), zlonamerna programska oprema (*malware*), sistemski dogodki, DoS itd.
14. Rešitev mora v korelacijskih pravilih podpirati uporabo kategorij dogodkov.
15. Rešitev mora podpirati iskanje po dnevniških zapisih s pomočjo regularnih izrazov ali logičnih operatorjev.
16. Rešitev mora podpirati pretakanje dohodnih dogodkov in zapisov toka v realnem času (*real time streaming*), s polno podporo filtriranja po podanih parametrih.
17. Rešitev mora podpirati spremenljivo nadzorno ploščo (*dashboard*) za vizualizacijo ustreznih varnostnih in omrežnih informacij.
18. Rešitev mora podpirati poglobljeno iskanje, tj. razčlenitev dogodkov za podatke, prikazane v uporabniškem vmesniku, kadar je to potrebno.
19. Rešitev mora podpirati generiranje opozoril za zaznane varnostne grožnje, na podlagi izpolnjenih pogojev korelacijskih pravil.
20. Rešitev mora podpirati generiranje korelacijskih pravil, ki vključujejo analizo zapisov dogodkov in tokov znotraj istega pravila, kot tudi posebna pravila samo za zapise dogodkov ali tokov.
21. Rešitev mora podpirati generiranje opozoril za opažene anomalije in vedenjske spremembe dogodkov, pridobljenih z zapisi dogodkov in tokov. Rešitev mora omogočiti, da se anomalije opazijo na več načinov:
 - na podlagi pragov, ko je dejavnost višja ali nižja od definirane,
 - temelji na spremembah vedenja, spremembah obsega glede na običajne vzorce,
 - na podlagi kratkotrajnih odstopanj v aktivnosti, glede na daljši časovni interval.
22. Rešitev mora podpirati omejevanje prikaza več enakih (podvojenih) opozoril.
23. Rešitev mora podpirati pretekle korelacije, na način da lahko uporabniki sprožijo korelacijski postopek nad starimi podatki, s čimer se zagotovi, da se nova pravila ovrednotijo tudi na podlagi starih dogodkov.
24. Rešitev mora podpirati možnost definiranja aktivnosti glede na izpolnjeno korelacijsko pravilo – e-pošta, sistemski dnevnik, interno obvestilo ali izvajanje skripta, ki ga je mogoče po potrebi parametrizirati glede na attribute dogodka.
25. Rešitev mora podpirati kombinacijo dveh ali več incidentov, povezanih z istim, v korelacijskih pravilih definiranim atributom (uporabnik, naslov IP, atribut po meri) v en sam varnostni incident.
26. Rešitev mora podpirati integracijo z viri obveščanja o grožnjah (*threat intelligence feeds*) in izmenjavo informacij prek protokola TAXII.
27. Rešitev mora nuditi integracijo in storitev obveščanja o grožnjah (*threat intelligence feed*), ki jo zagotavlja proizvajalec rešitve.
 - Storitev mora ponuditi poročanje za naslove IP, URL, zgoščene elemente datotek (*file hash*) z znanim zlonamernim ugledom.
28. Rešitev mora podpirati analizo vedenja uporabnikov (*user behavior analysis*) s korelacijo dnevniških zapisov, ki vključujejo uporabniška imena. Vrednost tveganja, dodeljenega uporabniku, se mora dinamično spreminjati v skladu z dejanji uporabnika, ki so v skladu z opredeljenimi pravili. Podprta mora biti možnost uporabe strojnega učenja. Funkcionalnost analize tveganega obnašanja uporabnikov mora biti integrirana v proizvajalčevo rešitev SIEM.
29. Rešitev mora podpirati analizo tokovnih zapisov z uporabo strojnega učenja in identifikacijo anomalij v omrežnem prometu.
30. Rešitev mora podpirati analizo DNS dnevnikov z uporabo strojnega učenja in identifikacijo anomalij, ki lahko kažejo na zlonamerne dejavnosti, kot na primer tuneliranje ali uporaba domensko generiranega algoritma (DGA).
31. Rešitev mora razlikovati lokalni promet od prometa v in iz javnega internetnega omrežja.
32. Rešitev mora podpirati profiliranje komunikacij v in iz javnega internetnega omrežja na podlagi geografskih regij/držav.
33. Rešitev mora podpirati izdelavo in pregled poročil o zbranih dnevniških zapisih.
 - a. Obstoječa poročila (v skladu s PCI DSS, ISO 27001 in podobnimi standardi in kontrolnimi okvirji).



- b. Prilagoditev obstoječih poročil brez posredovanja proizvajalca.
 - c. Kreiranje poročila v formatih PDF, HTML in CSV.
34. Rešitev mora podpirati avtomatsko distribucijo poročil določenim osebam po elektronski pošti.
35. Rešitev mora prepoznati strukturo dnevnika za naslednje sisteme:
- a. Microsoftovi strežniki in delovne postaje
 - b. Strežniki in delovne postaje na osnovi Linux/UNIX
 - c. Strežniki baz podatkov
 - d. Poštni strežniki
 - e. Spletni strežniki
 - f. DNS strežniki
 - g. Programska oprema za zaščito pošte in spleta
 - h. Komercialne aplikacije (WebSphere, aplikacijski strežniki WebLogic itd.)
 - i. Programska oprema za zaščito pred uhajanjem podatkov (Data Leak Protection -DLP).
 - j. Programska oprema za spremljanje aktivnosti baze podatkov (Database Activity Monitoring - DAM).
 - k. Programska oprema za spremljanje celovitosti datotek/dejavnosti (File Integrity/Activity Monitoring - FIM/FAM).
 - l. Programska oprema za upravljanje identitete in dostopa (Identity and Access Management - IAM).
 - m. Sistemi za odkrivanje in preprečevanje vdorov (Intrusion detection/protection systems - IDS / IPS)
 - n. Rešitve proti zlonamerni programski opremi (Anti-malware)
 - o. Imeniški strežniki (npr. AD, LDAP).
 - p. Omrežni tokovi (npr. NetFlow, J-Flow, sFlow, IPFIX itd.)
 - q. Omrežna infrastruktura (npr. stikala, usmerjevalniki itd.)
 - r. Virtualizacijska infrastruktura (npr. VMware ESX)
 - s. Skenerji ranljivosti (Vulnerability scanners)
36. Rešitev mora podpirati zbiranje in shranjevanje tudi dnevniških zapisov, ki niso že vključeni/podprti v rešitvi za razčlenjevanje in analizo. Za takšne zapise mora biti omogočeno definiranje strukture zapisa in pomen atributa dnevnika.
37. Rešitev mora podpirati formate dnevnikov JSON in XML, brez potrebe po ustvarjanju razčlenjevalnikov, ki temeljijo na regularnih izrazih (*regular expressions*).
38. Rešitev mora podpirati grafični urejevalnik za razčlenjevanje in mapiranje dogodkov za dogodke, ki niso že vključeni/podprti v rešitvi.
39. Rešitev mora podpirati vsaj naslednje protokole dogodkov: Syslog (TCP/UDP), WMI, SNMP, JDBC, Checkpoint LEA, Firepower eStreamer, Log File (FTP, SFTP ali SCP).
40. Rešitev mora podpirati vsaj naslednje pretočne protokole: NetFlow, IPFIX, sFlow, JFlow.
41. Rešitev mora podpirati filtriranje dohodnih dogodkov iz zapisov dnevnika v skladu s standardnimi atributi, brez vpliva na licenciranje.
42. Rešitev mora podpirati pošiljanje opozoril sistemskim skrbnikom v primerih, ko pride do težave pri zbiranju zapisov iz izvorne naprave (izvor dnevnika), tj. generiranje opozorila, če v določenem časovnem intervalu ni novih zapisov.
43. Rešitev mora podpirati avtentikacijo lokalnega skrbnika ter možnost preverjanja pristnosti z uporabo računov iz strežnikov Microsoft Active Directory in LDAP.



44. Rešitev mora podpirati dostop do baze vlog (*role bases access*), kjer je mogoče uporabniku omejiti dostop do informacij na določene skupine naprav ali omrežne obsege. Podpora vlog mora biti omogočena tudi prek skupin LDAP, če se LDAP uporablja za preverjanje pristnosti uporabnikov.
45. Rešitev mora podpirati dostop do baz vlog (*role bases access*), kjer je možno omejiti dostop uporabnika do funkcionalnih delov sistema, ki so specifični za njegovo vlogo, npr. administracija, poročanje, iskanje dogodkov itd.
46. Rešitev mora zagotoviti bazo podatkov o sredstvih (*asset database*), ki vsebuje pomembne informacije, pridobljene iz zbranih informacij (sistemski in omrežni atributi, informacije o ranljivosti). Obstajati mora možnost ročnega vnosa in spreminjanja podatkov, če jih ni mogoče samodejno naučiti. Uporabnik mora imeti možnost iskanja po tej bazi podatkov.
47. Rešitev mora omogočati tudi vzdrževanje ažurne baze naprav, ki lahko spreminjajo svoj IP naslov (npr. naprave, ki uporabljajo DHCP).
48. Rešitev mora podpirati samodejno razvrščanje naprav v zbirki sredstev, glede na informacije iz evidence toka. Na primer, sistem mora biti sposoben razvrstiti strežnik kot poštni strežnik ali strežnik baz podatkov.
49. Rešitev mora zagotoviti šifrirano komunikacijo med sistemskimi komponentami, v postavitvi porazdeljenega sistema.
50. Rešitev mora zagotoviti, da v primeru okvare posamezne komponente v postavitvi porazdeljenega sistema vse druge komponente sistema še naprej delujejo.
51. Rešitev mora podpirati notranje preglede stanja sistemskih procesov (*health check*) in uporabnika opozoriti, če se pojavijo težave pri njihovem delovanju.
52. Proizvajalec rešitve mora ponuditi tudi samostojne komponente za zbiranje dnevnikov dogodkov, ki jih je mogoče po potrebi namestiti v oddaljene in/ali zaščitene dele omrežja. Te komponente morajo omogočiti zbiranje zbranih dnevnikov dogodkov tudi v primerih, ko omrežna pravila dovoljujejo promet samo v eni smeri (primer: enosmerni komunikacijski kanal na podlagi UDP).
53. Rešitev mora podpirati več najemništvo (*multitenancy*).
54. Rešitev mora ponuditi dokumentiran REST API, ki omogoča integracijo z drugimi sistemi. Omogočeno mora biti delo z dogodki iz dnevniških zapisov in dogodki dnevnika toka, incidenti in tabelami iskanja (lookup).
55. Rešitev mora biti dimenzionirana in licencirana za podporo:
 - a. zbiranje 5000 dogodkov na sekundo (EPS), z možnostjo razširitve na isto programsko platformo le z dodajanjem licenc. Rešitev za povezovanje dnevnikov naj omogoča tudi zbiranje dogodkov v situacijah, ko pride do nenadnega (kratkoročnega) povečanja števila dogodkov na sekundo (vrh).
 - b. Število virov dnevnika ne sme biti licenčna postavka in ne sme biti omejeno.
 - c. Za izračune je treba upoštevati povprečno velikost dnevnika dogodkov 1500 bajtov.
56. Rešitev mora biti ponujena kot programska naprava, ki jo je mogoče namestiti v virtualizacijsko okolje VMware.
57. Za ponujeno rešitev je potrebno zagotoviti podporo proizvajalca za 12 mesecev.



Storitve:

Namestitev in konfiguracija sistema SIEM:

- Dobava in namestitev programske opreme v predpripravljeno virtualno okolje naročnika
- Sistemska konfiguracija sistema (licence, parametri omrežja, sistemski čas, čas hrambe, nadgradnje, nadzor, ipd.)
- Implementacija zajema dnevniških datotek iz naprav in strežnikov v okolju
- Implementacija varnostnih politik
- Integracija z aktivnim imenikom za avtentikacijo uporabnikov
- Priprava varnostnih skupin ter pravic in omejitev
- Izdelava vmesnikov in zbiranje dogodkov iz poljubnih (angl. Custom) virov
- Izdelava poročil
- Integracija s sistemi Cisco ISE, MS Defender, MVision Mobile, Extreme Hive Manager
- Izobraževanje uporabnikov sistema
- Izdelava projektne dokumentacije



Tehnična usposobljenost kadra:

- 2x IBM Cloud Pak for Security – Administrator
- 1x IBM Cloud Pak for Security – Security Analyst
- 1x IBM Cloud Pak for Security – Security Engineer
- 1x IBM Certified Associate Analyst – IBM Qradar SIEM
- 1x Certified ISO/IEC 27001 Lead Auditor

Komercialni pogoji:

- Rok plačila: 30 dni od prejema računa
- Rok dobave/izvedba storitve:
- Dostava blaga:

Pogoji sprejetih standardov transparentnega poslovanja in smernice korporativne integritete družbe Elektro Maribor d.d. so objavljeni na spletni strani naročnika:

- protikorupcijska klavzula skladno z določili Zakona o integriteti in preprečevanju korupcije – ZintPK (seznanitev)
- določila Kodeksa poslovno etičnega obnašanja v družbi Elektro Maribor d. d.(seznanitev)
- v kolikor ponudbena vrednost ponudnika znaša 10.000,00 EUR ali več, mora ponudnik skupaj s ponudbo oddati tudi ustrezno izpolnjeno Izjavo o lastniški strukturi (Zakon o integriteti in preprečevanju korupcije - ZIntPK). V kolikor so podatki v izjavi, ki jo poda ponudnik, neresnični, je pravni posel ničen. (izpolnitev izjave)

Ponudnik z oddano ponudbo potrjuje pogoje naročnika.

Z najugodnejšim ponudnikom se sklene pogodba za obdobje 1 leta.



ELEKTRO MARIBOR d.d.

TEHNIČNA SPECIFIKACIJA

O.NAB-01

ELEKTRO MARIBOR D.D.
VETRINJSKA ULICA 2
2000 MARIBOR

Kontaktna oseba za tehnično specifikacijo: mitja.trglec@elektro-maribor.si

Ponudbe je potrebno dostaviti na elektronski naslov: mitja.trglec@elektro-maribor.si , **vkjučno do ponedeljka, 27.3.2023, do 15:00 ure.**

PONUDBA MORA BITI PODPISANA IN OŽIGOSANA!

Podpis in žig ponudnika: