ხელშეკრულება № 36

სახელმწიფო შესყიდვის შესახებ
(ელექტრონული ტენდერი) - NAT220014925

ქ. თბილისი

სსიპ საფინანსო-ანალიტიკური სამსახური (შემდგომში - **„შემსყიდველი“**), წარმოდგენილი ადმინისტრაციული დეპარტამენტის უფროსის ლევან ბაიდოშვილის სახით და **შპს „გრინ სისტემს“** (შემდგომში - **„მიმწოდებელი“**) წარმოდგენილი მისი დირექტორის ლევან ჩაჩუას სახით, ორივე ერთად წოდებული როგორც **„მხარეები“**, ვმოქმედებთ რა საქართველოს კანონმდებლობის, „სახელმწიფო შესყიდვების შესახებ“ საქართველოს კანონის შესაბამისად, ამავე კანონის მე-3 მუხლის პირველი პუნქტის „ჟ“ ქვეპუნქტის საფუძველზე, ვთანხმდებით შემდეგზე:

1. გამოყენებული ტერმინების განმარტებები

ხელშეკრულებაში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

1. „ხელშეკრულება სახელმწიფო შესყიდვის შესახებ“ (შემდგომში - „ხელშეკრულება“) - შემსყიდველსა და მიმწოდებელს შორის დადებულ ხელშეკრულება, რომელიც ხელმოწერილია მხარეთა მიერ, მასზე თანდართული ყველა დოკუმენტით და ასევე მთელი დოკუმენტაციით, რომლებზეც ხელშეკრულებაში არის მინიშნებები.
2. „ხელშეკრულების ღირებულება“ - საერთო თანხა, რომელიც უნდა გადაიხადოს შემსყიდველმა მიმწოდებლის მიერ ხელშეკრულებით ნაკისრი ვალდებულებების სრული და ზედმიწევნით შესრულებისათვის.
3. „დღე“, „კვირა“, „თვე“ - კალენდარული დღე, კვირა, თვე.
4. „შემსყიდველი“ - ორგანიზაცია, რომელიც ახორციელებს შესყიდვას.
5. „მიმწოდებელი“ - პირი, რომელიც ახორციელებს საქონლის მიწოდებას ამ ხელშეკრულების ფარგლებში.
6. „საქონელი“ - წინამდებარე ხელშეკრულების მე-2 მუხლით გათვალისწინებული ხელშეკრულების საგანი.

2. ხელშეკრულების საგანი

წინამდებარე ხელშეკრულების საგანია დანართი N1-ით განსაზღვრული ქსელური მოწყობილობების და ვებ სერვერების მოწყვლადობის მართვის პროგრამული გადაწყვეტილების მიწოდება - CPV48210000.

3. ხელშეკრულების ღირებულება

1. ხელშეკრულების ღირებულება შეადგენს **38,207.00** (ოცდათვრამეტი ათას ორას შვიდი) ლარს.
2. ხელშეკრულების ღირებულება მოიცავს როგორც გასაწევი საქონლის ღირებულებას, ასევე წინამდებარე ხელშეკრულების შესრულებასთან დაკავშირებით მიმწოდებლის მიერ გაწეულ ყველა ხარჯს და საქართველოს კანონმდებლობით გათვალისწინებულ გადასახადებს.
3. წინამდებარე ხელშეკრულების პირობების, მათ შორის ფასის შეცვლა დაუშვებელია, თუ ამ ცვლილებების შედეგად იზრდება ხელშეკრულების ღირებულება ან უარესდება ხელშეკრულების პირობები შემსყიდველისათვის, გარდა საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული შემთხვევებისა.
4. საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული პირობების დადგენის შემთხვევაში დაუშვებელია ხელშეკრულების ჯამური ღირებულების 10%-ზე მეტი ოდენობით გაზრდა.

4. მხარეთა ვალდებულებები

1. მიმწოდებელი ვალდებულია:

ა) უზრუნველყოს ხელშეკრულების მე-2 მუხლით გათვალისწინებული საქონლის მიწოდება ხელშეკრულების ძალაში შესვლიდან 10 (ათი) დღის განმავლობაში, რომელის მხარდაჭერა აქტიური უნდა იყოს საქონლის მიწოდების მიღება-ჩაბარების აქტის გაფორმებიდან 1 (ერთი) წლის განმავლობაში. საქონლის მიწოდება უნდა განხორციელდეს სსიპ საფინანსო-ანალიტიკურ სამსახურში, ქ. თბილისი, გორგასლის ქ N16;

ბ) განიხილოს შემსყიდველის პრეტენზიები და მიაწოდოს მოტივირებული პასუხი ყველა საკითხზე;

გ) ხელი შეუწყოს შემსყიდველს ინსპექტირების განხორციელებაში.

დ) განახორციელოს ამ ხელშეკრულებითა და მოქმედი კანონმდებლობით მასზე დაკისრებული სხვა ვალდებულებები.

2. შემსყიდველი ვალდებულია:

ა) განახორციელოს ამ ხელშეკრულებით მასზე დაკისრებული სხვა ვალდებულებები.

5. ხარისხი

მოწოდებული საქონლის ხარისხი უნდა შეესაბამებოდეს ამ სფეროში დადგენილ სტანდარტებს (ასეთის არსებობის შემთხვევაში) და წინამდებარე ხელშეკრულებაში გათვალისწინებულ მაჩვენებლებს.

6. ხელშეკრულების შესრულების კონტროლი

1. შემსყიდველის მიერ ხელშეკრულების შესრულების კონტროლი განხორციელდება პერიოდულად, როგორც საქონლის მიწოდების დროს, ისე ხელშეკრულების მოქმედების მთელ პერიოდზე.

2. ხელშეკრულების პირობების შესრულების კონტროლს განახორციელებენ შემსყიდველის მიერ განსაზღვრული პირი ან/და პირთა ჯგუფი ან/და კონკრეტულ შემთხვევებში მხარეთა შეთანხმებით შესაძლებელია მოწვეულ იქნეს სპეციალური ცოდნის მქონე სპეციალისტი (ექსპერტი).

3. შემსყიდველის შესაბამისი წარმომადგენელი (წარმომადგენლები, მოწვეული ექსპერტი) უფლებამოსილია ჩაატაროს ხარისხის კონტროლი და თუ აღმოჩნდება წუნდებული საქონელი, მიმწოდებელი ვალდებულია წერილობითი შეტყობინებიდან 3 (სამი) სამუშაო დღეში გამოასწოროს წუნი, იმ შემთხვევაში თუ წუნის გამოსწორება შეუძლებელია და შემსყიდველს უკვე გადახდილი აქვს საქონლის ღირებულება დაუბრუნოს შემსყიდველს აღნიშნული წუნდებული საქონლის ღირებულება

7. მიღება-ჩაბარების წესი

1. საქონლის მიღება წარმოებს მიღება-ჩაბარების აქტის სახით. მიღება-ჩაბარების აქტი ფორმდება წერილობითი ფორმით, მხარეთა უფლებამოსილი წარმომადგენლების ხელისმოწერით, ინსპექტირების განმახორციელებელი პირის/პირების დადებითი დასკვნის საფუძველზე.

2. საქონლის მიღებას აწარმოებს შემსყიდველის შესაბამისი უფლებამოსილი პირი..

8. ანგარიშსწორება

1. ანგარიშსწორება განხორციელდება შემდეგი პირობებით:

ა) ანგარიშსწორების ვალუტა - ლარი;

ბ) ანგარიშსწორების ფორმა - უნაღდო, წინამდებარე ხელშეკრულებაში მითითებული მიმწოდებლის საბანკო რეკვიზიტების შესაბამისად.

2. შემსყიდველი იღებს ვალდებულებას გადაუხადოს მიმწოდებელს მიწოდებული საქონლის ღირებულება მიღება-ჩაბარების აქტის გაფორმებიდან 10 (ათი) სამუშაო დღის განმავლობაში.

9. ხელშეკრულების შესრულების შეფერხება

1. თუ ხელშეკრულების შესრულების პროცესში მხარეები წააწყდებიან რაიმე ხელშემშლელ გარემოებებს, რომელთა გამო ფერხდება ხელშეკრულების პირობების შესრულება, ამ მხარემ დაუყოვნებლივ უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება შეფერხების ფაქტის, მისი შესაძლო ხანგრძლივობის და გამომწვევი მიზეზების შესახებ. შეტყობინების მიმღებმა მხარემ შესაძლო უმოკლეს ვადაში უნდა აცნობოს მეორე მხარეს თავისი გადაწყვეტილება, მიღებული აღნიშნულ გარემოებებთან დაკავშირებით.

2. იმ შემთხვევაში, თუ ხელშეკრულების პირობების შესრულების შეფერხების გამო მხარეები შეთანხმდებიან ხელშეკრულების პირობების შესრულების ვადის გაგრძელების თაობაზე, ეს გადაწყვეტილება უნდა გაფორმდეს ხელშეკრულებაში ცვლილების შეტანის გზით, ხელშეკრულების მე-11 მუხლის შესაბამისად.

10. ხელშეკრულების პირობების შეუსრულებლობა

1. წინამდებარე ხელშეკრულების პირობების შეუსრულებლობის შემთხვევაში შემსყიდველი უფლებამოსილია შეწყვიტოს ხელშეკრულება და მიმწოდებელს დააკისროს პირგასამტეხლო ხელშეკრულების ღირებულების 20%-ის ოდენობით.

2. წინამდებარე ხელშეკრულების პირობების ნაწილობრივ შეუსრულებლობის შემთხვევაში შემსყიდველი უფლებამოსილია შეწყვიტოს ხელშეკრულება და მიმწოდებელს დააკისროს პირგასამტეხლო ხელშეკრულების ღირებულების არაუმეტეს 10%-ის ოდენობით.

3. წინამდებარე ხელშეკრულების პირობების არაჯეროვნად შესრულების შემთხვევაში (მათ შორის, ხელშეკრულების მე-4 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული საქონლის მიწოდების ან/და ხელშეკრულების მე-6 მუხლის მე-3 პუნქტით განსაზღვრული ვადების გადაცილების შემთხვევაში) მიმწოდებელს ეკისრება პირგასამტეხლო შესაბამისად ყოველ ვადაგადაცილებულ დღეზე ხელშეკრულების ღირებულების 0.02%-ის ოდენობით.

4. წინამდებარე ხელშეკრულებით განსაზღვრულ შემთხვევაში შემსყიდველი უფლებამოსილია შეწყვიტოს ხელშეკრულება მიმწოდებელთან და მოსთხოვოს ხელშეკრულების შეწყვეტის მომენტისათვის გადასახდელი პირგასამტეხლოს ანაზღაურება.

5. პირგასამტეხლოს გადახდა არ ათავისუფლებს მიმწოდებელს ხელშეკრულებით ნაკისრი ვალდებულებების შესრულებისაგან.

11. ხელშეკრულებაში ცვლილებების შეტანა

ნებისმიერი ცვლილება წინამდებარე ხელშეკრულებაში განხორციელდება წერილობით ორივე მხარის უფლებამოსილი წარმომადგენლების ხელმოწერით.

12. დავების გადაწყვეტა

1. ხელშეკრულების შესრულების პროცესში მხარეთა შორის წარმოქმნილი უთანხმოება წყდება მოლაპარაკებების გზით.

2. თუ ასეთი მოლაპარაკების დაწყებიდან 5 (ხუთი) დღის განმავლობაში მხარეები ვერ შეძლებენ სადაო საკითხის შეთანხმებით მოგვარებას, ნებისმიერ მხარეს დავის გადაწყვეტის მიზნით შეუძლია, მიმართოს საქართველოს სასამართლოს კანონმდებლობით დადგენილი წესით.

13. ხელშეკრულების შეწყვეტა

1. შემსყიდველი უფლებამოსილია შეწყვიტოს წინამდებარე ხელშეკრულების მოქმედება, თუ მეორე მხარე ვერ უზრუნველყოფს თავისი ვალდებულებების ჯეროვან შესრულებას, ან მოქმედი კანონმდებლობით დადგენილ სხვა შემთხვევებში.

2. ხელშეკრულების ცალკეული პირობების მოქმედების შეწყვეტა არ ათავისუფლებს მიმწოდებელს ხელშეკრულებით გათვალისწინებული ვალდებულებების შესრულებისაგან.

3. ხელშეკრულება აგრეთვე შეიძლება შეწყდეს მხარეთა წერილობითი შეთანხმების საფუძველზე.

14 ხელშეკრულების მოქმედების ვადა

1. წინამდებარე ხელშეკრულება ძალაში შედის მხარეთა მიერ მისი ხელმოწერის დღიდან და მოქმედებს 2022 წლის 31 დეკემბრის ჩათვლით.

2. წინამდებარე ხელშეკრულების შესაბამისი მუხლები რომელთა მოქმედების ვადებიც აღემატება მე-14 მუხლის პირველი პუნქტის მოქმედების ვადას ძალაშია მათ სრულ შესრულებამდე.

15. სხვა პირობები

1. წინამდებარე ხელშეკრულება შედგენილი და ხელმოწერილია „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის შესაბამისად. ხელშეკრულებასთან დაკავშირებული ნებისმიერი მიმოწერა შესრულებული უნდა იყოს ქართულ ენაზე.

2. ხელშეკრულებაზე თანდართული დანართი N1, წარმოადგენს წინამდებარე ხელშეკრულების განუყოფელ ნაწილს და განიხილება მასთან მთლიანობაში.

16. მხარეთა რეკვიზიტები:

შემსყიდველი:
სსიპ საფინანსო-ანალიტიკური სამსახური
მისამართი: ქ. თბილისი, გორგასლის ქ. N16,
ტელეფონი: 032 226-10-72, 032 226-16-56.
საბანკო რეკვიზიტები: ანგ. N200122900, სახელმწიფო ხაზინა, კოდი 220101222,
სკ-204577813

მიმწოდებელი:
შპს „გრინ სისტემს“
მისამართი: ქ. თბილისი, ილია ჭავჭავაძის გამზირი N75/10 (ფაქტიური: ქ. თბილისი, ოთარ ჩხეიძის ქ. N10)
საბანკო რეკვიზიტები: სს „ბაზისბანკი“ ა.ნ GE07BS0000000080136781, ბანკის კოდი: CBASGE22,
სკ-404862190

Green Systems LLC

Digitally signed by Green Systems LLC
Date: 2022.08.17 15:02:43 +04'00'

შესყიდვის ობიექტის დასახელება	მწარმოებელი ქვეყანა/კომპანია და მოდელი	შესყიდვის ობიექტის აღწერილობა	რაო-ბა (ცალი)	ერთეულის ფასი (ლარი)	მთლიანი ღირებულება (ლარი)
ქსელური მოწყობილობების უსაფრთხოების და ვებ სერვერების მოწყვლადობის მართვის პროგრამული გადაწყვეტილება. CPV 48210000	ირლანდია; Tenable Network Security Ireland Limited; TIOVM (Tenable.io Vulnerability Management) – 200 assets. TIO-WAS (Tenable.io Web Application Scanning) – 5 WEB Apps	**ზოგადი ინფორმაცია** • გადაწყვეტა სრულად აერთიანებს მოწყვლადობის შეფასებას (სკანირებას) და უსაფრთხოების კონფიგურაციის შეფასებას, რათა უზრუნველყოს მონაცემთა კომბინირებული ლიცენზირება და კონსოლიდაცია, ანალიზი და გამოკითხვა. • გადაწყვეტა შეიცავს აქტიური / პასიური სკანირების ინტეგრირებულ შესაძლებლობას, აქტივების, დაუცველობის და კონფიგურაციების 200 აქტივისათვის. სრული სურათის დემონსტრირებისთვის. • გადაწყვეტა გვთავაზობს აღდგენის პროგნოზირებად პრიორიტეტიზაციას ბიზნესრისკზე დაყრდნობით. • გადაწყვეტა ორგანიზაციებს აძლევს საშუალებას ეფექტურად შეაფასოს კიბერ საფრთხეების მიმართ საკუთარი დაუცველობა და განახორციელოს თავიანთი საქმიანობის შიდა შეფასება სხვადასხვა ჯგუფებთან შედარებით, ასევე გარე შეფასება ინდუსტრიულ კონკურენტებთან შედარებით. • გადაწყვეტა შეიცავს უფასო ტრენინგს. • გადაწყვეტა შეიცავს 24/7/365 გლობალურ ტექნიკურ მხარდაჭერას. • გადაწყვეტა შეიცავს ახალი მოწყვლადობის გამოვლენის / შემოწმების ავტომატურ განახლებას. • გადაწყვეტა არ ეყრდნობა IP მისამართებს, როგორც აქტივის მიკვლევის ერთადერთ საშუალებას. • გადაწყვეტა ლიცენზირებულია აქტივების საფუძველზე, IP– ს გარდა, ქსელის სხვა პარამეტრების გათვალისწინებით, იმ შემთხვევაში, თუ მოწყობილობას აქვს 2 IP. • გადაწყვეტის დასადგენად მიდგომამ ითვალისწინებს IP მისამართს, აპარატურის ტიპს, ოპერაციული სისტემებს, BIOS UUID, MAC მისამართს, NetBIOS სახელს, FQDN. • გადაწყვეტის გამოყენებით შესაძლებელია მრავალი IP-ის გადაჭრა ერთ აქტივზე, იმ აქტივებისთვის, რომლებსაც ერთდროულად ან დროთა განმავლობაში აქვთ მრავალი IP. • გადაწყვეტა წარმოადგენს ლიცენზირების მოქნილ მოდელს, რათა უზრუნველყოს პროდუქტის ფუნქციონირება შეფერხების გარეშე, მაშინაც კი, თუ ადგილი აქვს ლიცენზიის ლიმიტის დროებით გადაჭარბებას. • გადაწყვეტა უშვებს ლიცენზიის დროებით გადაჭარბებას დამატებითი რესურსების სკანირების საჭიროების შემთხვევაში.	1	38,207.00	38,207.00

		არქიტექტურა • გადაწყვეტა შეიცავს შენახვის ინტეგრირებულ მოდელს, რომელიც არ ეყრდნობა მესამე მხარის მონაცემთა ბაზის პროდუქტს. • გადაწყვეტა უზრუნველყოფს ღრუბლოვან ყოვლისმომცველ უსაფრთხოებას, რომელიც ითვალისწინებს უწყვეტ ხილვადობას, შეფასებას და შემოწმებას Amazon Web Services, Microsoft Azure და Google Cloud Platform- ში. • გადაწყვეტა უზრუნველყოფს ქსელის ტრაფიკის მუდმივ მონიტორინგს ხანმოკლე სისტემების და რთულად სკანირებადი მოწყობილობების დასადგენად და შესაფასებლად, როგორიცაა მგრძნობიარე OT და IoT სისტემები. • API მოწოდებულია დამატებითი ღირებულების გარეშე და უზრუნველყოფილია ერთი გამოწერის ფარგლებში. • გადაწყვეტის მასშტაბი ითვალისწინებს მილიონობით აქტივს. • გადაწყვეტა შეიცავს იმ აგენტების ვარიანტს, რომლებიც უზრუნველყოფენ მოწყვლადობის შეფასებას და უსაფრთხოების კონფიგურაციის შეფასებას. • გადაწყვეტას შეუძლია სკანერების ჯგუფების გამოყენება ერთი სამუშაოს პროცესში. • გადაწყვეტას შეუძლია, გააკონტროლოს როგორც შიდა ქსელებში არსებული აქტივები, ასევე იმ აქტივების სკანირება, რომლებიც ხელმისაწვდომია გარედან ან საჯაროდ. • სკანერები იმართება პლატფორმის მიერ, მაგ. ინფორმაცია დაუცველობის, კოდის და სხვა განახლებების შესახებ. • გადაწყვეტა უზრუნველყოფს შეუზღუდავი სრულფასოვანი პასიური სკანერების განლაგების შესაძლებლობას დამატებითი ღირებულების გარეშე. • გადაწყვეტამ უზრუნველყოფს შეუზღუდავი სრულფასოვანი აქტიური სკანერების განლაგების შესაძლებლობას დამატებითი ღირებულების გარეშე. • გადაწყვეტა უზრუნველყოფს შეუზღუდავი სრულფასოვანი აგენტების განლაგების შესაძლებლობას დამატებითი ღირებულების გარეშე. • აგენტს შეუძლია კონსოლთან დაკავშირება შესაბამისი სერვერის საშუალებით. • სკანერებს შეუძლია კონსოლთან დაკავშირება შესაბამისი სერვერის საშუალებით. • აგენტს შეუძლია დაინსტალირება მესამე მხარის გადაწყვეტილებების საშუალებით, როგორიცაა აქტიური დირექტორია ან SCCM. **წვდომის კონტროლი** • გადაწყვეტა ითვალისწინებს როლზე წვდომის კონტროლს (RBAC), რათა გააკონტროლოს მომხმარებლის წვდომა მონაცემთა კონკრეტულ ნაკრებებზე და ფუნქციონირება. • გადაწყვეტა შეიცავს მოწყვლადობის რისკის მიღების ან შეცვლის შესაძლებლობას, ამგვარი ფუნქციონირება შეიზღუდება მომხმარებლის როლით და დოკუმენტურად შეფასდება მოწყვლადობის რისკის მიღება.			

		• გადაწყვეტას შეუძლია მომხმარებლის ჯგუფების განსაზღვრა და მართვა, მათ შორის, სკანირების ფუნქციების შეზღუდვა და მოხსენებაზე წვდომა. • გადაწყვეტას შეუძლია, უზრუნველყოს გარკვეული IP ან პორტების სკანირების დაბლოკვა. • გადაწყვეტა აღჭურვილია ორი ფაქტორის ავთენტიფიკაციით. **სკანირება** • გადაწყვეტას აქვს სკანირების ძრავის სხვადასხვა პლატფორმა, რომელიც მოიცავს Windows, Linux, macOS და ვირტუალურ მოწყობილობებს. • გადაწყვეტა უზრუნველყოფს გეოგრაფიულად განაწილებული სკანირების მრავალი ძრავის მხარდაჭერას, რომელსაც მართავს ცენტრალური კონსოლი. • გადაწყვეტა შეიცავს სკანირების გამორთვის ფანჯრების დაგეგმვის შესაძლებლობას, აკრძალულ საათებში სკანირების თავიდან ასაცილებლად. • გადაწყვეტა შეიცავს პორტების, პროტოკოლებისა და სერვისების კონფიგურაციის შესაძლებლობას მთელ ქსელში განლაგებულ სკანერებთან. • გადაწყვეტა კონფიგურირებადია, რათა შესაძლებელი იყოს სკანირების ჩახშობა, ისეთი ტრაფიკის თავიდან ასაცილებლად, რომელმაც შეიძლება ხელი შეუშალოს ნორმალური ქსელის ინფრასტრუქტურას. • გადაწყვეტა უზრუნველყოფს მომხმარებლის საიდენტიფიკაციო მონაცემების შეყვანას და უსაფრთხო შენახვას, მათ შორის Windows– ის ლოკალურ და დომენურ ანგარიშებზე, და Unix su და sudo SSH– ზე • გადაწყვეტა უზრუნველყოფს სამიზნე სისტემებზე პრივილეგიების ესკალაციის შესაძლებლობას მომხმარებლის ნორმალური წვდომიდან ძირეულ / ადმინისტრაციულ წვდომამდე. • გადაწყვეტას შეუძლია სკანირების პერსონალურად დაგეგმვა, მათ შორის დაზუსტებული დროით, წინასწარ განსაზღვრული სიხშირით ჩატარებული შესაძლებლობის ჩათვლით. • გადაწყვეტას შეუძლია სენსიტიურ მონაცემთა ძიების განხორციელება, Windows– ის, Unix– ის და Linux– ის სისტემებზე მგრძნობიარე მონაცემების აღმოსაჩენად. • გადაწყვეტას შეუძლია ცენტრალიზებული სკანირება და სკანირების პოლიტიკის მართვა. • გადაწყვეტა შეიცავს ლიცენზიის "ავტომატური მოძველების"მოდელს ისე, რომ მოძველებული ან ჩამოწერილი აქტივები, რომლებიც 90 დღის განმავლობაში არ არის სკანირებული, აღარ ჩაითვალება ლიცენზიაში. • სისტემა მომხმარებლებს საშუალებას აძლევს, აწარმოონ დაუცველობის სკანირება, რათა დარწმუნდნენ, რომ იგი დაფიქსირებულია, სკანირების პარამეტრების კონფიგურაციის გარეშე.			

		აქტივის აღმოჩენა • პროდუქტი ხელს უწყობს აქტივის აღმოჩენის შესაძლებლობას, რომელიც არ ეწინააღმდეგება ლიცენზირებას. • პროდუქტი უზრუნველყოფს აქტივების აღმოჩენის პასიური ქსელის მონიტორინგის შესაძლებლობას. • პროდუქტი ხელს უწყობს რეალურ დროში ხილვადობის და საზოგადოებრივი ღრუბლების აქტივების ინვენტარიზაციის შესაძლებლობას, რადგან ღრუბლოვანი სივრცეები ჩართულია ან ექსპლუატაციიდან ამოღებული. • გადაწყვეტას შეუძლია მობილური მოწყობილობების აღმოჩენა და მობილური მოწყობილობების მართვის სხვადასხვა სისტემასთან (MDM) ინტეგრირება. • გადაწყვეტა შეიცავს ინტერნეტისა და მონაცემთა ბაზის ინტეგრირებულ მომსახურებას. • გადაწყვეტას შეუძლია სერვისების ამოცნობა, რომლებიც მუშაობს არასტანდარტულ პორტებზე. • გადაწყვეტას აქვს სერვისების ამოცნობის საშუალება, რომლებიც ისეა კონფიგურირებული, რომ არ გამოჩნდეს კავშირის ბანერები. • გადაწყვეტას შეუძლია, შეამოწმოს ერთი და იგივე სერვისის მრავალი შემთხვევა, რომლებიც სხვადასხვა პორტებზე ხორციელდება. • გადაწყვეტა შეუძლია მკვდარი ჰოსტების სკანირება (მოწყობილობები, რომლებიც არ რეაგირებენ სიგნალზე). • გადაწყვეტა მხარს უწერს netstat- ის სურვილისამებრ გამოყენებას სისტემაში ღია პორტების სწრაფი და ზუსტი აღრიცხვისთვის, “credential”-ის მიწოდებისას • გადაწყვეტა მხარს უჭერს SMB და WMI გამოყენებას Windows სისტემის სკანირებისთვის. • გადაწყვეტას აქვს ავტომატიზირებული დისტანციური რეესტრის სერვისები Windows სისტემებზე, სანდო მონაცემების შესწავლისას, შემდეგ კი უზრუნველყოფს სერვისის ავტომატურ შეჩერებას სკანირების დასრულების შემდეგ. • სკანერი უზრუნველყოფს secure shell (SSH), უნიქსის სისტემებზე დაუცველობის სკანირებისა და კონფიგურაციის აუდიტის პრივილეგიების ესკალაციის შესაძლებლობით. • გადაწყვეტა უზრუნველყოფს სკანირების პოლიტიკის სრულყოფის შესაძლებლობას ქსელებზე და სამიზნეებზე მინიმალური ზემოქმედებით. • პროდუქტი უზრუნველყოფს უკაბელო წვდომის წერტილების (WAP) აქტიურ და პასიურ აღმოჩენას.			

		პასიური სკანირება • პასიური სკანერი შეიცავს სისუსტეების სკანირების შესაძლებლობას ქსელის ტრაფიკის მონიტორინგის გზით, აქტიური სკანირების გარეშე. • პასიური სკანერი აჩვენებს რეალურ დროში ტრაფიკში გამოვლენილ სისუსტეებს. ეს მონაცემები გამოყენებულია აპლიკაციებზე, პორტებზე, პროტოკოლებზე, საფრთხეებზე და სხვა ქსელურ მოწყობილობებზე, რომლებსაც აქვთ შესაძლებლობა გამოძიების პროცესში გაანალიზონ ტრაფიკი. • პასიური სკანერი უზრუნველყოფს ინფორმაციას ინდივიდუალური ქსელის, ქსელის ან host ჯგუფის შესახებ. • პასიურ სკანერს შეუძლია ტრაფიკის ანალიზი და ცვლილებების შესახებ ინფორმაციის მოწოდება, მაჩვენებლების ცვლილების გარკვეული ლიმიტის შესაბამისად. • პასიური სკანერი ადგენს პოტენციურად საშიში პროგრამები ქსელს ტრაფიკში (მავნე პროგრამა, ბოტნეტი, დროებითი ქსელი). • პასიურ სკანერს შეუძლია ტრაფიკთან დაკავშირებული მოვლენების გაგზავნა სისტემის ჟურნალიდან მოვლენების კორელაციის სისტემაში. • პასიური სკანერი მოწოდებულია მთავარი სისტემის მომწოდებლისგან. • პასიურ სკანერს აქვს შესაძლებლობა გაანალიზოს ტრაფიკი და უზრუნველყოს ინფორმაცია დაუცველობის შესახებ, ინტერნეტის გარეშე. **დაუცველობის შეფასება** • პროდუქტი უზრუნველყოფს სამიზნე სისტემების როგორც ავტორიზებული, ისე არაავტორიზებული ქსელურ სკანირებას. • დაუცველობის სკანირებისთვის პროდუქტი არ ეყრდნობა მესამე მხარის რომელიმე სკანერს. • გადაწყვეტას შეუძლია აგენტის გარეშე ტესტირება, როგორც ადგილობრივი (ავტორიზებული), ისე დისტანციური (არაავტორიზებული) დაუცველობის გამოვლენის მიზნით, სამიზნე მოწყობილობაზე კლიენტის მხარის აგენტის დაინსტალირების საჭიროების გარეშე. • გადაწყვეტას შეუძლია აგენტის ტესტირება ადგილობრივი დაუცველობის გამოვლენის მიზნით, დამატებითი გადასახადის გარეშე. • გადაწყვეტა უზრუნველყოფს გარე ჰოსტის სკანირების სერვისს პერიმეტრული ქსელების სკანირებისთვის. • გადაწყვეტას შეუძლია DHCP ცვლილებებზე დაკვირვება, მოცემული სისტემის სკანირების შედეგების დაკავშირებით ნებისმიერთან, IP მისამართის გარდა. • გადაწყვეტა ადგენს და აფასებს საკითხებს, რისკებს და დაუცველობას. იგი ასევე წარმოადგენს დეტალურ ინფორმაციას რისკის ხასიათის შესახებ და რეკომენდაციებს მისი შემსუბუქების მიზნით.			

		• გადაწყვეტა შეიცავს სკანირების დასკვნების დეტალურ შედეგს და შეიცავს ინფორმაციას, როგორიცაა DLL ვერსიები, მათ შორის - მოსალოდნელი და ნაპოვნი. • გადაწყვეტა არის CVE– თან თავსებადი და უზრუნველყოფს მინიმუმ 10 წლიან CVE დაფარვას. • გადაწყვეტა მოიცავს Microsoft– ის ოპერაციული სისტემებისა და პროგრამების ხარვეზის აუდიტს, რომელიც მოიცავს Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 , Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange და ა.შ. • გადაწყვეტა უზრუნველყოფს ყველა მსხვილი ოპერაციული სისტემის ხარვეზის აუდიტს, მათ შორის macOS, Linux (სხვადასხვა დისტრიბუციები), Solaris, IBM AIX, HPUX და ა.შ. • გადაწყვეტა ითვალისწინებს მესამე მხარის პროგრამებს, როგორიცაა Java და Adobe. • გადაწყვეტა უზრუნველყოფს ხარვეზის მართვის სისტემებთან ინტეგრაციას ხარვეზის აუდიტისა და დელტა ანგარიშგების და სკანირების დასკვნებთან შედარების მიზნით, როგორიცაა Microsoft WSUS / SCCM, Red Hat Satellite, IBM Tivoli Endpoint Manager (ყოფილი BigFix), Symantec Altiris, Ques / Dell KACE. • გადაწყვეტა შეიცავს მობილური მოწყობილობების მართვის (MDM) პროდუქტებთან ინტეგრაციას, როგორიცაა VMware AirWatch, Apple Profile Manager, BlackBerry UEM, Good MDM, Microsoft Intune, IBM MaaS360 და MobileIron, მობილური მოწყობილობების აღმოჩენისა და აუდიტის მიზნით. • პროდუქტი უზრუნველყოფს პროგნოზირებადი დაუცველობის პრიორიტეტის განსაზღვრას, რომელიც იყენებს რეალურ დროში საფრთხის დადგენის მეთოდს და მანქანური სწავლების ალგორითმებს დაუცველობის შეფასების მიზნით, რათა წინასწარ განსაზღვროს, უახლოეს მომავალში რომელი დაუცველობა იქნება გამოყენებული. • პროდუქტი უზრუნველყოფს დაუცველობის პრიორიტეტების კონტექსტის განსაზღვრას, რომელიც მომხმარებლებს ეხმარება გააცნობიერონ ძირითადი ფაქტორები, რომლებიც გავლენას ახდენს თითოეული დაუცველობის ქულაზე (მაგ., საფრთხის ხანდაზმულობა, კოდის სიმწიფის განსაზღვრა, ინფორმაციის წყაროს კატეგორიები). • გადაწყვეტა ასევე მოიცავს დაუცველობის შეფასებას საერთო დაუცველობის შეფასების სისტემის 3 ვერსიის შესაბამისად (CVSS v3). • გადაწყვეტა მოიცავს დაუცველობის შესახებ ინფორმაციას მესამე მხარის წყაროებიდან, როგორიცაა Core Impact, Metasploit და Canvas. • გადაწყვეტა მოიცავს ინფორმაციას ექსპლუატაციის ნაკრებების არსებობის შესახებ მოცემული დაუცველობისთვის, მათ შორის, იმ დაუცველობების შეჯამება,რომელთა გამოყენება შესაძლებელია მავნე პროგრამებისა და დაზარალებული აქტივების მიერ.			

		• გადაწყვეტა ჭკვიანურად არჩევს მოწყვლადობისა და კონფიგურაციის ტესტებს მოცემული აქტივისთვის ამ აქტივის საწყისი სკანირებით მიღებული ინფორმაციის საფუძველზე. • გადაწყვეტა აკონტროლებს დაუცველობის აღმოჩენისა და დაკვირვების თარიღებს, რომლებიც შეიძლება გამოყენებულ იქნეს დროზე დაფუძნებულ ფილტრებში ფილტრაციისა და ანგარიშგების დროს. • გადაწყვეტა უშვებს შერჩეული დაუცველობისა და კონფიგურაციის ტესტების ჩართვას ან გამორთვას დაგეგმილი სკანირების დროს. • გადაწყვეტა არ არის დამოკიდებული ოპერაციული სისტემის დავალებების დაგეგმვის უნარზე. • გადაწყვეტა მხარს უჭერს IPv6 სკანირებას, IPv6 სამიზნეების პასიურ აღმოჩენასთან ერთად. • გადაწყვეტა აფასებს საზოგადოებრივი ღრუბლის აქტივების არასწორ კონფიგურაციასა და დაუცველობსს აქტიური სკანირებისა და აგენტების საშუალებით. • გადაწყვეტა ზუსტად აკონტროლებს აქტივებს და მათ სისუსტეებს, მათ შორის უაღრესად დინამიურ IT აქტივებს, როგორიცაა მობილური მოწყობილობები, ვირტუალური მანქანები და ღრუბლოვანი სივრცეები. **ვებ პროგრამების სკანირება (უსაფრთხოების ტესტირების დინამიური გამოყენება)** • გადაწყვეტას აქვს საშუალება, მოახდინოს როგორც შიდა, ასევე გარე ვებ – აპლიკაციების სკანირება. • გადაწყვეტას შეუძლია 5 ვებ აპლიკაციის სკანირება. • გადაწყვეტას შეუძლია განსაზღვროს კრიტიკული ვებ – აპლიკაციების ნაწილი, რომელთა სკანირება უსაფრთხოა და განსაზღვროს სხვა ნაწილი, რომელთა სკანირება არასოდეს არ უნდა მოხდეს, მუშაობის შეფერხებისა და დარღვევების პრევენციის მიზნით. • გადაწყვეტას შეუძლია HTML5 და AJAX ვებ პროგრამების სკანირება, ტრადიციულ HTML აპებთან ერთად. • გადაწყვეტას შეუძლია ანგარიშის წარდგენა ვებ – აპლიკაციების ყველა სისუსტის შესახებ - შიდა და გარეგანი - ერთიანი ხედვით. • გადაწყვეტას შეუძლია ვებ აპლიკაციების სკანირება: HTTP სერვერზე დაფუძნებული ავტორიზაციის მონაცემები, რეგისტრაციის ფორმის ავტორიზაცია, ქუქი-ჩანაწერების ავტორიზაცია, Selenium ავთენტიფიკაცია. • გადაწყვეტას შეუძლია დატვირთვის კორექტირება სკანირების დროს. • გადაწყვეტას შეუძლია რეგისტრაციის მონაცემების კორექტირება, რომლებიც გამოყენებულია სკანირებისთვის.			

		• გადაწყვეტა საზღვრავს და ახდენს პრობლემების, რისკების და დაუცველობის კლასიფიკაციას. იგი ასევე წარადგენსს დეტალურ ინფორმაციას რისკების ხასიათის შესახებ და რეკომენდაციებს მათი მინიმიზაციისთვის. • გადაწყვეტა აკონტროლებს დაუცველობის გამოვლენის თარიღს. • გადაწყვეტას შეუძლია ადგილობრივი ვებ – აპლიკაციების სკანერის განლაგება ვებ – აპლიკაციებში არსებული სისუსტეების დასადგენად, რომლებიც ინტერნეტით არ არის ხელმისაწვდომი. • გადაწყვეტა უზრუნველყოფს ადგილობრივი ვებ – პროგრამების სკანერის განლაგების შესაძლებლობას დამატებითი ხარჯების გარეშე. • ადგილობრივი ვებ – პროგრამების სკანერი არის იგივე მწარმოებლის. • გადაწყვეტას აქვს საკუთარი სკანერი ღრუბელში ვებ – პროგრამებში დაუცველობის დასადგენად. • გადაწყვეტას შეუძლია Selenium შრიფტის იმპორტი, რომელიც შეიცავს ერთ ან მეტ შიფრს, სკანერის მოქმედებების კონკრეტულ გვერდებზე შესაფასებლად. • გადაწყვეტა აფასებს ვებ პროგრამების ზოგად OWASP ტოპ 10 სისუსტისა და სპეციფიკური პროგრამის კომპონენტის სისუსტეების დასადგენად. • გადაწყვეტა არის მარტივი გამოსაყენებელი და მასშტაბური, რათა მოიცავს ორგანიზაციის ყველა ვებ – პროგრამას. • გადაწყვეტა ახდენს სკანირებას და გამოავლენს API– ს სისუსტეებს. • გადაწყვეტა ამოწმებს SSL / TLS ვებ – პროგრამების დანერგვის შესაძლებლობას. **უსაფრთხოების კონფიგურაციის აუდიტი** • პროდუქტი არ ეყრდნობა მესამე მხარის სკანერებს შესაბამისობის აუდიტის / უსაფრთხოების კონფიგურაციის შეფასების მიზნით. • პროდუქტი უზრუნველყოფს შესაბამისობის აუდიტის / უსაფრთხოების კონფიგურაციის შეფასებას დამატებითი ღირებულების გარეშე და მოქმედწბს ერთი გამოწერის ფარგლებში. • გადაწყვეტას აქვს აგენტის შესაბამისობის აუდიტის შესაძლებლობა, სამიზნე მოწყობილობაზე დამონტაჟებული კლიენტის მხარის აგენტის გარეშე. • გადაწყვეტა შეიცავს უსაფრთხოების და კონფიგურაციის აუდიტის ნიშნულებს მარეგულირებელი შესაბამისობის სტანდარტებისა და სხვა ინდუსტრიის და გამყიდველის საუკეთესო პრაქტიკის სტანდარტებისთვის. PCI DSS 2.0 და 3.0. HIPAA. • გადაწყვეტა შეიცავს უსაფრთხოების და კონფიგურაციის აუდიტის ნიშნულებს გამყიდველის საუკეთესო პრაქტიკისთვის, როგორიცაა Microsoft, Linux, MDM გადაწყვეტილებები, როგორიცაა VMware AirWatch, მარშრუტიზატორები და კონცენტრატორები, firewalls და ა.შ. • გადაწყვეტა მოიცავს Microsoft- ის ოპერაციული სისტემების აუდიტს უსაფრთხოების და კონფიგურაციის პარამეტრებისთვის.			

		• გადაწყვეტა ითვალისწინებს ყველა ძირითადი Linux / Unix ოპერაციული სისტემის აუდიტს უსაფრთხოების და კონფიგურაციის (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა ითვალისწინებს მონაცემთა ბაზების აუდიტს უსაფრთხოების და კონფიგურაციის პარამეტრებისთვის (დეტალური სია: https://www.tenable.com/plugins/nessus/families) . • გადაწყვეტა ითვალისწინებს პროგრამებისა და უსაფრთხოების კონფიგურაციის პარამეტრების შემოწმებას (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა ითვალისწინებს ქსელის ინფრასტრუქტურის შემოწმებას უსაფრთხოების და კონფიგურაციის პარამეტრებისთვის (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა ითვალისწინებს მობილური მოწყობილობის მართვის აუდიტს უსაფრთხოების და კონფიგურაციის პარამეტრებისთვის . (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა ითვალისწინებს საზოგადოებრივი ღრუბლის (მაგ., AWS, Microsoft Azure, Salesforce) და ღრუბლოვანი ინფრასტრუქტურის (მაგ. Docker, Kubernetes) აუდიტს უსაფრთხოების და კონფიგურაციის პარამეტრებისთვის (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა ითვალისწინებს უსაფრთხოების საბოლოო წერტილის კონკრეტული პროდუქტების შემოწმებას ინსტალაციისა და ჩატვირთვის სტატუსისთვის (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა ითვალისწინებს პერსონალურად იდენტიფიცირებადი ინფორმაციის (PII) და სხვა მგრძნობიარე შინაარსის აუდიტს (დეტალური სია: https://www.tenable.com/plugins/nessus/families). • გადაწყვეტა უშვებს, რომ აუდიტის პოლიტიკა იყოს მორგებული ორგანიზაციული საჭიროებების შესაბამისად. • გადაწყვეტა მოიცავს CIS-ის სერთიფიცირებულ ნიშნებს. • გადაწყვეტა სთავაზობს SCAP მხარდაჭერას. **მუშაობის პროცესი** • გადაწყვეტა აერთიანებს ინდივიდუალური სკანირების შედეგებს კუმულატიური დაუცველობის თვალსაზრისით, ფილტრაციითა და ანალიზით. • გადაწყვეტას აქვს შესაძლებლობა, აღმნიშვნელი ნიშნით გამოყოს სისუსტე, რომელიც წარსულში იქნა გადაწყვეტილი. • გადაწყვეტა უზრუნველყოფს მთლიანი დაუცველობის შედეგების ყოვლისმომცველ ფილტრაციას შესაბამისი შესაძლებლობების გამოყენებით. • გადაწყვეტას შეუძლია შეტყობინების გაგზავნა ელ.ფოსტით ან SMS- ით.			

		ანგარიშგება • გადაწყვეტა უზრუნველყოფს ანგარიშგების ავტომატიზირების შესაძლებლობას, რათა მოხდეს ანგარიშების დაგეგმვა. • გადაწყვეტა უზრუნველყოფს დროებითი ანგარიშების მომზადებას კონსოლში შედეგების ნახვის დროს. • გადაწყვეტა აქვს ანგარიშის წარმოების შესაძლებლობა ანგარიშის შემდეგ ფორმატებში: PDF, CSV, HTML და Nessus. • ანგარიშებში შესაძლებელია hostname-ის (NetBIOS, DNS) მითითება IP მისამართებთან ერთად. **ხელსაწყოთა პანელი** • გადაწყვეტა შეიცავს პერსონალურად დასაყენებელ გრაფიკულ და სიებზე დაფუძნებულ პანელის ელემენტებს, შეფასებული გარემოს სისუსტეების და სტატუსის გამოსახატავად. • სისტემა მომხმარებლებს საშუალებას აძლევს, შექმნან პერსონალური პანელები მონაცემთა ვიზუალიზაციისთვის. • ვიზუალიზაციის პანელებს აქვთ ავტომატური განახლების ფუნქცია. • სისტემა ხელს უწყობს მონაცემთა ვიზუალიზაციის პანელების გაზიარებას. **მონაცემთა უსაფრთხოება** • გადაწყვეტა შიფრავს უძრავ მონაცემებს AES-256 დაშიფვრის მინიმუმ ერთი დონის გამოყენებით. • გადაწყვეტა შიფრავს მოძრავ მონაცემებს TLS v1.2 გამოყენებით 4096 ბიტიანი გასაღებით. • გადაწყვეტას აქვს ერთჯერადი შესვლის (SSO) ავტორიზაციის მეთოდები. • SaaS პროდუქტს შეუზღია ერთი მომხმარებლის მონაცემების დაყოფა / დანაწევრება სხვა მომხმარებლების მონაცემებისგან. **გაფართოვების შესაძლებლობა:** **კონტეინერის უსაფრთხოება** • გადაწყვეტას შეუძლია სტატიკური კონტეინერის გამოსახულებების შემოწმება ან შეფასება სისუსტეების, მავნე პროგრამებისა და პოლიტიკის შესაბამისობის დასადგენად. • გადაწყვეტა უზრუნველყოფს სტატიკური კონტეინერის გამოსახულებების შრის მიხედვით სწრაფ და მარტივ შეფასებას. • გადაწყვეტას აქვს ადგილობრივი კონტეინერების სკანირების შესაძლებლობა ინტერნეტში ან ღრუბელზე სურათების გაგზავნის გარეშე. • გადაწყვეტა უზრუნველყოფს კონტეინერების სკანერების შეუზღუდავი განლაგების შესაძლებლობას დამატებითი ღირებულების გარეშე. • ადგილობრივი კონტეინერების სკანერები მოწოდებულია იმავე მწარმოებლის მიერ.			

		• გადაწყვეტა სწრაფად ასრულებს დაუცველობის და მავნე პროგრამების გამოვლენის ტესტირებას DevOps ინსტრუმენტთა ქსელში. • გადაწყვეტა საშუალებას იძლევა, ადვილად განხორციელდეს ინტეგრაცია CI / CD ჩაშენებულ საერთო სისტემებთან და კონტეინერების სურათების რეესტრებთან. • გადაწყვეტა უზრუნველყოფს Docker კონტეინერის შინაარსის დანომვრას განლაგების დაწყებამდე, მასალების დეტალური ქვითრის ჩათვლით, რომელიც მოიცავს სურათის ყველა შრეს და კომპონენტს. • გადაწყვეტაუზრუნველყოფს ,,ერთი შეხედვით" ხილვადობას როგორც კონტეინერების სურათების ინვენტარში, ასევე უსაფრთხოებაში. • გადაწყვეტა ავტომატურად ამოწმებს რეესტრებში შენახული კონტეინერის სურათებს, ახალი სისუსტეების გამოქვეყნებისთანავე. • გადაწყვეტა ადგენს წარმოების კონტეინერებს, რომლებიც არღვევენ პოლიტიკის შესაბამისობას (მაგ., ეს არის თაღლითური კონტეინერები, რომლებიც არ არის დამტკიცებული განლაგებისათვის ან შეცვლილია კონფიგურაცია პირველადი დამტკიცებისა და გამოყენების შემდეგ). • გადაწყვეტა დაუყოვნებლივ აწვდის დეველოპერებს კონკრეტულ სარეაბილიტაციო რჩევებს, როდესაც კონტეინერების სურათები გადალახავს ორგანიზაციის რისკის ზღურბლებს. • გადაწყვეტა შეიცავს ღია კოდის პროგრამულ უზრუნველყოფასა და მესამე მხარის ბიბლიოთეკებზე წვდომის შესაძლებლობას კონტეინერების სურათებში (Snyk integration) • გადაწყვეტა ინტეგრირებულია კონტეინერების უფრო ფართო ტექნოლოგიურ სივრცეში, როგორიცაა მასპინძლები და ვებ პროგრამები. • პროდუქტი ხელს უწყობს პროგრამის კონტეინერების განლაგების შესაძლებლობას მასპინძლებზე Docker- ის ინსტალაციის გამოვლენის გზით. • PCI ASV • გადაწყვეტა უზრუნველყოფს არასავალდებულო გარე ჰოსტინგის სკანირების სერვისს, რომელსაც აქვს PCI ASV სერტიფიკატი PCI DSS განყოფილების 6.6 და 11.2.2 მოთხოვნების დასაკმაყოფილებლად, კვარტალური გარე დაუცველობის სკანირებისთვის. • გადაწყვეტას აქვს PCI შესაბამისობის დაუცველობის სკანირება. გადაწყვეტა შეიცავს წინასწარ განსაზღვრულ PCI სკანირების პროფილებს, რომლებიც აკმაყოფილებს ქსელის სკანირების PCI DSS კრიტერიუმებს. ფუნქციონალობა არსებობს PCI– ს ყველა სხვა არასასურველი დაუცველობის გასაფილტრად. • გადაწყვეტას აქვს PCI– ს კვარტალური ატესტაციის შეუზღუდავი რაოდენობის მხარდაჭერის შესაძლებლობა. • გადაწყვეტას აქვს PCI– ს მრავალი აქტივის მხარდაჭერა. • გადაწყვეტას აქვს განსაზღვრული PCI აქტივების პერიოდული შეცვლის შესაძლებლობა.			

ნიშნულის მოდული

• გადაწყვეტა შეიცავს თითოეული მოწყობილობის შეფასებას მოწყობილობის ტიპის, ინტერნეტთან დაკავშირების შესაძლებლობისა და შესრულებული ამოცანების საფუძველზე.

• გადაწყვეტა ანიჭებს პრიორიტეტს ქსელში განთავსებულ თითოეულ შემოწმებულ მოწყობილობას, მანქანური სწავლების გამოყენებით, ბოლო მიმღებთან არსებული სისუსტეების შეფასების, აგრეთვე მოწყობილობის ტიპის, ინტერნეტზე წვდომის შესაძლებლობისა და ამ მოწყობილობის ამოცანების საფუძველზე.

• გადაწყვეტას შეუძლია მოწყობილობების დაჯგუფება და აქტივების თითოეული ჯგუფის პრიორიტეტულ წერტილებზე არსებული სისუსტეების შეფასება, აგრეთვე მოწყობილობების ტიპის, ინტერნეტის ხელმისაწვდომობისა და ამ მოწყობილობების ამოცანების განსაზღვრა.

• გადაწყვეტა თვლის მანქანური სწავლების საფუძველზე, ინფრასტრუქტურაში არსებულ რისკებს და აქვეყნებს ერთ ცალკეულ შეფასებას მთელი ორგანიზაციისათვის.

• გადაწყვეტას შეუძლია ანონიმურად შედარდეს რისკის შეფასებები ორგანიზაციაში სხვა კომპანიებთან.

• გადაწყვეტა აანალიზებს თითოეული მოწყობილობის სკანირების სიჩქარეს და ადარებს სხვა ორგანიზაციებთან ანონიმურ რეჟიმში.

• გადაწყვეტა აანალიზებს და ადგენს დაუცველობის გამოვლენის პროცესის ეფექტურობას და უშვებს მის შედარებას სხვა ორგანიზაციებთან ანონიმურად.

• გადაწყვეტა აანალიზებს და ადგენს რისკის შერბილების პროცესის ეფექტურობას და მას ანონიმურად ადარებს სხვა ორგანიზაციებთან.

• გადაწყვეტა შეიცავს ბოლოდროინდელი ინციდენტების შესახებ დეველოპერისგან მიღებულ სიახლეებს და მიუთითებს, თუ რამდენი საბოლოო წერტილია პოტენციური რისკის ქვეშ.

• გადაწყვეტა წარმოადგენს ანალიტიკურ ინფორმაციას იმ მოქმედებების შესახებ, რომლებიც ხორციელდება რისკის შემცირების მაქსიმალურად გაზრდის მიზნით.

აქტიური დირექტორიის უსაფრთხოება

• გადაწყვეტა უზრუნველყოფს უსაფრთხოების რეალურ დროში უსაფრთხოების მონიტორინგი Microsoft Active Directory (AD) ინფრასტრუქტურისთვის.

• გადაწყვეტა შეიცავს აუდიტის, საფრთხეების გამოვლენისა და ინციდენტებზე რეაგირების ამოცანების შესაძლებლობას.

• გადაწყვეტას შეუძლია მოიძიოს აქტიურ დირექტორიაში არსებული სისუსტეები.

• გადაწყვეტა ითვალისწინებს აქტიურ დირექტორიაში არსებული სისუსტეების პრიორიტეტებს.

• გადაწყვეტას ემატება ობიექტზე განლაგების და ღრუბელზე განლაგების ვარიანტები.

		• გადაწყვეტა ასახავს შეტევებს MITER ATT & CK– ზე. • გადაწყვეტა გთავაზობთ აქტიური დირექტორიის ტოპოლოგიის ნახვის შესაძლებლობას. • გადაწყვეტას აქვს Syslog ან ელექტრონული ფოსტის საშუალებით შეტყობინების გაგზავნის შესაძლებლობა. • გადაწყვეტა ითვალისწინებს multi-org და multi-forest ოფციებს აქტიური დირექტორიისთვის. • გადაწყვეტა უკავშირდება Microsoft Environment– ს WMI პროტოკოლის გამოყენებით აქტიურ დირექტორიაზე აგენტების დაინსტალირების გარეშე. • გადაწყვეტა ითხოვს მხოლოდ დომენის მომხმარებელს, ჟურნალების წაკითხვის ნებართვით. • გადაწყვეტა წარმოადგენს რეკომენდაციებს აქტიური დირექტორიის რისკის შესამცირებლად. • გადაწყვეტა გვაწვდის დეტალურ ინფორმაციას შესაძლო რისკების შესახებ. • გადაწყვეტა ავლენს აქტიურ დირექტორიაზე განხორციელებულ შეტევებს, როგორიცაა DCShadow, Brute Force, Password Spraying, DCSync და სხვა. • გადაწყვეტა შეიცავს შეტევის ინდიკატორებს იმის გასაგებად, თუ რა ტიპისაა ეს შეტევა.			

შემსყიდველი

მიმწოდებელი