სატენდერო დოკუმენტაცია

შპს „მეტრო სერვის +“ ს/კ 205150352 აცხადებს ელექტრონულ ტენდერს ინფორმაციული უსაფრთხოების ინციდენტების მონიტორინგისა და მართვის სისტების (SIEM) შესყიდვაზე/დანერგვაზე

მახასიათებლები

დაინტერესებულმა პირებმა წინადადება უნდა წარმოადგინონ შესყიდვების ელექტრონული სისტემის- www.tenders.ge საშუალებით

ტენდერი ჩატარდება ვაჭრობის გარეშე.

შესყიდვის ობიექტი:

დასახელება
ინფორმაციული უსაფრთხოების ინციდენტების მონიტორინგისა და მართვის სისტების (SIEM) შესყიდვაზე/დანერგვაზე

მოთხოვნა/მახასიათებლები

SIEM უნდა ახორციელებდეს მოვლენების შეგროვებას საკუთარი პროგრამული ხელსაწყოების (ე.წ. შემგროვებლების) მეშვეობით, სხვა მწარმოებლის რაიმე გადაწყვეტილების გამოყენების გარეშე. შემგროვებლის ამოცანას წარმოადგენს საინფორმაციო წყაროდან მოვლენების (LOG) შეგროვება, მათი ნორმალიზება შესაბამის ფორმატში ყველა საჭირო ველების მითითებითა (Source/Destination IP, Host, Username, Device Vendor და ა.შ.) და პირველადი მოვლენის სრული შემადგენლობის შენარჩუნებით მათი სისტემაში გადაცემა.

შემგროვებელს უნდა ჰქონდეთ მინიმუმ შემდეგი მეთოდების მხარდაჭერა:

- ტექსტური ფაილიდან წაკითხვა;
- Syslog;
- ა.შ.

შემგროვებელს უნდა ჰქონდეთ შემდეგი სისტემების მიერ გენერირებული LOG ფაილების წაკითხვის და დამუშავების მხარდაჭერა:

- სერვერული სისტემები -
- ვებ სერვერები -
- ქსელური მოწყობილობები -
- მონაცემთა ბაზები -
- DLP (Data Loss Prevention) სისტემები -
- Anti-Virus სისტემები -
- FIM (File Integrity Monitoring) სისტემები -

მზა შემგროვებლის არ არსებობისას, სისტემას უნდა შეეძლოს ნებისმიერი საინფორმაციო წყაროდან მიიღოს ყველა ტიპის მოვლენა, მათთვის შესაბამისი ველების განსაზღვრითა და მინიჭებით, გრაფიკული ინტერფეისის მეშვეობით;

შემგროვებელს უნდა შეეძლოს მოვლენების ნორმალიზება, კატეგორიზაცია, დაჯგუფება და აგრეგირება მომხმარებლის შედგენილი წესების მიხედვით ან სისტემის მიერ წინასწარ განსაზღვრული ველების მიხედვით..

სისტემასთან კავშირის შეწყვეტის შემთხვევაში, შემგროვებელს უნდა შეეძლოს მოვლენების მიღების გაგრძელება და მათი ბუფერში შენახვა, კავშირის აღდგენისას დაგროვებული მოვლენების სისტემაში გასაგზავნად. ამ დროს სისტემამის უნდა გააგრძელოს ფუნქციონირება ჩვეულ რეჟიმში.

დიდი მოცულობის მონაცემებთან მუშაობის ფუნქციონალი, რაც გულისხმობს საწყის ეტაპზე - შემგროვებელზე მიღებული ყველა მოვლენის ერთ სივრცეში შეგროვებას, შემდგომ კი მათ განაწილებასა და გადაცემას სხვადასხვა წყაროებზე, ავტომატურად ან წინასწარ განსაზღვრული წესების მიხედვით.

სისტემას კომპონენტების დამატების შემთხვევაში უნდა გააჩნდეს კომპონენტებს შორის საკომუნიკაციო არხის დაშიფრვის შესაძლებლობა.

SIEM უნდა უზრუნველყოს შემდეგი ფუნქციონალი:

- შემომავალი მოვლენების დამუშავება და ანალიზი „ქარხნულად“ ჩაშენებული ე.წ. Use Case-ების საფუძველზე;
- მიღებული მოვლენების კლასიფიკაცია შესაბამისი რისკის კოეფიციენტის მინიჭების გზით;
- თითოეული მოვლენისათვის დამატებითი სარეზერვო ველების არსებობა ან ახალი ველების შექმნის საშუალება, რათა მოხდეს დამატებითი საჭირო ინფორმაციის ჩაწერა მიღების დროს ან კორელაციის წესების ამოქმედებისას. ასევე, უნდა ჰქონდეს პირველადი მოვლენის შენახვის შესაძლებლობა ერთ-ერთ ველში უცვლელი შემადგენლობით.
- სისტემას უნდა ჰქონდეს გამოყოფილი შესაბამისობის სიების შექმნის ფუნქციონალი, მათი კორელაციის წესებში შემდგომი გამოყენებისათვის;
- სისტემას უნდა შეეძლოს მოვლენების შეგროვება და ანალიზი მომხმარებლის მიერ წინასწარ განსაზღვრული ფილტრების მიხედვით;
- სისტემას უნდა შეეძლოს მოვლენების შესახებ დეტალური ინფორმაციის ვიზუალიზაცია;
- სისტემამ უნდა უზრუნველყოს ფილტრაცია, ასევე, მოვლენების ჩვენება მომხმარებლის ინტერფეისიდან რეალური დროის რეჟიმში, სადაც მომხმარებელს შეუძლია დაუყოვნებლივ გამოიყენოს პოლიტიკები და ფილტრები;
- სისტემას უნდა შეეძლოს წესებისა და ანალიტიკური ანგარიშების შექმნა მომხმარებლის ინტერფეისიდან;
- საინფორმაციო უსაფრთხოების საშიშროებების ვიზუალიზაცია რეალურ დროში, სისტემაში შემომავალი მოვლენების ანალიზზე დაფუძნებით;
- სისტემას უნდა შეეძლოს მოვლენების ანალიზი დროის გარკვეული პერიოდის განმავლობაში, მომხმარებლის მიერ შექმნილი წესების თანახმად

- კონფიგურირებადი ანგარიშგების ფორმების შექმნა და მათი გაგზავნა ელ. ფოსტით ავტომატური ან წინასწარ განსაზღვრული გრაფიკისა და წესების თანახმად; სისტემას უნდა გააჩნდეს ე.წ. SOC (Security Operations Center) რეჟიმში მუშაობის საშუალება, რაც უზრუნველყოფს მომხდარი მოვლენების მონიტორინგსა და მართვას მომხმარებლის ეკრანზე რეალურ დროში (დაყოვნება არაუმეტეს 1წმ-მდე) საინფორმაციო დაფების მეშვეობით;
- სისტემას უნდა შეეძლოს ინფორმაციის კორელაცია სხვადასხვა ერთმანეთისგან დამოუკიდებელი და გამიჯნული წყაროდან;
- სისტემამ უნდა უზრუნველყოს კორელაცია მოვლენების განსაზღვრული თანმიმდევრობის მიხედვით. ასევე, შესაძლებელი უნდა იყოს, კორელირების რამდენიმე საფეხურისა და დონის რეალიზაცია. კორელირებული მოვლენა უნდა ემატებოდეს სხვა მოვლენებს საერთო ბაზაში და იყოს გამოყოფილი სტატუსის მიხედვით;
- სისტემას უნდა შეეძლოს კორელირებული და აგრეგირებული მოვლენებიდან დეტალური ინფორმაციის ცალკეულ ცხრილად გამოტანა. ამ ცხრილში, ასევე, უნდა ჩანდეს პირველადი მოვლენის სრული შემადგენლობა უცვლელად;
- სისტემას უნდა გააჩნდეს ე.წ. Threat Intelligence წყაროებთან (როგორც გარე, ისე შიდა) ინტეგრაციის შესაძლებლობა;
- სისტემას უნდა გააჩნდეს აქტივების და მომხმარებლების ქცევის ანალიტიკის (Behavior Analytics) შესაძლებლობა;
- სისტემას უნდა გააჩნდეს Active Directory-თან ინტეგრაციის შესაძლებლობა (LDAPS პროტოკოლის მხარდაჭერით);
- სისტემას უნდა გააჩნდეს შეტყობინებების მოდული, რომელიც უზრუნველყოფს უნიკალური შეტყობინებების შექმნასა და გაგზავნას მომხდარი მოვლენების შესაბამისად;
- სისტემას უნდა გააჩნდეს ჩაშენებული მექანიზმები საერთაშორისო უსაფრთხოების სტანდარტების მოთხოვნების დასაკმაყოფილებლად. აუცილებელია PCI DSS მხარდაჭერა, ხოლო NIST, ISO ჩაითვლება უპირატესობად;
- სისტემას უნდა გააჩნდეს შეტყობინებაზე რეაგირების განხორციელების საშუალება, მაგ. სკრიპტის გაშვება, წერილის გაგზავნა;
- სისტემას უნდა ჰქონდეს შეუზღუდავი რაოდენობის მომხმარებლის ერთდროულად მუშაობის საშუალება;
- სისტემას უნდა ჰქონდეს შეუზღუდავი რაოდენობის საინფორმაციო წყაროების მიერთების საშუალება;

სისტემის მოდერნიზაციისა და განვითარების შესაძლებლობები

SIEM უნდა ჰქონდეს გაუმჯობესების და ფუნქციონალის დამატების შესაძლებლობა იგივე მწარმოებლის პროგრამული პაკეტების დამატების ან/და ლიცენზიის დამატების საშუალებით, შემდეგი ფუნქციონალის მიღების მიზნით:

- მომხმარებლების ქმედებების შესახებ მონაცემების დაგროვება და ანალიზი, ანომალიური ქმედებების გამოვლენის მიზნით;
- ინციდენტებზე არასტანდარტული რეაგირების პროცესის ასაგებად სხვადასხვა ინტერპრეტატორების გამოყენების შესაძლებლობა:

- საჭიროების შემთხვევაში, დატვირთვის ოპტიმიზაციის მიზნით სისტემას უნდა შეეძლოს მისი კომპონენტების/აპლიკაციების განთავსება ცალკე გამოყოფილ კომპონენტზე/სერვერზე
- დაგროვებული მონაცემების ანალიზისა და ქმედებების სცენარების გამოვლენის საფუძველზე, არასტანდარტული აქტივობების აღმოჩენა;
- უსაფრთხოების დამატებითი სარეპუტაციო მონაცემების ბაზის (გეოგრაფიული განლაგება, ცნობილი ბოტნეტი, Ddos, Backdor, SQL Injection, Cross-site Scripting, Server side Scripting, Ransomware, მოწყვლადობა, გავრცელების არხები და ა.შ.) განახლებადი პაკეტის დამატების საშუალება. ეს მონაცემები ავტომატურად უნდა გროვდებოდეს იგივე გადაწყვეტით, სხვა მწარმოებლების დამატებითი სისტემების ჩართვის გარეშე;
- სისტემას უნდა ჰქონდეს საშუალება დაემატოს გამზადებული პაკეტები სხვადასხვა სტანდარტების შესაბამისობის გადასამოწმებლად (ISO, PCI და სხვა);
- სისტემას უნდა ჰქონდეს სისუსტეების მართვის (vulnerability management) მოდულის ან გადაწყვეტილების დამატების შესაძლებლობა (იგივე მწარმოებლის)/ინტეგრირების (სხვა მწარმოებლი));

მომწოდებელმა უნდა უზრუნველყოს შემდეგი თანმდევი მომსახურება:

- SIEM სისტემის ინსტალაცია და კონფიგურაცია;
- კომპანიას თანამშრომლებს გადასცეს ინსტალაციის, კონფიგურაციის და გამართული მუშაობის უზრუნველყოფისათვის აუცილებელი ცოდნა,კომპანიის ანსაზღვრული თანამშრომლების სწავლების გზით და შესაბამისი ელექტრონული მასალების გადმოცემა:
- ინფორმაციული სისტემების მიერთება SIEM სისტემასთან;
- კორელაციის პირველადი წესების ჩამოყალიბება და კონფიგურაცია;
- პირველადი რეპორტების გენერაცია;
- ტექნიკური მომსახურება ხელშეკრულების გაფორმებიდან 2 წლის განმავლობაში.

მხარდაჭერის პირობები:

- წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის მხარდაჭერა.
- პრეტენდენტს უნდა ქონდეს SIEM სისტემების დანერგვის გამოცდილება, რის შესაბამისადაც უნდა წარმოადგინოს ინფორმაცია რომლითაც დასტურდება, რომ ანალოგიური გადაწყვეტილება დანერგილი აქვს მინიმუმ სამ ორგანიზაციაში საქართველოს ტერიტორიაზე
- პრეტენდენტს უნდა ჰყავდეს შემოთავაზებული პროდუქტის, მწარმოებლის მიერ, სერტიფიცირებული მინიმუმ ერთი თანამშრომელი. დამადასტურებელ დოკუმენტად პრეტენდენტმა უნდა წარმოადგინოს მის თანამშრომელზე მწარმოებლის მიერ გაცემული სერტიფიკატი.
- პრეტენდენტს უნდა შეეძლოს SIEM გადაწყვეტილებაზე მორგებული ტექნიკური ტრენინგის განხორციელება (მოთხოვნის შემთხვევაში)

მიმწოდებელმა უნდა უზრუნველყოს შემდეგი მომსახურება:

SIEM სისტემის ინსტალაცია და კონფიგურაცია უნდა შესრულდეს შემსყიდველის წარმომადგენლებთან ერთად. კომპანიის მხრიდან ქვემოთ მითითებულ თანამშრომლებს,

მიმწოდებელმა უნდა გადასცეს ინსტალაციის, კონფიგურაციის და გამართული მუშაობის უზრუნველყოფისათვის აუცილებელი ცოდნა და შესაბამისი ელექტრონული მასალების გადმოცემა:

a. კონფიგურაცია და ადმინისტრირება - 1 თანამშრომელი;

b. ანალიტიკური ინსტრუმენტი - 1 თანამშრომელი;

- აუცილებელია პრეტენდენტმა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (ე.წ. MAF –Manufacturer Authorization Form)
- პრეტენდენტს უნდა ჰყავდეს შემოთავაზებული პროდუქტის, მწარმოებლის მიერ, სერტიფიცირებული მინიმუმ ერთი თანამშრომელი. დამადასტურებელ დოკუმენტად პრეტენდენტმა უნდა წარმოადგინოს მის თანამშრომელზე მწარმოებლის მიერ გაცემული სერტიფიკატი.
- კომპანიის კორპორატიული კლიენტების სარეკომენდაციო წერილი

მოწოდების ვადა

სამუშაოს დაწყების თარიღი - 2022 წლის მაისი

სამუშოს დასრულების თარიღი - 2022 წლის ივნისი

ანაზღაურება

პროდუქციის მოწოდებიდან 5 დღის ვადაში.

სატენდერო პირობები

ტენდერში მონაწილეობის მისაღებად პრეტენდენტმა საჭიროა სისტემაში ატვირთოს უფლებამოსილი პირის მიერ ხელმოწერილი და ბეჭდით დადასტურებული შემდეგი დოკუმენტაცია (PDF ფორმატის ფაილები):

- ✓ **დანართი N1**- კომპანიის რეკვიზიტები;
- ✓ **დანართი N2**- ფასების ცხრილი
    - ფასები დაფიქსირებული უნდა იყოს დოლარში, დღგ-ს და კანონმდებლობით გათვალისწინებული გადასახადების ჩათვლით;
    - ღირებულებაში გათვალისწინებული უნდა იყოს პროდუქციის ადგილზე მოწოდება;
- ✓ **დანართი N3**- განხორციელებული პროექტების და შესრულებული სამუშაოების ჩამონათვალი;

ტენდერის მსვლელობის დროს ტექნიკურ და ტენდერის პროცესთან დაკავშირებით კითხვებზე დაუკავშირდით:

ლელა ტყეშელაშვილი - +995 599 27 87 97; ltkeshelashvili@msplus.ge

შემოთავაზების მიღების ბოლო ვადაა 11/04/2022 15:00 საათი

- ტენდერში გამარჯვების კრიტერიუმია-ღირებულება და ხარისხი;

- განფასებაში შეცდომის არსებობის შემთხვევაში უპირატესობა მიენიჭება ერთეულის ფასს;

- სატენდერო შემოთავაზებაში და ელექტრონულად დაფიქსირებულ ფასთა ცდომილების (სხვაობის) შემთხვევაში უპირატესობა მიენიჭება ელექტრონულად დაფიქსირებულ ფასს;

- გამარჯვებულად მიიჩნევა და ხელშეკრულება დაიდება იმ მონაწილესთან, რომელიც წარმოადგენს უკეთეს ფასს და დააკმაყოფილებს სატენდერო ტექნიკურ მოთხოვნებს;

- ავანსის მოთხოვნის შემთხვევაში დამკვეთი უფლებამოსილია მოითხოვოს საბანკო გარანტია ავანსად გასაცემი თანხის ოდენობით, ასევე შემოსავლების სამსახურიდან გაცემული შედარების აქტი, რომელშიც არ უნდა ისახებოდეს დავალიანება.

- მომწოდებლის მხრიდან შესაძლებელია მოხდეს დასაბუთებული პრეტენზიის წარდგენა 3 დღის ვადაში. ვადის ათვლა ხორციელდება მომწოდებლისთვის იმ ინფორმაციის მიწოდების დღიდან, რომელსაც შეეხება პრეტენზია.

- დამკვეთის მიერ შესაძლებელია შეწყდეს ტენდერი, შესაბამისი მიზეზების არსებობის შემთხვევაში, რაზეც აუცილებლად ინფორმირებული იქნება ყველა მონაწილე; ასევე დამკვეთი იტოვებს უფლებას ტენდერი სცნოს ანულირებულად თუ ტენდერში მონაწილეობას მიიღებს მხოლოდ ერთი კომპანია;

- სხვა დანარჩენი პირობები, შემდგომში გამყიდველსა და მყიდველს შორის გათვალისწინებულ იქნება ნასყიდობის შესახებ ხელშეკრულებაში.

მადლობა დაინტერესებისთვის.

გისურვებთ წარმატებას.