პრივილეგირებული წვდომების მართვის გადაწყვეტილება - 60 პრივილეგირებული მომხმარებელი “HA (High Availability)” - ისთან ერთად.

|  |  |
| --- | --- |
| **რ/ნ №** | **პროდუქტის მიმართ წაყენებული ტექნიკური მოთხოვნების დასახელება და აღწერა, მოთხოვნილი დამკვეთის მიერ** |
|  | |
|  | **ზოგადი (სისტემური) მოთხოვნები** |
|  | პროდუქტის მიწოდება უნდა მოხდეს ვირტუალური მოწყობილობის (VA - virtual appliance) სახით. მიწოდების ტიპი - შესრულებული უნდა იყოს ერთანი პლატფორმის სახით, რომელიც იმპლემენტაციისთვის არ საჭიროებს დამატებით გარე სისტემურ უზრუნველყოფას ან პროგრამული უზრუნველყოფის (ოპერაციული სისტემების, აპლიკაციების, მონაცემთა ბაზების მართვის სისტემების და ა.შ.) გამოყენებას აპლიკაციის სახით. |
|  | პროდუქტს უნდა ქონდეს ოპტიმიზირებული და დაცული (Hardened) ოპერაციული სისტემა, რომელიც დაფუძნებულია Linux-ზე. სისტემა უნდა მუშაობდეს მხოლოდ საჭირო მინიმალურ სერვისებზე. |
|  | პროდუქტს უნდა ქონდეს ჩაშენებული მონაცემთა ბაზა და ვებ სერვერი, რომელიც არ საჭიროებს დამატებით ლიცენზიას (მათ შორის HA კლასტერის მეორე ნოდის არსებობის შემთხვევაში). |
|  | პროდუქტის ინტერფეისს უნდა ქონდეს მინიმუმ შემდეგი ენების მხარდაჭერა:   * ინგლისური * რუსული |
|  | პროდუქტს უნდა ქონდეს შესაძლებლობა, ყველა კომპონენტით განთავსებული განთავსდეს ვირტუალურ გარემოში და უნდა ქონდეს შემდეგი ჰიპერვიზორების მხარდაჭერა - VMWare, Citrix, Linux KVM, Hyper-V, Openstack, AWS, Azure, GCP. |
|  | პროდუქტს უნდა ჰქონდეს დაცვის ჩაშენებული მექანიზმი შენახულ ინფორმაციის დასაცავად არასანქცირებული წვდომისგან. შენახული ინფორმაცია უნდა ინახებოდეს დაშიფრული სახით. |
|  | 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. |
|  | პროდუქტის ადმინისტრირება უნდა მოიცავდეს პროდუქტის მართვის როლური მოდელის და პრივილეგირებულ მომხმარებლების მხარდაჭერის შესაძლებლობას. |
|  | პროდუქტი პრივილეგირებულ მომხმარებლებს საშუალებას უნდა აძლევდეს რომ კონტროლირებად (სამიზნე) სისტემებზე წვდომისათვის გამოიყენონ ვებ ინტერფეისი. ასევე პროდუქტმა უნდა უზრუნველყოს კონტროლირებად (სამიზნე) სისტემებზე წვდომა, ვებ ინტერფეისის გარეშეც, მათ შორის ისეთი სპეციალიზებული აპლიკაციების მეშვეობით როგორებიცაა: 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. |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული HA კლასტერის მხარდაჭერა და ერთი დამატებითი ნოდის განთავსების შესაძლებლობა დამატებითი ლიცენზიის შეძენის გარეშე (საერთო ჯამში HA კლასტერში 2 ნოდი დამატებითი ლიცენზიის გარეშე). |
|  | პროდუქტს უნდა ქონდეს დიაგნოსტირების ჩაშენებული სისტემები, დაკავშირებული კონტროლირებად (სამიზნე) სისტემებზე წვდომის შესამოწმებლად. |
|  | 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. |
|  | პროდუქტმა უნდა უზრუნველყოს დისტანციური სესიების ჩაწერა (RDP, SSH, Telnet, HTTP/S და ა.შ), შუალედური ჰოსტების (jump host) ან აგენტების გამოყენების გარეშე, სერვერებზე, აღჭურვილობასა და სამუშაო სადგურებზე. |
|  | პროდუქტს უნდა ქონდეს შესაძლებლობების და ფუნქციონალის გაფართოების მხარდაჭერა დამატებითი ლიცენზიის ხარჯზე, გარე აპლიკაციების ინსტალაციის გარეშე. |
|  | პროდუქტმა უნდა უზრუნველყოს მუშაობის შემდეგ რეჟიმების მხარდაჭერა დამკვეთის ქსელში:   * Web Proxy * SSH Proxy * RDP Proxy * Database Proxy |
|  | **ფუნქციური (ტექნიკური) მოთხოვნები:** |
|  | პროდუქტს უნდა ჰქონდეს მინიმუმ შემდეგი პროტოკოლების ხმარდაჭერა:   * HTTP * HTTPS * LDAP * LDAPS * MSSQL * RDP * SSH * Telnet * VNC * Windows RM * Windows RPC * X11 |
|  | 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).  პრივილეგირებული სესიის ჩანაწერი უნდა იყოს სრული და აკმაყოფილებდეს ვინ, სად, რა, როდის, როგორ - კითხვებზე პასუხს. |
|  | პროდუქტს უნდა ჰქონდეს ტექსტის ინდექსირების ფუნქციონალის მხარდაჭერა (OCR მექანიზმი ან მისი ანალოგი). |
|  | პროდუქტის ფუნქციონალს უნდა ჰქონდეს სეგმენტირებული ქსელის არქიტექტურაში მუშაობის მხარდაჭერა. |
|  | პროდუქტს უნდა შეეძლოს RDP, SSH გარემოში და ასევე მონაცემთა ბაზებში შეყვანილი ბრძანებების ჩაწერა და კონტროლი; |
|  | 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. |
|  | პროდუქტის ვებ-პორტალმა პრივილეგირებულ მომხმარებლებს უნდა შესთავაზოს შემდეგი შესაძლებლობები (მინიჭებული უფლებების შესაბამისად):   * დასაკავშირებლად ხელმისაწვდომი, მათთვის გამოყოფილი 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. |
|  | პროდუქტს შეეძლოს სხვადასხვა ბრძანებების კონტროლი როგორც RDP და SSH გარემოში, ასევე მონაცემთა ბაზებში (MS SQL Server, PostgreSQL და Oracle) |
|  | პროდუქტის გამოყენების როლურმა მოდელმა უნდა უზრუნველყოს მინიმუმ 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. |
|  | პროდუქტს უნდა შეეძლოს როგორც ლოკალური, ასევე შემდეგი გარე ავთენტიფიკაციის პროვაიდერების გამოყენება: Active Directory (LDAP), TACACS, OPENID, SAML და RADIUS.  ასევე შესაძლებელი უნდა იყოს ავთენტიფიკაციის თანმიმდევრობის დადგენა. |
|  | 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 მომხმარებლებისთვის სამიზნე სისტემებზე წვდომის მინიჭების ფუნქციონალი სხვადასხვა კრიტერიუმის მიხედვით:   * მოწყობილობა და მოწყობილობის ტიპი * პროდუქტი * მომხმარებელი (Username) * მოწყობილობების ტეგები (Device Tags) * ქრედენშალების ტეგები (Credential Tags) * ქრედენშალის ტიპი |
|  | 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. |
|  | 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 და პორტით) * სამიზნე სისტემების ჯგუფური დამატება * სამიზნე სერვერების/სისტემების წაშლა |
|  | პროდუქტს უნდა ჰქონდეს იმ პორტების ნუმერაციის განსაზღვრის ფუნქციონალი, რომლის მიხედვითაც ხდება სამიზნე სისტემებთან დაკავშირება. ასევე პროდუქტს უნდა შეეძლოს ერთი და იგივე მოწყობილობისთვის ერთი და იგივე პროტოკოლისთვის რამდენიმე პორტის განსაზღვრა. |
|  | პროდუქტს უნდა შეეძლოს სამიზნე სისტემებთან მუშაობა, რომლებზეც პრივილეგირებული მომხმარებლების ავთენტიფიკაცია ხორციელდება შემდეგნაირად:   * ლოკალური სააღრიცხვო ჩანაწერის შემოღებით; * დომენური სააღრიცხვო ჩანაწერის შემოღებით; * SSH გასაღების მეშვეობით. |
|  | პროდუქტს უნდა ქონდეს წვდომა იმ რეკვიზიტებთან (ლოგინები, პაროლები, დომენის სახელი, SSH გასაღებები და ა.შ.), რომლებსაც პრივილეგირებული მომხმარებლები იყენებენ სამიზნე სისტემებთან დასაკავშირებლად. |
|  | 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 სიმბოლოებზე, 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 ქონდეს პაროლის შეცვლისთვის საჭირო მზა შაბლონები (Templates). |
|  | პროდუქტს უნდა ქონდეს შესაძლებლობა რომ პერიოდულად განახორციელოს წვდომა მოწყობილობებსა და ანგარიშებზე, ავთენტიკაციის მცდელობით, ბოლო შენახული პაროლის გამოყენებით, რათა დადასტურდეს, კვლავ იმყოფება თუ არა პაროლი პაროლების საცავის კონტროლის ქვეშ და შესაბამისი კონფიგურაციის არსებობის შემთხვევაში შეცვალოს პაროლი. |
|  | პროდუქტმა ადმინისტრატორს უნდა მისცეს შესაძლებლობა რომ მესამე მხარის აპლიკაციებთან ინტერაქციის კონფიგურირებისთვის გამოიყენოს სკრიპტები, მაკროსები, სხვადასხვა პროგრამირების ენები და უზრუნველყოს მინიმუმ შემდეგი პროტოკოლების მხარდაჭერა: RPC, WinRM, SSH, HTTP/HTTPS REST API. |
|  | პროდუქტს უნდა ჰქონდეს ჩაშენებული ფუნქციონალი ცალკეული პრივილეგირებული მომხმარებლების, 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. შექმნილი სარეზერვო ასლები დაცული უნდა იყოს მათში შენახული მონაცემების არასანქცირებული დათვალიერებისა და აღდგენისგან.  პროდუქტს უნდა ქონდეს სარეზერვო ასლების ფიზიკურად განცალკევებულ ადგილზე შენახვის მხარდაჭერა. |
|  | პროდუქტს უნდა ქონდეს შესაძლებლობა რომ სისტემასთან წვდომა შეზღუდოს IP მისამართებზე დაყრდნობით ან პირიქით სისტემასთან წვდომა დაუშვას მხოლოდ გარკვეული IP მისამართებიდან. |
|  | პროდუქტს უნდა ქონდეს დაცული რესურსების გაშიფვრის შესაძლებლობა ე.წ MasterKey-ის გამოყენებით, რომელიც შედგება სხვადასხვა მომხმარებლის მფლობელობაში არსებული ფრაგმენტებისგან. მომხმარებელთა რაოდენობა, რომლებიც ფლობენ საერთო გასაღების ფრაგმენტებს, უნდა იყოს გაზრდადი, მინიმუმ ორ მომხმარებელზე გათვლით. |
|  | პროდუქტი უნდა ქონდეს შემდეგი ტიპის MFA ავთენტიფიკაციის მხარდაჭერა:   * RADIUS * RSA Authenticator * Duo Security * AuthID |
|  | 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 წვდომასთან დაკავშირებული მოვლენები * 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 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 შეეძლოს ინტეგრირება ServiceNow ან ანალოგიური ტიპის მომხმარებლების მუშაობის აღრიცხვის სისტემებთან (ITSM systems). |
|  | პროდუქტს უნდა შეეძლოს პაროლების მართვის შემდეგი ფუნქციონალის უზრუნველყოფა:   * პაროლების შეცვლა სესიის დასრულებისას * პაროლების შეცვლა პაროლის ნახვის შემდეგ * 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 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). |
|  | 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 ჰქონდეს ფაილებთან დაკავშირებული ოპერაციების იძულებით შეზღუდვის ფუნქციონალი ( მაგ. 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). |
|  | 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). |
|  | პროდუქტმა უნდა უზრუნველყოს პრივილეგირებული მომხმარებლების კონტროლი, რომლებიც სამიზნე სისტემებს HTTP და HTTPS-პროტოკოლით 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 ვიდეო ჩანაწერის სხვადასხვა ვიდეო ფორმატებში (მაგ. AVI, FLV, MP4, MPEG) 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 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 MySQL 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. |
|  | პროდუქტს უნდა ჰქონდეს ფუნქციონალი პოლიტიკის შესაქმნელად ბრძანებებისთვის, რომლებსაც იყენებენ პრივილეგირებული მომხმარებლები სამიზნე სისტემებთან მუშაობისას და უნდა შეეძლოს მინიმუმ შემდეგი წესის ამოქმედების შესაძლებლობა (თუ ასეთი პოლიტიკა ამოქმედდება) - მომხმარებლის 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. |
|  | 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 შეეძლოს მინიმუმ შემდეგი ტიპის ანგარიშების შექმნა და დაგეგმარება (თითოეული ანგარიშის ტიპში სხვადასხვა კრიტერიუმის/ფილტრის მითითების შესაძლებლობით):   * წვდომა სისტემაზე (Access to the system) * ქრედენშალები (Credentials) * იდენტობები (Machine identities) * მოვლენები (Events) * აუდიტი (Audit) * PCI * საგანგებო პანელი (Emergency panel) * მიკვლევადობა (Traceability) * წვდომის უფლებები (Access control) |
|  | პროდუქტს უნდა შეეძლოს ანგარიშების შექმნა გამოყენებული კრიტერიუმებიით/ფილტრებით მიღებული შედეგების საფუძველზე. შესაძლებელი უნდა იყოს ასეთი ანგარიშების ექსპორტი სხვადასხვა ფორმატის ფაილების სახით (მაგ.CSV, PDF, HTML). |
|  | 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 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 ქონდეს საგანგებო სიტუაციებში სამიზნე სისტემასთან დაკავშირების შესაძლებლობა დამატებითი დადასტურების გარეშე, კავშირის დამატებითი დადასტურების (დამტკიცების) ფუნქციონალის არსებობის შემთხვევაშიც. |
|  | პროდუქტს უნდა ჰქონდეს პრივილეგირებული მომხმარებლების მოქმედებებთან კავშირის ფუნქციონალი პასუხისმგებელი პირის ელექტრონული საკომუნიკაციო არხების (Email, SMS 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 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 ენაზე. |
|  | მწარმოებელმა უნდა უზრუნველყოს ღია წვდომა (ყოველგვარი წინასწარი რეგისტრაციის გარეშე) ტექნიკურ და პროდუქტის ადმინისტრირებასთან დაკავშირებულ დოკუმენტაციაზე ინტერნეტში.  ასეთი დოკუმენტაცია ხელმისაწვდომი უნდა იყოს ინგლისურ ენაზე. |
|  | შემოთავაზებულ პროდუქტს უნდა ჰქონდეს ლიცენზირების ოფციები შემდეგი ვარიანტებისთვის:   * ლიცენზირება მომხმარებელთა რაოდენობის მიხედვით   ლიცენზიებს უნდა ჰქონდეთ მფლობელობაში შეძენის ოფცია და გამოწერის ოფცია, ლიცენზირების მოდელებს შორის გადართვის შესაძლებლობით მომავალში. |
|  | მომწოდებელმა უნდა უზრუნველყოს პრივილეგირებული წვდომების მართვის გადაწყვეტილების დანერგვა და ბანკში არსებულ სისტემებთან ინტეგრაცია |