სახელმწიფო შესყიდვის შესახებ ხელშეკრულება N01-18

CPV48700000 - პროგრამული პაკეტების მომსახურე პროგრამები

CPV48781000 - სისტემის მართვის პროგრამული პაკეტები

ქ. თბილისი **30 მარტი 2022 წელი**

ერთი მხრივ **სსიპ განათლების მართვის საინფორმაციო სისტემა** (შემდგომში „შემსყიდველი"), წარმოდგენილი მისი უფროსის **დიმიტრი ბერიძის** სახით და მეორე მხრივ **შპს იუჯითი** (შემდგომში „მიმწოდებელი"), წარმოდგენილი მისი გენერალური დირექტორის **ერმილე სულაძის** სახით, შემსყიდველის მიერ 2022 წლის 11 მარტს გამოცხადებული **SPA220000704** ელექტრონული ტენდერისა და „სახელმწიფო შესყიდვების შესახებ" საქართველოს კანონის საფუძველზე, ვდებთ წინამდებარე ხელშეკრულებას შემდეგზე:

1. ტერმინთა განმარტება

1.1 „ხელშეკრულება სახელმწიფო შესყიდვის შესახებ" - შემსყიდველსა და ტენდერში გამარჯვებულ პრეტენდენტს შორის დადებული ხელშეკრულება, რომელიც ხელმოწერილია მხარეთა მიერ, მასზე თანდართული ყველა დოკუმენტით და დამატებებით, ასევე, სატენდერო დოკუმენტაციის პირობებით და იმ დოკუმენტაციით, რომლებზეც ხელშეკრულებაში არის მინიშნებები.

1.2 „ხელშეკრულების ღირებულება" - საერთო თანხა, რომელიც უნდა გადაიხადოს შემსყიდველმა მიმწოდებლის მიერ ხელშეკრულებით ნაკისრი ვალდებულებების სრული და ზედმიწევნით შესრულებისთვის.

1.3 „დღე", „კვირა", „თვე" - კალენდარული დღე, კვირა, თვე.

1.4 „შემსყიდველი" - ორგანიზაცია, რომელიც ახორციელებს შესყიდვას.

1.5 „მიმწოდებელი" - პირი, რომელიც ახორციელებს მომსახურების მიწოდებას ხელშეკრულების ფარგლებში.

1.6 „შესყიდვის ობიექტი" - ხელშეკრულების მე-2 მუხლით გათვალისწინებული ხელშეკრულების საგანი.

1.7 „ტექნიკური დავალება" - ელექტრონული ტენდერის სატენდერო დოკუმენტაციის ტექნიკური დავალება, რომელიც დაერთვება ხელშეკრულებას, როგორც მისი განუყოფელი ნაწილი.

2. ხელშეკრულების საგანი

2.1 Web Application Firewall-ის შესყიდვა.

2.2 შესყიდვის ობიექტის დასახელება, ტექნიკური მახასიათებლები, რაოდენობა, ერთეულის და საერთო ღირებულება განისაზღვრება წინამდებარე ხელშეკრულების დანართი N1-ის შესაბამისად.

3. ხელშეკრულების ღირებულება და ანგარიშსწორების პირობები

3.1 ხელშეკრულების საერთო ღირებულება შეადგენს **479 870.00** (ოთხასსამოცდაცხრამეტი ათას რვაასსამოცდაათი ლარი და 00 თეთრი) ლარს.

3.2 ხელშეკრულების ღირებულება მოიცავს შესყიდვის ობიექტის მიწოდებასთან დაკავშირებულ მიმწოდებლის ყველა ხარჯს და საქართველოს კანონმდებლობით გათვალისწინებულ გადასახადებს.

3.3 ანგარიშსწორება განხორციელდება უნაღდო ანგარიშსწორებით ლარში, წინამდებარე ხელშეკრულებაში მითითებული მიმწოდებლის საბანკო რეკვიზიტების შესაბამისად.

3.4 ანგარიშსწორება განხორციელდება მიწოდებული შესყიდვის ობიექტის ღირებულების მიხედვით, კანონმდებლობით გათვალისწინებული დოკუმენტების სრულყოფილად გაფორმებიდან 10 (ათი) სამუშაო დღეში.

3.5 დაფინანსების წყარო: **2022 წლის საბიუჯეტო სახსრები**.

3.6 მიმწოდებლის მოთხოვნის შემთხვევაში, შემსყიდველის თანხმობით, შესაძლებელია განხორციელდეს წინასწარი საავანსო გადახდა არაუგვიანეს 10 (ათი) სამუშაო დღის განმავლობაში, ხელშეკრულების ჯამური ღირებულების **100%**-ისა, იდენტური შესაბამისი საბანკო გარანტიის საფუძველზე (საბანკო გარანტიის მოქმედების ვადა არანაკლებ 30 (ოცდაათი) კალენდარული დღით უნდა აღემატებოდეს შესყიდვის ობიექტის მიწოდების ვადას).

4. ხელშეკრულების მოქმედების ვადები

ხელშეკრულება ძალაში შედის გაფორმებიდან და მოქმედებს 2025 წლის 30 აპრილის ჩათვლით.

5. შესყიდვის ობიექტის მიწოდების პირობები

შესყიდვის ობიექტის მიწოდება უნდა განხორციელდეს ხელშეკრულების გაფორმებიდან 20 (ოცი) კალენდარული დღის განმავლობაში, შემდეგ მისამართზე: ქ. თბილისი, გ. ფანჯიკიძის ქ. N1ა.

6. ხელშეკრულების ინსპექტირება

6.1 შემსყიდველი ახორციელებს კონტროლსა და ზედამხედველობას მიმწოდებლის მიერ ხელშეკრულების პირობების შესრულებაზე.

6.2 ამ მუხლის პირველი პუნქტით გათვალისწინებული კონტროლისა და ზედამხედველობის განმახორციელებელ პირს შემსყიდველის მხრიდან წარმოადგენს 7.2 პუნქტით განსაზღვრული პირი.

6.3 ყველა გამოვლენილი ხარვეზის ან ნაკლის აღმოფხვრასთან დაკავშირებული ხარჯების ანაზღაურება ეკისრება მიმწოდებელს საქართველოს კანონმდებლობით დადგენილი წესით.

7. შესყიდვის ობიექტის მიღება-ჩაბარების წესი

7.1 ხელშეკრულებით გათვალისწინებული შესყიდვის ობიექტის მიღება დასტურდება მხარეებს შორის მიღება-ჩაბარების აქტის გაფორმებით, მას შემდეგ რაც შემსყიდველის მხრიდან ინსპექტირებისას არ იქნება გამოვლენილი შესყიდვის ობიექტის რაიმე ნაკლი ან ხარვეზი.

7.2 შემსყიდველის მხრიდან მიღება-ჩაბარების აქტის ხელმოწერაზე პასუხისმგებელ პირს წარმოადგენს სსიპ განათლების მართვის საინფორმაციო სისტემის კომპიუტერული სისტემების, ქსელებისა და კომუნიკაციის სამსახურის სისტემური ადმინისტრატორი (უფროსი) **გიორგი მეზურნიშვილი** ან სსიპ განათლების მართვის საინფორმაციო სისტემის უფროსის ბრძანებით (სსიპ - განათლების მართვის საინფორმაციო სისტემის თანამშრომლებისათვის, სსიპ - განათლების მართვის საინფორმაციო სისტემის სახელით, მიღება-ჩაბარების აქტებზე ხელმოწერის უფლებამოსილების მინიჭების შესახებ) განსაზღვრული ერთ-ერთი პირი.

8. მხარეთა ვალდებულებები და პასუხისმგებლობა

8.1 მიმწოდებელი ვალდებულია უზრუნველყოს ხელშეკრულებით განსაზღვრული შესყიდვის ობიექტის მიწოდება უნაკლოდ, თუკი შესყიდვის ობიექტი არ აღმოჩნდება სრულყოფილი, მიმწოდებელი ვალდებულია, შემსყიდველის მოთხოვნისთანავე, გამოასწოროს ეს ნაკლი.

8.2 მიმწოდებელი უფლებამოსილია მოსთხოვოს შემსყიდველს შესყიდვის ობიექტის ღირებულების ანაზღაურება ხელშეკრულებით გათვალისწინებული ვადებისა და პირობების დაცვით.

8.3 შემსყიდველი ვალდებულია გადაიხადოს შესყიდვის ობიექტის ღირებულება ამ ხელშეკრულებით გათვალისწინებული პირობებით.

8.4 შემსყიდველი უფლებამოსილია ნებისმიერ დროს განახორციელოს მიმწოდებლის მიერ ნაკისრი ვალდებულებების შესრულებისა და ხარისხის ინსპექტირება.

8.5 ფორს-მაჟორული გარემოებების გარდა ხელშეკრულებით გათვალისწინებული ვალდებულებების შესრულების ვადების გადაცდენის შემთხვევაში მხარეებს დაეკისრება პირგასამტეხლოს გადახდა ყოველ ვადაგადაცილებულ დღეზე შეუსრულებელი ვალდებულების ღირებულების 0.02%-ის ოდენობით.

8.6 პირგასამტეხლოს გადახდა არ ათავისუფლებს მხარეებს ძირითადი ვალდებულებების შესრულებისაგან.

8.7 ხელშეკრულების პირობების შეუსრულებლობის შემთხვევაში მხარეს ეკისრება პირგასამტეხლო ხელშეკრულების საერთო ღირებულების 10%-ის ოდენობით.

8.8 იმ შემთხვევაში, თუ მხარისათვის დაკისრებული პირგასამტეხლოს საერთო თანხა გადააჭარბებს ხელშეკრულების საერთო ღირებულების 1 (ერთი) პროცენტს, მეორე მხარეს უფლება აქვს ცალმხრივად მოითხოვოს ხელშეკრულების შეწყვეტა და მიყენებული ზიანის ანაზღაურება.

9. ხელშეკრულების შესრულების უზრუნველყოფის გარანტია

9.1 იმისათვის, რომ თავიდან იქნას აცილებული მიმწოდებლის მიერ სახელმწიფო შესყიდვის შესახებ ხელშეკრულების პირობების შეუსრულებლობის რისკი, გამოიყენება ხელშეკრულების შესრულების უზრუნველყოფის საბანკო გარანტია.

9.2 ვინაიდან, მიმწოდებელი წარმოადგენს თეთრ სიაში რეგისტრირებულ იურიდიულ პირს, ხელშეკრულების შესრულების უზრუნველყოფის უპირობო და გამოუხმობი საბანკო გარანტია წარმოდგენილია წინამდებარე ხელშეკრულების საერთო ღირებულების **1.5%**-ით. საბანკო გარანტია გაცემულია 2022 წლის 29 მარტს სს საქართველოს ბანკი-ს მიერ (საბანკო გარანტია N PE73577973-22) **7 198.05** (შვიდი ათას ასოთხმოცდათვრამეტი ლარი და 05 თეთრი) ლარის ოდენობით, 2022 წლის 15 ივნისის ჩათვლით მოქმედების ვადით.

9.3 მიმწოდებელს, მისი წერილობითი მოთხოვნის საფუძველზე, ხელშეკრულების შესრულების უზრუნველსაყოფად გაცემული საბანკო გარანტია, ხელშეკრულებით გათვალისწინებული ვალდებულებების უნაკლოდ შესრულების შემთხვევაში, დაუბრუნდება მხარეთა შორის შესყიდვის ობიექტის მიღება-ჩაბარების აქტის გაფორმების შემდეგ.

9.4 მიმწოდებლისაგან დამოუკიდებელი მიზეზების გამო ხელშეკრულების შეწყვეტის შემთხვევაში, შემსყიდველი ვალდებულია მიმწოდებლის მოთხოვნისთანავე, დაუბრუნოს მას ხელშეკრულების შესრულების უზრუნველყოფის გარანტია.

10. ფორს-მაჟორი

10.1 მხარეებს არ დაეკისრებათ პასუხისმგებლობა ხელშეკრულებით გათვალისწინებული ვალდებულებების შეუსრულებლობის, არაჯეროვანი შესრულების ან ვადის გადაცილებისთვის თუკი, შეუსრულებლობა გამოწვეულია ფორს-მაჟორული გარემოებებით.

10.2 ამ მუხლის მიზნებისთვის ფორს-მაჟორი ნიშნავს ისეთ გარემოებებს, რომელთა არსებობის გამო მხარისათვის ობიექტურად შეუძლებელი იყო სახელშეკრულებო ვალდებულებების შესრულება (სტიქიური მოვლენები, საომარი მოქმედება, ეპიდემია, კარანტინი, საბიუჯეტო ასიგნებების მკვეთრი შემცირება, საქონლის მიწოდებაზე ემბარგოს დაწესება, სახელმწიფო გადატრიალება და სხვა).

10.3 ფორს-მაჟორული გარემოებების დადგომის შემთხვევაში ხელშეკრულების მხარემ, რომლისთვისაც შეუძლებელი ხდება ნაკისრი ვალდებულებების შესრულება, პირველი შესაძლებლობისთანავე უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება ასეთი გარემოებების და მათი გამომწვევი მიზეზების შესახებ. თუ შეტყობინების გამგზავნი მხარე არ მიიღებს მეორე მხარისაგან პასუხს, იგი თავისი შეხედულებისამებრ, მიზანშეწონილობისა და შესაძლებლობის მიხედვით აგრძელებს ხელშეკრულებით ნაკისრი ვალდებულებების შესრულებას და ცდილობს გამონახოს ვალდებულების შესრულების ისეთი ალტერნატიული ხერხები, რომლებიც დამოუკიდებელი იქნებიან ფორს-მაჟორული გარემოებებისაგან.

11. ხელშეკრულებაში ცვლილებების შეტანის და შეწყვეტის წესი

11.1 ხელშეკრულებაში ნებისმიერი ცვლილების, დამატების შეტანა შესაძლებელია მხოლოდ მხარეთა შორის წერილობითი ფორმით შედგენილი შეთანხმების საფუძველზე.

11.2 ხელშეკრულების პირობების, მათ შორის, ფასის შეცვლა დაუშვებელია, თუ ამ ცვლილებების შედეგად იზრდება ხელშეკრულების საერთო ღირებულება ან უარესდება ხელშეკრულების პირობები შემსყიდველისთვის, გარდა საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული შემთხვევებისა. ხელშეკრულების პირობების გადასინჯვა ხდება საქართველოს კანონმდებლობით დადგენილი წესით.

11.3 საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული გარემოებების დადგომის შემთხვევაში, ხელშეკრულების საერთო ღირებულების გაზრდა დაუშვებელია ხელშეკრულების ღირებულების **10%**-ზე მეტი ოდენობით.

11.4 ხელშეკრულების ერთ-ერთი მხარის მიერ ხელშეკრულების პირობების შეუსრულებლობის შემთხვევაში მეორე მხარე უფლებამოსილია ცალმხრივად მიიღოს გადაწყვეტილება ხელშეკრულების შეწყვეტის შესახებ.

11.5 ხელშეკრულების 11.4 პუნქტით გათვალისწინებულ შემთხვევაში ინიციატორი მხარე ვალდებულია გადაწყვეტილების მიღების განზრახვის შესახებ არანაკლებ **10** (ათი) სამუშაო დღით ადრე წერილობით აცნობოს ამის შესახებ მეორე მხარეს.

12. დავების გადაჭრის წესი

ამ ხელშეკრულების შესრულების დროს წამოჭრილი ყველა დავა შეძლებისდაგვარად გადაიჭრება მხარეთა შორის მოლაპარაკების გზით. შეთანხმების მიუღწევლობის შემთხვევაში დავას წყვეტს სასამართლო.

13. დასკვნითი დებულებები

ხელშეკრულება შედგენილია ქართულ ენაზე.

14. მხარეთა რეკვიზიტები

შემსყიდველი	მიმწოდებელი
სსიპ განათლების მართვის საინფორმაციო სისტემა ს/კ 205300048 მისამართი: ქ. თბილისი, გ. ფანჯიკიძის ქ. N1ა	შპს იუჯითი ს/კ 204892964 მისამართი: ქ. თბილისი, ჭავჭავაძის გამზირი N17ა საბანკო რეკვიზიტები: სს საქართველოს ბანკი ბანკის კოდი: BAGAGE22 ა/ა: GE88BG0000000261644601
სსიპ განათლების მართვის საინფორმაციო სისტემის უფროსი დიმიტრი ბერიძე _____	**შპს იუჯითი-ს გენერალური დირექტორი** UGT LLC Digitally signed by UGT LLC Date: 2022.03.30 17:41:36 +04'00' ერმილე სულაძე _____

ფასების ცხრილი

N	დასახელება	ტექნიკური მახასიათებლები	წარმოშობის წყარო (მწარმოებელი ქვეყანა)	მწარმოებელი კომპანია	მოდელი (ასეთის არსებობის შემთხვევაში)	რაოდენობა (ცალი)	ერთეულის ღირებულება (ლარი)	საერთო ღირებულება (ლარი)
1	Web Application Firewall-ის შესყიდვა	დეტალური ტექნიკური მახასიათებლები თანდართულია	აშშ	F5	F5 BIG-IP VE 1 Gbps	1	479,870.00	479,870.00
							სულ ჯამი:	479,870.00

საქონლის მიწოდების/მომსახურების გაწევის/სამუშაოს შესრულების ვადა: ხელშეკრულების გაფორმებიდან 20 (ოცი) კალენდარული დღე.

ანგარიშსწორების პირობები: წინასწარი საავანსო გადახდა ხელშეკრულების ჯამური ღირებულების 100%-ისა, იდენტური შესაბამისი საბანკო გარანტიის საფუძველზე.

გარანტია: გადაწყვეტილებას გააჩნია მწარმოებლის ოფიციალური მხარდაჭერის და განახლებების სერვისები 3 წლის ვადით

UGT LLC

Digitally signed by UGT LLC
Date: 2022.03.21 17:42:52 +04'00'

ტექნიკური დავალება

შემოთავაზებული ახალი მოდელი შესაძლებელია გაერთიანდეს არსებულ F5-ის გადაწყვეტილებასთან მაღალ მდგრადობის მისაღებად (Failover/Cluster)-ში .

სისტემა მოიცავს შემდეგ ფუნქციონალს: BIG IP VE Best Bundle - 1 Gbps, ვებ აპლიკაციის ფაირვოლს (Web Application Firewall) და დატვირთვის ბალანსერს (Load Balancer).

სისტემა მოიცავს 1 (ერთი) ცალ ვირტუალურ მოწყობილობას (VIRTUAL APPLIANCE) და დამატებითი კომპონენტების გარეშე აკმაყოფილებს ქვევით მოცემულ ტექნიკურ მახასიათებლებს:

1) სისტემა თავსებადია VMware vSphere 6.5 - 6.7 U3 ვირტუალიზაციის პლატფორმასთან.
2) ვირტუალური მოწყობილობის დაშიფრული ტრაფიკის ჯამური გამტარუნარიანობა არის 1 (ერთი) Gbps.
3) ვირტუალურ მოწყობილობას შეუძლია როგორც Active/Acitve, ისე Active/Passive მაღალმდგრადობის რეჟიმში მუშაობა. აღნიშნულ რეჟიმში შეუძლია 8 მოწყობილობის გაერთიანება, ასევე შეუძლია მათ შორის SSL და TCP სესიების სინქრონიზაცია.
4) სისტემას აქვს ქსელში გამართვის შემდეგი რეჟიმების მხარდაჭერა:
1. L2 Forwarding.
2. L3 IP Forwarding (Routing).
3. Packet Based Layer 4 traffic processing.
4. Reverse Proxy and Forward Proxy (Layer 7).

5) სისტემას აქვს შემდეგი ქსელური ტექნოლოგიების მხარდაჭერა:
1. L2 კომუტაცია: Vlan, Vlan Groups, VXLAN.
2. L3 მარშრუტიზაცია: IPV4, IPV6, NAT, SNAT, QOS, BGP, OSPF ასევე სტატიკური მარშრუტიზაციის მხარდაჭერა.

6) სისტემას აქვს მომხმარებელთა შემდეგი ავტორიზაციის წყაროს მხარდაჭერა:
1. მომხმარებელთა ლოკალური ბაზა.
2. LDAP.
3. Microsoft Active Directory.
4. RADIUS.
5. TACACS+.
6. HSM Systems.

7) სისტემას შეუძლია ვებ აპლიკაციებზე წვდომის დაშვება შემდეგი აუთენტიფიკაციის მექანიზმების გამოყენებით:
1. Kerberos.
2. NTLM v1, v2.
3. SAML 2.0.
4. Smart Card.
5. Security Token.
6. კლიენტის სერტიფიკატი.
7. ორ ფაქტორიანი აუთენტიფიკაცია.

8) სისტემას აქვს გარე ქსელიდან მომხმარებელთა კავშირის შემდეგი ფუნქციონალის მხარდაჭერა:
1. SSL VPN.

2. სისტემას შეუძლია წვდომის გახსნამდე, მომხმარებელთა მოწყობილობების ორგანიზაციის უსაფრთხოების სტანდარტებთან თავსებადობის შემოწმება.
3. სისტემას შეუძლია Client-side პროგრამული უზრუნველყოფა Windows, Linux და MacOS ოპერაციული სისტემებისთვის ასევე iOS და Android მობილური ოპერაციული სისტემებისთვის.
9) სისტემას შეუძლია მომხმარებელთა აპლიკაციებზე წვდომის პოლიტიკების შექმნა:
1. სისტემას შეუძლია მომხმარებელთა წვდომის მართვა როგორც ინდივიდუალური სააღრიცხვო ჩანაწერის ისე მომხმარებელთა ჯგუფების მიხედვით.
2. სისტემას შეუძლია ერთი პოლიტიკის ფარგლებში, სხვადასხვა HTTP პარამეტრის მიხედვით (Host Name, URI, Source IP, Source Browser), ავტორიზაციის სხვადასხვა მეთოდის გამოყენების, ასევე მომხმარებელთა სხვადასხვა ჯგუფის წევრობის შემოწმება.
3. მომხმარებელთა რესურსებზე წვდომის მართვა აუთენტიფიკაციის პორტალის მეშვეობით. შეუძლია აღნიშნული პორტალის ვიზუალური ნაწილის შეცვლა.
10) სისტემას შეუძლია ვებ აპლიკაციებს შორის L4/L7 დონეზე, დატვირთვის განაწილებას და მაღალმდგრადობას უზრუნველყოფა:
1. სისტემას შეუძლია დატვირთვის გადანაწილების შემდეგი მეთოდების გამოყენება:
- Round Robin.
- Ratio Round Robin.
- Least Connections.
- Weighted Least Connections.
- Least Sessions.
- Predictive.

2. სისტემას აქვს ვებ აპლიკაციის მონიტორინგისთვის შემდეგი მექანიზმების მხარდაჭერა:
- ICMP, ICMP Gateway, TCP, HTTP, HTTPS, URL, LDAP, MSSQL, RADIUS, SOAP,WMI, ასევე სისტემას შეუძლია დამატებით „Custom" მონიტორინგის მექანიზმის შექმნა.

3. სისტემას შუძლია სესიების მდგრადობას შემდეგი პარამეტრების მიხედვით უზრუნველყოფა:
- Source or Destination IP.
- Session ID Persistence.
- Cookie Persistence.
- MSRDP sessions Persistence.

4. სისტემას შეუძლია შემომავალი ტრაფიკის ოპტიმიზაცია:
- HTTP კომპრესია.
- HTTP სესიების, სერვერის მხარეს ერთ TCP სესიაში აგრეგირების შესაძლებლობა.
- HTTP შიგთავსის ქეშირება.

11) სისტემას შეუძლია "reverse proxy" რეჟიმში მუშაობისას განახორციელოს შემდეგი ოპერაციები: „digitally sign cookies", „encrypt cookies", „rewrite URLs" და "Rewrite Response URLs".
12) სისტემას შეუძლია შემდეგი ოპერაციები: „track session Ids", „prevent cookie injection, „cookie tampering" და „session hijacking attacks" შეტევების აღმოჩენა და ბლოკირება.
13) სისტემას შეუძლია როგორც მომხმარებელთან ასევე სერვერთან გააგზავნოს TCP და RST გზავნილები.
14) სისტემას აქვს შემდეგი ბლოკირების მეთოდების მხარდაჭერა:
1. Block the HTTP request.
2. Block the connection.
3. Block the IP address.
4. Block the application session.
5. Block the user.
6. Send a TCP connection reset.
7. Block the connection.

15) ვებ აპლიკაციების ბრენდმაუერს შეუძლია სერვერსა და კლიენტს შორის SSL ტრაფიკის

დეშიფრაცია და ხელმეორედ შიფრაცია გაგზავნამდე.
16) ვებ აპლიკაციების ბრენდმაუერს შეუძლია SSL ტრაფიკის დეშიფრაცია რათა განახორციელოს ინსპექტირება.
17) სისტემას შეუძლია უსაფრთხოების უზრუნველყოფა ვებ სერვისებისთვის, რომლებსაც გააჩნიათ ე.წ. „XML„ შიგთავსი.
18) სისტემის შეუძლია ინტეგრაცია WhiteHat, IBM, Cenzic და HP Qualys, ვებ სისუსტეების გამომვლენ სკანერებთან. მათ მიერ დაგენერირებული რეპორტის მიხედვით პოლიტიკების ავტომატური შექმნა. ასევე სისტემას შეუძლია ე.წ. „Application Virtual Patching" განხორციელება.
19) უსაფრთხოების უზრუნველსაყოფად სისტემას აქვს ე.წ. „White List" და "Black List" ტექნოლოგიების მხარდაჭერა.
20) სისტემას შეუძლია პოლიტიკების ისეთი სახით გამართვა, რომ სისტემამ დააგენერიროს შეტყობინებები ინციდენტებზე.
21) სისტემის ადმინისტრატორს მარტივად შეუძლია უსაფრთხოების პოლიტიკების შექმნა. ეს პროცესი არ საჭიროებდეს ე.წ. „scripting" ენის ცოდნას. ადმინისტრატორის მიერ შექმნილ უსაფრთხოების პოლიტიკებში შეიძლება რამდენიმე კრიტერიუმის განსაზღვრა. შეიძლება ისეთი კრიტერიუმების განსაზღვრა როგორებიცაა: ე.წ. „URL", მომხმარებელი, სიგნატურის ინციდენტი, მოვლენების რაოდენობა.
22) სისტემას აქვს ჩაშენებული უსაფრთხოების პოლიტიკები, რომლის საშუალებითაც ახორციელებს შესაბამისი საფრთხეების მოგერიებას. სისტემას აქვს შემდეგი ჩაშენებული უსაფრთხოების პოლიტიკების მხარდაჭერა:
1. Apache Expect Header XSS.
2. Cross Site Request Forgery.
3. Data Leakage Detection/Prevention.
4. Directory Browsing Detection.
5. Directory Traversal (In Cookies/Parameters Value).
6. Fullwidth/Halfwidth Unicode Decoding.
7. HTTP Response Splitting Vulnerability.
8. IE Discussion BarAccess to Internal Information.
9. Malformed HTTP Attack (Non compatible HTTP Results Error code).
10. OS Command Injection.
11. Plain Vanilla Scanner Detection.
12. Privacy Violation -Credit Card Number Insertion.
13. Sensitive Error Messages Leakage.
14. Suspected parameter tampering -Deprecated.
15. Suspicious Response Code.
16. Webdav Method Detections.

23) სისტემას აქვს ე.წ. „Negative Security/Black List" მოდელის მიხედვით უსაფრთხოების უზრუნველყოფის შესაძლებლობა:
1. სისტემას შეუძლია იმ ვებ ტრაფიკის ბლოკირება, რომელიც ემთხვევა ცნობილი შეტევების სიგნატურებს.
2. სისტემას აქვს ზუსტი შეტევების სიგნატურები.
3. სისტემაში ადმინისტრატორს შეუძლია არსებული სიგნატურების ცვლილება და ახალი სიგნატურების დამატება.
4. სისტემას შეუძლია სიგნატურების ავტომატური, რეგულარული განახლება, რათა უზრუნველყოფილი იყოს უსაფრთხოება ცნობილი შეტევებისგან. აღნიშნული განახლების სერვისი მოქმედებს მოთხოვნილი მხარდაჭერის სრულ პერიოდზე.

24) სისტემა უზრუნველყოფს ქსელურ უსაფრთხოებას ვებ სერვისებისთვის, სისტემას აქვს შემდეგი ტექნოლოგიების მხარდაჭერა:
1. Stateful firewall.

2. DoS prevention
• Behavioral denial-of-service (DoS) protection.
3. XML/SOAP profile enforcement.
4. Web services signatures.
5. XML protocol conformance.
6. Device-ID detection and finger printing.

25) სისტემას შეუძლია შემდეგი ტიპის ვებ აპლიკაციაზე მიმდინარე შეტევების აღმოჩენა და თავიდან აცილება:

1. OWASP Top 10.
2. OS Command Injection.
3. SQL Injection.
4. Session Hijacking.
5. Site Reconnaissance.
6. Site Scraping.
7. Cross Site Scripting.
8. Cross Site Request Forgery.

26) სისტემას შეუძლია HTTPS ტრაფიკის კონტროლი, შეტევების აღმოჩენა რომლებიც მიმართულია ე.წ. „ბუფერის" გადავსებაზე, არასასურველი კოდის გაშვებაზე და შეიცავს არაკორექტულ მოთხოვნებს.

27) სისტემას შეუძლია ადმინისტრატორის მიერ მორგებული კონტექსტუალური ატრიბუტები დაუნიშნოს მომხდარ მოვლენებს. სისტემას შეუძლია აღნიშნული ატრიბუტების გამოყენება უსაფრთხოების პოლიტიკების შესადგენად, მონაცემების აუდიტისთვის და რეპორტების დაგენერირებისთვის. სისტემას შეუძლია ატრიბუტების ინფორმაციის განსაზღვრა შემდეგი წყაროებიდან:

1. გარე წყაროები ე.წ. LDAP.
2. მომხდარი მოვლენიდან სისტემას შეუძლია ატრიბუტის ამოღება. HTTP თავსართიდან სისტემას შუძლია ისეთი ატრიბუტების ამოღება, როგორებიცაა წყაროს IP მისამართი, URL, Cookie-ს სახელი.

28) სისტემას შეუძლია ვებ სერვერიდან გამომავალი ტრაფიკის კონტროლი, რომ აღკვეთოს კონფიდენციალური ინფორმაციის გაჟონვა:

1. პერსონალური მონაცემები.
2. სისტემას შეუძლია შაბლონების შექმნა, რომლის მიხედვითაც ახორციელებს კონფიდენციალური ინფორმაციის აღმოჩენას.

29) სისტემას აქვს ვებ სერვისების უსაფრთხოების პოლიტიკის ავტომატურად შექმნის მხარდაჭერა:

1. სისტემას აქვს პროფილის ავტომატურად შედგენის ფუნქცია.
2. ვებ აპლიკაციის ცვლილებასთან ერთად სისტემას ავტომატურად შეუძლია პოლიტიკის შეცვლა, რათა იგი შესაბამისობაში მოვიდეს შეცვლილ ვებ აპლიკაციასთან.
3. სისტემას შეუძლია არაავტორიზებული სიმბოლოებისა და პარამეტრების ტიპების აღმოჩენა.
4. პოლიტიკის ავტომატურად შექმნის ფუნქციას შეუძლია ვებ აპლიკაციის სტრუქტურის და ელემენტების ავტომატური შესწავლა. აღნიშნული ფუნქციის ფარგლებში შეუძლია შემდეგი ელემენტების შესწავლა:

1. Directories.
2. URLs.
3. Parameters and form fields.
4. Cookies.
5. HTTP methods.
6. HTTP RFC Compliance.
7. Expected form field values (size, content, read-only).
8. Referrers.

9. XML files.
10. SOAP actions.
11. XML elements.
12. სისტემას შეუძლია JavaScript, CGI, ASP და PHP ით დინამიურად გენერირებული ინფორმაციის პროფილირება.

5. ვებ აპლიკაციის უსაფრთხოების პოლიტიკის შედგენისთვის, შეუძლია სისტემაში ნდობით აღჭურვილი მომხმარებლების განსაზღვრა, რათა მხოლოდ მათი მოთხოვნების მიხედვით განხორციელდეს პროფილის შედგენა.
6. სისტემის მიერ შედგენილი უსაფრთხოების პოლიტიკა ხელმისაწვდომია და მოდიფიცირებადი ადმინისტრატორისთვის.
7. სისტემას შეუძლია შექმნილი უსაფრთხოების პოლიტიკის შეფასება თუ რამდენად ოპტიმალურადაა იგი შედგენილი.
8. სისტემას შეუძლია უსაფრთხოების პოლიტიკის ოპტიმიზაცია.
9. სისტემის ადმინისტრატორს შეუძლია კონტროლი ოპტიმიზირების პოლიტიკების დაწესებაზე.

30) სისტემას შეუძლია ვებ აპლიკაციაში აუთენტიფიცირებული მომხმარებლების სახელის, HTTP სესიის და IP მისამართის იდენტიფიცირება და თვალყურის დევნება სესიის განმავლობაში. აღნიშნული ფუნქციის ფარგლებში შეუძლია აპლიკაციაში აუთენტიფიცირებული მომხმარებლების იდენტიფიცირება და თვალყურის დევნება.

31. სისტემას აქვს უსაფრთხოების პოლიტიკის დარღვევების კორელაციის შესაძლებლობა.

32. სისტემას აქვს სპეციალური IP რეპუტაციის ბაზის სერვისი, რომლის ფარგლებშიც სისტემას შეუძლია სხვადასხვა პოტენციურად მავნე მოთხოვნების ამოცნობა, მათი სიღრმისეული ანალიზის გარეშე. სერვისის ფარგლებში შეუძლია შემდეგი სახის ინფორმაციის დადგენა:

1. Anonymous Proxy.
2. GeoLocation.
3. IP Forensics.
4. Malicious IP addresses.
5. Phishing URLs.
6. TOR IP addresses.
7. Web Fraud Services.
8. სისტემას შეუძლია ინდივიდუალურად:

1. ამოიცნოს და შეაჩეროს პოტენციურად ე.წ. „Malicious IP" მისამართები.
2. ამოიცნოს და შეაჩეროს ე.წ. "Anonymous proxy" მისამართები.
3. ამოიცნოს და შეაჩეროს ე.წ. "TOR networks" მისამართები.
9. სისტემას შეუძლია მომხმარებლების ამოცნობა და შეჩერება ე.წ. "Geolocation" ინფორმაციის მიხედვით.
10. სისტემას შეუძლია მავნე რეპუტაციის ბაზის კატეგორიებიდან, კონკრეტული IP-ის, ქსელის ან ქვეყნის IP მისამართების ამოღება. აღნიშნული IP რეპუტაციის ბაზის განახლება უნდა ხდებოდეს ავტომატურ რეჟიმში მოთხოვნილი მხარდაჭერის სრულ პერიოდზე.

33) სისტემას აქვს DNS სერვისის დაცვის შესაძლებლობა:

1. წარმადობა წამში 200 000 (ორასი ათასი) მოთხოვნა.
2. DNS პროტოკოლის ინსპექტირება და ვალიდაცია.
3. გლობალური ტრაფიკის ბალანსირების შესაძლებლობა.
4. DNS სერვისზე შემდეგი ტიპის შეტევების აღმოჩენა და დაბლოკვა:

- DNS denial-of-service attacks.
- Cache Poisoning.
- DNS hijacking.

34) სისტემას აქვს სპეციალური ანგარიშის მოდული ანალიტიკური შესაძლებლობებით, რომელიც აფასებს დაცულობის დონეს სხვადასხვა უსაფრთხოების სტანდარტებთან მიმართებაში.
35) სისტემა არის სერტიფიცირებული "ICSA"-ის მიერ.
36) სისტემის მართვა და მონიტორინგი:
1. სისტემის მართვა შეიძლება როგორც ვებ ინტერფეისიდან ასევე „CLI"-ის მეშვეობით.
2. სისტემას შეუძლია მოთხოვნისამებრ რეპორტების გენერირება. რეპორტების გენერირება ასევე შეუძლია იყოს წინასწარ განსაზღვრული გრაფიკის მიხედვით.
3. სისტემას შეუძლია მომხდარი უსაფრთხოების ინციდენტების ლოგირება.
37) სისტემის შეუძლია ინტეგრაცია ქსელის ცენტრალიზებული მონიტორინგისა და შეტყობინებების შემგროვებელ სისტემებთან, შემდეგი ტექნოლოგიების საშუალებით:
1. SNMP.
2. Syslog.
3. SFlow.
4. Integration with leading SIEM vendors.
5. Email to data owners and other stakeholders.
6. Custom followed action.
7. Integrated graphical reporting.
8. Real-time dashboard.
9. Metadata and content-based via integration with third party Data Loss Prevention (DLP) vendors such as RSA, Websense, McAfee, and Symantec.
10. REST, SOAP API - მხარდაჭერა.
38) სისტემას აქვს აუდიტ ლოგირება და შეუძლია შემდეგი ლოგების ნახვა:
- Role based access controls to view audit data (read-only).
- Real-time visibility of audit data.

39) სისტემის მიმწოდებელი უზრუნველყოფს:
1. მიწოდებული მოწყობილობის არსებულ ვირტუალურ გარემოში ინსტალაციას.
2. არსებულ ქსელთან ინტეგრაციას.
3. ერთი ვებ სერვისისთვის WAF პოლიტიკის კონფიგურაციას.

შემოთავაზება მოიცავს გადაწყვეტილებისთვის მწარმოებლის ოფიციალური მხარდაჭერის და განახლებების სერვისებს 3 წლის ვადით.

BANK OF GEORGIA
BUSINESS

ხელშეკრულების შესრულების საბანკო გარანტია # PE73577973-22

29 მარტი 2022 წელი

საქართველო
გარანტი: სს საქართველოს ბანკი (შემდგომში „გარანტი“)
გარანტის საიდენტიფიკაციო კოდი: 204378869
გარანტის მისამართი: გაგარინის ქ. #29ა, თბილისი, 0160, საქართველო
პრინციპალი: შპს იუ-ჯი-თი (შემდგომში „პრინციპალი“)
პრინციპალის საიდენტიფიკაციო კოდი: 204892964
პრინციპალის მისამართი: საქართველო, თბილისი, ვაკის რაიონი, ჭავჭავაძის გამზირი, №17ა
ბენეფიციარი: სსიპ განათლების მართვის საინფორმაციო სისტემა (შემდგომში „ბენეფიციარი“)
ბენეფიციარის საიდენტიფიკაციო კოდი: 205300048
ბენეფიციარის მისამართი: ქ. თბილისის საბურთალოს რაიონი / ფანჯიკიძის ქ. 1ა
საგარანტიო თანხა: 7,198.05 (შვიდი ათას ას ოთხმოცდათვრამეტი და 50/1000) ლარი
ტენდერის უნიკალური ნომერი:SPA220000704

მხედველობაში ვიღებთ რა, რომ პრინციპალმა Web Application Firewall-ის შესყიდვის მიზნით წარდგენილი სატენდერო წინადადების შესაბამისად იკისრა ვალდებულება წარმოადგინოს საბანკო გარანტია მასზე დაკისრებული ვალდებულებების შესრულების გარანტიის სახით ხელშეკრულებაში მითითებულ თანხაზე, ჩვენ, გარანტი, თანახმა ვართ გავცეთ პრინციპალის სახელზე აღნიშნული უპირობო და გამოუთხოვადი საბანკო გარანტია.

ამასთან დაკავშირებით, ვადასტურებთ, რომ ვართ გარანტები და პასუხისმგებლები თქვენს წინაშე პრინციპალის სახელით საერთო თანხაზე, არაუმეტეს ჯამში 7,198.05 (შვიდი ათას ას ოთხმოცდათვრამეტი და 50/1000) ლარი და ვკისრულობთ ზემოთ აღნიშნული თანხის, გადახდას პრინციპალის მიერ ხელშეკრულების პირობების დარღვევის შემთხვევაში ბენეფიციარის წერილობითი მოთხოვნის წარმოდგენის საფუძველზე, მოთხოვნის მიღებიდან მომდევნო 5 (ხუთი) საბანკო დღის ვადაში.

ბენეფიციარის წერილობითი მოთხოვნა თანხის ანაზღაურებაზე წარმოდგენილ უნდა იქნეს ბენეფიციარის მხრიდან აღნიშნულ დოკუმენტზე უფლებამოსილი პირის მიერ ხელმოწერილი ფორმით, სადაც მითითებულ იქნება მოთხოვნილი თანხა ციფრობრივად და სიტყვიერად, საბანკო რ.კვიზიტები და განმარტებული უნდა იყოს კონკრეტულად პრინციპალსა და ბენეფიციარს შორის გაფორმებული ხელშეკრულების რა პირობები იქნა დარღვეული პრინციპალის მხრიდან. მოთხოვნას თან უნდა ერთვოდეს მოთხოვნაზე ხელმომწერი პირის უფლებამოსილების დამადასტურებელი დოკუმენტი (ბანკი უფლებამოსილია არ მოითხოვოს აღნიშნული საბუთი, თუ ხელმომწერი პირის უფლებამოსილების შესახებ ინფორმაცია საჯაროდ ხელმისაწვდომია) და საბანკო გარანტიის ასლი.

წინამდებარე გარანტია ძალაშია პრინციპალის მიერ ხელშეკრულების პირობების შესრულების საბოლოოდ დამთავრებამდე, მაგრამ არაუგვიანეს: 15 ივნისი 2022 წელი, შესაბამისად წინამდებარე გარანტია მოქმედებს აღნიშნული თარიღის ჩათვლით.

ზემოთქმულიდან გამომდინარე, ბენეფიციარის მიერ წარმოდგენილი წერილობით მოთხოვნის ორიგინალი დოკუმენტი თანხის ანაზღაურებაზე, გარანტის მიერ მიღებულ უნდა იქნას გარანტიის მოქმედების ვადის ჩათვლით სს "საქართველოს ბანკის" სათავო ოფისში, კანცელარიის სამსახურში ან/და კვალიფიციური ელექტრონული ხელმოწერითა და შტამპით (იმ შემთხვევაში თუ ბენეფიციარს წარმოადგენს ადმინისტრაციული ორგანო, მისაღებია მხოლოდ კვალიფიციური ელექტრონული შტამპი), ვაჭრობის სტრუქტურული დაფინანსების დეპარტამენტის საყურადღებოდ, თბილისის დროით (UTC / GMT +04: 00 საათი) 17:00 საათის ჩათვლით, შემდეგ მისამართზე: გაგარინის ქ.#29ა, თბილისი 0160, საქართველო.

საბანკო გარანტია ავტომატურად უქმდება/მცირდება ქვემოაღნიშნული გარემოებებიდან ერთ-ერთის დადგომისთანავე:

- საბანკო გარანტიის ვადის გასვლით;
- გარანტის მიერ ბენეფიციარისთვის იმ თანხის გადახდით, რომელზედაც გაიცა საბანკო გარანტია;
- ბენეფიციარის მიერ გარანტიიდან გამომდინარე თავის უფლებებზე წერილობით უარის თქმით;
- ბენეფიციარის მიერ საბანკო გარანტიის თანხის შემცირების შესახებ წერილობითი შეტყობინებით.

გარანტის მიმართ საბანკო გარანტიიდან გამომდინარე ბენეფიციარის კუთვნილი მოთხოვნის უფლების გადაცემა/დათმობა სხვა პირისათვის დაუშვებელია გარანტის წერილობითი თანხმობის გარეშე.

წინამდებარე საბანკო გარანტია რეგულირდება საქართველოს კანონმდებლობით.

თამარ ჭანტურიძე
ადგილობრივი გარანტიების მენეჯერი