პრივილეგირებული წვდომების მართვის გადაწყვეტილება - 25/50 პრივილეგირებული წვდომის სესია “HA (High Availability)” - ისთან ერთად.

|  |  |
| --- | --- |
|  **რ/ნ №** | **პროდუქტის მიმართ წაყენებული ტექნიკური მოთხოვნების დასახელება და აღწერა, მოთხოვნილი დამკვეთის მიერ** |
| **გადაწყვეტილება უნდა იყოს ESXi ვირტუალურ გარემოსთან სრულად თავსებადი.**  |
|  | **ზოგადი (სისტემური) მოთხოვნები** |
|  | პროდუქტის მიწოდება უნდა მოხდეს ვირტუალური მოწყობილობის (VA - virtual appliance) სახით, მიწოდების ტიპი - შესრულებული უნდა იყოს ერთი პლატფორმის სახით, რომელიც იმპლემენტაციისთვის არ საჭიროებს გარე სისტემურ უზრუნველყოფას ან პროგრამული უზრუნველყოფის (ოპერაციული სისტემების, აპლიკაციების, მონაცემთა ბაზების მართვის სისტემების და ა.შ.) გამოყენებას აპლიკაციის სახით. |
|  | პროდუქტს უნდა ჰქონდეს დაცვის ჩაშენებული მექანიზმი შენახულ ინფორმაციის დასაცავად არასანქცირებული წვდომისგან. ასეთმა დაცვამ უნდა უზრუნველყოს სპეციალური უსაფრთხოების გასაღების (პაროლის) გამოყენება პროდუქტის ყოველი გაშვებისას (გამორთვის ან გადატვირთვის შემდეგ). |
|  | პროდუქტის პარამეტრების შერჩევა და ადმინისტრირება შესაძლებელი უნდა იყოს ადმინისტრირებისთვის განკუთვნილი ცალკე ვებ-პორტალიდან, ნებისმიერი თანამედროვე ბრაუზერის გამოყენებით (IE, Mozilla, Chrome), დამატებითი კომპონენტების (პლაგინების, აპლიკაციების და ა.შ.) ინსტალაციის გარეშე. დაუშვებელია Flash ან Java (JRE) ტექნოლოგიებზე დაფუძნებული ვებ-კონსოლის გამოყენება. |
|  | პროდუქტის ადმინისტრირება უნდა მოიცავდეს პროდუქტის მართვის როლური მოდელის და პრივილეგირებულ მომხმარებლების მხარდაჭერის შესაძლებლობას. |
|  | პროდუქტი პრივილეგირებულ მომხმარებლებს უნდა სთავაზობდეს სპეციალურ დამატებით ვებ-პორტალ(ებ)ს კონტროლირებად (სამიზნე) სისტემებზე წვდომისათვის. ამ პორტალის გამოყენება უნდა იყოს ოფციური (არასავალდებულო), ანუ პროდუქტმა უნდა უზრუნველყოს კონტროლირებად (სამიზნე) სისტემებზე წვდომა, მათ შორის ასეთი პორტალის გარეშეც (სპეციალიზებული აპლიკაციების მეშვეობით: Microsoft Remote Desktop Client, Putty client, SQL Developer, Microsoft SQL Management Studio და ა.შ.). |
|  | პროდუქტს უნდა შეეძლოს მუშაობის შემაფერხებელი ფაქტორების მიმართ მდგრადი კონფიგურაციების შექმნა ჩაშენებული ტექნოლოგიების ბაზაზე, ასეთი (მდგრადი) კონფიგურაციების შესაქმნელად უცხო (გარე) საშუალებების გამოყენება დაუშვებელია.2 ან მეტი კვანძის მხარდაჭერა კლასტერში, ამოცანებისა და დატვირთვების განაწილების შესაძლებლობით (ცალკე კვანძი მხოლოდ კონფიგურაციის რეპლიკაციისთვის, ცალკე კვანძი ამოცანების შესასრულებლად გრაფიკული სესიების ამოცნობით OCR მექანიზმის მეშვეობით) |
|  | პროდუქტს უნდა ჰქონდეს დიაგნოსტირების ჩაშენებული სისტემები, დაკავშირებული კონტროლირებად (სამიზნე) სისტემებზე წვდომის შეცდომებთან. |
|  | პროდუქტს უნდა ჰქონდეს პროდუქტის მუშაობასთან დაკავშირებული ყველა მოვლენის შენახვის და დამუშავების ფუნქციონალი, ასევე, ასეთი მოვლენების ავტომატური გადაცემის ფუნქციონალი მოვლენების დამუშავების გარე სისტემებისთვის.  |
|  | პროდუქტს უნდა ჰქონდეს სარეზერვო ასლების შექმნის ჩაშენებული ფუნქციონალი, რომელიც უნდა შეიცავდეს პროდუქტის ყველა კონფიგურაციას და პარამეტრს, ასევე პრივილეგირებული მომხმარებლების ჩაწერილ სესიებს. ამგვარად შექმნილი ასლები დაცული უნდა იყოს არასანქცირებული წვდომისგან. |
|  | პროდუქტს უნდა ჰქონდეს სხვადასხვა ობიექტის მართვის ფუნქციონალი, როგორიცაა მომხმარებლები, სამიზნე სისტემები, როგორც ადგილობრივი (ვებ-პორტალის მეშვეობით), ისე დისტანციური (ღია API-ინტერფეისების მეშვეობით) დაკავშირების მეთოდები. |
|  | პროდუქტის ინტერფეისი ხელმისაწვდომი უნდა იყოს ინგლისურ და რუსულ ენებზე. |
|  | პროდუქტმა უნდა უზრუნველყოს სესიების ჩაწერა ქსელური აღჭურვილობით SSH, Telnet, HTTP/S პროტოკოლების მიხედვით, შუალედური ჰოსტების (jump host) ან აგენტების გამოყენების გარეშე, სერვერებზე, აღჭურვილობასა და სამუშაო სადგურებზე. |
|  | პროდუქტმა უნდა უზრუნველყოს მუშაობის შემდეგ რეჟიმების მხარდაჭერა დამკვეთის ქსელში:* Transparent bridge
* Gateway და/ან Proxy
* Bastion
 |
|  | **ფუნქციური (ტექნიკური) მოთხოვნები:** |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლების ქმედებების ჩაწერის მხარდაჭერა ჩაშენებული საშუალებების გამოყენებით, ნებისმიერი კომპონენტის (აგენტი, სერვისი, დრაივერი და ა.შ.) ინსტალაციის აუცილებლობის გარეშე, როგორც პრივილეგირებული მომხმარებლების საბოლოო წერტილებზე, ასევე იმ სისტემებზე, რომლებსაც უკავშირდებიან პრივილეგირებული მომხმარებლები (სამიზნე სისტემები). |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული ფუნქციონალი (OCR მექანიზმი ან მისი ანალოგი) ტექსტური ინფორმაციის ამოსაცნობად ჩაწერილ გრაფიკულ სესიებში, მათ შორის - კირილიცას სიმბოლოები, ასეთი ინფორმაციის შემდგომში მოძიების მიზნით.ეს ფუნქციონალი უნდა მუშაობდეს როგორც ხელით სამართავ, ისე ავტომატურ რეჟიმში (გამოიყენება თითოეული შენახული სესიისთვის, პროდუქტის ადმინისტრატორის ჩარევის გარეშე). |
|  | პროდუქტის ფუნქციონალს უნდა ჰქონდეს ქსელის გაფართოებული კონფიგურირების მხარდაჭერის შესაძლებლობა, როგორიცაა:* ვირტუალური (VLAN) ქსელების მხარდაჭერა;
* ქსელური არხების აგრეგაცია;
* საკუთარი ARP ცხრილების შექმნა;
* სტატიკური მარშრუტიზაციის კონფიგურირება ცალკეული ქსელებისთვის.
 |
|  | პქროდუქტს უნდა გააჩნდეს OCR მხარდაჭერა ქომანდების შეზღუდვა როგორც ვინდოუს ასევე ლინუქსზე. |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული პანელი ინფორმაციის მიწოდების შესაძლებლობით პროდუქტის კომპონენტების მუშაობისუნარიანობასა და დატვირთვაზე, მინიმუმ: დისკური სისტემის აქტივობის, პროცესორ(ებ)ის დატვირთვის, ოპერატიული მეხსიერების დატვირთვის და ქსელური კომპონენტების დატვირთვის შესახებ.ასეთი საინფორმაციო პანელი ხელმისაწვდომი უნდა იყოს მხოლოდ პროდუქტის ადმინისტრატორებისთვის, ადმინისტრირების შესაბამის ვებ-პორტალზე. |
|  | პროდუქტს უნდა შეეძლოს მუშაობა ვირტუალური ქსელის არანაკლებ რვა ადაპტერთან.პროდუქტს უნდა შეეძლოს ქსელის თითოეულ ადაპტერს მიანიჭოს უნიკალური IP-მისამართი (მათ შორის - ქსელის სხვადასხვა სეგმენტიდან) როგორც სტატიკურ, ასევე დინამიურ რეჟიმში (DHCP სერვისის გამოყენებით).თითოეული ასეთი უნიკალური IP მისამართისთვის პროდუქტს უნდა შეეძლოს პრივილეგირებულ მომხმარებლებს გამოუყოს სპეციალური ცალკე ვებ-პორტალი კონტროლირებად (სამიზნე) სისტემებზე წვდომისთვის.პროდუქტს უნდა ჰქონდეს ასეთ ვებ-პორტალებზე წვდომის სეგმენტირების ფუნქციონალი მომხმარებელთა ჯგუფებისა და სამიზნე სისტემების საფუძველზე. |
|  | პრივილეგირებული მომხმარებლებისთვის გამოყოფილმა თითოეულმა ვებ-პორტალმა პრივილეგირებულ მომხმარებლებს უნდა შესთავაზოს შემდეგი შესაძლებლობები:* დასაკავშირებლად ხელმისაწვდომი სამიზნე სისტემების ჩამონათვალი, სესიების გახსნის შესაძლებლობით სტანდარტული კლიენტების მეშვეობით (RDP ,VNC და SSH პროტოკოლებისთვის)
* სამიზნე სისტემების IP-მისამართებისა და პორტების სია;
* პროტოკოლის ტიპი, რომელიც გამოიყენება სამიზნე სისტემასთან დასაკავშირებლად;
* სამიზნე სისტემის პაროლის დათვალიერება (თუ ასეთი უფლებები პრივილეგირებულ მომხმარებელს მიენიჭება შესაბამისი პაროლის პოლიტიკით);
* სააღრიცხვო ჩანაწერის პაროლის შეცვლა ვებ-პორტალზე (თუ პაროლი ინახება პროდუქტის საკუთარ დაცულ საცავში).

ისეთი დამატებითი პარამეტრების არჩევის შესაძლებლობა, როგორიცაა დამატებითი ინფორმაციის გამოტანა პრივილეგირებული მომხმარებლებისთვის, დამკვეთის ლოგოებისვის და ა.შ. იქნება დამატებითი უპირატესობა. |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული დაცული საცავი პრივილეგირებული მომხმარებლების ჩაწერილი სესიების, პროდუქტსა და სამიზნე სისტემებზე და მოვლენების ჟურნალზე წვდომის რეკვიზიტების შესანახად (ლოგინი, პაროლი, გასაღებები, დომენური სახელები და ა.შ.) დაცული საცავი უნდა იყენებდეს არანაკლებ AES-256 დონის სტანდარტულ კრიპტო ალგორითმებს. |
|  | პროდუქტი უნდა უზრუნველყოფდეს სესიის ფარგლებში განხორციელებული ქმედებების ჩანაწერზე ციფრული ხელმოწერის შესრულების შესაძლებლობას საიმედოობის იმ ხარისხით, რომელსაც მოითხოვს სასამართლო ორგანოები საკითხის განსახილველად. |
|  | პროდუქტის გამოყენების როლურმა მოდელმა უნდა უზრუნველყოს შემდეგი გამიჯვნა სხვადასხვა სააღრიცხვო ჩანაწერის ბაზაზე:* სრული უფლებები ადმინისტრირებაზე - მათ შორის პროდუქტის კონფიგურირების შესაძლებლობა.
* ნაწილობრივ შეზღუდული უფლები ადმინისტრირებაზე - ნებისმიერი ქმედება, გარდა პროდუქტის კონფიგურირებისა
* შეზღუდული უფლებები ადმინისტრირებაზე - კონკრეტულად განსაზღვრული სამიზნე სისტემებისა და პრივილეგირებული მომხმარებლების კონფიგურირების და მათი შემდგომი მონიტორინგის შესაძლებლობა.
* მომხმარებლის უფლებები - მხოლოდ კონკრეტულად განსაზღვრულ სამიზნე სისტემებთან დაკავშირების შესაძლებლობა, ადმინისტრირების ვებ-პორტალზე შესვლის შესაძლებლობის გარეშე.
 |
|  | პროდუქტს უნდა ჰქონდეს ადმინისტრატორების დამატების ფუნქციონალი პროდუქტის ადმინისტრირების ვებ-პორტალიდან, ადმინისტრატორების როლის, სააღრიცხვო ჩანაწერის მოქმედების ვადის, ენისა და ავთენტიფიკაციის მეთოდის განსაზღვრის შესაძლებლობით.ადმინისტრატორის თითოეული სააღრიცხვო ჩანაწერისთვის ერთდროულად უნდა არსებობდეს რამდენიმე მეთოდით ავთენტიფიკაციის შესაძლებლობა, მინიმუმ:* სტატიკური პაროლით, რომელიც ინახება პროდუქტის დაცულ საცავში.
* ერთჯერადი პაროლით, რომელიც გენერირდება გარე მომსახურებით (მაგალითად, RADIUS-სერვერით)
* მომხმარებლის გარე კატალოგის გამოყენებით (AD / LDAP)
* SSH გასაღების გამოყენებით.
 |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლის დამატების ფუნქციონალი პროდუქტის ადმინისტრირების ვებ-პორტალიდან, ადმინისტრატორების როლის, სააღრიცხვო ჩანაწერის მოქმედების ვადის, ენისა და ავთენტიფიკაციის მეთოდის განსაზღვრის შესაძლებლობით.პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლების დამატების ფუნქციონალი შემდეგი გზით:* ხელით შერჩევის რეჟიმში;
* სინქრონიზაცია მომხმარებლთა უკვე არსებულ კატალოგიდან (AD/LDAP)
* API ინტერფეისის საშუალებით.

პრივილეგირებული მომხმარებლის თითოეული სააღრიცხვო ჩანაწერისთვის ერთდროულად უნდა არსებობდეს რამდენიმე მეთოდით ავთენტიფიკაციის შესაძლებლობა, მინიმუმ:* სტატიკური პაროლით, რომელიც ინახება პროდუქტის დაცულ საცავში.
* ერთჯერადი პაროლით, რომელიც გენერირდება გარე მომსახურებით (მაგალითად, RADIUS-სერვერით)
* მომხმარებლის გარე კატალოგის გამოყენებით (AD / LDAP)
* SSH გასაღების გამოყენებით.
 |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლების და პროდუქტის ადმინისტრატორების, AD და LDAP მომხმარებლების კატალოგების სერვერების გარე ავთენტიფიკაციის ერთდროულად მინიმუმ სამი სისტემა.მომხმარებლთა კატალოგის თითოეული სერვერისთვის (AD ან LDAP) პროდუქტს უნდა შეეძლოს გამოყენების პრიორიტეტის (სხვა ასეთ სერვერებთან შედარებით) და შემდეგი პარამეტრების განსაზღვრის შესაძლებლობა:* მომხმარებლის სახელი და პაროლი, რომელსაც აქვს წვდომა მომხმარებელთა ჯგუფების წაკითხვაზე AD და LDAP მომხმარებლების კატალოგების სერვერზე;
* ორგანიზაციული ჯგუფი (OU) მომხმარებელთა კატალოგში, რომელშიც უნდა იძებნებოდეს პრივილეგირებული მომხმარებლები;
* მომხმარებელთა კატალოგის სერვერის მისამართი (FQDN ან IP) და პორტი;
* დაშიფრული (უსაფრთხო) კავშირის გამოყენების შესაძლებლობა სერთიფიკატების გამოყენებით.
 |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლებისთვის სამიზნე სისტემების პულზე ავტომატური წვდომის მინიჭების ფუნქციონალი კონკრეტული ორგანიზაციული ჯგუფის (OU) ბაზაზე (AD ან LDAP) მომხმარებელთა კატალოგის სერვერზე. |
|  | პროდუქტს აუცილებლად უნდა ჰქონდეს უსაფრთხო (დაშიფრული) საკომუნიკაციო არხების შექმნის შესაძლებლობა პრივილეგირებულ მომხმარებლებსა და პროდუქტს შორის და პროდუქტსა და სამიზნე სისტემებს შორის, SSL სერთიფიკატების ბაზაზე.ასეთი უსაფრთხო (დაშიფრული) საკომუნიკაციო არხები უნდა შეიქმნას როგორც თვითხელმოწერადი სერთიფიკატების საფუძველზე (წყვილის "ღია" - "პირადი" გასაღებების გამოყენებით), ასევე სერტიფიცირების ცენტრის სერტიფიკატების (CA) საფუძველზე.პროდუქტმა უნდა უზრუნველყოს სერთიფიკატების შინაარსის ("ღია" ნაწილის) გაცნობის შესაძლებლობა ჰეშ-სიდიდის ნახვის შესაძლებლობით MD5 და SHA1 ალგორითმების გამოყენებით. |
|  | გასაკონტროლებელი სამიზნე სისტემების, პრივილეგირებული მომხმარებლების სესიების დამატება უნდა მოხდეს შესაბამისი მენიუდან ადმინისტრირების ვებ-პორტალზე, ამასთანავე, პროდუქტს უნდა ჰქონდეს შემდეგი ფუნქციონალი:* სამიზნე სერვერების ერთჯერადი დამატება (IP- მისამართით ან FQDN-ით, ქსელის ნიღბით და პორტით)
* სამიზნე სისტემების ჯგუფური დამატება (IP-მისამართების პულთან დაკავშირებული ქსელის ნიღბის გამოყენებით).
 |
|  | პროდუქტს უნდა ჰქონდეს იმ პორტების ნუმერაციის განსაზღვრის ფუნქციონალი, რომლის მიხედვითაც ხდება პრივილეგირებული მომხმარებლების დაკავშირება და იმ პორტებისა, რომლებითაც ხდება სამიზნე სისტემებთან დაკავშირება, ანუ პროდუქტის ადმინისტრატორს უნდა ჰქონდეს შესაძლებლობა იძულებით შეუცვალოს პრივილეგირებულ მომხმარებლებს ცალკეული სამიზნე სისტემასთან ან სამიზნე სისტემების ჯგუფებთან დაკავშირების პორტები. |
|  | პროდუქტმა ხელი უნდა შეუწყოს სამიზნე სისტემებთან მუშაობას, რომლებზეც პრივილეგირებული მომხმარებლების ავთენტიფიკაცია ხორციელდება შემდეგნაირად:* ლოკალური სააღრიცხვო ჩანაწერის შემოღებით;
* დომენური სააღრიცხვო ჩანაწერის შემოღებით;
* SSH გასაღების მეშვეობით.
 |
|  | პროდუქტს უნდა ჰქონდეს წვდომის იმ რეკვიზიტებთან (ლოგინები, პაროლები, დომენის სახელი, SSH გასაღებები და ა.შ.) მუშაობის შესაძლებლობა, რომლებსაც პრივილეგირებული მომხმარებლები იყენებენ სამიზნე სისტემებთან დასაკავშირებლად:* წვდომის რეკვიზიტების ხელით შექმნა და შენახვა პროდუქტის დაცულ საცავში
* ავთენტიფიკაციის გარე სისტემების გამოყენება (მათ შორის - პაროლების სპეციალიზებული გარე საცავები)
* ანონიმური წვდომა (წვდომის რეკვიზიტების შეყვანის საჭიროების გარეშე).

სამიზნე სისტემებთან წვდომის რეკვიზიტების ხელით შექმნისა და შენახვის შემთხვევაში პროდუქტს უნდა ჰქონდეს ამ რეკვიზიტების პრივილეგირებული მომხმარებლებისგან სრული შენიღბვის ფუნქციონალი (გარდა შემთხვევებისა, როდესაც ასეთი რეკვიზიტების ხელმისაწვდომობა ნებადართულია პაროლის პოლიტიკით).პროდუქტმა უნდა უზრუნველყოს სამიზნე სისტემებზე წვდომისთვის დამატებითი (განმეორებითი) იძულებითი ავთენტიფიკაციის ფუნქციონალი მაშინაც კი, თუ პრივილეგირებული მომხმარებლების წვდომის რეკვიზიტები პროდუქტზე და სამიზნე სისტემებზე სრულად ემთხვევა ერთმანეთს. |
|  | პროდუქტს უნდა ჰქონდეს ცალკეულ სამიზნე სისტემებზე პაროლის იძულებითი შეცვლის შესაძლებლობა, აღნიშნული პაროლის პოლიტიკის შესაბამისად, პრივილეგირებული მომხმარებლის ცალკე განსაზღვრული სააღრიცხვო ჩანაწერებისთვის.პაროლის ასეთმა პოლიტიკამ უნდა უზრუნველყოს შემდეგი შესაძლებლობები:* პაროლის სიგრძე;
* პაროლის სირთულე (მათ შორის მოთხოვნები მთავრულ ასოებზე, ციფრულ სიმბოლოებზ,ე, სპეციალურ სიმბოლოებზე)
* პაროლის შეცვლის სიხშირე.

პაროლის იძულებითი ცვლილება პაროლის მითითებული პოლიტიკის შესაბამისად მხარდაჭერილი უნდა იყოს, როგორც მინიმუმ, ასეთ სამიზნე სისტემებზე:* Unix / Linux-based ოპერაციული სისტემები (SSH-ის საშუალებით)
* Windows ოპერაციული სისტემები (WMI-ს საშუალებით)
* Cisco სისტემები (SSH-ის მეშვეობით)

პროგრამულ აპლიკაციებს შორის პაროლის უსაფრთხო გაცვლის ფუნქციონალი იქნება უპირატესობა. |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული ფუნქციონალი როგორც ცალკეული პრივილეგირებული მომხმარებლების, ისე პრივილეგირებული მომხმარებლების ჯგუფების სამიზნე სისტემებთან მუშაობის ეფექტურობის შესაფასებლად. სამიზნე სისტემებთან მუშაობის ეფექტურობის ფუნქციონალმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების აქტიური მოქმედებების შესახებ სტატისტიკა (აქტიური მუშაობის დრო სამიზნე სისტემასთან მუშაობის მთლიან დროსთან მიმართებით), სტატისტიკის დეტალიზაციის და ექსპორტის შესაძლებლობით გარე ანგარიშგებაში.  |
|  | სარეზერვო ასლების შექმნისას გამოყენებული უნდა იქნას მონაცემთა გაცვლის დაშიფრული (უსაფრთხო) პროტოკოლი (მაგალითად, წყვილის - საჯარო და კერძო SSH გასაღების ბაზაზე).შექმნილი სარეზერვო ასლები დაცული უნდა იყოს მათში შენახული მონაცემების არასანქცირებული დათვალიერებისა და აღდგენისგან. |
|  | პროდუქტი უნდა უზრუნველყოფდეს შემდეგი ტიპის ავთენტიფიკაციის ფუნქციონალს:* მრავალფაქტორიანი ავთენტიფიკაცია RADIUS მხარდაჭერით
* Google Autheticator
* Microsoft Authenticator
* Cisco DUO
* OTPH
 |
|  | პროდუქტმა უნდა უზრუნველყოს ერთჯერადი წვდომა OTP პაროლის გამოყენებით. |
|  | პროდუქტს უნდა ჰქონდეს მოვლენების შენახვისა და დამუშავების სისტემა, წარმოდგენილი დაცულ საცავში შენახული ჟურნალების სახით.მოვლენების ყველა ჟურნალი დაცული უნდა იყოს წაშლისგან, მათ შორის პროდუქტის ადმინისტრატორების მიერ, რომლებსაც მინიჭებული აქვთ წვდომის უმაღლესი დონე (უფლებები).მოვლენების ჟურნალები უნდა შეიცავდეს მინიმუმ შემდეგ ინფორმაციას:* პროდუქტის მუშაობისუნარიანობასთან დაკავშირებული მოვლენები (კონფიგურირების ჟურნალების ჩათვლით)
* პრივილეგირებული მომხმარებლების სამიზნე სისტემებთან მუშაობასთან დაკავშირებული მოვლენები;
* პროდუქტის ადმინისტრირებასთან დაკავშირებული მოვლენები.
 |
|  | პროდუქტს უნდა შეეძლოს მოვლენების ჟურნალის სრული ან ნაწილობრივი ექსპორტი ტექსტური ფორმატის გარე ფაილში. ნაწილობრივი ექსპორტი უნდა განხორციელდეს სხვადასხვა კრიტერიუმების მიხედვით, როგორიცაა პრივილეგირებული მომხმარებლის ანგარიშ(ებ)ი, მოვლენების ტიპი, სამიზნე სისტემის სახელი, თარიღი და მისთ. |
|  | პროდუქტს უნდა შეეძლოს მოვლენის დამუშავების გარე სისტემებთან ინტეგრაცია ისეთი სტანდარტული პროტოკოლების გამოყენებით, როგორიცაა SNMP, syslog და ა.შ. |
|  | პროდუქტს უნდა ჰქონდეს ჩაწერილი სესიების ციფრული ხელმოწერის ფუნქციონალი სპეციალური გასაღებებით/სერთიფიკატებით, რომლებიც მოპოვებულია ასეთი გასაღებების/სერთიფიკატების სანდო მომწოდებლებისგან, მონაცემების შეცვლისგან დაცვის უზრუნველსაყოფის მიზნით. |
|  | პროდუქტს უნდა შეეძლოს ინტეგრირება ServiceNow ან ანალოგიური ტიპის მომხმარებლების მუშაობის აღრიცხვის სისტემებთან (ticketing systems). |
|  | პროდუქტს უნდა შეეძლოს პაროლების მართვის შემდეგი ფუნქციონალის უზრუნველყოფა:* პაროლების შეცვლა სესიის დასრულებისას
* პაროლების შეცვლა გრაფიკით
 |
|  | **პრივილეგირებული მომხმარებლების კონტროლის ფუნქციონალის მიმართ მოთხოვნები:** |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც უკავშირდებიან სამიზნე სისტემებს RDP პროტოკოლის საშუალებით.პროდუქტს უნდა შეეძლოს დაკავშირების კონტროლი RDP პროტოკოლის მუშაობის სხვადასხვა რეჟიმში, მათ შორის Enhanced RDP Security (TLS) და NLA რეჟიმებში.პროდუქტს უნდა ჰქონდეს ფუნქციონალი RDP სესიის ფერის გარჩევადობისა და სიღრმის იძულებითი შეზღუდვისთვის, გაცვლის ბუფერის იძულებითი გამორთვისთვის, მოწყობილობის სამიზნე სისტემაზე წვდომის შეზღუდვისთვის, მულტიმედიურ მოწყობილობებთან მუშაობის შეზღუდვისთვის.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს RDP პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს ჩაწერილი გრაფიკული ვიდეომასალა (ვიდეორგოლი).პროდუქტს უნდა ჰქონდეს შენახული გრაფიკული ვიდეომასალის (ვიდეორგოლების) განსაზღვრული გარჩევადობის მქონე გარე AVI, FLV, MPEG ვიდეო ფორმატებში ექსპორტის ფუნქციონალი.პროდუქტმა უნდა უზრუნველყოს RDP სესიასთან დაკავშირების ფუნქციონალი, პრივილეგირებული მომხმარებლების ქმედებების მართვაში ჩარევის შესაძლებლობით. ანუ, პროდუქტმა უნდა უზრუნველყოს მომხმარებლის და იმ ადმინისტრატორის ერთდროულად მუშაობა, რომელიც ერთვება აქტიურ სესიაში და თავის თავზე იღებს საბოლოო სისტემის მართვას ლოგების ფიქსაციით, ვინ და როდის ასრულებს კონკრეტულ ქმედებას. |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს SSH პროტოკოლის საშუალებით უკავშირდებიან.პროდუქტს უნდა შეეძლოს X11 სტანდარტთან მუშაობა SSH პროტოკოლის საშუალებით, მათ შორის გრაფიკის რეპროდუცირების შესაძლებლობა X11-ის საშუალებით.პროდუქტს უნდა ჰქონდეს ფაილებთან დაკავშირებული ოპერაციების იძულებით შეზღუდვის ფუნქციონალი (ფაილების პროტოკოლური SFTP და SCP გაცვლის აკრძალვა).იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს SSH (ან X11) პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს ჩაწერილი გრაფიკული ვიდეომასალა (ვიდეორგოლი).პროდუქტს უნდა ჰქონდეს შენახული გრაფიკული ვიდეომასალის (ვიდეორგოლების) განსაზღვრული გარჩევადობის მქონე გარე AVI, FLV, MPEG ვიდეო ფორმატებში ექსპორტის ფუნქციონალი. |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს Telnet პროტოკოლის საშუალებით უკავშირდებიან.პროდუქტს უნდა შეეძლოს Telnet 3270 და Telnet 5250 სტანდარტებთან მუშაობა.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგად, რომლებიც სამიზნე სისტემებს Telnet პროტოკოლის საშუალებით (მათ შორის Telnet 3270 და Telnet 5250) უკავშირდებიან, ჩაწერილი უნდა იქნას გრაფიკული ვიდეომასალა (ვიდეორგოლი) ან მოქმედებების ტექსტური ჟურნალი (მომხმარებლის ბრძანებები და სამიზნე სისტემის პასუხები ასეთ ბრძანებებზე). |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს VNC პროტოკოლის საშუალებით უკავშირდებიან.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს VNC პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს ჩაწერილი გრაფიკული ვიდეომასალა (ვიდეორგოლი).პროდუქტს უნდა ჰქონდეს შენახული გრაფიკული ვიდეომასალის (ვიდეორგოლების) განსაზღვრული გარჩევადობის მქონე გარე AVI, FLV, MPEG ვიდეო ფორმატებში ექსპორტის ფუნქციონალი.  |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს HTTP და HTTPS-პროტოკოლით (SSLv2 და SSLv3 სტანდარტების მხარდაჭერით) უკავშირდებიან.პრივილეგირებული მომხმარებლების კონტროლის შედეგად, რომლებიც სამიზნე სისტემებს HTTP და HTTPS პროტოკოლებით (რესურსები HTML ბაზაზე) საშუალებით უკავშირდებიან, ჩაწერილი უნდა იქნას გრაფიკული ვიდეომასალა (ვიდეორგოლი).პროდუქტს უნდა ჰქონდეს შენახული გრაფიკული ვიდეომასალის (ვიდეორგოლების) განსაზღვრული გარჩევადობის მქონე გარე AVI, FLV, MPEG ვიდეო ფორმატებში ექსპორტის ფუნქციონალი.  |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს ICA პროტოკოლით (SSLv2 და SSLv3 სტანდარტების მხარდაჭერით) უკავშირდებიან.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს ICA პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს გრაფიკული ვიდეომასალა (ვიდეორგოლი) ან მოქმედებების ტექსტური ჟურნალი (მომხმარებლის ბრძანებები და სამიზნე სისტემის პასუხები ასეთ ბრძანებებზე). |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს Citrix StoreFront პროტოკოლით (SSLv2 და SSLv3 სტანდარტების მხარდაჭერით) უკავშირდებიან.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს Citrix StoreFront პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს გრაფიკული ვიდეომასალა (ვიდეორგოლი) ან მოქმედებების ტექსტური ჟურნალი (მომხმარებლის ბრძანებები და სამიზნე სისტემის პასუხები ასეთ ბრძანებებზე). |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს MS SQL პროტოკოლით (TDS - Tabular Data Stream სტანდარტების მხარდაჭერით) უკავშირდებიან.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს MS SQL პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს მოქმედებების ტექსტური ჟურნალი (მომხმარებლის ბრძანებები და სამიზნე სისტემის პასუხები ასეთ ბრძანებებზე).პროდუქტს უნდა ჰქონდეს შენახული ტექსტური ჟურნალების ექსპორტის ფუნქციონალი ტექსტური სტრუქტურის მქონე გარე ფორმატებში. |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს MySQL პროტოკოლის საშუალებით უკავშირდებიან.იმ პრივილეგირებული მომხმარებლების კონტროლის შედეგს, რომლებიც სამიზნე სისტემებს MS SQL პროტოკოლის საშუალებით უკავშირდებიან, უნდა წარმოადგენდეს მოქმედებების ტექსტური ჟურნალი (მომხმარებლის ბრძანებები და სამიზნე სისტემის პასუხები ასეთ ბრძანებებზე).პროდუქტს უნდა ჰქონდეს შენახული ტექსტური ჟურნალების ექსპორტის ფუნქციონალი ტექსტური სტრუქტურის მქონე გარე ფორმატებში. |
|  | პროდუქტმა უნდა უზრუნველყოს პროტოკოლების ჩაწერა "ნედლ" (RAW) ფორმატში, როგორც არის.  |
|  | პროდუქტს უნდა ჰქონდეს ფუნქციონალი პოლიტიკის შესაქმნელად ბრძანებებისთვის, რომლებსაც იყენებენ პრივილეგირებული მომხმარებლები სამიზნე სისტემებთან მუშაობისას. პროდუქტს უნდა ჰქონდეს რეგულარული გამონათქვამების სინტაქსის მხარდაჭერა POSIX სტანდარტის ბაზაზე.პროდუქტს უნდა შეეძლოს მინიმუმ შემდეგი წესების ამოქმედების შესაძლებლობა, თუ ასეთი პოლიტიკა ამოქმედდება: მომხმარებლის, პასუხისმგებელი პირის შეტყობინების დაბლოკვა, სესიის გათიშვა. |
|  | პროდუქტს უნდა ჰქონდეს იმ დროის ინტერვალთან დაკავშირებული პოლიტიკის შექმნის ფუნქციონალი, რა ინტერვალშიც პრივილეგირებულ მომხმარებლებს ეძლევათ სამიზნე სისტემებზე წვდომის შესაძლებლობა.პროდუქტს უნდა შეეძლოს ასეთი პოლიტიკის მინიმუმ შემდეგი წესების ამოქმედების შესაძლებლობა: კვირის დღეები, როდესაც პრივილეგირებულ მომხმარებლებს შეუძლიათ დაუკავშირდნენ სამიზნე სისტემებს, დროები და წუთები, როდესაც პრივილეგირებულ მომხმარებლებს შეუძლიათ დაუკავშირდნენ სამიზნე სისტემებს, ასეთი პოლიტიკის მოქმედების ინტერვალი (დაწყების და დასრულების თარიღებისა და დროის მითითებით). |
|  | პროდუქტს უნდა შეეძლოს მიმდინარე სესიის ლაივ რეჟიმში მიყოლა საჭიროების შემთხვევაში ჩარევა და ასევე სხვისთვის გაზიარება სესიის |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული მექანიზმები პრივილეგირებული მომხმარებლების ქმედებების შედეგების გადახედვისთვის, კერძოდ, ჩაწერილი სესიების დათვალიერება, გამოყენებული ბრძანებები და სამიზნე სისტემის პასუხები ასეთ ბრძანებებზე. შედეგების გადახედვის შესაძლებლობა უზრუნველყოფილი უნდა იყოს ადმინისტრირების ვებ-პორტალიდან, რაიმე საშუალებების (პროგრამული აპლიკაციები, პლაგინები და ა.შ.) ინსტალაციის გარეშე.პროდუქტს უნდა ჰქონდეს ჩაშენებული ფილტრები პრივილეგირებული მომხმარებლების ქმედებების შედეგების მოსაძებნად სხვადასხვა კრიტერიუმით, მინიმუმ, პრივილეგირებული მომხმარებლის ან მომხმარებლების სახელით, გამოყენებული ბრძანებების, პროტოკოლის ტიპის, სამიზნე სისტემის სახელის მიხედვით, ასევე თარიღის კონკრეტული დიაპაზონით. პროდუქტს უნდა შეეძლოს ანგარიშების შექმნა გამოყენებული ფილტრებით მიღებული შედეგების საფუძველზე. შესაძლებელი უნდა იყოს ასეთი ანგარიშების ექსპორტი CSV, PDF, HTML ფორმატის ფაილების სახით. |
|  | პროდუქტს უნდა ჰქონდეს ფუნქციონალი ცალკეული პრივილეგირებული მომხმარებლების მიერ იმ სამიზნე სისტემებთან წვდომის პაროლის (პაროლების) ნახვის შესაძლებლობასთან დაკავშირებული პოლიტიკის შექმნისთვის, რომლებსაც ისინი უკავშირდებიან, როცა ასეთი პაროლი მათთვის უცნობია.პროდუქტს უნდა ჰქონდეს ჩაშენებული მექანიზმები ასეთი პაროლების ნახვისთვის ნებისმიერ საჭირო დროს (წარსულში) იმ შემთხვევაში, თუ ისინი (პაროლები) შეიცვალა პროდუქტის შესაბამისი ფუნქციონალის გამოყენებით (პაროლის პოლიტიკა). |
|  | პროდუქტს უნდა ჰქონდეს ფუნქციონალი იძულებით მოითხოვოს პრივილეგირებული მომხმარებლის სამიზნე სისტემასთან დაკავშირების მიზეზი, რომელსაც ექნება შესაბამისი ველი მომხმარებლის საპასუხო რეაგირებისთვის. |
|  | პროდუქტს უნდა ჰქონდეს პასუხისმგებელი პირის მიერ პრივილეგირებული მომხმარებლების სამიზნე სისტემასთან კავშირის დამატებითი დადასტურების (დამტკიცების) ფუნქციონალი. |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლების მოქმედებებთან კავშირის ფუნქციონალი პასუხისმგებელი პირის ელექტრონული საკომუნიკაციო არხების (email, sms, push და ა.შ.) გამოყენებით (სამიზნე სისტემასთან დაკავშირება, სამიზნე სისტემიდან გათიშვა, სხვა პირის სესიაში ჩართვა, კონკრეტული პოლიტიკის ამოქმედება). |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლების სესიების დათვალიერების ფუნქციონალი პასუხისმგებელი პირების მიერ რეალურ დროში, ამგვარი დათვალიერების შესახებ პრივილეგირებული მომხმარებლების რაიმე სახით აშკარა ინფორმირების გარეშე.დამატებით, პროდუქტმა პასუხისმგებელ პირს უნდა მიაწოდოს ინფორმაცია სესიის შესახებ: სამიზნე სისტემის სახელი და IP მისამართი, პრივილეგირებული მომხმარებლის სახელი, გამოყენებული პროტოკოლის ტიპი და სესიის დაწყების დრო.სესიები დათვალიერება უნდა შეიძლებოდეს ვებ-ბრაუზერის ფანჯარაში HTML ტექნოლოგიის გამოყენებით, ვიდეოგამშვების ან პლაგინის დამატებითი ინსტალაციის გარეშე. |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლის სესიების დროებითი ან სრული იძულებითი შეწყვეტის ფუნქციონალი პასუხისმგებელი პირების მიერ რეალურ დროში. ასევე, პროდუქტს უნდა შეეძლოს პრივილეგირებული მომხმარებლის სესიის შეწყვეტასთან ერთად დაბლოკოს იმ პრივილეგირებული მომხმარებლის სააღრიცხვო ჩანაწერი, რომლის სესიაც შეწყდა.  |
|  | პროდუქტს უნდა შეეძლოს მესამე მხარის წვდომის უზრუნველყოფა პრივილეგირებული მომხმარებლების სესიებზე რეალურ დროში და შენახულ (ჩაწერილ) სესიებზე. ასეთი წვდომა უზრუნველყოფილი უნდა იყოს უნიკალური URL ბმულის გამოყენებით, მესამე მხარის მოცემულ სესიასთან დაკავშირების შესაძლებლობით დამატებითი ავტორიზაციის გარეშე. URL-ბმულის შექმნისას აუცილებლად შესაძლებელი უნდა იყოს ასეთი ბმულის მოქმედების ვადის და წვდომის რეჟიმის განსაზღვრა (სრული წვდომა სესიაზე ან წვდომა მხოლოდ დათვალიერების რეჟიმში). |
|  | პროდუქტს უნდა ჰქონდეს საკუთარი ნიშნულების (კომენტარების) დამატების ფუნქცია პრივილეგირებული მომხმარებლების სესიებზე რეალური დროის რეჟიმში. პროდუქტს უნდა ჰქონდეს ასეთი ნიშნულების (კომენტარების) დამატების ფუნქციონალი დროის შკალის ნებისმიერ ნაწილში, ასეთი ობიექტების შემდგომი ძიების შესაძლებლობით. |
|  | პროდუქტი უნდა უზრუნველყოფდეს მოქმედებების შესახებ ინფორმაციის დაყოფის შესაძლებლობას, ასევე სესიების ფარგლებში განხორციელებული მოქმედებების გამოყოფის შესაძლებლობას ფერით ან სხვა სახით იმ მომხმარებლისთვის, ვინც წამოიწყო სესია და მომხმარებლისთვის, რომელიც ჩაერთო სესიაში და თავის თავზე აიღო მართვა.  |
|  | პროდუქტს უნდა ჰქონდეს ქცევის ანალიზის ფუნქციონალი, მომხმარებელთა ქცევის ანალიზის საშუალებას უნდა იძლეოდეს შემდეგი კრიტერიუმების მიხედვით: RDP სესიები - კომპიუტერის მაუსის გამოყენებით შესრულებული მოქმედებების ანალიზი; SSH სესიები - ბრძანებების ანალიზი, რომლებიც მომხმარებლებს შეჰყვათ კლავიატურის გამოყენებით. |
|  | **მოთხოვნები მხარდაჭერასა და შეძენის მიმართ:** |
|  | პროდუქტი ხელმისაწვდომი უნდა იყოს ვირტუალური მოწყობილობის (VA - virtual appliance) სახით შესაძენად. |
|  | პროდუქტი უზრუნველყოფილი უნდა იყოს მომსახურების მხარდაჭერით მინიმუმ 5x9 რეჟიმში (სამუშაო საათები სამუშაო დღეებში), მწარმოებლის მიერ ამ პროდუქტისთვის გათვალისწინებული სტანდარტული პირობებით. ასეთი სტანდარტული მხარდაჭერა უნდა იძლეოდეს პროდუქტის ექსპლუატაციასთან დაკავშირებული პრობლემების უსასყიდლოდ გადაწყვეტის და პროდუქტის პროგრამული კოდის უსასყიდლოდ განახლების (ახალი ვერსიების მიწოდება) შესაძლებლობას.მწარმოებელმა, მომხმარებლის მოთხოვნით, უნდა უზრუნველყოს გაფართოებული მომსახურების შეძენის შესაძლებლობა 24x7 (სადღეღამისო) რეჟიმში, რეაგირების და პრობლემის გადაჭრის დროის ინტერვალის გარანტიით. |
|  | მწარმოებელმა პროდუქტის ექსპლუატაციის დროს წარმოქმნილი პრობლემების გადასაჭრელად უნდა უზრუნველყოს ელექტრონული სერვისის მიწოდება (ვებ-პორტალი, სპეციალური ელექტრონული ფოსტის მისამართი, მობილური აპლიკაცია და ა.შ.) დამკვეთის ან მისი წარმომადგენლების მიერ განაცხადების შექმნისა და მათი ავტომატური რეგისტრაციისთვის მწარმოებლის მხარდაჭერის სისტემაში. ასეთ სერვისს უნდა ჰქონდეს ფუნქციონალი განაცხადის შექმნის, განაცხადის სტატუსის ცვლილების და მისთ. დადასტურებისთვის. ასეთ სერვისთან მუშაობა და მწარმოებლის წარმომადგენლებთან კომუნიკაცია ხელმისაწვდომი უნდა იყოს ინგლისურ ან რუსულ ან უკრაინულ ენებზე. |
|  | მწარმოებელმა უნდა უზრუნველყოს ღია წვდომა (ყოველგვარი წინასწარი რეგისტრაციის გარეშე) ტექნიკურ და პროდუქტის ადნინისტრირებასთან დაკავშირებულ დოკუმენტაციაზე ინტერნეტში.ასეთი დოკუმენტაცია ხელმისაწვდომი უნდა იყოს ინგლისურ ან რუსულ ენაზე. |
|  | შემოთავაზებულ პროდუქტს უნდა ჰქონდეს ლიცენზირების ოფციები შემდეგი ვარიანტებისთვის:* ლიცენზირება საბოლოო სამიზნე სისტემების მიხედვით
* ლიცენზირება ერთდროული სესიების რაოდენობის მიხედვით

ლიცენზიებს უნდა ჰქონდეთ მფლობელობაში შეძენის ოფცია და გამოწერის ოფცია, ლიცენზირების მოდელებს შორის გადართვის შესაძლებლობით მომავალში. |