სამუშაო სადგურების დაცვის პროგრამული უზრუნველყოფის და EDR გადაწყვეტილების შესყიდვის ტექნიკური დავალება

შესასყიდი პროდუქტი

Part Number	აღწერა	რაოდენობა	ლიცენზიის ვადა
CEBAJE-AA	Complete EP Protect Bus 1:1TE [P+]	1500	10 აპრილი, 2025 წელი
MV4ECE-AA	Trellix EDR 1:1 TE 30 Day Storage	1500	10 აპრილი, 2025 წელი

ტექნიკური მოთხოვნები სამუშაო სადგურების ცენტრალური მართვის კონსოლისა და EDR სისტემისთვის

1. EDR სისტემას უნდა ქონდეს შესაძლებლობა დაინტეგრირდეს კომპანიის ინფრასტრუქტურაში არსებულ სამუშაო სადგურების ცენტრალურ მართვის კონსოლთან
2. EDR სისტემა აგენტების საშუალებით უნდა უკავშირდებოდეს სამუშაო სადგურებს
3. EDR სისტემას უნდა შეეძლოს მუდმივად ამონიტორინგოს, აღმოაჩინოს და გამოიკვლიოს პოტენციური საფრთხეები სამუშაო სადგურებზე
4. EDR სისტემას უნდა ქონდეს ღრუბლოვან სერვისზე დაფუძნებული ანალიტიკა
5. EDR სისტემას უნდა ქონდეს ქცევაზე დაფუნძნებული გამოვლენის რუკა MITRE ATT&CK™
6. EDR სისტემას უნდა ქონდეს ისტორიული და რეალური დროში ძებნის ფუნქცია
7. EDR სისტემას უნდა ქონდეს ხელოვნური ინტელექტის დახმარებით კვლევის ფუნქციონალი
8. სამუშაო სადგურების ცენტრალური მართვის კონსოლიდან უნდა ხდებოდეს ლიცენზიების მართვა
9. სამუშაო სადგურების ცენტრალური მართვის კონსოლიდან მონაცემების შენახვა უნდა ხდებოდა მონაცემთა ბაზაში
10. სამუშაო სადგურების ცენტრალური მართვის კონსოლის უნდა შეეძლოს ინტეგრაცია ავთენთიფიკაციისთვის ისეთ სისტემებთან როგორებიცაა LDAP, AD და სხვა ფართოდ გავრცელებული სისტემები.
11. კავშირი სამუშაო სადგურების ცენტრალური მართვის კონსოლისა და აგენტს შორის უნდა იყოს დაშიფრული თანამედროვე შიფრაციის მეთოდებით
12. სამუშაო სადგურების ცენტრალური მართვის კონსოლს უნდა ქონდეს მაღალი ხელმოსაწვდომობის ფუნქციონალის (HA) რეჟიმის მხარდაჭერა
13. სამუშაო სადგურების ცენტრალური მართვის კონსოლის უნდა ქონდეს REST API მხარდაჭერა
14. სამუშაო სადგურების ცენტრალური მართვის კონსოლს და EDR სისტემას უნდა ქონდეს აგენტების ავტომატურად ან მექანიკურად დაყენება წაშლის შესაძლებლობა
15. EDR სისტემას უნდა შეეძლოს მინიმუმ შემდეგი მოქმედებების დისტანციურად გაშვება სამუშაო სადგურებზე:
    15.1. სამუშაო სადგურის იზოლირება კომპიუტერული ქსელიდან
    15.2. საფრთხის შემცვლელი ფაილების ატვირთვა / კოპირება / წაშლა
    15.3. საფრთიხს შემცვლელი პროცესების გაჩერება / წაშლა
    15.4. პროცესის მეხსიერების დამუშავება
    15.5. სკრიპტის გაშვება CMD , PowerShell, Python და სხვა საშუალებით
16. სამუშაო სადგურების ცენტრალური მართვის სისტემას უნდა შეეძლოს აგენტების დაჯგუფება (ავტომატური და მანუალური მეთოდის გამოყენებით)
17. სამუშაო სადგურების ცენტრალური მართვის სისტემას უნდა შეეძლოს დააყაროს კავშირი აგენტებთან რომლებიც არ იმყოფებიან კომპანიის ქსელში
18. სამუშაო სადგურების ცენტრალური მართვის სისტემას უნდა შეეძლოს კონფიგურაციის და მონაცემთა ბაზის სარეზერვო ასლის აღება

19. სამუშაო სადგურების ცენტრალური მართვის სისტემას უნდა შეეძლოს EDR სისტემის მონაცემების დამუშავება და რეპორტის მომზადება
20. სამუშაო სადგურების ცენტრალური მართვის სისტემას უნდა შეეძლოს ინტეგრაცია SIEM სისტემასთან.
21. სამუშაო სადგურების დაცვის სისტემას უნდა შეეძლოს ფაილებზე მიმართვის დროს (ე.წ. On-Access Scan), წაკითხვისას, ჩაწერისას და მათი დეტალური სკანირება;
22. სამუშაო სადგურების დაცვის სისტემას უნდა შეეძლოს ინფორმაციის შენახვა წარსული შემოწმებიდან და სკანირების ასაჩქარებლად ქეშის გამოყენება;
23. სამუშაო სადგურების დაცვის სისტემას უნდა გააჩნდეს ჩაშენებული მოდული ექსპლოიტების აღმოსაფხვრელად;
24. სამუშაო სადგურების დაცვის სისტემას უნდა შეეძლოს ოპერაციული სისტემის და გავრცელებული პროგრამების სისუსტეების სიგნატურების (ხელწერის) რეგულარული განახლებები შეღწევადობის გამაფრთხილებელი ჩაშენებული მოდულით;
25. სამუშაო სადგურების დაცვის სისტემას უნდა შეეძლოს სიგნატურული (ხელწერის) და ღრუბლოვანი ანალიზის შედეგებისგან დამოუკიდებლად პოტენციურად საფრთხის შემცველი აპლიკაციის ქმედების ბლოკირება;
26. სამუშაო სადგურების დაცვის სისტემას უნდა შეეძლოს სხვადასხვა კატეგორიის წყაროებზე წვდომის ბლოკირება;
27. სამუშაო სადგურების დაცვის სისტემას უნდა შეეძლოს სამუშაო სადგურის სრული დაცვა, რომელიც არ არის დაკავშირებული ცენტრალურ მართვის სისტემასთან;

აგენტის ტექნიკური მოთხოვნები

1. აგენტს უნდა ქონდეს შესაძლებლობა რომ შეზღუდოს სამუშაო სადგურის პროცესორის რესურსის გამოყენება
2. აგენტის დაინსტალირება შესაძლებელი უნდა იყოს შემდეგი მეთოდებით:
   2.1. დისტანციურად ინსტალაცია სამართავი პანელიდან ან სხვა დისტანციური მეთოდებით
   2.2. მექანიკურად ინსტალაცია
3. აგენტის უნდა ქონდეს შესაძლებლობა შეცვალოს საცავის ლოგირების ზომა და მათი შენახვის პერიოდი
4. აგენტის დაყენება უნდა შეიძლებოს შემდეგ ოპერაციულ სისტემებზე:
   4.1. Windows 10 და ზევით
   4.2. Windows Server 2016 და ზევით
   4.3. Oracle Linux 7
   4.4. Red Hat Linux 7/8
   4.5. CentOS 7/8
   4.6. macOS Sonoma / Ventura / Monterey
5. აგენტს უნდა ქონდეს დაცვა ცენტრალიზირებული პოლიტიკიდან მისი წაშლის ან მოდიფიკაციაზე
6. აგენტს უნდა შეეძლოს დააგენერიროს პროცესების / ფაილების „hash sum“ MD5, SHA-1, SHA-256 ალგორითმების მიხედვით.

მოთხოვნები პროდუქტის მწარმოებლის მიმართ

1. სამუშაო სადგურის მართვის და EDR სისტემა უნდა იყოს ერთიდაიმავე მწარმოებლის.
2. შემოთავაზებული პროდუქტს უნდა შეეძლოს როგორც მინიმუმ იმავე მწარმოებლის მონაცემთა გაჟონვის პრევენციის (DLP) სისტემასთან ინტეგრაცია.

მოთხოვნები პრეტენდენტი კომოანიის მიმართ

1. პრეტენდენტი კომპანია უნდა იყოს მწარმოებელი კომპანიის ოფიციალური პარტნიორი საქართველოში და უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა.
2. პრეტენდენტ კომპანიას უნდა ჰქონდეს მინიმუმ 1 ანალოგიურ პროექტის განხორციელების გამოცდილება.
3. პრეტენდენტ კომპანიას უნდა ჰყავდეს მინიმუმ 1 სერთიფიცირებული ქართველ ენოვანი ინჟინერი End point და EDR მიმართულებით.