# Prilog 3. Tehnički uvjeti
# Usluga pronalaska proboja

## Uvod

Sa obzirom na aktualne prijetnje, potrebno je analizirati IT okruženje kako bi se ustanovilo da li postoje potencijalni proboji na krajnjim točkama koji su zaobišli postojeće sigurnosne kontrole. Uslugu pronalaska proboja je potrebno izvršiti za sve radne stanice i poslužitelje unutar tvrtke. Broj krajnjih točaka na kojima se potrebno izvršiti uslugu je 1200.

## Opseg projekta

Ponuditelj mora izvršiti skeniranje svih krajnjih točaka alatom za pronalazak i analizu proboja te izvršiti automatsku i ručnu analizu svih indikatora koji upućuju na proboj ili neautorizirani pristup sustavima koji su u opsegu.

Analiza i prikupljanje indikatora sa krajnjih točaka treba biti izvršena sa centralne konzole. Svi indikatori moraju bit prikupljeni na centralno lokaciju gdje će se mora izvršiti automatska i ručna analiza od strane stručnjaka za pronalazak naprednih prijetnji.

Ponuditelj u usluzi analize i pronalaska prijetnji i proboja mora obuhvatiti najmanje sljedeće:

| R. Br. | Specifikacija tražene usluge | Popunjava ponuditelj | |
|---|---|---|---|
| | | Ponuđeno (Da/Ne) | Bilješke/ Napomene |
| 1. | Analizu arhitekture okruženja te izradu plana za instalaciju softverskih agenata | | |
| 2. | Instalaciju agenata softverskog rješenja za pronalazak, detekciju i analizu proboja na 1200 krajnjih točaka. U slučaju nemogućnosti instalacije agenta, spajanje na krajnju točku bez agenata (eng. „*agentless*“). | | |
| 3. | Implementaciju komponenti za prikupljanje artefakata i indikatora kompromisa. | | |
| 4. | Izvršiti skeniranja krajnjih točaka u svrhu prikupljanje artefakata i indikatora kompromitacije i/ili proboja. Indikatori proboja i/ili kompromitacije koji najmanje moraju biti prikupljeni su:<br>• **Procesi**: procesi s određenim imenima, putovima datoteka, kontrolnim zbrojevima i mrežnom aktivnošću. Potrebno je pronaći procese koji mijenjaju stavke registra, imaju određene podređene procese, pristupaju određenim softverskim bibliotekama, imaju specifične MD5 hash-eve, vrše određene izmjene ključa registra i uključuju poznate loše datoteke<br>• **Binarne datoteke**: Pretraživanje binarnih datoteka s određenim kontrolnim zbrojevima, imenima datoteka, stazama, meta podacima, određenim izmjenama registra.<br>• **Mrežna aktivnost**: Analiza komunikacije mrežne aktivnosti prema određenim imenima domena i IP adresama. | | |

| | | | |
|---|---|---|---|
| | • **Izmjene ključa registra**: dodavanja i izmjene ključa registra<br>• **Memorija**: Pretraživanje memorijskih lokacija za sumnjivim stringovima („strings“). Rekonstrukcija događaja vezanih za command line. Analiza artefakata prisutnih u memoriji<br>• **Trajne lokacije („autoruns“)**: Prikupljanje i analiza artefakata na lokacijama koje omogućavaju trajnu mogućnost izvršavanja naredbi i koda | | |
| 5. | Izvršiti automatsku analizu prikupljenih artefakata i indikatora od strane softvera za pronalazak i analizu proboja i indikatora kompromitacije | | |
| 6. | Izvršiti ručnu analizu prikupljenih artefakata i indikatora od strane stručnjaka za detekciju i pronalazak naprednih prijetnji i proboja | | |
| 7. | Izvršiti inicijalnu analizu malicioznog koda i datoteka ukoliko isti bude pronađen sa ciljem ukazivanja na vektor kompromitacije, metodu širenja i način trajnog prisustva | | |
| 8. | Izvršiti dodatnu analizu pronalazaka koji upućuju na proboj ili kompromitaciju ručnim forenzičkim tehnikama i/ili prema potrebi alatima otvorenog koda | | |
| 9. | U slučaju pronalaska prijetnji i proboja odmah obavijestiti odgovorno osoblje Naručitelja o pronađenim prijetnjama sa prijedlozima i uputama za rješavanje | | |
| 10. | Izraditi izvještaj o izvršenim aktivnostima i potencijalno pronađenim prijetnjama sa uputama o uklanjaju i rješavanju istih | | |

## Tehnička specifikacija mogućnosti alata za pronalazak, detekciju i analizu proboja

U svrhu osiguranja kvalitete usluge, alat za pronalazak, detekciju i analizu proboja treba zadovoljavati najmanje sljedeće tehničke karakteristike:

| | **TEHNIČKE SPECIFIKACIJE** | **Popunjava ponuditelj** | |
|---|---|---|---|
| | | **Ponuđeno (Da/Ne)** | **Bilješke/ Napomene** |
| 1. | Rješenje mora imati mogućnost instalacije u oblaku i na lokaciji Naručitelja | | |
| 2. | Rješenje mora podržavati način rada sa instalacijom agenata | | |
| 3. | Rješenje mora podržavati način rada bez instalacije agenata | | |
| 4. | Rješenje mora podržavati pronalazak krajnjih točaka na mreži | | |
| 5. | Rješenje pora podržavati protokole za spajanje na krajnje točke (SSH, WMI) | | |
| 6. | Podrška za operativne sustave OSX, Windows i Linux | | |
| 7. | Mogućnost analize reputacije procesa | | |
| 8. | Integracija sa VirtusTotal analizom | | |
| 9. | Podrška za strojno učenje | | |
| 10. | Podrška za statičku analizu | | |
| 11. | Podrška za detonaciju sumnjivih datoteka u virtualnom okruženju u oblaku (Sandboxing) | | |
| 12. | Podrška za Yara pravila | | |
| 13. | Mogućnost analize memorije | | |
| 14. | Mogućnost detekcije tehnike „Process Injection“ | | |
| 15. | Mogućnost detekcije tehnike „Atom Bombing“ | | |
| 16. | Mogućnost detekcije tehnike „Process Hollowing“ | | |
| 17. | Mogućnost detekcije tehnike „In-Memory Module Injection“ | | |
| 18. | Mogućnost detekcije tehnike „Reflective DLL Injection“ | | |
| 19. | Mogućnost detekcije tehnike „Process doppelganging“ | | |
| 20. | Mogućnost izračuna količine vremena koje je napadač proveo u sustavu | | |
| 21. | Podrška za izradu ekstenzija pisanih u LUA formatu | | |
| 22. | Rješenje mora moći pronaći ranjivosti na sustavima koji su skenirani te prikazati razinu ranjivosti prema CVSS rangu | | |

**IZJAVA**

**D52/21**

Izjavljujemo da prihvaćamo ove Tehničke uvjete

Naziv ponuditelja: .....

Ovlaštena osoba: .....

Potpis: .....

U ..... 2021. godine