ელექტრონული მონაცემების შეგროვების და ანალიზის სისტემის (SIEM სისტემა) თანმდევი მომსახურებით ტექნიური დავალება

აღნიშნული ტექნიკური დავალება მიზნად ისახავს სახელმწიფო სერვისების განვითარების სააგენტოში ელექტრონული მონაცემების შეგროვების და ანალიზის სისტემის (საინფორმაციო სისტემების ხდომილებების ჟურნალირების, დამუშავების, ანალიტიკის და რეპორტინგის გენერაციის პროგრამული უზრუნველყოფის (შემდგომში SIEM სისტემა)) შესყიდვას.

1. არსებული მდგომარეობა

სერვისების განვითარების სააგენტოში დღეისათვის ფუნქციონირებეს კომპანია IBM-ის მიერ წარმოებული QRADAR SIEM სისტემა, რომლის ლიცენზიის მოქმედების ვადა არის 2020 წლის 31 აგვისტო.

2. შემსყიდველი იძლევა შესაძლებლობას, რომ პრეტენდენტის მიერ შემოთავაზებაში გამოყენებული იყოს სააგენტოში უკვე არსებული SIEM სისტემა.

2.1 იმ შემთხვევაში თუ პრეტენდენტის მიერ შემოთავაზებული იქნება სააგენტოში უკვე არსებული სისტემისთვის ლიცენზიის მოწოდება, მიმწოდებელმა ხელშეკრულების გაფორმებიდან ორი კვირის ვადაში უნდა უზრუნველყოს შემოთავაზებული პროდუქციის მოწოდება ელექტრონული სახით, რომლის ლიცენზიის მოქმედების ვადა იქნება მინიმუმ 2021 წლის 31 აგვისტომდე;

2.2 იმ შემთხვევაში თუ პრეტენდენტის მიერ შემოთავაზებული იქნება სააგენტოში უკვე არსებული სისტემისაგან განსხვავებული სისტემა, პრეტენდენტის შემოთვაზება უნდა აკმაყოფილებდეს **მე-3 მუხლში** მოცემულ ტექნიკურ პარამეტრებს და შესყიდვის ობიექტის მიწოდების ვადებს.

3. არსებულისაგან განსხვავებული შემოთავაზებული შესყიდვის ობიექტის ტექნიკური პირობები

3.1 SIEM სისტემის ყველა კომპონენტის, ფუნქციონალის მართვა უნდა ხორციელდებოდეს ცენტრალიზებულად ერთიანი Web ინტერფეისის საშუალებით;

3.2 SIEM სისტემას უნდა ქონდეს კომპონენტებს შორის კომუნიკაციის შიფრაციის შესაძლებლობა;

3.3 SIEM-ის სისტემაში შესაძლებელი უნდა იყოს ქვემოთ ცხრილებში ჩამოთვლილი საინფორმაციო რესურსების (წყაროების) ხდომილებელის ჟურნალირება, დამუშავება, კორელაცია და ანალიტიკა (აღნიშნული ჩამონათვალი არის მინიმალური):

Servers and Services:

დასახელება	რაოდენობა
VMware ESXi 6.7	8
Microsoft Windows server 2008 R2, 2012, 2016	75
Microsoft Active Directory 2012	3
Microsoft Exchange Server 2013	1
Microsoft SQL Server 2014	4
Symantec Backup exec 2014	1
SEP Server	1
Symantec DLP	1
IIS (Internet Information Services)	10
Linux Servers	12
Oracle, Linux Server	2
JBOSS Server	10
Vulnerability scanner, Rapid 7	1

Firewalls and Load Balancers

დასახელება	რაოდენობა
Cisco Firepower Firewall	3
CheckPoint R77	2
Citrix WAF	3

Cisco Routers

დასახელება	რაოდენობა
Router ASR 1001-X	3
Cisco R3945E	3
Cisco R3925E	1
Cisco R3925	1
Cisco R3825	2
Cisco R1841	62
Cisco R881	76

3.4 SIEM-ის სისტემაში შესაძლებელი უნდა in-house სისტემის და არასტანდარტული სისტემის ჩართვის შესაძლებლობა;

3.5 SIEM სისტემას უნდა ქონდეს ღია API მონაცემთა ბაზაში განთავსებული ინფორმაციის გაზიარებისათვის;

3.6 შესყიდვის ობიექტმა უნდა უზრუნველყოს მინიმუმ ოთხი ადმინიტრატორის და ექვსი ანალიტიკოსის მუშაობის შესაძლებლობა;

3.7 SIEM სისტემა უნდა ინტეგრირდებოდეს MS AD-ს მომხმარებლების აუტენტიფიკაციის უზრულველყოფისათვის;

3.8 SIEM სისტემას უნდა შეეძლოს ინტეგრაცია სხვა და სხვა უსაფრთხოების სისტემებთან:

- ✓ IPS / IDS ;
- ✓ IDM / AM;
- ✓ Vulnerability Scanners;

3.9 SIEM სისტემის ძირითად კომპონენტს უნდა გააჩნდეს მაღალ-მდგრადი გარემოში მუშაობის შესაძლებლობა;

3.10 SIEM სისტემას უნდა ქონდეს ცალკეული კომპონენტების მუშაობის უზრუნველყოფის საშუალება ერთ-ერთი კომპონენტის მწყობრიდან გამოსვლის შემთხვევაშიც (მაგალითად, ცენტრალური კონსოლის მწყობრიდან გამოსვლის შემთხვევაში ლოგების კოლექტორები უნფა აგრძელებდეს ფუნქციონირებას);

3.11 SIEM სისტემას უნდა ქონდეს კონფიგურაციის ავტომატიზირებული რეზერვირების (Backup) და აღდგენის (Recovery) შესაძლებლობა მომხმარებლის გრაფიკული კონსოლიდან;

3.12 SIEM სისტემას უნდა ქონდეს თავისი მდგომარეობის ანალიზის შესაძლებლობა და მომხმარებლის შეტყობილების საშუალება პრობლემის წარმოქმნის შემთხვევაში;

3.13 SIEM სისტემის ყველა კომპონენტი წარმოდგენილი უნდა იყოს ვირტუალური მანქანის სახით (Virtual Appliance) რომელიც თავსებადია VmWare 6.7 გარემოსთან;

3.14 SIEM სისტემას უნდა ქონდეს ადვილად გაფართოების შესაძლებლობა, როგორც წარმადობის ასევე ფუქციონალის გაზრდით. სისტემის გაფართოება უნდა ხორციელდებოდეს არსებული სისტემაზე შესაბამისი კომპონენტების დამატებით;

3.15 SIEM სისტემას უნდა შეეძლოს ნაკადების (Flows) წაკითხვა და დამუშავება:

- ✓ კერძოთ უნდა ქონდეს NetFlow პროტოკოლის და IPFIX სხვა ტიპის პროტოკოლების მხარდაჭერა;
- ✓ ქონდეს ქსელის ნაკადების წაკითხვის, დამუშავების, ანალიზის და ჩაწერის შესაძლებლობა L7 დონეზე (ქსელის OSI მოდელის მიხედვით);
- ✓ Vmware-ს ვირტუალური ინფრასქტრუქტურის ნაკადების წაკითხვა და დამუშავება;

3.16 SIEM სისტემას უნდა შეეძლოს ქსელის ტრაფიკის პროფილირება L7 დონეზე (ქსელის OSI მოდელის მიხედვით);

3.17 SIEM სისტემა უნდა იყოს გათვლილი:

- ✓ შემომავალი ხდომილებების დამუშავება წამში - 5.000 ხდომილება / წამში;

- ✓ ქსელური ნაკადების დამუშავება 25.000 flow/წუთში ან 500 mbps ქსელური ტრაფიკის დამუშავება;

3.18 პიკური დატვირთვის დროს თუ ხდომილებების და/ან ნაკადების რაოდენობამ წამში გადააჭარბა ზემოთ მოთხოვნილი რაოდენობა, SIEM სისტემამ უნდა შეატყობინოს სისტემის ადმინისტრატორი და მონაცემების დაუკარგავად გააგრძელოს ფუნქციონირება;

3.19 ხდომილებელის და ქსელური ნაკადების გაზრდის შემთხვევაში SIEM სისტემას უნდა ქონდეს რაოდენობის გაზრდის შესაძლებლობა;

3.20 SIEM სისტემამ უნდა უზრუნველყოს შეგროვებული ინფორმაციის მთლიანეობს შენარჩუნება;

3.21 SIEM სისტემას უნდა შეეძლოს მონაცემების კორელაცია კომპონენტების განაწილებული ინსტალაციის მოდელის შემთხვევაში;

3.22 SIEM სისტემას უნდა ქონდეს ხმოლილებების ჟურნალების შეგროვების და არქივაციის შესაძლებლობა. ჟურნალების შენახვა შესაძლებელი უნდა იყოს როგორც online-ში ასევე offline რეჟიმში;

3.23 SIEM სისტემას უნდა შეეძლოს ჟურნალების შენახვა გარე მატარებლებზე;

3.24 SIEM სისტემას უნდა შეეძლოს მონაცემების წაკითხვა Hadoop-ის სანახიდან;

3.25 SIEM სისტემას უნდა შეეძლოს შეგროვებული ინფორმაციის შეკუმშვა;

3.26 SIEM სისტემას უნდა ქონდეს აგენტების გარეშე ხდომილებების შეგროვების შესაძლებლობა, იქ სადაც ეს შესაძლებელია;

3.27 SIEM სისტემას უნდა შეეძლოს ხდომილებების სრული ინფორმაციიზე წვდომის უზრუმველყოფა ხდომილებების არსებობის პერიოდის განმავლობაში;

3.28 SIEM სისტემას უნდა შეეძლოს ხდომილებების ინფორმაციის შენახვა, როგორც საწყის ფორმაში, ასევე ნორმალიზებული სახით, შემდგომი ანალიზისათვის;

3.29 SIEM სისტემას უნდა ქონდეს ხდომილებების ანალიზის შესაძლებლობა რეალურ რეჟიმში;

3.30 SIEM სისტემას უნდა ქონდეს ხდომილებების ანალიზის შესაძლებლობა კონკრეტული პერიოდის განმავლობაში, რომელიც მითითებული იქნება მომხმარებლის/ადმინისტრატორის მიერ;

3.31 SIEM სისტემას უნდა ქონდეს მომხმარებლის ფილტრის მიხედვით მონაცემების შეგროვების და ანალიზის შესაძლებლობა;

3.32 SIEM სისტემაში რეალიზებული უნდა იყოს რეპორტების გენერაციის შესაძლობა. სისტემში უნდა არსებობს წინასწარ განსაზღვრული რეპორტების ნიმუშები (შაბლონები). ასევე სისტემაში უნდა იყოს საკუთარი რეპორტების გენერაციის შესაძლებლობა;

3.33 SIEM სისტემაში რეალიზებული უნდა იყოს, გარკვეული დროს პერიოდში, რეპორტების ავტომატიზირებული გენერაციის შესაძლებლობა;

3.34 SIEM სისტემაში უნდა არსებობდეს რეპორტების ჩამოყალიბების შესაძლებლობა საერთაშორისო სტანდარტების მიხედვით (ISO 27002, PCI, FISMA);

3.35 SIEM სისტემას უნდა გააჩნდეს რეპორტების ავტომატიზირებული განაწილების შესაძლებლობა;

3.36 SIEM სისტემაში უნდა არსებობს ხდომილებების კორელაციის გამზადებული წესები (წესების ჩამონათვალი);

3.37 SIEM სისტემაში რეალიზებული უნდა იყოს ხდომილებების დამუშავების საკუთარი წესების შექმნის ინსტრუმენტი, რომელიც რეალიზებული უნდა იყოს გრაფიკული ინტერფეისის სახით;

3.38 SIEM სისტემას უნდა გააჩნდეს ინციდენტების ერთ „საქმეში“ ავტომატური გაერთიანების შესაძლებლობა და ამ „საქმის“ გადაწერის შესაძლებლობა შესაბამის პასუხიმგებელ თანამშრომელზე;

3.39 ერთ „საქმეში“ შესაძლებელი უნდა იყოს უსაფრთხოების ხდომილებების და ქსელური ნაკადების ინფორმაციის გაერთიანება;

3.40 უკვე არსებული „საქმის” განახლება შესაბამისი უსაფრთხოების ხდომილებების და ქსელური ნაკადებიდან ინფორმაციის დამატებით;

3.41 SIEM სისტემას უნდა გააჩნდეს ქსელური ტრაფიკის და პროცესების ანომალური ქმედებების აღმოჩენის და ანალიზის შესაძლებლობა;

3.42 SIEM სისტემას უნდა შეეძლოს DoS შეტევების დეტექტირება;

3.43 SIEM სისტემას უნდა შეეძლოს პოტენციაურად საშიში პროგრამული უზრუნველყოფის დეტექტირება ქსელის ტრაფიქში;

3.44 SIEM სისტემაში რეალიზებული უნდა იყოს სერვისების ამოცნობის მექანიზმი;

3.45 SIEM სისტემას უნდა შეეძლოს ქსელურ ტრაფიკში განასხვავოს და პროფილირება გაუწიოს სხვა და სხვა აპლიკაციებს, არა მარტო ცნობილი TCP პორტების საშუალებით;

3.46 SIEM სისტემა უნდა შეეძლოს ქსელურ ტრაფიკში ნაკადების დეტექტირება და იდენტიფიცირება გეოგრაფიული რეგიონების მიხედვით რეალურ დროში;

3.47 SIEM სისტემას უნდა შეეძლოს გამოვლენილი ხდომილების სერიოზულობის დონის განსაზღვრა ობიექტის/აქტივის უსაფრთხოების და დაუცველობის მიმართებაში;

3.48 SIEM სისტამაში რეალიზებული უნდა ოყოს აქტივების (Asset) ბაზა და მისი მართვის ინსტრუმენტები. აქტივების ბაზაში უნდა იყოს ინფორმაცია:

- ✓ მოწყობილობების, სერვისების შესახებ. აქტივების ბაზაში ინფორმაცია უნდა შედიოდეს ავტომატიზირებულად;

3.49 SIEM სისტემაში ავტომატიზირებული გზით უნდა გროვდებოდეს ინფორმაცია სხვადასხვა უსაფრთხოების სისტემებისად, მაგალითად IPS/IDS, IDM/AM, უსაფრთხოების სკანერებიდან;

3.50 SIEM სისტემაში რეალიზებული უნდა იყოს IP Reputation მექანიზმები. სისტემას ავტომატიზირებულად უნდა შეეძლოს შეერთებების გამოვლენა:

- ✓ BotNet ქსელებთან;
- ✓ Mailware რესერსებთან;
- ✓ Anonym Proxy;
- ✓ Spam საიტებთან ;

3.51 SIEM სისტემაში აქტივების ბაზა ფართოდ უნდა იყოს გამოყენებული როგორც კონტექსტის მიმწოდებელი, რამაც უნდა უზრუნველყოს კორელაციის სიზუსტე;

3.52 SIEM სისტემას უნდა გააჩნდეს რისკების მართვის ინსტრუმენტი. სისტემაში შესაძლებელი უნდა იყოს ინფრაქტრუქტურის რისკების პრიორიტიზაცია ქსელური ტრაფიკის, ხდომილებათა ჟურნალების, უსაფრთხოების სკანერების ინფორმაციის საფუძველზე;

3.53 SIEM სისტემაში რეალიზებული უნდა იყოს Vulnerability Manager ფუნქციონალი. სისტემაში ინტეგრირებული უნდა იყოს უსაფრთხოების სკანერი (Vulnerable scanners) და მოწოდებული იყოს ლიცენზია მინიმუმ 70 სერვერის (ობიექტების) სკანირებისათვის. უსაფრთხოების სკანერებიდან მიღებული ინფორმაცია უნდა იყოს ასახული აქტივების ბაზაში. აღნიშნული ინფორმაცია გამოყენებული უნდა იყოს რისკების მართვის ინსტრუმენტში, უზრუნველყოფდეს კორელაციის სიზუსტეს და „საქმის“-ის სრულყოფას;

3.54 შესყიდვის ობიექტს უნდა გააჩნდეს სკანირების ობიექტების რაოდენობს გაზრდის შესაძლებლობა;

3.55 წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს საგარანტიო მომსახურება მინიმუმ 2021 წლისნ 31 აგვისტოს ვადით. საგარანტიო პირობები უნდა ვრცელდებოდეს SIEM სისტემის ნებისმიერ ხარვეზზე, რაც არ არის გამოწვეული შემსყიდველის ან მესამი პირის ბრალეულობით. საგარანტიო ვადა იწყება მიღება-ჩაბარების აქტის გაფორმებიდან;

3.56 წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის საგარანტიო მხარდაჭერა.

თანმდევი მომსახურება

მომწოდებელმა უნდა უზრუნველყოს შემდეგი თანმდევი მომსახურება:

1. მიმწოდებელი ვალდებულია უზრუნველყოს სისტემის ინსტალაცია და კონფიგურაცია უნდა შესრულდეს შემსყიდველის წარმომადგენლებთან ერთად.

2. SIEM სისტემის ინსტალაციია და კონფიგურაცია უნდა განხორციელდეს ქვემოთ მოცემულ ვადებში:

   a. სისტემის ინსტალაცია, კონფიგურაცია - ხელშეკრულების დადებიდან ორი კვირის ვადაში;
   b. საინფორმაციო რესურსების მიბმა - ხელშეკრულების დადებიდან სამი კვირის ვადაში;
   c. კორელაციის პირველადი წესების ჩამოყალიბება - ხელშეკრულების დადებიდან ერთი თვის ვადაში;
   d. პირველადი რეპორტების გენერაცია - ხელშეკრულების დადებიდან ერთი თვის ვადაში;

4. დამატებითი მოთხოვნა

ანალიტიკური კომპანია Gartner-ის 2015 და 2016 წლების SIEM პროდუტების შეფასების მიხედვით, შემოთავაზებული პროდუქტი უნდა ეკუთვნოდეს ლიდერის კვადრატს.