ა(ა)იპ სავალდებულო დაზღვევის ცენტრი აცხადებს ტენდერს უსაფრთხოების ინფორმაციისა და შეტყობინებების მართვის სისტემის (SIEM) და ანტივირუსის (Endpoint security) შესყიდვაზე, 1 წლიანი ლიცენზიითა და მწარმოებლის მხარდაჭერით

ტენდერის ამოცანა:

ტენდერის ამოცანას წარმოადგენს - ტექნიკური მოთხოვნების შესაბამისად უსაფრთხოების ინფორმაციისა და შეტყობინებების მართვის სისტემის (SIEM) და მისი ინსტალაციასა და კონფიგურირების მომსახურების შესყიდვას, ასევე 120 ერთეული ანტივირუსის და ორივე პროგრამული პაკეტის ცენტრალური მართვის კონსოლზე მიერთების მომსახურების შესყიდვას ოპტიმალურ ფასად. უსაფრთხოების ინფორმაციისა და შეტყობინებების მართვის სისტემას (SIEM) და ანტივირუსის (Endpoint security) უნდა მოყვებოდეს შესაბამისი რაოდენობის 1 წლიანი ლიცენზია და მწარმოებლის მხარდაჭერა.

მოთხოვნები SIEM გადაწყვეტილების შესყიდვასთან დაკავშირებით:

- SIEM გადაწყვეტილების შემავალი ყველა კომპონენტი უნდა ფუნქციონირებდეს ერთი ვირტუალური მანქანის (All-in-one) მეშვეობით.
- SIEM გადაწყვეტილების ყველა კომპონენტის, ფუნქციონალის მართვა უნდა ხორციელდებოდეს ცენტრალიზებულად, ერთიანი Web ინტერფეისის საშუალებით;
- SIEM-ის გადაწყვეტილებაში შესაძლებელი უნდა იყოს საინფორმაციო რესურსების (წყაროების) ხდომილებების ჟურნალირება, დამუშავება, კორელაცია და ანალიტიკა;
- SIEM გადაწყვეტილებას უნდა ჰქონდეს API, მონაცემთა ბაზაში განთავსებული ინფორმაციის გაზიარებისათვის;
- SIEM გადაწყვეტილება უნდა ინტეგრირდებოდეს MS AD-სთან, მომხმარებლების აუტენტიფიკაციის უზრუნველყოფისათვის;
- SIEM გადაწყვეტილებას უნდა ჰქონდეს ცალკეული კომპონენტების მუშაობის უზრუნველყოფის საშუალება ერთ-ერთი კომპონენტის მწყობრიდან გამოსვლის შემთხვევაშიც (მაგალითად, ცენტრალური კონსოლის მწყობრიდან გამოსვლის შემთხვევაში ხდომილებების მიმღები სისტემა უნდა აგრძელებდეს ფუნქციონირებას);
- SIEM გადაწყვეტილებას უნდა ჰქონდეს კონფიგურაციის ავტომატიზებული რეზერვირების (Backup) და აღდგენის (Recovery) შესაძლებლობა მომხმარებლის გრაფიკული კონსოლიდან;
- SIEM გადაწყვეტილებას უნდა ქონდეს თავისი მდგომარეობის ანალიზის შესაძლებლობა და მომხმარებლის შეტყობინების საშუალება პრობლემის წარმოქმნის შემთხვევაში;
- SIEM გადაწყვეტილებას ლიცენზიით უნდა შეეძლოს ნაკადების (Flows) წაკითხვა და დამუშავება:
    - უნდა ქონდეს NetFlow პროტოკოლის პროტოკოლების მხარდაჭერა;
    - VMware-ს ვირტუალური ინფრასტრუქტურის ნაკადების წაკითხვა და დამუშავება;
- პიკური დატვირთვის დროს თუ ხდომილებების და/ან ნაკადების რაოდენობამ წამში გადააჭარბა 1,250-ს, SIEM გადაწყვეტილებამ უნდა შეატყობინოს სისტემის ადმინისტრატორს და მონაცემების დაუკარგავად გააგრძელოს ფუნქციონირება;
- SIEM გადაწყვეტილებას უნდა ქონდეს საინფორმაციო რესურსების (წყაროების) ხდომილებების ჟურნალების არქივაციის შესაძლებლობა. ჟურნალების შენახვა შესაძლებელი უნდა იყოს როგორც online, ასევე offline რეჟიმში;
- SIEM გადაწყვეტილებას უნდა შეეძლოს ჟურნალების შენახვა გარე მატარებლებზე;
- SIEM გადაწყვეტილებას უნდა ჰქონდეს აგენტების გარეშე ხდომილებების შეგროვების შესაძლებლობა, იქ სადაც ეს შესაძლებელია;
- SIEM გადაწყვეტილებას უნდა შეეძლოს ხდომილებების სრულ ინფორმაციაზე (პირვანდელი მდგომარეობით) წვდომის უზრუნველყოფა, ხდომილებების არსებობის პერიოდის განმავლობაში;
- SIEM გადაწყვეტილებას უნდა შეეძლოს ხდომილებების ინფორმაციის შენახვა, როგორც საწყის ფორმაში, ასევე ნორმალიზებული სახით, შემდგომი ანალიზისათვის;
- SIEM გადაწყვეტილებას უნდა ჰქონდეს ხდომილებების ანალიზის შესაძლებლობა რეალურ

რეჟიმში;

- SIEM გადაწყვეტილებას უნდა ჰქონდეს ხდომილებების ანალიზის შესაძლებლობა კონკრეტული პერიოდის განმავლობაში, რომელიც მითითებული იქნება ანალიტიკოსის/ადმინისტრატორის მიერ;
- SIEM გადაწყვეტილებაში რეალიზებული უნდა იყოს რეპორტების გენერაციის შესაძლებლობა. სისტემაში უნდა არსებობდეს წინასწარ განსაზღვრული რეპორტების ნიმუშები (შაბლონები). ასევე სისტემაში უნდა იყოს საკუთარი რეპორტების გენერაციის შესაძლებლობა;
- SIEM გადაწყვეტილებაში რეალიზებული უნდა იყოს, გარკვეული დროის პერიოდში, რეპორტების ავტომატიზირებული გენერაციის შესაძლებლობა;
- SIEM სისტემაში უნდა არსებობდეს ხდომილებების კორელაციის გამზადებული წესები (წესების ჩამონათვალი);
- SIEM გადაწყვეტილებაში რეალიზებული უნდა იყოს IP Reputation მექანიზმები. სისტემას ავტომატიზირებულად უნდა შეეძლოს შეერთებების გამოვლენა:
    - BotNet ქსელებთან;
    - Mailware რესურსებთან;
    - Spam საიტებთან;

- SIEM გადაწყვეტილებას უნდა შეეძლოს ცენტრალიზებული Web ინტერფეისიდან არსებული McAfee/Trellix მონაცემთა გაჟონვის პრევენციის მართვის ცენტრის ინტერფეისის გახსნა და შემდგომი კონფიგურაცია. აღნიშნული ფუნქციონალი იმპლემენტირებული უნდა იყოს სისტემის კონფიგურაციის პროცესში მომწოდებლის მიერ.

მინიმალური მოთხოვნები SIEM გადაწყვეტილების წარმადობაზე:

ხდომილებების დამუშავება	არანაკლებ 1,250 ხდომილება წამში
მაქსიმალური ხდომილებების მიღების შესაძლებლობა	არანაკლებ 3,000 ხდომილება წამში.

- SIEM გადაწყვეტილების ლიცენზირება უნდა ზღუდავდეს საინფორმაციო რესურსების / წყაროების (Data Sources) რაოდენობას, საიდანაც სისტემა მიიღებს ხდომილებებს (Events/Flow)

1. დეტალური ტექნიკური მოთხოვნები SIEM გადაწყვეტილებაში შემავალი კომპონენტების (All-in-one) მიმართ:

მართვის ძირითადი სისტემა:

- მართვის ძირითად სისტემაში უნდა ინტეგრირდებოდეს SIEM გადაწყვეტილებაში შემავალი ყველა სისტემა;
- მართვის ძირითად სისტემას უნდა შეეძლოს რეალურ დროში სისტემების, ქსელების, მონაცემთა ბაზებისა და აპლიკაციების ქმედების ჩვენება, ხდომილებების შეგროვება, დამუშავება;
- მართვის ძირითად სისტემას უნდა გააჩნდეს ინტერაქტიული და რედაქტირებადი ხელსაწყოთა პანელი, რომლის გამოყენებაც შესაძლებელი იქნება ინციდენტის გამოძიებისას;
- მართვის ძირითად სისტემას უნდა გააჩნდეს ცენტრალიზებული ანალიტიკის ხელსაწყოთა პანელი;
- მართვის ძირითად სისტემას უნდა გააჩნდეს წინასწარ შედგენილი ხელსაწყოთა პანელი;
- მართვის ძირითად სისტემა უნდა წარმოადგენდეს პროგრამულ გადაწყვეტილებას;

ჟურნალების მართვის სისტემა

- ჟურნალების მართვის სისტემა უნდა იძლეოდეს წვდომის საშუალებას ე.წ. ერთი ღილაკის დაჭერით, მის მოდულში არსებული ყველა ჟურნალის ჩანაწერის ორიგინალში ნახვის საშუალებას;
- ჟურნალების მართვის სისტემას უნდა გააჩნდეს ჟურნალების შეგროვებისა და შენახვის საჭირო ფუნქციონალი;
- ჟურნალების მართვის სისტემა უნდა იძლეოდეს ჟურნალების შენახვის საშუალებას ლოკალურად მოდულში, ან გარე შესანახ არეაში (storage area);
- ჟურნალების მართვის სისტემა უნდა იძლეოდეს მეხსიერების საცავის რამდენიმე აპარატურისგან შედგენის საშუალებას და მონაცემების მიბმას კონკრეტულ მეხსიერების საცავზე.

ხდომილებების მიმღები სისტემა

- სისტემას უნდა შეეძლოს ხდომილებებისა და ნაკადების (Flows) სხვადასხვა სისტემებიდან მიღება.
- სისტემას უნდა შეეძლოს ფუნქციონალურად დაამუშაოს ხდომილებები და შეინახოს მონაცემთა ბაზაში ინდექსირებული სახით, რათა შესაძლებელი იყოს სწრაფი წვდომა საჭიროების შემთხვევაში;
- სისტემა უნდა წარმოადგენდეს პროგრამულ გადაწყვეტილებას.

2. მოთხოვნები ანტივირუსის შესყიდვასთან დაკავშირებით:

- სისტემას უნდა შეეძლოს ინფორმაციის შენახვა წარსული შემოწმებიდან და სკანირების ასაჩქარებლად ქეშის გამოყენება.
- სისტემას უნდა გააჩნდეს ჩაშენებული მოდული ექსპლოიტების აღმოსაფხვრელად.
- სისტემას უნდა შეეძლოს ოპერაციული სისტემის და გავრცელებული პროგრამების სისუსტეების სიგნატურების (signatures) რეგულარული განახლებები.

- სისტემას უნდა შეეძლოს ფაილის საკონტროლო ჯამის (checksum) რეპუტაციის ღრუბლოვანი ანალიზი.
- სისტემას უნდა შეეძლოს სიგნატურული (signatures) და ღრუბლოვანი ანალიზის შედეგებისგან დამოუკიდებლად პოტენციურად საფრთხის შემცველი აპლიკაციის ქმედების ბლოკირება.
- სისტემას უნდა შეეძლოს ანტივირუსული მოდულების (ინდივიდუალური ან ყველა) პარამეტრების პაროლით დაცვა.
- სამუშაო სადგურის ფაერვოლი მხარდაჭერილი უნდა იყოს სწავლების ან ავტომატიზებული მუშაობის რეჟიმით.
- სისტემას უნდა გააჩნდეს შეღწევადობის აღმომჩენი სისტემა გაშვებული პროცესების მეხსიერების კონტროლით.
- სისტემას უნდა შეეძლოს იმ ოპერაციული სისტემებისა და პროგრამების დაცვა, რომლებიც გარკვეული მიზეზების გამო ხშირად ვერ იღებენ განახლებებს.
- სისტემას უნდა შეეძლოს URL-ის რეპუტაციაზე შემოწმება
- სისტემას უნდა შეეძლოს გარკვეული კატეგორიის წყაროებზე წვდომის ბლოკირება.
- სისტემას უნდა შეეძლოს ე.წ. „შავი სიის“ შექმნა URL-ის რეპუტაციისაგან დამოუკიდებლად;
- სისტემას უნდა შეეძლოს აპლიკაციის ან/და სკრიპტების გაშვების ბლოკირება დროებითი ფაილების კატალოგებიდანაც.
- სისტემას უნდა შეეძლოს ფაილური სისტემის და რეესტრის დონეზე დაცვის საკუთარი წესების შექმნის შესაძლებლობა.
- სისტემას უნდა შეეძლოს ბრაუზერების, ქსელის პარამეტრების და ფაილური ასოციაციების ცვლილებებისაგან დაცვა.
- სისტემას უნდა შეეძლოს გარე მატარებლების (USB) მონიტორინგი, იძულებით ბლოკირება ან გადაყვანა “readonly” რეჟიმში.
- სისტემას უნდა შეეძლოს გარე მატარებლების (მოდემების, გაფართოების ბარათების და ა.შ.) მონიტორინგი და/ან ბლოკირება.
- სისტემას უნდა შეეძლოს გარე მატარებლებზე ან/და გარე მატარებლებიდან დოკუმენტების ჩაწერა/კოპირების მცდელობის ბლოკირება, რომელიც ემთხვევა კლიენტის მიერ მითითებულ ციფრულ ხელმოწერას ან შეიცავენ სიტყვებს და განსაზღვრულ ფრაზებს.
- სისტემას უნდა შეეძლოს გამოყენებაზე თვალთვალის და ბლოკირების შესაძლებლობა.
- სისტემას უნდა შეეძლოს მყარ დისკებზე (სისტემური) თვალთვალის და ბლოკირების შესაძლებლობა.
- სისტემას უნდა შეეძლოს ინფორმაციის მოხსნადი მოწყობილობაზე არსებული ფაილების წვდომის

- სისტემას უნდა შეეძლოს ლოკალურ და დომენურ მომხმარებლებზე წესების გავრცელება.
- სისტემის მხარდაჭერილი ოპერაციული სისტემების ჩამონათვალი:
  და ზემოთ
  და ზემოთ

მოთხოვნები ანტივირუსის ლიცენზიების რაოდენობაზე:

ლიცენზიების რაოდენობა	ერთეული

3. მოთხოვნები SEIM-ის და ანტივირუსის ცენტრალური მართვის კონსოლზე მიერთებასთან დაკავშირებით:

- ცენტრალური მართვის კონსოლს უნდა შეეძლოს მოდულების დაყენება როგორც ავტომატურ, ასევე მექანიკურ რეჟიმში;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს განახლებული სისტემების მხარდაჭერა

- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს დროის რეალურ რეჟიმში სამუშაო სადგურების მდგომარეობის კონტროლი.
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს სისტემების ავტომატური დახარისხება მათი ტიპებით, აპარატურული რესურსებით და სხვა პარამეტრებით;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს ინდივიდუალური სისტემების და სისტემათა ჯგუფების დონეზე განსხვავებული პოლიტიკების დანიშვნის შესაძლებლობა
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს დაცვის მოდულების ინსტალაციის, განახლების და კონტროლის ამოცანების დაგეგმვის ჩაშენებული მექანიზმი.
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს პოლიტიკების კატალოგების შენახვა, მათი ასლების შექმნა და რეკონფიგურირების შესაძლებლობა სპეციფიურ ჯგუფებზე;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს განსხვავებული პოლიტიკებისა და განსხვავებული ამოცანების (Task) შედარების შესაძლებლობა;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს პოლიტიკის ცვლილებისას უნდა გამოჩნდეს რამდენ სისტემაზე მოახდენს გავლენას პოლიტიკის ცვლილება;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს სავალდებულო კონსოლის ოპერატორების ქმედებების აღრიცხვა (აუდიტი);
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს აუთენტიფიკაციისთვის Active Directory-ის ანგარიშების გამოყენების შესაძლებლობა;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს სამუშაო სადგურებიდან აღრიცხული ხდომილების მიღება და დამუშავება;
- ცენტრალური მართვის კონსოლ სისტემას უნდა შეეძლოს ინდივიდუალური სამუშაო სადგურების და ჯგუფების დონეზე კავშირის ინტერვალის კონფიგურაციის შესაძლებლობა;

4. სისტემების მწარმოებლის და მათი ინტეგრაციის მოთხოვნები:

- SIEM გადაწყვეტილება უნდა ინტეგრირდებოდეს ანტივირუსის ცენტრალურ მართვის კონსოლთან, რომლიდანაც შესაძლებელი იქნება ანტივირუსის და არსებული მონაცემთან გაჟონვის საწინააღმდეგო პროგრამული უზრუნველყოფის ცენტრალიზებული მართვა.
- მართვა უნდა შეიძლებოდეს ცენტრალური Web Console-დან.
- შემოთავაზებული SIEM გადაწყვეტილება და ანტივირუსის პროგრამული უზრუნველყოფა უნდა იყოს ერთი მწარმოებლის.

5. მწარმოებლისა და მხარდაჭერის სერვისის მოთხოვნები:

- გადაწყვეტილების ყველა კომპონენტზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ 1 წლიანი გარანტია და მხარდაჭერა;
- გადაწყვეტილებაზე მხარდაჭერა უნდა ვრცელდებოდეს პირდაპირ მწარმოებელთან კომუნიკაციით;

6. მოთხოვნები პრეტედენტის მიმართ:

- მომწოდებელს უნდა ჰყავდეს შემოთავაზებული სისტემის მწარმოებლის მიერ სერტიფიცირებული არანაკლებ 1 (ერთი) თანამშრომელი (ინჟინერი), რის დასტურად პრეტენდენტმა უნდა წარმოადგინოს მის თანამშრომლებზე გაცემული მწარმოებლის მიერ სერტიფიცირებული არანაკლებ 1 (ერთი) ინჟინრის სერტიფიკატი და დოკუმენტი იმის შესახებ, რომ წარმოდგენილი სერტიფიცირებული თანამშრომელი მუშაობს აღნიშნულ მომწოდებელთან კომპანიაში.
- მომწოდებელმა უნდა წარმოადგინოს ინფორმაცია მის მიერ განხორციელებული მინიმუმ 1 ანალოგიური პროექტის შესახებ (ერთიანად ყველა კომპონენტის ერთობლიობით ან/და თითოეული კომპონენტი ორჯერ).
- მომწოდებელმა კომპანიამ უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა ე.წ. MAF ამ კონკრეტული პროექტისთვის.

7. საინსტალაციო სამუშაოს და ინსტალაციის შემდგომი მწარმოებლის მხარდაჭერის პერიოდის მოთხოვნები

- SIEM სისტემის ინსტალაცია. VM გამართვა.
- ცენტრალური მართვის კონსოლის გამართვა და SIEM-ის და ანტივირუსის და არსებული მონაცემთან გაჟონვის საწინააღმდეგო პროგრამული უზრუნველყოფის მოდულების მიერთება.
- SIEM-ის ლიცენზიების აქტივაცია.
- 10 სტანდარტული Log Source-ის დამატება. (სტანდარტული ნიშნავს რაც SIEM-ს აქვს გამზადებული ტემპლეიტი) და კონსულტაციები SIEM-ის სხვა Log Source-ების მიერთებასთან დაკავშირებით.
- სისტემის სარეზერვო ასლების (Backup) გენერაცია.
- SIEM-ის 10-მდე სტანდარტული პოლიტიკის (Rule) აქტივაცია და კონსულტაციები SIEM-ის სხვა არასტანდარტული პოლიტიკების აქტივაციაზე.
- SIEM-ის 10-მდე სტანდარტული რეპორტინგის ტემპლეიტების გენერაცია და კონსულტაციები SIEM-ის სხვა არასტანდარტული რეპორტების გენერაციაზე.
- SIEM-ის ინსტალაციის შემდგომი მწარმოებლის მხარდაჭერის პერიოდში, კონსულტაციები მწარმოებლის მხარდაჭერის სერვისის მიღების პროცესზე.

8. მოთხოვნები პრეტედენტის მიმართ და გამოსაგზავნი/ასატვირთი დოკუმენტები:

- პრეტენდენტს უნდა ჰყავდეს შემოთავაზებული სისტემის მწარმოებლის მიერ სერტიფიცირებული არანაკლებ 1 (ერთი) თანამშრომელი (ინჟინერი), რის დასტურად პრეტენდენტმა უნდა წარმოადგინოს მის თანამშრომლებზე გაცემული მწარმოებლის მიერ სერტიფიცირებული არანაკლებ 1 (ერთი) ინჟინრის სერტიფიკატი და დოკუმენტი იმის შესახებ, რომ წარმოდგენილი სერტიფიცირებული თანამშრომელი მუშაობს აღნიშნულ მომწოდებელთან კომპანიაში.
- პრეტენდენტმა უნდა წარმოადგინოს ინფორმაცია მის მიერ განხორციელებული მინიმუმ 1 ანალოგიური პროექტის შესახებ (ერთიანად ყველა კომპონენტის ერთობლიობით ან/და თითოეული კომპონენტი ორჯერ).
- პრეტენდენტმა კომპანიამ უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა ე.წ. MAF ამ კონკრეტული პროექტისთვის.
- პრეტენდენტმა უნდა წარმოადგინოს კომპანიის ბეჭდით დამოწმებული ინვოისი ატვირთვის თარიღის მითითებით **დოლარში,** ზემოთ მოთხოვნილი პირობების შესაბამისად.

შემოთავაზებები წარმოადგინეთ ცხრილის სახით სადაც ცალკე-ცალკე პუნქტებად იქნება გაწერილი:

- პროდუქტის დასახელება, ვერსია და ღირებულება (ასევე მითითებული ექნება შედის თუ არა აღნიშნულ ვერსიაში მწარმოებლის ერთწლიანი მხარდაჭერა);
- საინსტალაციო და საკონფიგურაციაო სამუშაოების ღირებულება და ვადები;

პრეტენდენტმა წინადადება უნდა ატვირთოს ელექტრონული შესყიდვების ვებ-გვერდზე: **www.tenders.ge**
2023 წლის 20 მარტიდან 2023 წლის 24 მარტის 18:00 საათამდე

ტენდერის პროცედურების და შესყიდვების მიმართულებით საკონტაქტო პირი:
ნიკოლოზ მინდიაშვილი,
საკონტაქტო პირის ელ-ფოსტის მისამართი: **nmindiashvili@tpl.ge**
მობ: 591404046

ტექნიკურ საკითხების მიმართულებით საკონტაქტო პირი:
გიორგი გიორგანაშვილი
საკონტაქტო პირის ელ-ფოსტა: **ggiorganashvili@tpl.ge**
მობ:595184444