Trellix-ის მონაცემთა გაჟონვის პრევენციის (DLP) სისტემის შესყიდვის ტექნიკური დავალება

1.სისტემის დანერგვის მიზნები და მოცულობა

DLP სისტემის 1-წლიანი ლიცენზია, რომელიც იმუშავებს სხვა სისტემებისგან დამოუკიდებლად და მოახდენს ყველა იმ წინასწარ განსაზღვრული კონფიდენციალური დოკუმენტის მოძრაობის მონიტორინგს, რომლებიც ინახება სამუშაო სადგურებზე, ლეპტოპებში, USB ფლეშ მეხსიერებებზე, გაზიარებულ ფოლდერებში, სერვერებზე და მონაცემთა ბაზებში. ნებისმიერი ქმედებისას, რომელიც არღვევს არსებულ პოლიტიკას, უნდა იქნას ინიცირებული შესაბამისი შემთხვევა. აღნიშნული შემთხვევების მონიტორინგს მოახდენს ავტორიზებული პერსონალი.

DLP სისტემამ უნდა უზრუნველყოს საკომუნიკაციო არხების ფართო სპექტრის დაფარვა. სისტემა უნდა მოიცავდეს ინფორმაციის სამ მდგომარეობას (data at rest, data in motion, data in use) და ინტეგრირდებოდეს კომპანიაში არსებულ ცენტრალიზებული მართვის სისტემაში და EDR სისტემასთან. აგრეთვე DLP სისტემას უნდა შეეძლოს ქართულ და ინგლისურ ენებზე დაწერილი წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის დაცვა. პროდუქტს უნდა ჰქონდეს პოლიტიკის შექმნისა და მათი მართვის ფუნქციები: როგორც ჩაშენებული პოლიტიკების რედაქტირება/მორგების, ასევე სრულიად ახალი პოლიტიკების შექმნის შესაძლებლობა; აგრეთვე, სისტემას უნდა ჰქონდეს წინასწარ დაკონფიგურირებული ისეთი პოლიტიკები (წესები). სისტემას უნდა გააჩნდეს არსებული პოლიტიკებისა და კონფიგურაციის რეზერვირების და აღდგენის ფუნქციები.

სისტემის დანერგვის ძირითადი მიზანი:

- წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის უსაფრთხოების უზრუნველყოფა (data at rest, data in motion, data in use);
- წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის ქვემოთ ჩამოთვლილი არხებითა და პერიფერიული მოწყობილობებით მიზანმიმართული და შემთხვევითი გაჟონვის კონტროლი და მონიტორინგი.
- კორპორატიულ ქსელში არსებული წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის მდებარეობის დადგენა, მისი გამოყენების მონიტორინგი და არაავტორიზებული გავრცელება/გამოყენება/დამუშავებისგან დაცვა;
- წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის არაავტორიზებულ პირებზე გავრცელების კონტროლი და პრევენცია;
- კომპანიის საინფორმაციო სისტემებში წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის აღმოჩენა;

2.ძირითადი მოთხოვნები DLP სისტემისთვის

- სისტემის ყველა არსებული ფუნქციონალი უნდა იქნას გააქტიურებული;
- სისტემას უნდა გააჩნდეს ქართული უნიკოდის მხარდაჭერა;
- სისტემის დანერგვამ არ უნდა გამოიწვიოს სამუშაო სადგურების, სერვერებისა და ქსელური მოწყობილობების მწარმოებლურობის 15%-ზე მეტით შემცირება.
- DLP სისტემას უნდა ქონდეს ჩაშენებული კლასიფიკატორი

2.1 პოლიტიკის განსაზღვრა

- DLP სისტემას უნდა შეეძლოს ერთი პოლიტიკის ფარგლებში რეაგირების სხვადასხვა ქმედების უზრუნველყოფა, იმის და მიხედვით, თუ სად მდებარეობს სამუშაო სადგური - კორპორატიული ქსელის გარეთ თუ მის ფარგლებში;
- DLP სისტემას უნდა ჰქონდეს წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის აღმოჩენის ცენტრალიზებული პოლიტიკის შექმნის მხარდაჭერა, რომელიც გავრცელდება

ყველა ტიპის ინფორმაციაზე, რომელიც ინახება და მუშავდება სამუშაო სადგურებში, ქსელურ რესურსებზე და გადაიცემა ციფრული საკომუნიკაციო არხების საშუალებით;

- სისტემამ მომხმარებელი უნდა უზრუნველყოს წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის გადაცემის გაგრძელების შესაძლებლობით, მიუხედავად უსაფრთხოების პოლიტიკის დარღვევის შესახებ გაფრთხილებისა;
- DLP სისტემამ უნდა უზრუნველყოს მართვის ერთიანი, ცენტრალიზებული კონსოლი ყველა მისი კომპონენტისა და მოდულის, აღმოჩენისა და რეაგირების წესებისათვის.

2.2 აღმოჩენა

2.2.1 DLP სისტემამ უნდა გამოიყენოს წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის აღმოჩენის სხვადასხვა გზები, მათ შორის, როგორც მინიმუმ ქვემოთ ჩამოთვლილი მეთოდებზე დაფუძნებული ანალიზი:

- საკვანძო სიტყვებით (ქართული და ინგლისური ლექსიკონის გამოყენებით)
- საკვანძო სიტყვების წყვილით (ქართული და ინგლისური ლექსიკონის გამოყენებით);
- ე.წ. რეგულარული გამოხატვის (regular expression) საშუალებით;
- ფაილის ტიპისა და ზომის მიხედვით;
- სტრუქტურირებული ფაილების ციფრული ანაბეჭდით;
- არასტრუქტურირებული ფაილების ციფრული ანაბეჭდით.

2.2.2 DLP სისტემას უნდა შეეძლოს ფოტოდან ტექსტის ანალიზის ფუნქცია.

2.2.3 DLP სისტემას უნდა შეეძლოს აღმოაჩინოს, დააკლასიფიციროს, გადაიტანოს ან დააკოპიროს სენსიტიური ინფორმაცია.

2.2.4 DLP უნდა შეეძლოს აგენტის გარეშე firewall-თან ინტეგრაციის შედეგად გააკონტროლოს ინტერნეტის და მეილის ტრაფიკი.

2.2.5 DLP სისტემას უნდა შეეძლოს წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის აღმოჩენის პოლიტიკების აგება შემდეგი ლოგიკური ოპერატორების გამოყენებით: "AND", "OR", "NOT";

2.2.6 სისტემას უნდა ჰქონდეს შემდეგ მონაცემებზე დაყრდნობით წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის აღმოჩენის პოლიტიკების შექმნის შესაძლებლობა:

- დოკუმენტის შიგთავსი;
- გამგზავნი/მიმღები;
- ფაილის ატრიბუტები (ფაილის ტიპი, შიფრაცია)
- ინფორმაციის გადაცემის პროტოკოლი;
- მომხმარებლის ან ჯგუფის სახელი;
- სამუშაო სადგურის/სერვერის ადგილმდებარეობა ქსელში.

2.2.7 DLP სისტემას უნდა ჰქონდეს წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის აღმოჩენის პოლიტიკებში მეხსიერების USB მატარებლებისთვის გამონაკლისის დაშვების შესაძლებლობა;

2.2.8 სისტემას უნდა ჰქონდეს ფაილებზე დაფუძნებული სწავლების ფუნქციონალი, წინასწარ დახარისხებული ფაილების ჯგუფების გამოყენებით (წინასწარ განსაზღვრული კონფიდენციალური და არა-წინასწარ განსაზღვრული კონფიდენციალური);

2.2.9 სისტემას უნდა ჰქონდეს დაშიფრული და პაროლით დაცული დაარქივებული ფაილების იდენტიფიცირების შესაძლებლობა;

2.2.10 DLP სისტემას უნდა შეეძლოს ფაილების 300-ზე მეტი ტიპის ე.წ. „true file types” გარჩევა;

2.2.11 სისტემას უნდა ჰქონდეს ფუნქციონალი, განსაზღვროს ფაილის რაიმე ახალი, მოთხოვნაზე მორგებული (ე.წ. custom) ტიპი.

2.3 მახასიათებლები

2.3.1 ინსტრუმენტების მართვის პანელი და რეპორტინგი

შემოთავაზებული DLP სისტემა უნდა აგროვებდეს თითოეული იმ შემთხვევის შესახებ მონაცემებს, როდესაც ხდება წინასწარ განსაზღვრული კონფიდენციალური ინფორმაციის გადაწერა, ატვირთვა ან გაგზავნა. თითოეული ასეთი შემთხვევის შესახებ ინფორმაცია უნდა შეიცავდეს უშუალოდ იმ წინასწარ განსაზღვრული კონფიდენციალურ ინფორმაციასაც, რომლის გადაწერაც, ატვირთვაც ან გაგზავნაც ხდება.

ინსტრუმენტების მართვის პანელი უნდა უზრუნველყოფდეს ამ ინფორმაციაზე სწრაფ და მოსახერხებელ წვდომას. მას უნდა გააჩნდეს გრაფიკულად მრავალფეროვანი და მოთხოვნაზე მორგებული ინსტრუმენტები.

ინსტრუმენტების პანელს უნდა ჰქონდეს შემდეგი მახასიათებლების განსაზღვრის შესაძლებლობა:

- წესები და პირობები;
- როგორც ტექსტური, ასევე გრაფიკული ინტერფეისები დაშვების სხვადასხვა უფლებებით;
- ინსტრუმენტების პანელს უნდა ჰქონდეს სხვადასხვა მოთხოვნებზე მორგების შესაძლებლობა;
- ინსტრუმენტების პანელზე უნდა შეიძლებოდეს განსხვავებული როლებისათვის განსხვავებული ტიპის წვდომის უზრუნველყოფა;
- სისტემამ უნდა უზრუნველყოს დროთა განმავლობაში ინციდენტების შესახებ გრაფიკის აგება;
- სისტემამ უნდა უზრუნველყოს მომხდარი ინციდენტების რაოდენობების დიაგრამების აგება, რომლებიც შეიძლება გაიფილტროს თარიღის დიაპაზონის, ინციდენტის სიმძიმის, სტატუსისა და პოლიტიკის მიხედვით;
- სისტემას უნდა შეეძლოს მონაცემების ექსპორტი რეპორტინგის და ანგარიშგების სხვა სისტემებში;
- სისტემას უნდა გააჩნდეს გამოვლენილი ინციდენტებისათვის შემდეგი ინფორმაციის თანდართვის შესაძლებლობა: პოლიტიკის დამრღვევი მომხმარებლის საკონტაქტო მონაცემები, მისი დეპარტამენტის ხელმძღვანელის საკონტაქტო მონაცემები და სხვა. აგრეთვე, ტექსტური ან ნებისმიერი სხვა ისეთი ფორმატის ფაილის თანდართვის შესაძლებლობა, რომელიც შეიძლება იქნას გაანალიზებული სკრიპტული ენების საშუალებით;
- სისტემას უნდა შეეძლოს საკუთრივ DLP სისტემის მონაცემების გაერთიანება სხვა შესაბამის მონაცემებთან, რათა შემდგომი ანალიზისთვის საბოლოო რეპორტები ერთიან კონტექსტში იქნას მიღებული.
- DLP სისტემას უნდა ჰქონდეს მარტივი და ამავდროულად მაღალი დონის რეპორტინგის სისტემა. მას უნდა ჰქონდეს შემდეგი მახასიათებლების მხარდაჭერა:
  - მონაცემების ისეთი ფორმატის გარე ფაილებში ექსპორტი, როგორებიცაა CSV, PDF ან სხვა.
  - რამდენიმე კრიტერიუმზე დაფუძნებული რეპორტების გენერირება;
  - რეპორტების შემუშავებისა და გენერირების შესაძლებლობა;
  - რეპორტების რამდენიმე ადრესატთან ელექტრონული ფოსტით გაგზავნის დაგეგმვის შესაძლებლობა.

2.3.2 ინციდენტების მართვა

სისტემას უნდა გააჩნდეს:

- ინციდენტებზე რეაგირების დაკონფიგურირების შესაძლებლობა, რომელიც მართვის ცენტრალიზებულ სისტემას საშუალებას მისცემს კონკრეტული ინციდენტები შესაბამის მხარეებთან გადაამისამართოს (დარღვევის ტიპის, სიმკაცრის, მომხმარებლის ვინაობის და სხვა ფაქტორების გათვალისწინებით);
- ინციდენტების რეპორტში იმის ნათლად ჩვენება, თუ როგორ დაარღვია ფაილის გადაცემამ არსებული პოლიტიკა. აგრეთვე, უფრო ზუსტი აღრიცხვიანობისა და მომავალში მსგავსი დარღვევების პრევენციისათვის, იმის ჩვენებაც თუ ფაილის შიგთავსის რომელი კონკრეტული ნაწილი გახდა პოლიტიკის დარღვევის მიზეზი;
- ინფორმაციის გამგზავნის ვინაობის (სახელი, გვარი, ხელმძღვანელის სახელი, სტრუქტურული ერთეული) და ფაილის გადაცემის დანიშნულების (ინფორმაცია აიტვირთა ბლოგზე) ნახვის შესაძლებლობა, რათა მოხდეს შესაბამისი ინციდენტის აღმოფხვრა;
- ინციდენტების გარკვეული ჯგუფის აღმოფხვრისათვის კონკრეტული მომხმარებლის იდენტიფიცირების საშუალება, რათა შესაბამისმა პიროვნებამ შეძლოს ინციდენტის მართვა;
- ახალი ინციდენტების აღმოჩენის შემთხვევაში ინციდენტის მართვაზე პასუხისმგებელი პირებისთვის ავტომატური შეტყობინებების გენერირების საშუალება;
- დაჯგუფებული ინციდენტების ისეთ ფორმატში ექსპორტის შესაძლებლობა, რომელიც წაკითხვადი იქნება სისტემაზე წვდომის არ მქონე პირისთვის;
- კონკრეტულ ბიზნეს პროცესზე მორგებული ატრიბუტების დამატების შესაძლებლობა;
- სისტემას უნდა შეეძლოს დაინტერესებული მხარეებისთვის (Active Directory-ს მიხედვით უშუალო ხელმძღვანელი და ა.შ.) ინციდენტის შესახებ შეტყობინების გაგზავნა;
- სისტემას უნდა შეეძლოს ინციდენტის ესკალაციის ავტომატური შეტყობინების გაგზავნა;
- სისტემას უნდა ჰქონდეს განსხვავებული, მოთხოვნაზე მორგებული (custom) შეტყობინების მხარდაჭერა თითოეული პოლიტიკისთვის;
- სისტემას უნდა შეეძლოს მომხდარი ინციდენტების მომხმარებლებზე ან მომხმარებელთა ჯგუფებზე მიბმა Active Directory-ს საშუალებით;
- სისტემას უნდა შეეძლოს ინციდენტში დაფიქსირებულ წინასწარ განსაზღვრულ კონფიდენციალურ ინფორმაციაზე დაშვების კონტროლი.

2.3.3 თავსებადობა და ინტეგრაცია

DLP სისტემა უნდა იყოს თავსებადი და შეეძლოს ინტეგრირება ყველა ქვემოთ ჩამოთვლილ სისტემასთან:

- MS Active Directory-სთან და DNS სერვისებთან, იმისათვის რომ შეძლოს IP მისამართის უშუალოდ მომხმარებელთან დაკავშირება და რეალურ დროში პოლიტიკის დამრღვევი მომხმარებლის იდენტიფიცირება;
- სპამის ფილტრაციის სისტემებთან MTA რეჟიმში მუშაობის შესაძლებლობა.
- Firewall-ებთთან ინტეგრაცია ICAP პროტოკოლის საშუალებით
- SIEM სისტემებთან ინტეგრაცია;
- MS Exchange Server და MS Outlook 2013, 2016, 2019
- მონაცემთა ბაზები: Microsoft SQL Server 2012 ან უფრო ახალი ვერსია, MySQL (Enterprise) version 5.0.x ან უფრო ახალი ვერსია, Oracle 10 g ან უფრო ახალი ვერსია.
- დესკტოპებისა და სერვერების ვირტუალიზაციის ცნობილ სისტემებთან: Hyperv, VMware, Citrix და ა.შ

2.3.4 აგენტის მახასიათებლები

- სისტემამ უნდა განახორციელოს მომხმარებლების სამუშაო სადგურების კონტროლი და მონიტორინგი შემდეგი ოპერაციული სისტემებისთვის: Windows 8.1, Windows 10 ან უფრო ახალ ვერსიებზე; Windows Server 2012 R2, Windows Server 2016 R2, Windows Server 2019 R2 ან უფრო ახალ ვერსიებზე;
- სისტემას უნდა შეეძლოს ლეპტოპების ლოკალური დისკების სკანირება;
- სისტემას უნდა შეეძლოს აგენტების მდგომარეობის მონიტორინგი და სერვისის გათიშვისგან დაცვა მაშინაც კი, როდესაც მომხმარებელი ადმინისტრატორის უფლებებითაა აღჭურვილი;
- DLP სისტემას უნდა შეეძლოს რეალურ დროში მონიტორინგის ჩატარება და მონაცემთა გაჟონვის ქვემოთ ჩამოთვლილ არხებში მონაცემთა გადინების შეჩერება, როგორც სერვერის, ასევე სამუშაო სადგურის მხარეს:
  - ელ. ფოსტა;
  - ინფორმაციის სხვადასხვა მატარებელზე გადაწერა (USB, SD/CF ბარათები და ა.შ.)
  - ინფორმაციის CD/DVD მატარებლებზე გადაწერა;
  - დოკუმენტების ლოკალურ და ქსელურ პრინტერებზე ამობეჭდვა;
  - მონაცემების გადაცემა შემდეგი პროტოკოლების და სერვისების გამოყენებით: HTTP, HTTPS, FTP, SFTP, IM;ინფორმაციის გადაცემა საერთო ქსელურ რესურსებში;
  - ინფორმაციის ნაკადის კონტროლი სამუშაო სადგურებზე დაინსტალირებული აპლიკაციების საშუალებით;

3. მოთხოვნები მომწოდებელ კომპანიის მიმართ:

3.1 მომწოდებელი კომპანია უნდა იყოს რეგისტრირებული საქართველოში.

3.2 მომწოდებელი კომპანია უნდა იყოს შემოთავაზებული პროდუქტის მწარმოებლის ოფიციალური პარტნიორი და უნდა წარმოადგინოს ავტორიზაციის ფორმა ამ კონკრეტული შესყიდვისთვის (MAF).

3.3 მომწოდებელ კომპანის უნდა ჰყავდეს შემოთავაზებული ვენდორის მინიმუმ 1 ქართულენოვანი სერთიფიცირებული ინჟინერი.

3.4 მომწოდებელ კომპანიას უნდა ჰქონდეს დანერგილი მინიმუმ 1 ანალოგიური პროექტი, ბოლო 5 წლის განმავლობაში.

3.5 მომწოდებელი კომპანიას უნდა ჰქონდეს ბაზარზე ოპერირების მინიმუმ 10 წლიანი გამოცდილება.

3.6 მომწოდებელ კომპანიას უნდა გააჩნდეს შესაძლებლობა დამკვეთს გაუწიოს ლოკალური მხარდაჭერის (ქართულ ენოვანი სერტიფიცირებული ინჟინრის ჩართულობით) მომსახურება ასეთის მოთხოვნის შემთხვევაში.

მომწოდებლემა კომპანიამ შემოთავაზება უნდა წამოადგინოს დანართ#1-ში მითითებული ინფორმაციის მიხედვით.

დანართი #1

N	Trellix პროდუქტის დასახელება და აღწერა	Trellix პროდუქტის პარტ.ნომერი	ერთეულის ღირებულება	რაოდენობა	ჯამი
1	Trellix Data Loss Prevention Endpoint Complete - Subscription	DLPECE-AT		1010	
2	Trellix Data Loss Prevention OCR (Add-on) - Subscription	OCRECE-AT		1010	
3	Trellix Data Loss Prevention Discover - Subscription	DDSECE-AT		1010	
4	Trellix Data Loss Prevention Network Prevent - Subscription	DPVECE-AT		1010	
ჯამური ფასი დოლარში დღგ-ს გათვალისწინებით:					