ინფორმაციული უსაფრთხოების ხდომილებების და ინციდენტების მონიტორინგისა და მართვის სისტემის (SIEM) შესყიდვის ტექნიკური დავალება

მოთხოვნები მომწოდებელი კომპანიის მიმართ:

- მომწოდებელი კომპანია უნდა იყოს კომპანია IBM-ის ოფიციალური პარტნიორი
- უნდა ჰყავდეს მინიმუმ 2 ქართულენოვანი სერთიფიცირებული სპეციალისტი.
- უნდა ჰქონდეს მინიმუმ 2 ანალოგიური პროდუქტის დანერგვის გამოცდილება.
- განიხილება მხოლოდ ის კომპანიები, რომელთა დაფუძნებიდანაც გასულია მინიმუმ 5 (ხუთი) წელიწადი.

მოთხოვნები პროდუქტის მიმართ:

შესყიდვა ფასების ცხრილის (დანართი N1) მიხედვით.

შპს „სოკარის“ საჭიროებიდან გამომდინარე, დაინტერესებულია IBM QRadar-ის შესყიდვით 500 “EPS”-ების რაოდენობით. სისტემა უნდა წარმოადგენდეს პროგრამულ პაკეტს და უდნა იყოს გათვალისწინებული მაღალმდგრადობა (High Availability). შემოთავაზებაში უნდა იყოს გათვალისწინებული მწარმოებლის 1 წლიანი მხარდაჭერა.

SIEM უნდა ახორციელებდეს მოვლენების შეგროვებას საკუთარი პროგრამული ხელსაწყოების (ე.წ. შემგროვებლების) მეშვეობით, სხვა მწარმოებლის 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;
- WMI;
- Syslog;
- SNMP;
- ხდომილებების მონაცემთა ბაზიდან წაკითხვა JDBC ან ODBC დრაივერების მეშვეობით;
- XML;
- IP Flow (NetFlow, J-Flow);
- IPFIX;
- sFlow

შემგროვებელს უნდა ჰქონდეთ შემდეგი სისტემების მხარდაჭერა:

- სერვერული სისტემები - Microsoft Servers (Windows, AD, Exchange,), Linux, DNS & DHCP, VmWar ESXi;
- ვებ სერვერები - Microsoft IIS, Apache და სხვები;
- ქსელური მოწყობილობები - Cisco, Dell, Aruba, Fortinet, Palo Alto, CheckPoint, Barracuda, F5 და სხვები ;
- მონაცემთა ბაზები - Microsoft SQL, MySQL, Oracle , Mongo, Postgre და სხვები;
- SCADA 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;
- 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 ჩვენება;
- 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 შეტყობინებების მოდული, რომელიც უზრუნველყოფს უნიკალური შეტყობინებების შექმნასა და გაგზავნას მომხდარი მოვლენების შესაბამისად;
- სისტემას უნდა გააჩნდეს შეტყობინებაზე რეაგირების განხორციელების საშუალება, მაგ. სკრიპტის გაშვება, წერილის გაგზავნა;
- სისტემას უნდა ჰქონდეს შეუზღუდავი რაოდენობის მომხმარებლის ერთდროულად მუშაობის საშუალება;

SIEM სისტემების/მოდულების ფუნქციონალში უნდა შედიოდეს:

1. საინფორმაციო მოვლენების შეგროვება, შენახვა და დაჯგუფება/აგრეგირება დროის, წყაროსა, მოვლენის და სხვა ტიპების მიხედვით. ამასთანავე, უნდა შეეძლოს/გააჩნდეს:
- მიღებული მოვლენების ვიზუალიზაცია და დაჯგუფება გრაფიკული ინტერფეისის მეშვეობით;
- საჭირო მოვლენების მოძებნის საშუალება ფილტრების გამოყენებით;
- მომხდარი მოვლენის აღმოჩენა გარკვეული დროის მომენტში მოვლენის წყაროს განურჩევლად;
- საძიებო სისტემა, რომელსაც შეუძლია ერთდროულად არანაკლებ 25 სხვადასხვა სცენარის რეალიზება ავტომატურ რეჟიმში;

2. მოვლენების ანალიზი და კორელაცია რეალურ დროში (დაყოვნება არაუმეტეს 1წმ-მდე), შემდეგი პარამეტრებით:
- უნდა ჰქონდეს გრაფიკული-ინტერფეისი სისტემის ადმინისტრირების, ანგარიშგებების შექმნისა და მართვის, შემომავალი მონაცემების ნაკადების მონიტორინგისთვის წყაროების მიხედვით, საინფორმაციო დაფების შექმნის, მართვის და რეალურ დროში მონიტორინგისათვის;
- უნდა შეეძლოს მომხმარებლის უფლებების განსაზღვრა მომხმარებლის დადგენილი როლების მიხედვით;
- სისტემას უნდა შეეძლოს არანაკლებ 150 საინფორმაციო წყაროს დაერთების საშუალება.

- სისტემას უნდა ქონდეს შეუზღუდავი რაოდენობის მოვლენის წამში (EPS) მიღება და დამუშავების შესაძლებლობა.
- სისტემას უნდა ქონდეს შეუზღუდავი რაოდენობის ქსელური ნაკადებისა და პაკეტების მიღება და დამუშავების შესაძლებლობა.

SIEM სისტემის დამატებითი შესაძლებლობები:
- მომხმარებელს უნდა შეეძლოს სისტემაში შექმნილი კონფიგურაციების (წესების, პოლიტიკების, სიების) ექსპორტი, მისი შემდგომში აღდგენის ან სხვა სისტემაზე გადატანის მიზნით;
- სისტემას უნდა ჰქონდეს მონაცემების სარეზერვო ასლის შექმნის და სარეზერვო ასლიდან მონაცემების აღდგენის საშუალება;

სისტემის მოდერნიზაციისა და განვითარების შესაძლებლობები

SIEM უნდა ჰქონდეს გაუმჯობესების და ფუნქციონალის დამატების შესაძლებლობა იგივე ან სხვა 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, CoBIT 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:
1. SIEM სისტემის ინსტალაცია და პირველადი კონფიგურაცია;
2. 5 საინფორმაციო რესურსების მიერთება SIEM სისტემასთან;
3. 10 კორელაციის პირველადი წესების ჩამოყალიბება და კონფიგურაცია;
4. 2 პირველადი რეპორტების გენერაცია;
5. საგარანტიო და ტექნიკური მოსახურება ხელშეკრულების გაფორმებიდან 1 წლის განმავლობაში.

SIEM-ის დანერგვის სამუშაოების მიზნობრიობა მოიცავს:

- საინფორმაციო უსაფრთხოების მოვლენებისა და ინციდენტების ერთიანი სანახის შექმნას;
- საინფორმაციო უსაფრთხოების მოვლენების ნორმალიზაციას, აგრეგირებასა და კორელაციას, დასახული პრიორიტეტებისა და კონფიგურირებადი წესების მიხედვით;
- საინფორმაციო უსაფრთხოების მოვლენების დამუშავების ხარისხის ამაღლებას;
- საინფორმაციო უსაფრთხოების ინციდენტების აღმოჩენისა და რეაგირების ავტომატიზაციას.

SIEM უნდა შეეძლოს შემდეგი ამოცანების გადაწყვეტა:
- კრიტიკული ბიზნეს სისტემების ხელმისაწვდომობის, კონფიდენციალურობისა და ერთიანობის მონიტორინგი;
- მონაცემების გაჟონვის აღმოჩენა წინასწარ დადგენილი წესების მიხედვით;
- შეღწევადობისა და შეტევების აღმოჩენა;
- დაუშვებელი ქმედებების აღმოჩენა ორგანიზაციის შიდა სისტემებში;
- ინფორმაციული უსაფრთხოების პოლიტიკების შესრულების კონტროლი.

საქონლის მიწოდების/მომსახურების გაწევის/სამუშაოს შესრულების ვადა
შესყიდვის ობიექტის მიწოდება უნდა განხორციელდეს ხელშეკრულების დადებიდან 50 კალენდარული დღის განმავლობაში.
ინსტალაცია 14 დღე.

დანართი1:

Part number	Part description	Quantity	U/Price inc. VAT	T/Price inc. VAT
	IBM Security QRadar Software Node Install License + SW Subscription & Support 12 Months	1		
	IBM Security QRadar Software Install License + SW Subscription & Support 12 Months	1		
	IBM Security QRadar Event Capacity 100 Events per Second License + SW Subscription & Support 12 Months	4		