**საინფორმაციო უსაფრთხოების ინციდენტების მონიტორინგისა და მართვის სისტემის ტექნიკური აღწერა (SIEM)**

*«საინფორმაციო უსაფრთხოების ინციდენტების მართვისა და მონიტორინგის სისტემის (SIEM) დანერგვა*

**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;
* საინფორმაციო უსაფრთხოების პოლიტიკების შესრულების კონტროლი.

**მოთხოვნები SIEM-ის მიმართ**

სისტემა უნდა წარმოადგენდეს პროგრამულ პაკეტს.

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;
* 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, VmWare 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 და სხვები

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;
* სისტემას უნდა ჰქონდეს შეუზღუდავი რაოდენობის საინფორმაციო წყაროების მიერთების 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 გრაფიკულიინტერფეისის 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;
1. 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 1500 მოვლენის წამში (EPS) მიღება და დამუშავება,

SIEM სისტემას უნდა შეეძლოს:

ლიცენზიით გათვალისწინებული მოცულობების გადაჭარბების შემთხვევაში, ყველა მომხდარი მოვლენის დანაკარგების გარეშე დამუშავება , შექმნილი წესების თანახმად.

 **SIEM სისტემის დამატებითი შესაძლებლობები:**

* შემომავალი და გამავალი ინფორმაციული არხის ანალიზი, მონაცემების მიმოცვლის სპეციფიური პროტოკოლის გამოვლენის მიზნით;
* კრიტიკული სისტემების კონფიგურაციის ცვლილების ცენტრალიზებული მონიტორინგი და დოკუმენტირება;
* კრიტიკული სისტემების წვდომის კონტროლის ცვლილებების შესახებ ინფორმაციის ცენტრალიზებული შენახვა;
* დომენში მომხმარებლის პროფილის უფლებებისა და პრივილეგიების შეცვლის გამოვლენა;
* გარკვეული მომხმარებლის პროფილებიდან წვდომასთან დაკავშირებული საეჭვო განსხვავებული ქმედებების გამოვლენა;
* სამსახურიდან განთავისუფლებული თანამშრომლების პროფილის გამოყენების ფაქტების გამოვლენა;
* სამუშაო ადგილებიდან დაუშვებელ/აკრძალულ სეგმენტთან კავშირის გამოვლენა;
* ცალკეულ სერვერებზე და სამუშაო სადგურებზე მიმართული აქტივობების გამოვლენა;
* ქსელის სკანირების გამოვლენა;
* მომხმარებლების მუშაობის სტატისტიკის გამოვლენა (შემომავალი/გამავალი ტრაფიკი, ხშირად გამოყენებული საიტები და მსგავსი);
* კორპორატიულ ქსელში ვირუსული აქტივობის ანგარიშგებების ფორმირება;
* კრიტიკული რესურსების დაუცველობის შესახებ ინფორმაციის კორელირებისა და ადრე მომხდარი საეჭვო აქტივობების საფუძველზე რისკებისა და საფრთხეების პრიორიტეტების განსაზღვრა;
* სისტემის დაუცველობის შესახებ ინფორმაციის ცენტრალიზებული შენახვა;
* სტატისტიკისა და ანგარიშგებების გენერირება მომხმარებლების მიხედვით;
* მომხმარებელს უნდა შეეძლოს სისტემის ფუნქციონალის გაზრდა მწარმოებლის სპეციალიზებული პორტალიდან დამატებითი პაკეტების გადმოწერის და სისტემაში იმპორტის გზით;
* 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 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));

**მომწოებელმა უნდა უზრუნველყოს შემდეგი თანმდევი მომსახურება:**

1. SIEM სისტემის ინსტალაცია და კონფიგურაცია;
2. საინფორმაციო რესურსების მიერთება SIEM სისტემასთან;
3. კორელაციის პირველადი წესების ჩამოყალიბება და კონფიგურაცია;
4. პირველადი რეპორტების გენერაცია;
5. საგარანტიო და ტექნიკური მოსახურება ხელშეკრულების გაფორმებიდან 1 წლის განმავლობაში.
6. საგარანტიო ვადის განმავლობაში (1წელი) მომწოდებელმა, შემსყიდველის მოთხოვნის საფუძველზე, ასეთის არსებობის შემთხვევაში, უნდა მოახდინოს თვეში 10 კორელაციის წესის აწყობა და 2 საინფორმაციო რესურსის მიერთება SIEM სისტემაში.

**საგარანტიო პირობები:**

* წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს მინიმუმ 1 წლიანი საგარანტიო მომსახურება მის ყველა კომპონენტზე;
* საგარანტიო მომსახურება უნდა ხორციელდებოდეს მომწოდებლის მიერ;
* წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის მხარდაჭერა.