აღნიშნულ ტექნიკურ დავალებაში მოცემულია სამუშაო სადგურების და სერვერების ვირუსული თუ სხვა ტიპის საფრთხეებისგან დაცვის პროგრამული უზრუნველყოფის ფუნქციონალური მოთხოვნები.

სამუშაო სადგურების დაცვის პროგრამული უზრუნველყოფის ტექნიკური დავალება

სამუშაო სადგურების მართვის კონსოლის ფუნქციონალი:

- მართვის ერთიანი კონსოლის მეშვეობით სისტემის ყველა კომპონენტის (მოდულის) მართვა;
- ადგილობრივი მონაცემთა ბაზის მომხმარებლებით და დომენური ანგარიშების მეშვეობით კონსოლის ოპერატორების აუთენტიფიკაცია;
- მართვის სისტემასთან დაშვების როლური მოდელი;
- კონსოლის ოპერატორების მოქმედებების ჟურნალირება (აღრიცხვა);
- სამუშაო სადგურებზე მომხდარი მოვლენების მიღება, დამუშავება და ჟურნალირება (აღრიცხვა);
- ჩაშენებულ მონაცემთა რეზერვირება Disaster Recovery-ის მეშვეობით;
- კონსოლში სისტემების სიის ფორმირება ჯგუფების მიხედვით, როგორც ხელით მართვის რეჟიმში, ასევე Active Directory სტრუქტურის სინქრონიზაციით;
- დაცვის მოდულების განვრცობა ავტომატურ და ხელით მართვის რეჟიმში;
- ფუნქციონირებადი (განვრცობილი) სისტემების მუშა მდგომარეობის მხარდაჭერა (პროგრამული უზრუნველყოფის და ანტივირუსული ბაზის განახლება, პოლიტიკების სინქრონიზაცია);
- სამუშაო სადგურების მდგომარეობის კონტროლი რეალური დროის რეჟიმში;
- მონაცემთა ვიზუალიზაციის გზით აღრიცხვის წარმოება;
- ცალკეული ჯგუფების და სისტემების დონეზე სხვადასხვა პოლიტიკების გამოყენება;
- დაცვის მოდულების განახლებასთან და კონტროლთან დაკავშირებული დავალებების დაგეგმვის ჩაშენებული მექანიზმი;
- ორგანიზაციის სტრუქტურის, ჯგუფების, ქვეჯგუფების დონეზე ცალკეული დავალებების განსაზღვრა;
- სამუშაო სადგურსა და კონსოლს შორის არაგეგმიური სეანსის ინიციალიზაცია;
- სისტემათა ჯგუფების დონეზე საბოლოო წვდომის წერტილსა და კონსოლს შორის კავშირის ინტერვალის დაკონფიგურირება;
- განახლების ძირითადი რეპოზიტორიების სარკეების შექმნა (LAN, HTTP, FTP);
- დიაგრამული ანგარიშების გენერირება სამუშაო სადგურებიდან მიღებული მონაცემებით;
- პოლიტიკების კატალოგის არსებობა, მათი კოპირების და სისტემათა სხვადასხვა ჯგუფზე მიბმა;
- ორ მართვის კონსოლს (მენეჯმენტ სერვერი) შორის მართვადი სისტემების ტრანსფერი და პოლიტიკების სინქრონიზაცია.

სამუშაო სადგურების დაცვის ფუნქციონალი:

- ყველა ტიპის ვირუსული საშიშროებისაგან (virus, worm, trojan, malware, adware, spyware, rootkits, bots და ა.შ.) დაცვის სიგნატურული და ევრისტიკული ანალიზი;
- ექსპლოიტების, საფრთხის შემცველი პროგრამების ქმედების ანალიზი და მათი ბლოკირება.
- აპლიკაციების, ფაილების და პროცესების მოქმედების უწყვეტი მონიტორინგი;
- ქსელის ტრაფიკის მონიტორინგი და კონტროლი, URL ფილტრაცია, ბროუზერიდან შეღწევა/დაინფიცირების რისკის აღმოფხვრა. დაცვა ინტერნეტ საფრთხეებისაგან, ვებ-გვერდების შემოწმება/ბლოკირება მავნე კოდების, ზიანის მომტანი ბმულების და საეჭვო ფიშინგ გვერდის შემთხვევაში. ვებ რესურსებზე წვდომის მართვა, დაბლოკილი ან ნებადართული ვებ-გვერდების სიის შექმნა;
- ვებ-გვერდების, ფაილების და აპლიკაციების რეპუტაციული ანალიზი, საჭიროების შემთხვევაში - დაბლოკვა. რეპუტაციისა და სანდოობის მიხედვით მათი დაჯგუფება და კლასიფიკაცია;
- ღრუბლოვანი ტექნოლოგიის გამოყენებით ფაილის რეპუტაციის შემოწმება;
- სიგნატურული და ღრუბლოვანი ანალიზის შედეგებისგან დამოუკიდებლად პროგრამის პოტენციურად საფრთხის შემცველი ქმედების ბლოკირება;
- სხვადასხვა აპლიკაციებში ინფორმაციული უსაფრთხოების კუთხით არსებული მოწყვლადობების (zero-day exploit) აღმოჩენა და დაცვა;
- უცნობი საფრთხეებისაგან ოპტიმიზირებული დაცვის ფუნქციონალი;
- ემულატორი, რომელიც ავტომატურ რეჟიმში პოტენციურად სახიფათო პროგრამის გაშვებამდელ ქცევით ანალიზს ახდენს შეუმჩნეველი საფრთხეების აღმოსაჩენად;
- MS Outlook-ში ელ-ფოსტის სკანირება;
- ანტივირუსული მოდულების პარამეტრების დაცვა ცვლილებისაგან ან წაშლისაგან პაროლის მეშვეობით;
- მომხმარებლის მიერ დაცვის მოდულების მუშაობის შეჩერებისას მუშაობის ავტომატური აღდგენა;
- შემოტევის აღმომჩენი სისტემა გაშვებული პროცესების მეხსიერების კონტროლით;
- შემოტევის აღმკვეთი სისტემის ფუნქციონალი (Host IPS) განახლებადი IPS სიგნატურებით;
- ქსელური ფაერვოლის მოდული წინასწარ განსაზღვრული პოლიტიკებით;
- სისტემის დროებითი საქაღალდეებიდან პროგრამების გაშვების აკრძალვა;
- სისტემურ საქაღალდეებში გამშვები ფაილების შექმნის აკრძალვა;
- საკუთარი წესების შექმნა სისტემის რეესტრის და ფაილური სისტემის დონეზე;
- სისტემური სერვისების მუშაობაში ანტივირუსის ჩარევის ბლოკირება;
- ფაილების სკანირება პროცესებზე მიმართვის დროს (On-Access Scan), წაკითხვისას და ჩაწერისას (მათ შორის ფაილის ჩრდილოვანი ასლების);
- ფაილების გეგმიური სკანირება, როგორც ცენტრალიზებულად დაგეგმილი, ასევე მომხმარებლის მიერ განსაზღვრული;

- სკანირების აჩქარებისათვის, სისტემის წინა სკანირების შესახებ ინფორმაციის შენახვა და ქეშის გამოყენება;
- ფაილებზე და სისტემის რეგისტრებზე აპლიკაციებისა და პროცესების დაშვების და ქცევის კონტროლი;
- ინფორმაციის პორტატული შემნახველების და სხვა მოწყობილობების ბლოკირება მოწყობილობების ტიპების ჩაშენებული კონტროლით;
- USB მოწყობილობების მონიტორინგი, მათი იძულებითი ბლოკირება ან Read-Only რეჟიმში გადაყვანა;

ოპერაციული სისტემების მხარდაჭერა:

- Microsoft Windows - 10;
- Windows Server – 2008, 2012, 2016;
- Mac OS X 12 და ზემოთ;
- RedHat 7.2
- Debian 8 Jessie
- Ubuntu 16.04 და ზემოთ
- SUSE Linux Enterprise Server (SLES) 11-12
- SUSE Linux Enterprise Desktop (SLED) 11 SP3
- CentOS 7
- Fedora
- Oracle Linux (OEL) 7

საფოსტო სერვერის დაცვის ფუნქციონალი:

- საფოსტო სერვერის (Microsoft Exchange Server) ანტივირუსული და ანტი-სპამ გადაწყვეტილება;
- საფოსტო წერილების ნაკადის სხვადასხვა ვირუსულ საფრთხეებზე შემოწმება;
- წერილების ბლოკირება, რომელთაც დანართებად გააჩნიათ გამშვები ფაილები ან დოკუმენტები, რომლებიც შეიცავს მაკროსს;

საფოსტო სერვერების მხარდაჭერა:

- Exchange 2016

შიფრაციის მოდულის ფუნქციონალი:

- Microsoft BitLocker და Apple FileVault შიფრაციის მართვა;
- Microsoft Windows სისტემებზე მყარი დისკის სექტორულ დონეზე შიფრაცია;
- ფაილების, საქაღალდეების და გარე მოწყობილებების ფაილურ დონეზე შიფრაცია;
- მოწყობილობათა კონტროლის მოდულთან ინტეგრაცია ფაილების ავტომატურ რეჟიმში შიფრაციის უზრუნველსაყოფად გარე მოწყობილობებზე ჩაწერისას;

- მობილური მოწყობილობების (iOS და Android) სისტემებზე ჩაშენებული შიფრაციის აქტივაცია;
- დაშიფრულ დოკუმენტებზე წვდომების გამიჯვნისათვის სხვადასხვა დეპარტამენტის თანამშრომლებს შორის შიფრაციის გასაღებების დელეგირება;
- გარე მოწყობილობების შიფრაცია, როგორც მომხმარებლის სურვილისამებრ ასევე აუცილებელ რეჟიმში;
- მობილური მოწყობილობებიდან (iOS, Android) დაშიფრულ ფაილებზე წვდომა;
- შიფრაციის წარმადობის გაზრდა AES-NI ტექნოლოგიის მხარდაჭერა.

ოპერაციული სისტემების მხარდაჭერა:

- Windows 10 Pro (32-bit და64-bit edition)
- Windows 10 Enterprise (32-bit და64-bit edition)
- Windows 10 Pro November Update (32-bit და64-bit edition)
- Windows 10 Enterprise November Update (32-bit და64-bit edition)
- Microsoft Windows 10 Pro Anniversary Update (32-bit და64-bit edition)
- Microsoft Windows 10 Enterprise Anniversary Update (32-bit და64-bit edition)
- Microsoft Windows 10 Pro Creators Update (32-bit და 64-bit)
- Microsoft Windows 10 Enterprise Creators Update (32-bit და 64-bit)
- Mac OS X 12 და უფრო მაღალი ვერსია;

ვირტუალური სერვერების დაცვის პროგრამული უზრუნველყოფის ტექნიკური დავალება

მართვის კონსოლის ფუნქციონალი:

- მოდულების განვრცობა, როგორც ავტომატურ ასევე ხელით მართვის რეჟიმში;
- სისტემების სიის ფორმირება ჯგუფებად, როგორც ხელით მართვის რეჟიმში, ასევე Active Directory სერვერთან სინქრონიზაციით;
- სხვადასხვა წყაროებიდან განახლების შესაძლებლობა: მართვის სერვერი, სარკე (WEB, FTP, SMB), ინტერნეტი;
- ანტივირუსული ბაზების ოფლაინ რეჟიმში განახლება;
- სისტემების ავტომატური სორტირება მათი ტიპებით, აპარატული რესურსებით და სხვა თვისებებით;
- პოლიტიკების განსაზღვრა ცალკეული სისტემების და სისტემათა ჯგუფების დონეზე;
- ადმინისტრირებასთან დაშვების როლური მოდელი, სხვადასხვა შაბლონების ფორმირებით;
- აუტენტიფიკაცია ლოკალური ბაზით და Active Directory-ის მომხმარებელთა ჩანაწერების გამოყენების შესაძლებლობა;
- მინიმუმ სამ განშტოებიანი პაკეტების მხარდაჭერა (მიმდინარე, წინა, სატესტო);
- სამუშაო სადგურებიდან მიღებული მონაცემებით გრაფიკების, დიაგრამების, ანგარიშების და ინფორმაციული შკალების აგება.
- დამატებითი დაცვის ფუნქციონალის გაზრდის შესაძლებლობა სამუშაო სადგურების მონაცემთა გაჟონვის და შეღწევადობის აღკვეთის მოდულთან, დინამიური და სტატიკური კოდის ანალიზის მექანიზმთან და გაძლიერებული ვებ-ფილტრაციასთან გამჭვირვალე ინტეგრაციით.

ანტივირუსული დაცვის ფუნქციონალი:

- ფაილებზე წვდომისას მათ სკანირება, წაკითხვისას, ჩაწერისას, ასევე მათი ჩრდილოვანი კოპიის შექმნისას;
- ფაილის საკონტროლო ჯამის რეპუტაციის ღრუბლოვანი ანალიზი;
- სიგნატურული და ღრუბლოვანი ანალიზის რეზულტატების მიუხედავად პროგრამის პოტენციურად სახიფათო ქმედების ბლოკირება (აპლიკაციების კონტროლი);
- წინა სკანირების შესახებ ინფორმაციის შენახვა და ქეშის გამოყენებით სკანირების აჩქარება;
- ანტივირუსული მოდულის კონფიგურაციაზე წვდომის პაროლით დაცვა;
- დაცვითი მოდულების გათიშვის შემთხვევაში მათი მუშაობის ავტომატურად აღდგენა.

ვირტუალიზირებული სისტემების ანტივირუსული აგენტის გარეშე დაცვის ფუნქციონალი:

- ერთიან მართვის კონსოლთან ინტეგრაცია;
- VMware 5.x – 6.0 ჰიპერვიზორის ქვეშ განვრცობილი ვირტუალიზირებული Windows სისტემების ანტივირუსული დაცვა;
- vShield მექანიზმით ვირტუალური სისტემის ფაილებზე წვდომა ანტივირუსული ოპერაციების განსახორციელებლად.
- შემოწმებულ ფაილთა საკონტროლო ჯამის რეპუტაციის ლოკალური ბაზის ფორმირება სკანირებულ სერვერებზე;
- სკანირებადი სერვერების ავტომატური განვრცობის NSX-ის მექანიზმებით მხარდაჭერა;
- ფაილთა საკონტროლო ჯამის დამატებითი შემოწმება ღრუბლოვანი რეპუტაციის ბაზაში (გარდა სიგნატურებისა);
- ჰიპერვიზორის ვირტუალური ინტერფეისების დონეზე ვირტუალიზირებულ სისტემებს შორის ტრაფიკის კონტროლისათვის ფაერვოლის ამოქმედება;
- როგორც წვდომაზე ასევე მოთხოვნაზე სკანირების აქტივაცია;
- დაარქივებული ფაილების შემოწმება;
- საფრთხის აღმოჩენისას განსხვავებული ქმედების განსაზღვრა - ცალკე წვდომაზე სკანირებისთვის და ცალკე მოთხოვნაზე სკანირებისთვის.
- ცალკეული ქსელური რესურსის კონფიგურირება როგორც კარანტინის;
- დროის მონაკვეთის მითითება, როდესაც წვდომაზე სკანირება შესაძლებელია.

ვირტუალიზირებული სისტემების ანტივირუსული აგენტით დაცვის ფუნქციონალი:

- ერთიან მართვის კონსოლთან ინტეგრაცია;
- VMware 5.x – 6.0, MS Hyper-V 2008 SP2, 2008R2, 2012 (R2), Citrix Xen Server 5.5 - 6.1, KVM ჰიპერვიზორების ქვეშ განვრცობილი ვირტუალიზირებული Windows სისტემების ანტივირუსული დაცვა;
- სპეციალური მოდულის მეშვეობით ფაილების შემოწმების ფუნქციის რეალიზაცია (არაკლასიკური ანტივირუსი);
- შემოწმებულ ფაილთა საკონტროლო ჯამის რეპუტაციის ლოკალური ბაზის ფორმირება, როგორც სერვერებზე ასევე საბოლოო წერტილების (სისტემების) დონეზე;
- ლოკალური კარანტინის მხარდაჭერა სისტემების დონეზე;
- ცალკე ჩაშენებული მოდულით დატვირთვის გადანაწილება;
- სიმძლავრის ოპტიმიზაციისათვის სკანირებად სერვერებზე Ram Disk-ის გამოყენება;
- ქსელურ დისკებზე შენახული ფაილების შემოწმება;
- დაარქივებული ფაილების შემოწმება;
- დროის მონაკვეთის მითითება, როდესაც წვდომაზე სკანირება შესაძლებელია.
- გარკვეული ფაილური გზებისა და პროცესებისთის გამონაკლისების ფორმირება;
- აღმოჩენილ საფრთხეებზე მომხმარებლის ინფორმირება.

ღრუბლოვანი ვირტუალიზაციის სერვისებთან ინტეგრაციის მოდულის ფუნქციონალი:

- ერთიან მართვის კონსოლთან ინტეგრაცია;
- Amazon AWS, Microsoft Azure, VMware vSphere და OpenStack ღრუბლოვანი სერვისების მხარდაჭერა;
- ერთიან მართვის კონსოლში ზემოთ ჩამოთვლილი ღრუბლოვანი სერვისების ანგარიშების რეგისტრაცია;
- საჯარო ან კერძო სერვისებზე მომუშავე ჩართული და გამორთული სისტემების შესახებ მონაცემთა სინქრონიზაცია.
- ერთიან მართვის კონსოლზე კონტროლირებული და დაცული სისტემების რაოდენობის მიხედვით ანგარიშების ფორმირება;

Amazon Elastic Block Storage (EBS)-ის დაცვის ცალკეული მოდულის ფუნქციონალი:

- ერთიან მართვის კონსოლთან ინტეგრაცია;
- Amazon Elastic Block Storage (EBS) საცავების იდენტიფიკაციის მხარდაჭერა;
- ახალი დაშიფრული საცავის შექმნა და მონაცემების გადატანა ახალ დაშიფრულ საცავში AWS API-ით.

სერვერებზე შეღწევის აღმომჩენი მოდულის ფუნქციონალი:

- ერთიან მართვის კონსოლთან ინტეგრაცია;
- სერვერული ოპერაციულ სისტემების შეღწევის აღმომჩენი სისტემა Web სერვერების სერვისების დაცვის მხარდაჭერით.
- სერვერული პლატფორმების მოწყვლადობის სიგნატურების არსებობა და მათი დროული განახლება;
- სერვერული ოპერაციული სისტემების და გაშვებული აპლიკაციების (Apache, Java, MySQL, CGI, PHP და სხვა) სისუსტეების (მოწყვლადობის) გამოყენების მცდელობის აღკვეთა.

მოთხოვნები პროდუქტის მწარმოებლის მიმართ:

- ყველა შემოთავაზებული პროდუქტი უნდა იყოს ერთი მწარმოებლის
- შემოთავაზებული პროგრამული უზრუნველყოფის მწარმოებელი იყოს ასევე DLP სისტემის მწარმოებელი და უნდა გააჩნდეს ინტეგრაციის შესაძლებლობა SIEM სისეტემბთან.
- ტექნოლოგიების დამოუკიდებელი საერთაშორის შემფასებლების უახლეს შეფასებებში “Magic Quadrant for Endpoint Protection Platform” უნდა იკავებდეს “ვიჟენარი” ან “ლიდერ” პოზიციებს

- ტექნოლოგიების დამოუკიდებელი საერთაშორის შემფასებლების უახლეს შეფასებებში “The Forester Wave Endpoint Security Suites” უნდა იკავებდეს “ძლიერი მონაწილე” ან “ლიდერ” პოზიციებს

მოთხოვნები პროდუქტის მიმწოდებლის მიმართ:

- პრეტენდენტმა კომპანიამ უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა ამ პროექტისთვის (MAF)
- უნდა ქონდეს განხორციელებული საქართველოში მინიმუმ 2 ანალოგიური პროექტი.
- სისტემის დანერგვის სამუშაოები უნდა განხორციელდეს ორგანოზაციის ტერიტორიაზე პროდუქტის მწარმოებლის მიერ სერთიფიცირებული ინჟინრის მიერ.
- სისტემის მხარდაჭერის მიზნით კომპნიას უნდა ყავდეს სერთიფიცირებული ინჟინრები

ლიცენზიების რაოდენობა:

- სამუშაო სადგური - 40 ლიცენზია (Endpoint Protection + Endpoint Encryption)
- ვირტუალური სერვერი - 40ლიცენზია (Protection for Virtual Servers)

თანმდევი მომსახურება

მიმწოდებელმა უნდა უზრუნველყოს შემდეგი თანმდევი მომსახურება:

1. მოწოდებული სისტემების ინსტალაცია და კონფიგურაცია უნდა შესრულდეს შემსყიდველის წარმომადგენლებთან ერთად. შემსყიდველის მხრიდან ქვემოთ მითითებულ თანამშრომლებს, მიმწოდებელმა უნდა გადასცეს ინსტალაციის, კონფიგურაციის და გამართული მუშაობის უზრუნველყოფისათვის აუცილებელი ცოდნა და შესაბამისი ელექტრონული მასალები:

a. კონფიგურაცია და ადმინისტრირება - 2 თანამშრომელი;

2. მოწოდებული სისტემების ინსტალაცია, კონფიგურაცია და საგარანტიო მომსახურება უნდა განხორციელდეს ქვემოთ მოცემულ ვადებში:

a. სისტემის ინსტალაცია, კონფიგურაცია - არაუგვიანეს ხელშეკრულების გაფორმებიდან 15 (თხუთმეტი) სამუშაო დღის ვადაში;

b. საგარანტიო და ტექნიკური მომსახურება - ხელშეკრულების გაფორმებიდან 1 წლის განმავლობაში; ინსტალაცია-კონფიგურირების სამუშაოები უნდა იწარმოებოდეს ქ.თბილისში, შემსყიდველის ტერიტორიაზე, მწარმოებლის სერტიფიცირებული ინჟინრების მიერ.