ტექნიკური დავალება

პრივილეგირებული მომხმარებლების მონიტორინგისა და კონტროლის სისტემა

1. სისტემის გამოყენების მიზანი

მოცემული სისტემის გამოყენების მიზანია ორგანიზაციაში არსებული რისკების შემცირება. პრივილეგირებული მომხმარებლების, რომლებიც აწარმოებენ IT ინფრასტრუქტურის სხვადასხვა ელემენტების მხარდაჭერას მათი კონტროლი და მონიტორინგი.

2. პრივილეგირებული მომხმარებლების, სამართავი ობიექტების რაოდენობა და მახასიათებლები

- ავტომატიზირებული ქცევის კონტროლის სისტემის სისტემური ადმინისტრატორების რაოდენობა: 5;
- ინფორმაციული რესურსების რაოდენობა, რომლებზეც მოხდება პრივილეგირებული მომხმარებლების წვდომის გაკონტროლება და სესიების ჩაწერა: 211;
- პაროლების და SSH გასაღებების ინფორმაციული რესურსების რაოდენობა: IT-ის ქსელში 27 პაროლი და 2 SSH გასაღები. SCADA-ს ქსელში 8 პაროლი და 50 SSH გასაღები;
- რაოდენობა დამკვეთის ინფორმაციული რესურსების, რომლებიც გამოყენებული იქნება პროექტში, იხ. ცხრილში (ცხრილი N1):

ცხრილი N1 - დამკვეთის პროექტში მონაწილე ინფორმაციული რესურსების სია:

სისტემის ტიპები	პლატფორმა	რაოდენობა
Windows სერვერები (SCADA)	Server 2016	70
Unix სერვერები (SCADA)	RedHat Linux 5.6,5.7,5.8, 6.5	10
Windows სერვერები (IT)	Different versions	67
Unix სერვერები (IT)	Linux different versions	55
Database	SQL different versions	9

3. პრივილეგირებული მომხმარებლების ქცევის კონტროლის სისტემის ტექნიკური მოთხოვნები

3.1. ზოგადი მოთხოვნები:

სისტემა უნდა წარმოადგენდეს პროგრამულ უზრუნველყოფას, რომელიც უნდა დაყენდეს ორგანიზაციაში არსებულ ვირტუალიზაციის გარემოში(VMware).

სისტემას უნდა ჰქონდეს შესაძლებლობა მომხმარებლების დამატებისა და მათთვის სხვადასხვა უფლებების(წვდომების) მინიჭების. სისტემის წვდომის შეზღუდვის მექანიზმი განხორციელებული უნდა იყოს დისკრეციული მოდელით, ასევე უნდა ჰქონდეს საშუალება როლის მოდელებით უფლებების(წვდომის) მინიჭების. წვდომების შეზღუდვა შესაძლებელი უნდა იყოს ობიექტებზე: პაროლებზე, კონტროლირებული ანგარიშების(მომხმარებლების) ჩანაწერებზე, ლოგების ფაილებზე და სესიების ჩანაწერებზე. ასევე შესაძლებელი უნდა იყოს ივენთების ჟურნალზე წვდომის შეზღუდვა.

სისტემას საშუალება უნდა ჰქონდეს ზრდის, დამატებითი მოდულების დაყენებით, ასევე უნდა ჰქონდეს ფუნქციონალის გაზრდის და ცვლილებების შეტანის საშუალება.

სისტემა მარტივად უნდა მასშტაბირდებოდეს და იზრდებოდეს დამატებითი ლიცენზიის შეძენით, ან არქიტექტურაში ახალი კომპონენტების დამატებით, რომელიც არ უნდა საჭიროებდეს არსებული კომპონენტების შეცვლას.

3.2. სისტემის ფუნქციური მოთხოვნები:

N	მოთხოვნების აღწერა
	1. ადმინისტრირებისთვის საჭირო პროტოკოლები
1,1	ინფრასტრუქტურის ობიექტების ადმინისტრირება SSH პროტოკოლით
1,2	ინფრასტრუქტურის ობიექტების ადმინისტრირება RDP პროტოკოლით
1,3	ინფრასტრუქტურის ობიექტების ადმინისტრირება HTTP/HTTPS პროტოკოლით
1,4	სისტემას უნდა ჰქონდეს შესაძლებლობა სხვადასხვა ადმინისტრაციული ინტერფეისის ინტეგრაციის და ინფრასტრუქტურული ობიექტების უსაფრთხო ადმინისტრირების ნებისმიერი პროტოკოლით.
1,5	პრივილეგირებული ანგარიშების მართვის პროცესის ჩანაწერების ორგანიზება. პრივილეგირებული ანგარიშების მართვის პროცესის ჩანაწერები უნდა უზრუნველყოფდეს ახალი პაროლის გენერაციას პაროლების პოლიტიკის მოთხოვნების მიხედვით, პაროლების რეგულარულ ცვლას ყველა სამართავ ობიექტზე. შესაძლებელი უნდა იყოს პაროლის აღდგენა მისი არასანქცირებულად შეცვლის შემთხვევაში. დროულად აღმოჩენა ახალი ანგარიშების ჩანაწერების შესახებ და ინფორმირება უფლებამოსილი პირების (თანამშრომლების). ასევე სისტემების SSH გასაღებების მართვა.
1,6	პაროლების პოლიტიკის და პრივილეგირებული მომხმარებლების სესიის ჩაწერისთვის არ უნდა საჭიროებდეს აგენტის დაყენებას ობიექტებზე.
	2. ადმინისტრირებადი ობიექტების მხარდაჭერის მოთხოვნები
2,1	სერვერების ადმინისიტრირება: UNIX (AIX, HP-UX, Solaris)
2,2	სერვერების ადმინისიტრირება : Windows Server (2003, 2008,2012,2016,2019)
2,3	ვირტუალიზაციის სისტემების ადმინისტრირება : VMware (ყველა კომპონენტი) და Microsoft Hyper-V
2,4	Citrix-ის ტერმინალ სერვერების ადმინისტრირება
2,5	Oracle მონაცემთა ბაზის სერვერების ადმინისტრირება
2,6	MS SQL მონაცემთა ბაზის სერვერების ადმინისტრირება
2,7	ფაილსერვერების ადმინისტრირება (NAS)
2,8	ლოკალურ ქსელში არსებული კომპუტატორების ადიმინისტრირება (წამყვანი მწარმოებლების)
2,9	ლოკალურ ქსელში არსებული მარშრუტიზატორების ადიმინისტრირება (წამყვანი მწარმოებლების)
2,10	ე.წ. ფაერვოლების ადმინისტრირება (წამყვანი მწარმოებლების)
2,11	Windows (XP, 7, 8,10) ოპერაციულ სისტემათა ადმინისტრირება
	3. არქიტექტურის, ინტეგრაციის და ექსპლუატაციისთვის საჭირო მოთხოვნები
3,1	სისტემის დაყენება შესაძლებელი უნდა იყოს შემდეგ რეჟიმებში: პირდაპირი(inline) - სისტემა გამყოფია ქსელურ დონეზე მომხმარებელსა და ადმინისტრირებად ობიექტს შორის. გვერდითი(out of band) - სისტემა ყოფს მომხმარებელსა და ადმინისტრირებად ობიექტს ლოგიკურად. ასეთ შემთხვევაში არ უნდა იყოს საჭირო ქსელის ცვლილება. ორივე შემთხვევაში სისტემამ უნდა უზრუნველყოს სესიების ჩაწერა.
3,2	პრივილეგირებული მომხმარებლების ობიექტებთან წვდომა უნდა ხორციელდებოდეს ადმინისტრირების პორტალის საშუალებით, სადაც გადის აუთენთიფიკაციას. პორტალის დახმარებით პრივილეგირებულ მომხმარებელს შეუძლია სასურველი მართვადი ობიექტის არჩევა და მასთან დაკავშირება.
3,3	პრივილეგირებული მომხმარებლების ანგარიშების ჩანაწერები, ინფრასტრუქტურის ობიექტების ვიდეო არქივი, უნდა ინახებოდეს დაცულ, ცალკე გამოყოფილ სანახში.

3,4	სისტემას უნდა გააჩნდეს პაროლების შეცვლის პოლიტიკების შექმნის შესაძლებლობა, რომლის მიხედვითაც შეცვლის პრივილეგირებული მომხმარებლების პაროლებს სამართავ ობიექტებზე.
3,5	სისტემას უნდა გააჩნდეს გარემო სადაც მოხდება ადმინისტრირების ხელსაწყოების გაშვება და მოხდება პრივილეგირებული მომხმარებლების ქმედებების ჩაწერა.
3,6	სანახის უსაფრთხოება და მასზე წვდომები დაცული უნდა იყოს როლური მოდელით. სონაცემები სანახში უნდა ინახებოდეს დაშირფრული სახით. სანახი დაცული უნდა იყოს არასანქცირებული წვდომისგან.
3,7	აუდიტის აღრიცხვის ჟურნალის SIEM სისტემაში გაგზავნის შესაძლებლობა.
3,8	ინტეგრაცია მოთხოვნების სარეგისტრაციო სისტემებთან (ე.წ. ticketing system)
3,9	უსაფრთხოების სკანერებთან ინტეგრაცია. ანგარიშების ჩანაწერების შენახვა, რომლებიც გამოიყენება სკანირებისას სკანერის მიერ, დაცულ სანახში.
3,10	შესაძლებლობა აქტივ დირექტორიაში ობიექტების(მომხმარებლების) ავტომატურად ძებნის/აღმოჩენის და იმპორტის, მოცემულ ობიექტებზე(მოხმარებლებზე) ავტომატური პაროლის ცვლილების ფუნქციონალი.
3,11	პრივილეგირებული მომხმარებლის ობიექტებთან დაკავშირებისას გამოყენებული ხელსაწყოები უნდა ეშვებოდეს იზოლირებულ და უსაფრთხო გარემოში პრივილეგირებული მომხმარებლის სისტემისგან დამოუკიდებლად და უნდა ხდებოდეს მათი ვიდეოინფორმაციის სახით ჩაწერა.
3,12	პრივილეგირებული მომხმარებლის სესიასთან მხოლოდ ხედვის უფლებით დაკავშირება.
3,13	არანაკლებ 100 კონკურენტული სესიის ადმინისტრირების საშუალება.
3,14	სისტემას უნდა ჰქონდეს ერთი სამართავი კონსოლი, საიდანაც მოხდება ყველა ფუნქციონალის და მოდულის მართვა.
3,15	სისტემას უნდა ჰქონდეს შესაძლებლობა შეზღუდოს Linux/Unix ბრძანებები, ბრძანებათა შავი სიის შექმნის საშუალებით.
3,16	დაცულ საცავში შენახული პაროლით სესიის წამოწყება, მომხმარებლისთვის ჩვენების გაერშე.
3,17	პაროლის ცვლილების საშუალება ყოველი სესიის დასრულების შემდეგ.
3,18	პრივილეგირებული მომხმარებლისთვის ობიექტზე უფლებების მინიჭებისას შესაძლებელი უნდა იყოს: · უფლების მინიჭება დროისა და თარიღის განსაზღვრით. · უფლების მინიჭება დროითი ინტერვალის განსაზღვრით (განსაზღვრულ დროში მრავალჯერადი დაკავშირების შესაძლებლობა) · ობიექტთან წვდომის მოთხოვნისას პასუხისმეგებლი პირის მიერ კავშირზე თანხმობა/უარყოფა.
4. აუდიტის სისტემისთვის განკუთვნილი "ოთხოვნები (ჟურნალი, ვიდეო ჩანაწერები, ანგარიშგებები)	
4,1	აუდიტის პროცესის ორგანიზება. პრივილეგირებული მომხმარებლების აუდიტის არქივი უნდა ხორციელდებოდეს უფლებამოსილი თანამშრომლის სამუშაო ადგილდან სისტემის ვებ ინტერფეისის საშუალებით, ასევე შესაძლებელი უნდა იყოს პრივილეგირებული მომხმარებლის რეგისტრირებული აქტივობების ფაილის ნახვა. გათვალისწინებული უნდა იყოს ძებნა შემდეგი კრიტერიუმებით: პრივილეგირებული მომხმარებლის სახელით, მომხმარებლის ან ქსელური მოწყობილობის ობიექტის სახელით, სესიის დაწყების და დასრულების დროის მიხედვით.
4,2	საკუთარი აუდიტის ჟურნალის წარმოება, მონიტორინგის სისტემის გავლით მომუშავე ყველა ანგარიშისთვის.
4,3	აუდიტის ჟურნალში უნდა ისახებოდეს პრივილეგირებული მომხმარებლის იდენთიფიკაციისა და აუთენთიფიკაციის შესახებ ინფორმაცია.(სისტემაში იდენთიფიკაციის დროს და ობიექტზე აუთენთიფიკაციის დროს გამოყენებულ ანგარიშებს შორის კავშირი)
4,4	სისტემის აუდიტის ჟურნალში უნდა ისახებოდეს პრივილეგირებული მომხმარებლის მიერ განხორციელებული ყველა ქმედება.
4,5	სისტემის აუდიტის ჟურნალში უნდა ისახებოდეს პრივილეგირებული მომხმარებლის ბრძანებები ტექსტური პროტოკოლების გამოყენების დროს.
4,6	არცერთ პრივილეგირებულ მომხმარებელს არ უნდა ჰქონდეს აუდიტის ჟურნალის წაშლის შესაძლებლობა.
4,7	აუდიტის ჟურნალში უნდა ისახებოდეს ინფორმაცია პრივილეგირებული მომხმარებლის ვიდეო სესიის პარამეტრების შესახებ.

4,8	სრული ტექსტის ძიების შესაძლებლობა აუდიტის ჟურნალში. ქმედებათა დროის მიხედვით აღდგენის შესაძლელობა სესიისთვის.
4,9	ვიდეოარქივში ძებნის უზრუნველყოფა. (თარიღი,დრო,მომხმარებელი, მართვადი ობიექტები).
4,10	აქტიურ/მიმდინარე სესიებში ბრძანებების ძებნა.
4,11	სესიის ჩამოწერა ვიდეო ფაილის სახით შემდგომში სანახავად.
4,12	ჩაწერილი სესიების დაცვა მოდიფიკაციისგან, მთლიანობის უზრუნველსაყოფად.
4,13	დაცული საცავიდან შეუძლებელი უნდა იყოს ფაილების წაშლა, ნებისმიერი მომხმარებელის მიერ 90 დღის განმავლობაში(ცვალებადი პარამეტრი).
4,14	სტატისტიკური რეპორტების გენერაციის შესაძლებლობა დამატებითი(გარე) სისტემის გამოყენების გარეშე.
4,15	დაცულ სისტემებთან მაკონტროლირებელი სისტემის გვერდის ავლით დაკავშირების მცდელობების გამოვლენა.
4,16	სისტემაში დაგროვებული სტატისტიკური ინფორმაციის ანალიზით ადმინისტრატორთა ნორმალური ქცევიდან გადახრის გამოვლენა და პასუხისმგებელ პირთათვის შეტყობინება.
4,17	ქცევითი ანალიზის მოდულის ორმხრივი ინტეგრაცია SIEM სისტემასთან. სისტემას უნდა ჰქონდეს შესაძლებლობა მიიღოს ინფორმაცია SIEM სისტემიდან და დაუბრუნოს SIEM სისტემას ანალიზის რეზულტატები.
4,18	პრივილეგირებული მომხმარებლის არასტანდარტული ქცევის ანალიზზე რეაგირებისთვის სისტემა უნდა იყენებდეს მანქანური სწავლების ალგორითმებს, რომლის მეშვეობითაც სისტემა სწავლობს პრივილეგირებული მომხმარებლის ქცევის ტიპიურ მოდელს.
4,19	მანქანური სწავლების ანალიზის დახმარებით სისტემამ უნდა აღმოაჩინოს პრივილეგირებული მომხმარებლის არასტანდარტული (ატიპიური) ქცევა, შეაფასოს მისი სიმძიმის რისკი და აცნობოს სისტემის პასუხისმგებელ პირს.
4,20	სისტემას უნდა შეეძლოს ქცევის ანალიზატორის მიერ აღმოჩენილი ანომალიური ქცევის SIEM გადაწყვეტილების სისტემაში გაგზავნა შემგდომი ანალიზისა და ანგარიშგებისთვის.
5. საიმედოობის მოთხოვნები	
5,1	სისტემას უნდა ჰქონდეს შესაძლებლობა იმუშაოს გეოგრაფიულად დაშორებული მაღალმდგრადი კლასტერის რეჟიმში.
5,2	გეოგრაფიულად დაშორებულ კომპონენტების ცენტრალური მართვის შესაძლებლობა.
5,3	სისტემის მწყობრიდან გამოსვლის შემთხვევაში ანგარიშების პარამეტრების აღდგენის შესაძლებლობა.