|  |  |
| --- | --- |
| მოთხოვნები მოწყვლადობების მართვის სისტემის მიმართ | |
|  | |
| არქიტექტურა | 1. სისტემა უნდა უზრუნველყოფდეს არა ნაკლებ **505** ჰოსტის ერთდროულ მოწყვლადობების მართვას. |
| 1. სისტემას უნდა ჰქონდეს ცენტრალური კონსოლი ყველა სისტემის კომპონენტის სამართავად, რომელიც დაინსტალირებული იქნება ღრუბელში. |
| 1. სისტემას უნდა შეეძლოს ქსელში აქტიური სკანერების ლოკალურად დაყენება და ცენტრალურ კონსოლთან მათი დაკავშირება. |
| 1. სისტემას უნდა შეეძლოს ადგილობრივად დააინსტალიროს აგენტები საბოლოო წერტილებზე და დააკავშიროს ისინი ცენტრალურ კონსოლთან. |
| 1. სისტემამ უნდა მოახდინოს მიმწოდებლისგან მოწყვლადობის მონაცემთა ბაზის ყოველდღიური განახლების ცენტრალიზება და სრულად ავტომატიზირება. |
| 1. სისტემამ უნდა უზრუნველყოს მონაცემთა შენახვის ინტეგრირებული მოდელი, რომელიც დამოუკიდებელია მესამე მხარის მონაცემთა ბაზის პროდუქტისგან. |
| 1. სისტემას უნდა ჰქონდეს კომპლექსური, ღია API REST, რათა ავტომატურად შექმნას სკანირების სცენარები და მოახდინოს უსაფრთხოების მონაცემთა ექსპორტი, დამატებითი ხარჯების გარეშე. |
|  |
| წვდომის კონტროლი | 1. სისტემამ უნდა უზრუნველყოს როლებზე დაფუძნებული წვდომის მართვა, რათა გააკონტროლოს მომხმარებელთა წვდომა კონკრეტულ მონაცემთა ნაკრებებზე და ფუნქციებზე, რომლებიც ხელმისაწვდომია ამ მომხმარებლებისთვის. |
| 1. სისტემამ უნდა მისცეს ადმინისტრატორებს შესაძლებლობა, განსაზღვროს როლები თანამდებობრივი მოვალეობებისა და ფუნქციებზე წვდომის შესაბამისი დონეების მიხედვით. |
| 1. სისტემას უნდა შეეძლოს LDAP-თან ინტეგრირება მომხმარებლის იდენტურობის შემოწმებისთვის (აუთენტიფიკაციისთვის). |
| 1. სისტემამ უნდა უზრუნველყოს რამდენიმე LDAP სერვერის მხარდაჭერა აუთენტიფიკაციისთვის. |
| 1. სისტემას უნდა შეეძლოს მომხმარებლის აქტივობის შესახებ დეტალური ანგარიშის გენერირება. |
| 1. სისტემამ უნდა მისცეს ადმინისტრატორებს საშუალება შეზღუდონ წვდომა ცალკეული მომხმარებლებისთვის ან ჯგუფებისთვის გარკვეული აქტივების სიებზე, სკანირების პოლიტიკასა და მოწყვლადობის რეპოზიტორიუმებზე. |
| 1. სისტემამ უნდა მისცეს ადმინისტრატორებს საშუალება დანიშნონ რესურსები თითოეული მომხმარებლისთვის ან ჯგუფისთვის, მაგალითად, სკანირების პოლიტიკა, აქტივების სიები, მოთხოვნები და სააღრიცხვო მონაცემები. |
| 1. სისტემამ უნდა მისცეს ადმინისტრატორებს უფლება შეზღუდონ ნებართვა: სრული სკანირების შესრულებაზე, გარკვეული პოლიტიკების გამოყენებით სკანირების ჩატარებაზე. |
| 1. სისტემაში გათვალისწინებული უნდა იყოს დროის დაგეგმვის შესაძლებლობა, აკრძალულ საათებში სკანირების პრევენციის მიზნით. |
| 1. სისტემამ უნდა უზრუნველყოს მოწყვლადობის რისკის მიღებისა და შეცვლის შესაძლებლობა. |
| სკანირება | 1. სისტემა უნდა შეიცავდეს აქტიური სკანირების ჩაშენებულ შესაძლებლობას მოწყვლადობის აღმოსაჩენად და სტანდარტებთან შესაბამისობის შემოწმების საშუალებას, ასევე პასიური სკანირებისთვის უკვე არსებული და ახალი აქტივების აღმოსაჩენად. |
| 1. სისტემამ უნდა უზრუნველყოს სკანირება აგენტებით და აგენტების გარეშე. |
| 1. სისტემამ უნდა უზრუნველყოს სხვადასხვა პლატფორმის მხარდაჭერა სკანერის განსათავსებლად, Windows, Linux და ასევე ვირტუალური და აპარატული მოწყობილობების ჩათვლით. |
| 1. სისტემამ უნდა უზრუნველყოს სხვადასხვა პლატფორმის მხარდაჭერა აგენტის განსათავსებლად, Windows, Linux, macOS-ის ჩათვლით. |
| 1. სკანირების მოდულებისა და კონსოლის დამატებითი ვირტუალური image ხელმისაწვდომი უნდა იყოს დამატებითი დანახარჯების გარეშე. |
| 1. სისტემამ უნდა უზრუნველყოს რამდენიმე გეოგრაფიულად ან ლოგიკურად განაწილებული სკანირების მექანიზმის მხარდაჭერა, რომელსაც მართავს ცენტრალური კონსოლი. |
| 1. სისტემას უნდა ჰქონდეს დატვირთვის ბალანსირების და რამდენიმე სკანერს შორის გადართვის მხარდაჭერა, სკანერებს შორის სკანირების დატვირთვის დინამიური განაწილების გზით, რაც დამოკიდებულია სკანერის ხელმისაწვომობაზე მთელი სკანირების განმავლობაში. |
| 1. სისტემამ უნდა მისცეს შესაძლებლობა, განათავსონ დამატებითი სკანერები თავიანთ გარემოში დამატებითი ხარჯების გარეშე. |
| 1. სკანერების და აგენტების საერთო რაოდენობა უნდა იყოს შეუზღუდავი. |
| 1. სისტემამ უნდა უზრუნველყოს შესაძლებლობა პორტების, პროტოკოლების და სერვისების დაყენება მთელ ქსელში განთავსებულ სკანერებთან დაკავშირებისთვის. |
| 1. სისტემას უნდა შეეძლოს სკანირების კონფიგურირება, რათა თავიდან აიცილოს ისეთი ტრაფიკის წარმოქმნა, რომელიც საკმარისია ქსელის ინფრასტრუქტურის გამართული მუშაობისთვის. |
| 1. სისტემამ უნდა უზრუნველყოს ავტონომიური სკანირებისა და სერვერზე სკანირების შედეგების იმპორტის მხარდაჭერის შესაძლებლობა. |
| 1. სისტემამ უნდა დაუშვას მომხმარებლების სააღრიცხვო მონაცემების შეყვანა და უსაფრთხო შენახვა, მათ შორის Windows ლოკალური და დომენური სააღრიცხვო ჩანაწერები, ასევე su და sudo Unix სისტემებისთვის ssh წვდომით. |
| 1. სისტემამ უნდა უზრუნველყოს "ssh" სააღრიცხვო მონაცემების შეუზღუდავი რაოდენობის მხარდაჭერა. |
| აქტივები | 1. სისტემამ უნდა უზრუნველყოს აქტივების აღმოჩენის შესაძლებლობა, რომლებზეც არაა შეძენილი ლიცენზიების ოდენობა. |
| 1. სისტემამ უნდა უზრუნველყოს ქსელის აქტიური სკანირებისა და პასიური მონიტორინგის შესაძლებლობა აქტივების აღმოჩენის მიზნით. |
| 1. სისტემას უნდა შეეძლოს მობილური მოწყობილობების აღმოჩენა. |
| 1. სისტემამ უნდა უზრუნველყოს ვებ სერვისებისა და მონაცემთა ბაზის სერვისების აღმოჩენა. |
| 1. სისტემას უნდა შეეძლოს აღმოაჩინოს სერვისები, რომლებიც არასტანდარტულ პორტებზე მუშაობს. |
| 1. სისტემას უნდა შეეძლოს სხვადასხვა პორტებზე მომუშავე ერთი და იმავე სერვისის რამდენიმე ეგზემპლარის ტესტირება. |
| 1. სისტემას უნდა შეეძლოს "მკვდარი" საბოლოო წერტილების სკანირება (მოწყობილობები, რომლებიც არ პასუხობენ ICMP მოთხოვნებს). |
| 1. სისტემამ მხარი უნდა დაუჭიროს netstat-ის არასავალდებულო გამოყენებას, სისტემაში ღია პორტების სწრაფი და ზუსტი ჩამოთვლისათვის სააღრიცხვო მონაცემების მიწოდებისას. |
| 1. სისტემამ უნდა უზრუნველყოს SMB და WMI გამოყენება Windows სისტემების სკანირებისთვის. |
| 1. სკანერმა უნდა უზრუნველყოს უსაფრთხო კავშირის (ssh) მხარდაჭერა პრივილეგიების გაზრდის შესაძლებლობით მოწყვლადობების სკანირებისთვის და კონფიგურაციის აუდიტისთვის Unix სისტემებზე. |
| 1. სისტემას უნდა ჰქონდეს შესაძლებლობა შეაგროვოს/განახორციელოს იმპორტი და ასახოს მონაცემები IT და OT ქსელების აქტივების შესახებ ერთიან კონსოლში. |
| 1. სისტემამ უნდა უზრუნველყოს სკანირების პოლიტიკების კონფიგურირების შესაძლებლობა, ქსელებზე და სკანირების მიზნებზე მინიმალური ზემოქმედებისათვის. |
| 1. სისტემამ უნდა უზრუნველყოს ახალი მოწყობილობების აღმოჩენისა და სკანირების ავტომატური გაშვების შესაძლებლობა. |
| 1. სისტემას უნდა ჰქონდეს აგენტის გამოყენების მხარდაჭერა SCAP აუდიტისთვის. |
| 1. სისტემას უნდა შეეძლოს გამოავლინოს ყველა აქტივი, ლიცენზიების გამოყენების გარეშე და შემდეგ ჰქონდეს შესაძლებლობა აირჩიოს, რომელი აქტივები დაასკანეროს მოწყვლადობის არსებობაზე. |
| სკანირება მოწყვლადობების არსებობაზე | 1. სისტემას უნდა ჰქონდეს აუთენტიფიკაციით და აუთენტიფიკაციის გარეშე სკანირების მხარდაჭერა მოწყვლადობების ლოკალური და დისტანციური აღმოჩენისთვის, სამიზნე მოწყობილობაზე აგენტის დაყენების საჭიროების გარეშე. |
| 1. სისტემამ უნდა უზრუნველყოს სამიზნე სისტემების სკანირება როგორც აუთენტიფიკაციით, ასევე აუთენტიფიკაციის გარეშე. |
| 1. სისტემა არ უნდა დაეყრდნოს გარე სკანერებს მოწყვლადობების სკანირებისთვის. |
| 1. სისტემას უნდა შეეძლოს DHCP ცვლილებების თვალის დევნება, სკანირების შედეგების სისტემის მოწყობილობების სახელებთან ასოცირებით. |
| 1. სისტემამ მხარი უნდა დაუჭიროს არააქტიური საბოლოო წერტილების სკანირების შედეგების შენახვის შესაძლებლობას, კონფიგურირებული დროის პერიოდის განმავლობაში. |
| 1. სისტემა უნდა შეიცავდეს დეტალურ მონაცემებს სკანირების შედეგების შესახებ, მათ შორის ისეთ ინფორმაციას, როგორიცაა ნაპოვნი DLL ვერსიები. |
| 1. სისტემამ უნდა შეატყობინოს სამიზნე სისტემის ცნობილი მოწყვლადობების შესახებ, როგორც იდენტიფიცირებულია უსაფრთხოების მრჩეველთა ორგანიზაციების მიერ (მაგ. Common Vulnerabilities and Exposures მონაცემთა ბაზა(CVE)), Open Source Vulnerabilities მონაცემთა ბაზა (OSVDB), SecurityFocus Bugtraq (BID) ან მათი ნებისმიერი კომბინაცია). |
| 1. სისტემას უნდა ჰქონდეს მოწყვლადობების სკანირების მხარდაჭერა PCI DSS-სთან შესაბამისობაზე. სისტემა უნდა შეიცავდეს PCI DSS სკანირების წინასწარ განსაზღვრულ პროფილებს, რომლებიც აკმაყოფილებენ PCI DSS მიმდინარე კრიტერიუმებს ქსელის სკანირებისთვის. უნდა არსებობდეს ფუნქცია ყველა სხვა მოწყვლადობების გასაფილტრად, რომლებიც არ არის დაკავშირებული PCI DSS-სთან. |
| 1. სისტემამ უნდა უზრუნველყოს შესწორებების აუდიტი Microsoft-ის ოპერაციული სისტემებისა და აპლიკაციებისთვის, როგორიცაა Windows XP, Windows 7, Windows 8/8.1, Windows 10, Windows 11, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange და სხვა. |
| 1. სისტემამ უნდა უზრუნველყოს შესწორებების აუდიტი ყველა ძირითადი Unix ოპერაციული სისტემისთვის, მათ შორის macOS, Linux, Solaris, IBM AIX, HP-UX-სთვის და სხვა. |
| 1. სისტემამ უნდა უზრუნველყოს შესწორებების აუდიტი ქსელური ინფრასტრუქტურისთვის, მათ შორის Cisco, Juniper-სთვის და სხვა. |
| 1. სისტემამ უნდა უზრუნველყოს გარე აპლიკაციების სკანირება, როგორიცაა Java და Adobe. |
| 1. სისტემამ უნდა უზრუნველყოს ანგარიშები საფრთხეების, აღმოჩენილი მავნე პროგრამებისა და ბოტნეტების რეპუტაციის შესახებ. |
| 1. სისტემამ უნდა უზრუნველყოს მოწყვლადობების პრიორიტიზაცია რეალურ დროში საფრთხეების ანალიტიკისა და მანქანური სწავლების ალგორითმების გამოყენებით, მოწყვლადობების შეფასებისა და იმის პროგნოზირების მიზნით, თუ რომელი მათგანი იქნება ყველაზე სავარაუდოდ გამოყენებული უახლოეს მომავალში. |
| 1. სისტემამ უნდა უზრუნველყოს მოწყვლადობების პრიორიტიზაცია, რომელიც ეხმარება მომხმარებლებს გააცნობიერონ ძირითადი ფაქტორები, რომლებიც გავლენას ახდენენ მოწყვლადობის თითოეულ შეფასებაზე (მაგალითად, საფრთხის სიახლეზე, გამოყენების კოდის სიმწიფეზე, Threat Intelligence წყაროების კატეგორიებზე). |
| 1. სისტემა უნდა მოიცავდეს მოწყვლადობის შეფასებას მოწყვლადობების შეფასების საერთო სისტემის (CVSS) შესაბამისად. |
| 1. სისტემამ უნდა დაუშვას ტესტების არჩევა პირველადი სკანირების შედეგად მიღებული ინფორმაციის საფუძველზე, რათა ჩატარდეს შემდგომი ტესტირება მოცემული მოწყობილობის ან საბოლოო წერტილის შესახებ მიღებული ინფორმაციის საფუძველზე. |
| 1. სისტემამ უნდა განახორციელოს მოწყვლადობების სასიცოცხლო ციკლის თვალმიდევნება ცალკეულ საბოლოო მოწყობილობებთან და ასევე გარემოსთან მიმართებაში, პირველი აღმოჩენის თარიღის, ბოლო დაკვირვებისა და მოწყვლადობის აღმოფხვრის ჩათვლით. |
| 1. სისტემამ მხარი უნდა დაუჭიროს VMware სერვერების სკანირებას საკუთარი API VMware-ის დახმარებით. |
| 1. სისტემა უნდა იძლეოდეს მოწყობილობების სკანირების საშუალებას განრიგის მიხედვით. |
| 1. სისტემა უნდა იძლეოდეს შემოწმების ჩართვის ან გამორთვის საშუალებას გარკვეული მოწყვლადობების არსებობაზე სკანირების დროს. |
| 1. სისტემამ ავტომატურად უნდა გაუშვას და გააჩეროს განრიგით დაგეგმილი სკანირება მომხმარებლის ჩარევის გარეშე. |
| 1. სისტემამ უნდა დაუშვას სკანირების შეწყვეტა და განახლება ხელით. |
| 1. სისტემას უნდა ჰქონდეს შესაძლებლობა გაუშვას სკანირება, რომელიც არ სრულდება დადგენილ ვადაში, ან გადაიტანოს მომდევნო დაგეგმილი პერიოდისთვის. |
| 1. სისტემას უნდა შეეძლოს მიიღოს სკანირების სამიზნეები სხვადასხვა ფორმატში, მათ შორის DNS სახელები, IP მისამართების დიაპაზონები და IP კლასები, აგრეთვე აქტივების წინასწარ განსაზღვრული სიები. მაგალითად, 10.0.1.1 - 10.0.1.100. ასევე უნდა იყოს მხარდაჭერილი ფაილში შემავალი IP მისამართების სიის იმპორტი. |
| 1. სისტემას უნდა ჰქონდეს IPv6 სკანირების მხარდაჭერა IPv6 აქტივების პასიური აღმოჩენით. |
| 1. სისტემამ უნდა უზრუნველყოს პერიფერიული მოწყობილობების სკანირების გამორთვის შესაძლებლობა, მაგალითად, პრინტერების. |
| აგენტები | 1. სისტემამ უნდა უზრუნველყოს სრულფასოვანი აგენტების დაყენების შესაძლებლობა მოწყვლადობების სკანირებისთვის, კონფიგურაციების აუდიტის შესამოწმებლად მარეგულირებელ მოთხოვნებთან და ინდუსტრიის სტანდარტებთან შესაბამისობაში. |
| 1. აგენტმა უნდა შეაგროვოს და გაგზავნოს მონაცემები ცენტრალურ კონსოლზე, რათა შეამციროს დატვირთვა ქსელზე და საბოლოო მოწყობილობაზე. |
| 1. აგენტმა უნდა უზრუნველყოს საბოლოო წერტილზე მისი დატვირთვის რეგულირების შესაძლებლობა, სამუშაო პროცესების დარღვევის თავიდან აცილების მიზნით. |
| 1. აგენტს უნდა შეეძლოს კონსოლთან დაკავშირება პროქსი-სერვერის მეშვეობით. |
| 1. აგენტი შეიძლება დაინსტალირდეს გარე გადაწყვეტილებების გამოყენებით, როგორიცაა Active Directory ან SCCM. |
| 1. სისტემას უნდა ჰქონდეს აგენტთა ჯგუფების შექმნის შესაძლებლობა მოწყვლადობების აღმოჩენის პროცესის ავტომატიზაციისთვის. |
| 1. სისტემამ უნდა უზრუნველყოს ინფორმაცია აგენტების სტატუსის შესახებ. |
| 1. აგენტს უნდა ჰქონდეს უნიკალური იდენტიფიკატორი სხვადასხვა ქვექსელებში ერთი და იმავე მოწყობილობის აღმოსაჩენად. |
| პასიური სკანირება | 1. პასიური სკანერი უნდა შეიცავდეს აქტივების აღმოჩენის შესაძლებლობას ქსელური ტრაფიკის მონიტორინგის გზით, აქტიური სკანირების გარეშე. |
| 1. პასიურმა სკანერმა უნდა უზრუნველყოს ინფორმაცია ცალკეული ქსელის, ზოგადად ქსელების ან ჰოსტების ნებისმიერი კონკრეტული ჯგუფის შესახებ. |
| 1. პასიური სკანერი უნდა იყოს მიწოდებული იმავე მწარმოებლის მიერ, როგორც ძირითადი სისტემა. |
| 1. პასიურ სკანერს უნდა შეეძლოს SIEM სისტემების ჟურნალის მოხმარება, რათა სისტემაში შექმნას შეტყობინებები აქტივების აღმოჩენის, პროგრამული უზრუნველყოფის აღმოჩენის, მომხმარებლის ანგარიშის აქტივობისა და სერვისის ცვლილებების შესახებ. |
| შესაბამისობის აუდიტი | 1. სისტემამ უნდა შეუწყოს შესაბამისობის აუდიტს ავთენტიფიკაციასთან ან მის გარეშე, ბოლო წერტილში აგენტის დაყენების აუცილებლობით ან მის გარეშე. |
| 1. სისტემა არ უნდა დაეყრდნოს გარე სკანერებს უსაფრთხოების კონფიგურაციის აუდიტის/შეფასების მიზნით. |
| 1. სისტემამ უნდა უზრუნველყოს ერთიანი ხედვა მოწყვლადობების აუდიტის ყველა შედეგისა და მოთხოვნებთან შესაბამისობის შესახებ. |
| 1. სისტემამ უნდა უზრუნველყოს კონფიგურაციების აუდიტი ნორმატიულ მოთხოვნებთან და სხვა სადარგო სტანდარტებთან შესაბამისობა, ასევე მიმწოდებლების საუკეთესო პრაქტიკის სტანდარტებთან შესაბამისობა.. |
| 1. სისტემამ უნდა უზრუნველყოს კონფიგურაციების აუდიტი, რომელიც დაფუძნებულია საუკეთესო პრაქტიკაზე ისეთი მიმწოდებლებისთვის, როგორიცაა Microsoft, Cisco და VMware, f5, Fortinet და სხვა. |
| 1. სისტემამ უნდა უზრუნველყოს VMWare ESXi და vCenter-ის აუდიტი VMWare SOAP API-ის მეშვეობით. |
| 1. სისტემამ უნდა უზრუნველყოს Microsoft ოპერაციული სისტემების აუდიტი უსაფრთხოების პარამეტრებისა და კონფიგურაციების შემოწმების მიზნით. |
| 1. სისტემამ უნდა უზრუნველყოს Unix-ის ყველა ძირითადი ოპერაციული სისტემის აუდიტი უსაფრთხოების პარამეტრებისა და კონფიგურაციების შემოწმების მიზნით. |
| 1. სისტემამ უნდა უზრუნველყოს აპლიკაციების აუდიტი უსაფრთხოების პარამეტრებისა და კონფიგურაციების შემოწმების მიზნით, როგორიცაა: Internet Explorer, Microsoft Edge, Google Chrome, Microsoft Office და ა.შ. |
| 1. სისტემამ უნდა უზრუნველყოს ქსელური ინფრასტრუქტურის აუდიტი უსაფრთხოების პარამეტრებისა და კონფიგურაციების შემოწმების მიზნით, როგორიცაა: Cisco, Kubernetis, HP, F5 და ა.შ. |
| 1. სისტემამ უნდა უზრუნველყოს საბოლოო წერტილების უსაფრთხოების გარკვეული პროდუქტების აუდიტი ინსტალაციისა და განახლების სტატუსის დადგენის მიზნით. |
| 1. სისტემამ უნდა უზრუნველყოს პერსონალური ინფორმაციისა (PII) და სხვა კონფიდენციალური კონტენტის აუდიტი. |
| 1. სისტემამ უნდა დაუშვას აუდიტის პოლიტიკების კონფიგურირება ორგანიზაციის საჭიროებების შესაბამისად. |
| 1. სისტემა უნდა იძლეოდეს აუდიტების ჩატარების შესაძლებლობას CIS სტანდარტებთან შესაბამისობაზე. |
| ავტომატიზაცია | 1. სისტემამ უნდა უზრუნველყოს სკანირების, ანგარიშების და შეტყობინებების შექმნის სრული ავტომატიზაცია. |
| 1. სისტემამ უნდა გააერთიანოს მოწყვლადობების ცალკეული სკანირებების შედეგები, გაფილტვრის შესაძლებლობით, რათა უზრუნველყოს დეტალიზაციის და ანალიზის შესაძლებლობა. |
| 1. სისტემას უნდა ჰქონდეს აქტიური და აღმოფხვრილი მოწყვლადობების ცალკეული ხედვები, მოწყვლადობების ავტომატური გადატანით აქტიურიდან აღმოფხვრილებზე მას შემდეგ, რაც სკანირება დაადგენს, რომ მოწყვლადობა აღარ არის. |
| 1. სისტემას უნდა ჰქონდეს შესაძლებლობა მონიშნოს მოწყვლადობა, როგორც ადრე აღმოფხვრილი, მაგრამ ხელახლა გაჩენილი, ეს შეიძლება მოხდეს, როდესაც ხდება სისტემის აღდგენა სარეზერვო ასლიდან ან ვირტუალური მანქანის ძველი ასლი ბრუნდება ოპერატიულ რეჟიმში. |
| 1. სისტემამ უნდა უზრუნველყოს აღმოჩენილი მოწყვლადობების კომპლექსური გაფილტვრა, შემდეგი პარამეტრების მიხედვით დეტალიზაციის შესაძლებლობით, მაგრამ არ შემოიფარგლოს ამით: IP მისამართი, აგენტის იდენტიფიკატორი, აქტივი, აუდიტის ფაილი, CCE იდენტიფიკატორი, CVE იდენტიფიკატორი, CVSS v2 შეფასება, CVSS v3 შეფასება, DNS სახელი, ექსპლოიტის ხელმისაწვდომობა, პორტი, პროტოკოლი, კრიტიკულობის დონე, პირველი აღმოჩენის თარიღი, ბოლო აღმოჩენის თარიღი, მოწყვლადობის ტექსტი. |
| 1. სისტემაში უნდა იყოს აქტივებზე, პოლიტიკებზე, სააღრიცხვო მონაცემებზე ან მოთხოვნებზე თეგების დამატების შესაძლებლობა კონფიგურირებული აღწერით, გაფილტვრისა და ობიექტების მართვის გასაუმჯობესებლად. |
| 1. სისტემას უნდა ჰქონდეს პანელი უსაფრთხოების ანალიტიკოსისთვის, რომელიც ავტომატურად ადგენს პრიორიტეტებს და ახორციელებს გადაწყვეტილებების ოპტიმიზაციას მოწყვლადობების შესასწორებლად, კერძოდ კი, ანიჭებს პროცენტულ მნიშვნელობას რისკების შემცირებას მოწყობილობების ჯგუფზე მოწყვლადობების დახურვისას. |
|
| 1. სისტემამ მომხმარებლებს უნდა შესთავაზოს მოწყვლადობის სკანირების შესაძლებლობა, რათა დაადასტურონ, რომ ის გამოსწორებულია სკანირების პარამეტრების კონფიგურაციის გარეშე. 2. სისტემამ უნდა უზრუნველყოს საბოლოო წერტილების ავტომატური დაჯგუფების შესაძლებლობა, ანუ აქტივების დინამიური სიების შექმნა სკანირების შედეგებზე დაყრდნობით, შემდეგი კრიტერიუმების მიხედვით, მაგრამ არ შემოიფარგლოს ამით: IP მისამართი, DNS სახელი, ოპერაციული სისტემის ტიპი, მოწყვლადობის კრიტიკულობის დონე, პორტი, ექსპლოიტის ხელმისაწვდომობა, პირველი აღმოჩენის თარიღი, ბოლო აღმოჩენის თარიღი, მოწყვლადობის ტექსტი. |
| 1. სისტემამ უნდა მისცეს მომხმარებელს შესაძლებლობა მიიღოს რისკი (დაუშვას გამონაკლისი) აღმოჩენილი მოწყვლადობისთვის კონფიგურირებული ვადის გასვლის თარიღებით, ან შეცვალოს რისკის (სიმძიმის) დონე განსხვავებულ დონეზე, ვიდრე განსაზღვრულია ამ მოწყვლადობისთვის. 2. სისტემამ უნდა უზრუნველყოს ამოცანების შექმნის ფუნქცია და გარეშე სისტემებთან ინტეგრაციის შესაძლებლობა ამოცანების თვალმიდევნების მიზნით. |
| 1. სისტემას უნდა ჰქონდეს ცალკეული მომხმარებლებისთვის ამოცანების დანიშვნის მხარდაჭერა. |
| 1. სისტემამ ხელი უნდა შეუწყოს შეტყობინებების შექმნას მოწყვლადობების სკანირების ან კონფიგურაციის აუდიტის შედეგებზე დაყრდნობით. |
| ანგარიშების შედგენა | 1. სისტემამ ხელი უნდა შეუწყოს ანგარიშების(Report) შექმნას, რომლებიც კონფიგურირებადია მიმწოდებლის მიერ მიწოდებული შაბლონების გამოყენებით ან შაბლონების გარეშე. |
| 1. სისტემამ უნდა უზრუნველყოს ანგარიშებში შედეგების გაფილტვრის შესაძლებლობა სხვადასხვა კრიტერიუმების მიხედვით. |
| 1. სისტემას უნდა გაზჩნდეს სკანირების ჩაშენებული ანგარიშები. |
| 1. სისტემამ უნდა უზრუნველყოს ანგარიშების სრული ავტომატიზაციის შესაძლებლობა, მათ შორის შესრულება და გაგზავნა განრიგის მიხედვით, ასევე ანგარიშების გაგზავნა სკანირების შემდეგ. |
| 1. სისტემამ უნდა უზრუნველყოს შედეგების კონსოლში ნახვის შესაძლებლობა, ანგარიშგების შექმნის პროცესისგან დამოუკიდებლად. |
| 1. სისტემამ ხელი უნდა შეუწყოს ანგარიშების შექმნის შესაძლებლობას შემდეგ ფორმატებში: PDF, HTML, CSV. |
| 1. სისტემამ უნდა უზრუნველყოს უსაფრთხოების ანალიტიკოსისთვის ანგარიშების ავტომატური გაგზავნა სტანდარტებთან შესაბამისობაზე. |
| 1. სისტემამ უნდა წარმოადგინოს ნორმატიულ მოთხოვნებთან შესაბამისობის ანგარიშები დამატებითი ხარჯების გარეშე. |
| 1. ანგარიშებს უნდა შეეძლოს ჩართოს მოწყობილობების სახელები (NetBIOS, DNS) IP მისამართებთან ერთად. |
| 1. სისტემამ უნდა უზრუნველყოს ანგარიშების დაშიფვრისა და პაროლით დაცვის შესაძლებლობა. |
| 1. სისტემამ უნდა უზრუნველყოს ანგარიშების ავტომატური გაგზავნის შესაძლებლობა ელექტრონული ფოსტით. |
| 1. სისტემამ უნდა უზრუნველყოს ანგარიშების გაგზავნის შესაძლებლობა ვებ გამოქვეყნების სერვისების გამოყენებით. |
| 1. სისტემამ უნდა უზრუნველყოს მაღალი დონის ანგარიშები უსაფრთხოების მაჩვენებლებისა და სტანდარტებთან შესაბამისობის თაობაზე. |
| ინფორმაციული პანელები | 1. სისტემას უნდა ჰქონდეს ინფორმაციული პანელები და პანელების შაბლონები მოწყვლადობისა და უსაფრთხოების სტატუსის საჩვენებლად. |
| 1. სისტემამ თითოეულ მომხმარებელს უნდა მისცეს საშუალება შექმნას რამდენიმე სამომხმარებლო საინფორმაციო პანელი. |
| 1. საინფორმაციო პანელის ელემენტები ადვილად უნდა შეიცალოს გაფილტვრის გზით, რათა განხორციელდეს მონაცემების ასახვა აქტივების სიის, მოწყვლადობების ან შესაბამისობების შემოწმების, დროის, საკვანძო სიტყვების მიხედვით ძიების, IP მისამართების საფუძელზე და ა.შ. |
| 1. საინფორმაციო პანელების განახლების სიხშირე უნდა იყოს კონფიგურირებადი, რათა განახლდეს განრიგის მიხედვით. |
| 1. სისტემამ უნდა უზრუნველყოს საინფორმაციო პანელების შაბლონების იმპორტის/ექსპორტის შესაძლებლობა. |
| 1. სისტემამ უნდა უზრუნველყოს სხვადასხვა პერსონალური ვიზუალური ელემენტების დამატების შესაძლებლობა საინფორმაციო პანელების კონფიგურირების მიზნით, მათ შორის წრიული დიაგრამების, ჰისტოგრამების, მატრიცების და ტენდენციების ჩათვლით. |
| 1. სისტემამ მომხმარებლებს უნდა მისცეს საშუალება ერთობლივად გამოიყენონ საინფორმაციო პანელები. |
| 1. სისტემამ უნდა უზრუნველყოს ინტერნეტ რესურსი საინფორმაციო პანელების ჩასატვირთად, რომელიც მოიცავს შაბლონებს: რომლებიც ეძღვნება სხვადასხვა დონის მომხმარებლებს, შესაბამისობის სტანდარტებს და უსაფრთხოების მართვის საშუალებებს. |
| 1. სისტემას უნდა ჰქონდეს შაბლონის პარამეტრების დაყენების და საინფორმაციო პანელების ფორმატირების მხარდაჭერა. |

## დამატებითი მოთხოვნები

* „სისტემის“ მიმწოდებელს უნდა ჰქონდეს ქვეყანაში მინიმუმ 3 განხორციელებული პროექტის გამოცდილება.
* შემოთავაზებული „სისტემა“ მიწოდებული უნდა იყოს „გამოწერის“ (Subscription) ლიცენზიების სახით, ყველა აუცილებელ ფუნქციონალურ მოდულზე 1 წლის ვადით.
* მომწოდებელმა უნდა წარმოადგინოს შემოთავაზებული სისტემის მწარმოებლის მიერ გაცემული Manufacturer's Authorization Form (MAF).