ტექნიკური დავალება პროგრამულ უზრუნველყოფაზე პრივილეგირებული მომხმარებლების

ქმედებების მონიტორინგისა და კონტროლისათვის (შემდგომში - „სისტემა“)

„სისტემის“ დანერგვის მიზნები:

- მაღალკრიტიკულ აი-ტი ინფრასტრუქტურაზე (სერვერები, მონაცემთა ბაზები, აქტიური ქსელური აღჭურვილობა, პროგრამული უზრუნველყოფა და სხვა) ადმინისტრატორის უფლებების მქონე მომხმარებელთა მხრიდან მომხმარებელთა ანგარიშებთან არასანქცირებული წვდომის აღკვეთა;
- აი-ტი ინფრასტრუქტურის ადმინისტრაციული მომხმარებელთა ანგარიშების პრივილეგირებულ მომხმარებელთან დაკავშირებული მტკიცებულებითი ბაზის შექმნა, მონაცემთა მიღება და მათი უსაფრთხო შენახვა;
- საპაროლო პოლიტიკის დაცვისავტომატიზაცია;
- SSH გასაღებების მართვის ავტომატიზაცია;
- სერვერებზე, კომპიუტერებზე და აი-ტი ინფრასტრუქტურაზე მინიმალურ პრივილეგიათა პრინციპის დაცვის ავტომატიზაცია.
- აი-ტი ადმინისტრატორთა მოქმედებების ქცევითი ანალიზი და მაღალ კრიტიკულ აი-ტი ინფრასტრუქტურასთან მუშაობისას არასტანდარტული ქცევის შესახებ რეალური დროში ინფორმირება. SIEM სისტემებზე არასტანდარტული/უჩვეულო ქცევის შესახებ ინფორმაციის გადაცემის შესაძლებლობა;
- მოშორებული პრივილიგირებული მომხმარებლებისთვის დაცული და საიმედო წვდომის უზრუნველყოფა კრიტიკულ სამართავ ობიექტებზე
- ადმინისტრატორის უფლებების მქონე მომხმარებლებისთვის MFA მრავალფაქტორიანი აუტენტიფიკაციის დანერგვა
- ბრძანებათა შავი და თეთრი სიების მეშვეობით SSH სესიის ფარგლებში შექმნილი არაავტორიზებული ბრძანებების დაბლოკვა;
- აი-ტი ადმინისტრატორთა სამუშაო გარემოს იზოლირება სერვერებსა და აი-ტი ინფრასტრუქტურაზე პირდაპირი წვდომის აღკვეთის მიზნით;
- სერვერებზე და აი-ტი ინფრასტრუქტურაზე აი-ტი ადმინისტრატორთა წვდომის სესიების ავტომატური ვიდეოჩაწერა.

„სისტემის“ დანერგვის ამოცანები:

- პრივილეგირებულ მომხმარებელთა ანგარიშების მართვის პროცესის ორგანიზება. პრივილეგირებულ მომხმარებელთა ანგარიშების მართვის პროცესი უნდა უზრუნველყოფდეს ახალი პაროლის გენერაციას საპაროლო პოლიტიკის მოთხოვნათა შესაბამისად, მართვის ყველა ობიექტზე ყველა პაროლის რეგულარულ ცვლას, პაროლის აღდგენას მისი არასანქცირებული შეცვლის შემთხვევაში, ახალი მომხმარებელთა ანგარიშების შექმნის დროულ გამოვლენას და ამ მოვლენის შესახებ შესაბამისი თანამშრომლების ინფორმირებას, ასევე, სამიზნე სისტემებში SSH გასაღებების მართვას;
- შიდა აი-ტი თანამშრომლებისთვის და გარე აი-ტი პარტნიორ კომპანიების მომხმარებლებისთვის, მოშორებული მუშაობის რეჟიმის შემთხვევაში, დაცული ადმინისტრაციული წვდომებისუზრუნველყოფა კრიტიკულ შიდა ინფრასტრუქტურულ მართვის ობიექტებზე, ბრაუზერის და მრავალფაქტორიანი აუტენტიფიკაციის საშუალებით, ე.წ. VPN კლიენტების გამოყენების გარეშე

- აი-ტი ადმინისტრატორთა აქტივობის რეგისტრაციის ორგანიზება. ადმინისტრატორთა ქმედებების რეგისტრაციის პროცესი უნდა უზრუნველყოფდეს:

    - აი-ტი ინფრასტრუქტურის ადმინისტრირებისას გამოყენებული პროგრამული უტილიტების სამუშაოგარემოს იზოლირებას დანარჩენი, პოტენციურად არასაიმედო გარემოსაგან;
    - ადმინისტრატორთა მიერ შიდა აი-ტი ინფრასტრუქტურის საბოლოო ობიექტებზე განხორციელებული აქტივობის სრულ რეგისტრირებას. რეგისტრაცია უნდა გაფორმდეს ტექსტური ან ვიზუალური ოქმის სახით, გამოყენებული ადმინისტრირების კლიენტის შესაბამისად;

- აი-ტი ინფრასტრუქტურაზე წვდომის მინიჭების პროცედურის ორგანიზება. ეს პროცედურა უნდა იყოს გამჭვირვალე და კონტროლირებადი, იძლეოდეს აუდიტის შესაძლებლობას. ამისათვის, „სისტემაში“ უნდა არსებობდეს ინსტრუმენტები, რომლებიც საშუალებას მისცემს ადმინისტრატორს, აღწეროს მოთხოვნილი წვდომის მახასიათებლები, როგორიცაა:

    - წვდომის მინიჭების დაწყების თარიღი და დრო;
    - წვდომის მინიჭების ინტერვალის ხანგრძლივობა;
    - ამ დროის განმავლობაში მართვის ობიექტთან მრავალჯერადი მიერთების შესაძლებლობა;
    - წვდომის მინიჭების მიზეზები, მიზნები და საფუძვლები.

  ამავე დროს, „სისტემას“ საკუთარი ინსტრუმენტების მეშვეობით უნდა შეეძლოს წვდომის მიღებაზე მოთხოვნის გაზავნა შესაბამის თანამშრომელთან და მოთხოვნილი წვდომის დაკმაყოფილება ან დაბლოკვა.
  „სისტემის“ მეშვეობით ზემდგომ მენეჯერს უნდა შეეძლოს თანამშრომლების მიერ სამიზნე სისტემებთან მოთხოვნილი წვდომის დადასტურებაა.

- აუდიტის პროცესის ორგანიზება. აი-ტი ადმინისტრატორთა მიერ წარმოებული ოპერაციების არქივის აუდიტი (მათ შორის, თანამშრომელთა აქტივობის რეგისტრაციის ფაილების ნახვა) უნდა განხორციელდეს „სისტემის“ სტანდარტული საშუალებებით, . გათვალისწინებული უნდა იქნას ძიება შემდეგი რეკვიზიტებით: სააღრიცხვო ჩანაწერი, მომხმარებლის სახელით ან საკონტროლო ობიექტის ქსელური სახელი, სესიის დაწყებისა და დამთავრების დრო..

სისტემის დანერგვის მასშტაბები.

„სისტემის“ მომხმარებელთა რაოდენობა: 3 (სამი) წლიანი ლიცენზია, 15 (თხუთმეტი) პრივილიგირებული მომხმარებლისთვის, 24/7 მხარდაჭერით მწარმოებლის მხრიდან.

სისტემის გაფართოების მოთხოვნები.

„სისტემას“ უნდა ჰქონდეს, გაფართოების შესაძლებლობა დამატებითი მოდულების ან ლიცენზიების დაყენებით, რასაც თან სდევს მისი ფუნქციონალური შესაძლებლობების გაფართოება;

„სისტემას“ უნდა ჰქონდეს გაფართოების შესაძლებლობა დამატებითი ლიცენზიების შესყიდვის მეშვეობით:

- Unix სისტემების დაცვისათვის „სისტემას“ უნდა შეეძლოს Unix სისტემების სუპემომხმარებლებისათვის მხოლოდ აუცილებელი უფლებების მინიჭება.
- შესაძლებელი უნდა იყოს root-უფლებებით განხორციელებული ქმედებები დაუკავშირდეს ამ უფლებების მქონე მომხმარებლის ანგარიშს. მართვის ფუნქციონალის მინიჭიება;
- სისტემას უნდა შეეძლოს ე.წ. Golden Ticket, Over-Pass-the-Hash, PAC manipulation, DCSync კიბერ იერიშების დეტექტირება, Active Directory სერვერებზე აგენტების და ქსელური სენსორების დანერგვის მეშვეობით.
- სკრიპტებში, სამსახურებსა და პროგრამულ უზრუნველყოფაში ჩასმული პაროლების შეცვლა, პროგრამული უზრუნველყოფის მუშაობის შეჩერების გარეშე.
- პაროლების ავტომატური სინქრონიზაცია და მონაცემებზე წვდომისათვის მხოლოდ ნებადართული პროგრამული უზრუნველყოფის აუტენტიფიცირება;
- „სისტემას“ უნდა შეეძლოს პაროლების ცენტრალური მართვა და გამოყენება, რომლებიც გამოიყენება აპლიკაციებში, მიკრო სერვისებში, კონტეინერებში, CI / CD ინსტრუმენტებში: Jenkins, Chef, Ansible, Puppet; კონტეინერების ორკესტრირების სისტემებში: Kubernetes, Openshift, PCF
- „სისტემას“ უნდა გააჩნდეს ინტეგრირების მხარდაჭერა ე.წ vulnerability სკანირების პროდუქტებთან, ამ პროდუქტებში გამოყენებული პაროლების დაცვის და როტაციის მიზნით. „სისტემა“ უნდა იყოს მხარდაჭერილი შემდეგი Vulnerability სკანერების პროდუქტების მიერ: Rapid7 Nexpose, McAfee Vulnerability Manager, QualysGuard Vulnerability & Compliance Scanning, Tenable Nessus. ინტეგრაციის მხარდაჭერა უნდა იყოს დამოწმებული ორივე მომწოდებლის მიერ („სისტემის“ და Vulnerability სკანერების პროდუქტების მწარმოებლების მიერ)

„სისტემა“ უნდა მასშტაბირდებოდეს და ფუნქციონალის დამატება ხდებოდეს დამატებითი ლიცენზიების შესყიდვით, ან არქიტექტურაში ახალი კომპონენტების დამატებით, არსებული კომპონენტების შეცვლის გარეშე.

სისტემის ფუნქციური მოთხოვნები.

1. **ადმინისტრირების პროტოკოლების მოთხოვნები**

1.1 ინფრასტრუქტურის ობიექტების ადმინისტრირება SSH პროტოკოლის მეშვეობით
1.2 ინფრასტრუქტურის ობიექტების ადმინისტრირება RDP პროტოკოლის მეშვეობით
1.3 მართვის Web ინტერფეისის მქონე ინფრასტრუქტურის ობიექტების ადმინისტრირება HTTP/HTTPS პროტოკოლების მეშვეობით
1.4 ინფრასტრუქტურის ობიექტების უსაფრთხო ადმინისტრირება დამკვეთის მიერ გამოყენებული სხვა პროტოკოლების მეშვეობით
1.5 საპაროლო პოლიტიკის დაცვა და პრივილეგირებული სესიების ჩაწერა ადმინისტრირების ობიექტებზე აგენტების დაყენების გარეშე

2. მოთხოვნები ადმინისტრირების მხარდაჭერილი ობიექტებისადმი

2.1 UNIX სისტემების სერვერების ადმინისტრირება

2.2 Windows Server სისტემების სერვერების ადმინისტრირება

2.3 Microsoft Windows Domain Controller-ის ადმინისტრირება

2.4 VMware (ყველა კომპონენტის) და Microsoft Hyper-V ინფრასტრუქტურის ობიექტების ადმინისტრირება

2.5 Citrix ტერმინალური სერვერების ადმინისტრირება

2.6 DBMS სერვერების ადმინისტრირება

2.7 MS SQL Server-ის ადმინისტრირება

2.8 ფაილ სერვერების ადმინისტრირება (სერვერები და NAS)

2.9 წამყვანი მწარმოებლების კომუტატორების ადმინისტრირება

2.10 წამყვანი მწარმოებლების მარშრუტიზატორების ადმინისტრირება

2.11 წამყვანი მწარმოებლების ფაერვოლების ადმინისტრირება

2.12 FC-კომუტატორებისა და SAN მარშრუტიზატორების ადმინისტრირება

2.13 Windows (XP, 7, 8, 10) სისტემების სამუშაო სადგურების ადმინისტრირება

2.14 დამკვეთის მიერ არჩეული ადმინისტრირების ინტერფეისის, მათ შორის "სქელი კლიენტების" „სისტემასთან“ ინტეგრაციის უზრუნველყოფა ადმინისტრატორთა უსაფრთხო შესვლის უზრუნველყოფა “სისტემის” ვებ-აპლიკაციებთან ინტეგრაციის მეშვეობითა -, სამიზნე სისტემის პაროლის გამჟღავნების გარეშე და სესიის ვიდეოჩანაწერის წარმოებით.

2.15 Out-of-Box მხარდაჭერილი მართვის ობიექტების გარდა, „სისტემას“ უნდა გააჩნდეს ინტეგრირების მხარდაჭერა, სქრიპტების ან სხვა მეთოდების საშუალებით, არანაკლებ 200 მართვის სისტემასთან, მწარმოებლის მიერ მხარდაჭერილ ე.წ. marketplace - ვებ პორტალის მეშვეობის

3. არქიტექტურული, საინტეგრაციო და საექსპლუატაციო მოთხოვნები

3.1 ადმინისტრატორის წვდომა ადმინისტრირების ობიექტებზე უნდა ხდებოდეს სპეციალური პორტალის საშუალებით, რომელზეც იგიაუთენტიფიცირდება და ირჩევს მისთვის ხელმისაწვდომ ადმინისტრირების ობიექტს,

3.2 პრივილეგირებულ მომხმარებელთა ანგარიშების პარამეტრებზე წვდომა და მათი შენახვა, ასევე ადმინისტრირების ოპერაციების ვიდეოარქივის შენახვა უნდა მოხდეს გამოყოფილ დაცულ სანახზე.

3.3 . საცავის მონაცემები დაშიფრული უნდა იყოს. საცავი დაცული უნდა იქნას არასანქცირებული წვდომისგან.

3.4 აუდიტის მონაცემთა გადაცემის შესაძლებლობა SIEM სისტემაში.

3.6 Microsoft Active Directory-დან ადმინისტრირების ობიექტების ავტომატური აღმოჩენა და იმპორტიი ა"სისტემაში" არსებულ ადმინისტრაციულ მომხმარებელთა ანგარიშების პაროლების შემდგომი ავტომატური შეცვლით. „სისტემა" უნდა იყოს საპაროლო პოლიტიკის დასახვის უმთავრესი საშუალება ადმინისტრატორებისთვის, მათ შორის, In-house სისტემებისთვისაც.

3.7 ადმინისტრირების სესიაში "View Only" რეჟიმში ჩართვის შესაძლებლობა.

3.8 ტერმინალური მოდულიდან სამიზნე სისტემებში შეერთებები უნდა ხდებოდეს ნატიური პროტოკოლებისა და კლიენტების გამოყენებით.

3.9 „სისტემას" უნდა ჰქონდეს ყველა ფუნქციური მოდულის მართვის ერთიანი კონსოლი.

3.10 ინციდენტების რეგისტრაციის სისტემებთან ინტეგრაცია.

3.11 სისტემას უნდა შეეძლოს არანაკლებ 100 000 ერთეული ინფრასტრუქტურის კონტროლირებადი ობიექტების დამუშავება.

3.12 "სისტემაში" წვდომის ერთდროული სესიების რაოდენობა უნდა იყო ულიმიტო.

3.13 "სისტემას" უნდა შეეძლოს Linux / Unix ოპერაციულის სისტემებისათვის-ბრძანებების დაბლოკვა, და ასევერე ბრძანებების შავი სიის შექმნა.

3.14 შენახული ანდა გამოცვლილი პაროლის ავტომატური გადაცემის შესაძლებლობა სესიაში, ადმინისტრატორისთვის მისი გამჟღავნების გარეშე.

3.15 პაროლის როტაციის განხორციელების შესაძლებლობა თითოეული სესიის დასრულების შემდეგ.

3.16 პაროლების დაცვა და როტაცია აი-ტი ადმინისტრატორების ლოკალურ Windows და MacOS ოპერაციულ სისტემებზე, იგივე მწარმოებლის სპეციალიზებული აგენტის საშუალებით

3.17 პაროლების დაცვა და ავტომატური როტაცია ნებისმიერი მართვის ობიექტისთვის, რომელიც მხარს უჭერს ODBC 2.7 ან უფრო მაღალ ვერსიებს

3.18 გააჩნდეს ანგარიშების ავტომატურად აღმოჩენის შესაძლებლობა Windows მოწყობილობებში, Windows სერვისებში, Windows დაგეგმილ დავალებებში და IIS სერვისულ ანგარიშებში. აგრეთვე, ავტომატურ რეჟიმში განახორციელოს ამ ანგარიშების სისტემაში დამატება (on-boarding) და როტაცია, შესაბამის გამზადებულ ანგარიშების უსაფრთხოების პოლიტიკების მიხედვით.

3.18 სისტემის მომხმარებლების მოშორებული მუშაობის რეჟიმის შემთხვევაში, სისტემამ უნდა უზრუნველყოს დაცული ადმინისტრაციული წვდომების უზრუნველყოფა, კრიტიკულ შიდა ინფრასტრუქტურულ მართვის ობიექტებზე, ბრაუზერ კლიენტის და მრავალფაქტორიან MFA აუტენტიფიკაციის საშუალებით, ე.წ. VPN პროგრამული უზრუნველყოფის გამოყენების გარეშე.

ამ ფუნქციონალის დანერგვა უნდა იყოს შესაძლებელი იგივე მწარმოებლის ღრუბლოვანი SaaS სერვისების მეშვეობით, დამატებითი ლიცენზიის გარეშე. სისტემას უნდა გააჩნდეს შემდები ბრაუზერების მხარდაჭერა: Chrome, Internet Explorer, Edge, Firefox

3.19 სისტემაში ლიცენზირებული მომხმარებლების რაოდენობისთვის უნდა იყოს უზრუნველყოფილი მრავალფაქტორიანი MFA და ე.წ. Single Sign On აუტენტიფიკაციის მექანიზმების დანერგვის საშუალება, იგივე მწარმოებლის მიერ მოწოდებული ღრუბლოვანი SaaS სერვისების მეშვეობით, დამატებითი ლიცენზიის გარეშე.

MFA აუტენტიფიკაციის სისტემამ უნდა უზრუნველყოს არანაკლებ შემდეგი მრავალფაქტორიანი აუტენტიფიკაციის მეთოდები: sms, email, oauth, mobile application, phone call და უნდა გააჩნდეს Active Directory სერვერთან ინტეგრაციის საშუალება.

3.20 „სისტემაში“ კიბერ საფრთხეების აღმოჩენის შემთხვევაში, მწარმოებელმა უნდა აცნობოს დამკვეთს ამ საფრთხეების შესახებ, მეილის საშუალებით, შესაბამისი დეტალური აღწერით და სამიტიგაციოს ქმედებების რეკომენდაციებით

4. მოთხოვნები აუდიტის ქვესისტემისადმი (აღრიცხვა, ვიდეოჩაწერა, ანგარიშები)

4.1 „სისტემამ“ უნდა აწარმოოს მისი საშუალებით მომუშავე ყველა მომხმარებლის ანგარიშის ქმედებათა აუდიტის საკუთარი ჟურნალი.

4.2 „სისტემის“ აუდიტის ჟურნალებში ასახული უნდა იქნას ინფორმაცია ადმინისტრატორის საიდენტიფიკაციო და სააუთენტიფიკაციო პარამეტრების შესახებ (ტარდება ადმინსტრატორისა და გამოყენებული მომხმარებლის ანგარიშის ცალსახა დაკავშირება).

4.3 „სისტემის“ აუდიტის ჟურნალებში ასახული უნდა იქნას ინფორმაცია ადმინისტრატორის ყველა ქმედების შესახებ.

4.4 „სისტემის“ აუდიტის ჟურნალებში აისახება ადმინისტრატორთა ბრძანებები “Command Line”-ის გამოყენებისას.

4.5 სისტემის ნებისმიერი ადმინისტრატორის მომხმარებლის ანგარიშის მეშვეობით ჟურნალების განადგურების შეუძლებლობა.

4.7 ტექსტური ძიება ადმინისტრირების ობიექტების აუდიტის ჟურნალებში იმ მოვლენების დროითი თანმიმდევრობის აღდგენა, რომლებიც ხდება კონკრეტული ადმინისტრატორის სესიების ფარგლებში.

4.8 ვიდეოარქივში ძებნის უზრუნველყოფა (თარიღი, დრო, მომხმარებელი, ადმინისტრირების ობიექტები).

4.9 ვიდეოჩანაწერის გადმოტვირთვის შესაძლებლობა შემდგომი ნახვის მიზნით.

4.10 ჩაწერილი სესიების მოდიფიკაციებისა და მანიპულაციებისაგან დაცვის უზრუნველყოფა.

4.11 დაცული სანახიდანრომელიმე ფაილის რომელიმე მომხმარებლის სახელით წაშლის შეუძლებლობა 90-დღიან ვადაში (რეგულირებადი პარამეტრი).

4.12 სტატისტიკური ანგარიშების ფორმირება რეორტების გარე გენერატორების დახმარების, ან გარე სისტემებში ინფორმაციის ატვირთვის გარეშე.

4.13 მართვის ობიექტებთან „სისტემის“ გვერდის ავლით მიერთების ფაქტებისა და მცდელობების აღმოჩენის შესაძლებლობა.

4.14 ადმინისტრატორთა ქმედებების ავტომატური ანალიზი „სისტემაში“ დაგროვილი სტატისტიკური ინფორმაციის საფუძველზე და პასუხისმგებელ

პირთა გაფრთხილება ადმინისტრატორის ქცევის სტატისტიკური ნორმიდან გადახრის გამოვლენის შესახებ.

4.15 ქცევითი ანალიზის მოდულის ორმხრივი ინტეგრირება SIEM სისტემასთან: ინფორმაციის მიღება SIEM-დან და ანალიზის შედეგების დაბრუნება SIEM-ში.

4.16 „სისტემას“ უნდა შეეძლოს მომხმარებლის აქტივობების მონაცემების შეგროვება და გაანალიზება, გარე SIEM სისტემების საშუალებით და უნდა იყოს მხარდაჭერილი შემდეგი გადაწყვეტილებები: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee და ოპერაციული სისტემები: rsyslog (Unix / Linux სისტემებიდან), Windows Event Forwarder (Windows სისტემებიდან), AWS CloudTrail, Azure Function App

4.17 სისტემას უნდა გააჩნდეს SIEM სისტემებში გასაგზავნი მოვლენების სიის და ტიპის კონფიგურაციის საშუალება

4.18 ბრძანებების მიხედვით ძიების უზრუნველყოფა დაუმთავრებელ სესიებში.

5. **საიმედოობის მოთხოვნები**

5.1 „სისტემას“ უნდა შეეძლოს მაღალი წვდომადობის უზრუნველოყოფა გეოგრაფიულად განაწილებული კლასტერის სახით, კვანძებს შორის გადართვის შესაძლებლობით ინფორმაციის დაკარგვის გარეშე.

5.2 „სისტემის“ გეოგრაფიულად განაწილებული კომპონენტების ცენტრალიზებული მართვის შესაძლებლობა.

5.3 სადიაგნოსტიკო საშუალებები უნდა იძლეოდეს „სისტემის“ მუშაობის მონიტორინგის საშუალებას.

5.4 მომხმარებელთა ანგარიშების პარამეტრების ავარიული აღდგენის პროცედურის არსებობა “სისტემის“ მოდულების მწყობრიდან გამოსვლის შემთხვევაში.

6. **ანალიზის შესაძლებლობები**

6.1 სისტემამ უნდა გამოავლინოს ადმინისტრატორთა ქცევის სტატისტიკური ნორმიდან გადახრების რიგი პარამეტრების მიხედვით, რომლებიც ცალსახად აღწერს თითოეული ადმინისტრატორის მიერ სისტემასთან მუშაობის უნიკალურ თავისებურებას. ტესტირების ნაწილში მოწმდება: ჩვეულო დროს წვდომის გამოვლენა, უჩვეულო მისამართებიდან წვდომის აღმოჩენა.

7. მოთხოვნები სისტემის არქიტექტურის მიმართ

დასანერგი სისტემა უნდა შედგებოდეს შემდეგი კომპონენტებისგან:

- ავტორიზაციის მოდული (ულიმიტო)- კონტროლირებადი ადმინისტრატორების წვდომის ვებ-ინტერფეისი, Microsoft IIS-ის ბაზაზე, რომელიც ახორციელებს აუთენტიფიკაციას, მართვის ობიექტის შერჩევას და კლიენტის გაშვებას;
- ტერმინალური მოდული (ულიმიტო)- ადმინისტრირების უტილიტების გაშვებისა და ადმინისტრატორების ოპერაციების ჩაწერის გარემო. რეალიზებულია ტერმინალური სერვერის ბაზაზე Windows Server-ის მართვის ქვეშ.
- SSH ტერმინალური მოდული (ულიმიტო)- უზრუნველყოფს SSH ადმინისტრირების მართვის სესიების გაშვებას და ჩაწერას, მომხმარებლის მხარეს ნებისმიერი SSH პროგრამული უზრუნველყოფის კლიენტის მეშვეობით. რეალიზებულია ტერმინალური სერვერის ბაზაზე Linux Server-ის მართვის ქვეშ.
- პოლიტიკების მოდული(ხუთი ცალი) - უზრუნველყოფს პრივილეგირებული მომხმარებელთა ანგარიშების პაროლების მართვას სამიზნე სისტემებზე. რეალიზებულია სერვერის ბაზაზე, რომელიც Windows Server-ის მართვის ქვეშ ფუნქციონირებს.
- დაცული სანახის მოდული - უზრუნველყოფს პრივილეგირებულ მომხმარებელთა ანგარიშების პარამეტრების გადაცემასდა შენახვას. რეალიზებულია ცალკე სერვერის ბაზაზე, რომელიც Windows Server-ის მართვის ქვეშ ფუნქციონირებს. უნდა გააჩნდეს Active/Passive მაღამდგრადობის კლასტერის და DR სარეზერვო დატაცენტრის კომპონენტების დანერგვის მხარდაჭერა, დამატებითი ლიცენზიის გარეშე
- ქცევის ანალიზის მოდული, SIEM სისტემებთან ორმხრივი ინტეგრაციის შესაძლებლობით.
- HTML5 ვებ მოდული - უზრუნველყოფს იზოლირებულ ადმინისტრაციულ სესიებს მართვის ობიექტებზე, მომხმარებლის ბრაუზერის საშუალებით, სხვა დამატებითი პროგრამული უზრუნველყოფის გარეშე. რეალიზებულია სერვერის ბაზაზე, რომელიც Linux Server-ის მართვის ქვეშ ფუნქციონირებს