**შესასყიდი საქონლის მოკლე აღწერა**

**შესასყიდი მომსახურების დასახელება და მოცულობა**

Log-ების მართვის სისტემის (SIEM)+ აუთსორსინგი

**შესრულების ვადები:**

მიმწოდებელმა უნდა უზრუნველყოს სერვისის მიწოდება 1 წლის ვადით

**მოთხოვნები საქონლის მიმართ**

მიწოდებული სერვისს უნდა გააჩნდეს შემდეგი შესაძლებლობები:

* შეეძლოს შემდეგი წყაროებიდან Log-ების მიღება და დამუშავება - FortiNet FortiAnalyzer, Active Directory, graylog, Web applications, Databases,E-mail server,DNS, Windows security logs
* შესაძლებლობა ჰქონდეს მოხდეს არასაჭირო ლოგების დადროპვა (უარყოფა)
* ლოგების შენახვის ვადა - 1 წელი
* მონიტორინგის ვადა - 24x7
* ინციდენტების კატეგორიზაციის შესაძლებლობა: მაღალი, საშუალო, დაბალი.
* ინციდენტის ან საეჭვო ქმედების რეპორტინგი GWP-ში.
* ყოველთვიური რეპორტინგი

**მოთხოვნები საგარანტიო ვადის და (ან) მისაწოდებელი უფლებების ხარისხის უზრუნველყოფის მოცულობის მიმართ.**

მომწოდებელმა უნდა უზრუნველყოს 1 წლით

|  |
| --- |
|  |
|  |
|  |