Doo” Vodovod i kanalizacija “ Herceg Novi

Herceg Novi, 13.01.2025.g

IZMJENE I DOPUNE TENDERSKE DOKUMENTACIJE , postupak ESJN 85668 ,jednostavna nabavka, Implementacija platforme za rano prepoznavanje IT bezbednosnih incidenata

1.Ovaj uslov se briše:

Ponudjač dostavlja potvrdu/e izdatu/e od strane naručilaca navedenih u prethodnoj izjavi , Kontakt telephone I lica radi provjere od starne naručioca u slucaju potrebe provjere od strane naručioca

2. Sledeći uslov :

“Izjava ponuđača da raspolaže poslovnim kapacitetom, odnosno da je za period koji nije duži do 1 (jedne) godine do dana objavljivanja poziva 31.12.2024..2024. godine), u ugovorenom roku i kvalitetu izvršio najmanje 3 (tri) usluge na bazi istih tehnologija , ponuđač dostavlja:za to treeba da se naglasi u izjavi: - spisak naručilaca kod kojih su izvršene usluge …” se sada mijenja I sada glasi:

Izjava ponuđača da raspolaže poslovnim kapacitetom, odnosno da je za period koji nije duži do 1 (jedne) godine do dana objavljivanja poziva 31.12.2024..2024. godine), u ugovorenom roku i kvalitetu izvršio najmanje 3 (tri) usluge na bazi istih tehnologija i ponuđač dostavlja:za to treeba da se naglasi u izjavi: - spisak naručilaca kod kojih su izvršene usluge , gdje predmetna Izjava treba da sadrzi informacije:

* vrijeme realizacije ugovora I to mjesec i godina početka i zavrsetka posla,
* vrijednost realizovanog ugovora sa PDV-om,
* naziv kupca usluga kome su realizovane predmetne usluge
* kontakt telefon i lice radi provjere naručioca u slučaju potrebe .

3. Tehnička specifikacija se mijenja i sada glasi:

Opis predmeta nabavke:

Implementacija platforme za rano prepoznavanje IT bezbednosnih incidenata

Bitne karakteristike predmeta nabavke:

Implementirana platforma za rano prepoznavanje IT bezbednosnih incidenata MORA DA ISPUNI sledeće funkcionalne zahteve: Prikupljanje i analiza podataka i obaveštavanje o incidentima • Prihvatanje, pohranjivanje i analiza događaja u realnom vremenu poslatih sa postojećih IT sistema (OS radnih stanica, OS servera, rutera, aplikacija, baze podataka, web servera, IDS sistema, firewall-a i dr.). • Brza pretraga, kroz velike količine podataka u cilju digitalne forenzike cyber incidenata • Sistem mora da podrži analizu neograničene količine podataka, limitirane isključivo hardverskim kapacitetima, dok softver ne sme da ima ograničenja u količini podataka za analizu pretraživanja • Pohranjivanje podataka u sledećim oblicima: o originalni tekstualni oblik (originalni, nepromenjen oblik podataka koji će se automatski arhivirati i koristiti pre svega za pravne potrebe); o goli pretraživi podaci (originalni oblik podataka sa dodatnim meta podacima vezanim za način prijema , sa mogućnošću brze pretrage); o parsirani podaci (analizirani podaci na osnovu konteksta i/ili sintaksne strukture u cilju brze pretrage i korelacije događaja); o obogaćeni događaji (originalni događaji kojima se dodaju u realnom vremenu kritične informacije nastale na osnovu korelacije); o sintetički događaji: podaci nastali putem korelacije originalnih podataka. • Platforma za rano prepoznavanje IT incidenata predstavlja ključni element u savremenom informacionom društvu, osiguravajući brzu i efikasnu identifikaciju potencijalnih pretnji i problema u okviru IT okruženja. S obzirom na sve veći broj sajber napada i bezbednosnih izazova, potreba za sopstvenim alatom koji će aktivno monitorisati, analizirati i odgovarati na incidente postaje kritična. U tom kontekstu, ključna specifikacija koja se zahteva za ovakvu platformu je integracija i korišćenje standardizovanog formata IDMEF (Intrusion Detection Message Exchange Format), kako je definisano u IETF RFC 4765. IDMEF predstavlja standard koji omogućava uniformnost u obliku poruka koje se koriste za izveštavanje o sigurnosnim incidentima. Specifičnost ovog formata je u njegovoj univerzalnosti - on ne samo što podstiče saradnju i integraciju između različitih sigurnosnih sistema, već takođe omogućava upoređivanje i korelaciju upozorenja iz više heterogenih izvora, poput različitih operativnih sistema, mrežnih uređaja, aplikacija, i drugih sistema. Ovo je posebno značajno u detektovanju složenih napada koji zahtevaju analizu preko više sistema. Navedena platforma, s tim u vidu, mora imati sposobnost da transformiše klasične logove, koji su proizvedeni od strane različitih izvora (OS radnih stanica, OS servera, rutera, aplikacija, baza podataka, web servera, IDS sistema, firewall-a i dr.) u IDMEF upozorenja. Ova konverzija omogućava standardizaciju svih sigurnosnih upozorenja, što doprinosi efikasnijoj obradi i odgovoru na incidente. Dalje, interfejs platforme mora biti dizajniran tako da pruža intuitivan i jasan pristup svim sigurnosnim upozorenjima koja se generišu, s obzirom na to da IT stručnjaci treba da imaju mogućnost da brzo identifikuju i odgovore na potencijalne pretnje. Stoga, interfejs mora podržavati bilo koju vrstu pretraživanja, sortiranja i filtriranja na svakom polju unutar IDMEF sadržaja. Ova funkcionalnost omogućava personalu da efektivno upravlja upozorenjima, prilagođavajući prikaz podataka svojim potrebama, i time značajno ubrzava proces odlučivanja. Uključivanjem ovih specifikacija, platforma za rano prepoznavanje IT incidenata postaje moćan alat koji ne samo da povećava sigurnost informacionog sistema, ali takođe značajno doprinosi optimalnom raspredelom resursa, jer omogućava IT stručnjacima da se fokusiraju na najkritičnije upozorenja i incidente, time povećavajući ukupnu efikasnost upravljanja informacionim sistemima. • Anonimizacija svih logova u skladu sa GDPR Kreiranje, uspostavljanje i održavanje jedinstvenog registra informacionih logova na ključnim elementima informacionog sistema, u okviru kojeg je neophodno pseudonimizirati i/ili anonimizirati sve prikupljene podatke u realnom vremenu, kao jednoj od ključne mere zaštite podataka o Anonimizacija podataka u realnom vremenu, čime se onemogućava bilo koji vid pretrage i skladištenja privatnih podataka korisnika sistema o Mogućnost otkrivanja anonimiziranih podataka, a na osnovu dodatnih informacija poznatih samo korisniku, na specifične ili zahteve u skladu sa zakonom. • Korelacija: o korelacija u realnom vremenu u cilju prepoznavanja poznatih vektora napada, a takođe i prepoznavanja anomalija u ponašanju na osnovu statističkih modela; o mogućnost „obogaćivanja“ originalnih podataka na osnovu korelacije; o kreiranje „Skupovnih“ događaja koji uključuju sve varijacije međusobno korealisanih događaja u događaju, isključujići potrebu za čuvanjem svih relevatnih događaja; o mogućnost adekvatne reakcije u cilju prevencije ili minimizacija posledica. o mogućnost implementairanja bilo koje poslovne logike u korelacionim pravilima; o Predefinisana baza korelacionih pravila , kao i mogućnost povezevanja na centralnu bazu korelacionih pravila proizvođača rešenja/platforme o istorijska korelacija za otkrivanje sporih, niskoprofilnih napada, kao i retroaktivne korelacije novootkrivenih vektora napada nad starim podacima; o integracija sa bazom VirusTotal(Virustotal) u cilju višestruke detekcije malicioznih/inficiranih procesa, a takođe i radi retroaktivne analize svih ikada startovanih procesa; o integracija sa javnim i komercijalnim threat intelligence sistemima u cilju korelacije sa lokalnim podacima i detekcije APT napada. • Vizuelna rekonstrukcija aktivnosti sistema/procesa/zaposlenih i mogućnost praćenja aktivnosti kroz vreme, a u cilju praćenja kompleksnih lanaca događaja radi lakše detekcije i forenzike napada. • Mogućnost vizuelnog praćenja aktivnosti administratora u realnom vremenu (praćenje pristupa sistemima, startovanih procesa, pristupa fajlovima i druge aktivnosti) i prikaz kroz interaktivne grafove. Raspoređivanje i praćenje sajber zamki Raspoređivanje i praćenje cyber zamki je potrebno u cilju proaktivne detekcije aktivnosti uljeza kod Naručioca. Zamke moraju biti podržane za svaku fazu napada, uključujući zamke na nivou operativnih sistema, mreža, lažnih servisa, memorije sistema, markiranih dokumenata. Raspoređivanje i praćenje cyber zamki podrazumeva sledeće: • Mogućnost postavljanja zamki koje simuliraju regularne sisteme a u cilju navođenja napadača na pogrešne korake, u cilju detekcije u realnom vremenu, svakog pokušaja i to vezano za lokaciju napadača (njegov IP i geolokaciju), način napada (vektor napada koji ukazuje na način na koji je izvršen napad (npr SQL injection string, vrsta logona…), kao i konkretne alatke koje napadač pokušava da uploaduje (malware, C&C programme, exploite..). • Zamke se postavljaju eksterno (na javnim IP adresama) ili interno (unutar korisničke LAN mreže). • Sledeće vrste zamki moraju da budu zadovoljene: o standardni servisi (zamke koje pružaju standardne servise kao što su samba, ftp, telnet, ssh, http i drugi), o digitalni klonovi: kloniranje specifičnog servisa u cilju otkrivanja njegovih ranjivosti i ranog otkrivanja napadača (npr kloniranje web kamera, web servisa, IoT uređaja...) o ubacivanje zamki u memoriju računara u cilju pogrešne detekcije postojećih servisa i korisničkih lozinki, o ubacivanje zamki u dokumente (doc, pdf) u cilju detekcije pokušaja otvaranje dokumenta. • Sistem za praćenje aktivnosti na svim zamkama u realnom vremenu, sa geo mapom i identifikacijom geo lokacije odakle napad dolazi kao i praćenje statistike napada za svaku od zamki. • Centralna registracija svake zamke pre integracije u sistem, u cilju sprečavanja slanja lažnih informacija. • Mogućnost rada zamki na virtualnim mašinama kao i rada na eksternim uređajima. • Mogućnost pravljenja zamki po narudžbini, po specifičnim zahtevima. • Integracija zamki sa centralnim sistemom za praćenje, u cilju integracije podataka, korelacije sa drugim događajima u sistemu, vizuelne rekonstrukcije, kao i automatske remedijacije • Arhitektura: o mogućnost distribuiranog procesiranja: mogućnost horizontalne skalabilnosti Sistema tako da se određene faze procesiranje mogu izvršavati paralelno na različitim sistemima; o dinamičko rutiranje događaja: mogućnost rutiranja događaja na različite putanje procesiranja u zavisnosti od sadržaja samog događaja; o kompletan sistem mora podražavati izvršavanje na virtuelnim mašinama. \* Broj radnih stanica je 100, sa mogućim proširenjem do 200.

Količina: 1

jedinica mjere je: komplet usluga.

Napomena: rok podnošenja I otvaranja ponuda ostaje nepromijenjen, 17.01.2025.g. - 09 časova.

Službenik za javne nabavke

Svetlana Grubač