

SIEM QRADAR სისტემის იმპლემენტაციის ტექნიური დავალება

აღნიშნული ტექნიკური დავალება მიზნად ისახავს სახელმწიფო სერვისების განვითარების სააგენტოში არსებული ელექტრონული მონაცემების შეგროვების და ანალიზის სისტემის (შემდგომში SIEM სისტემა) იმპლემენტაციის (ინსტალაცია და კონფიგურაცია) სამუშაოების შესყიდვას.

სერვისების განვითარების სააგენტოში დღეისათვის ფუნქციონირებს კომპანია IBM-ის მიერ წარმოებული QRADAR SIEM სისტემა.

მიმწოდებელმა ხელშეკრულების გაფორმებიდან 10 სამუშაო დღის ვადაში უნდა უზრუნველყოს შემდეგი სამუშაოების შესრულება:

- 1.1 სააგენტოში არსებული QRADAR SIEM სისტემის განახლება და წარმადობის პრობლემების აღმოფხვრა;
- 1.2 QRADAR SIEM სისტემის კონფიგურაციის ოპტიმიზაცია;
- 1.3 შემდეგი Log Sources ჩართვა SIEM სისტემაში

Servers and Services:

დასახელება	რაოდენობა
VMware ESXi 6.7	12
Microsoft Windows Server 2012, 2016	10
Microsoft Active Directory	3
Microsoft Exchange Server	1
Microsoft SQL Server	4
Symantec Backup exec 2014	1
SEP Server	1
SMG server	1
IIS (Internet Information Services)	10
Linux Servers	12
Oracle, Linux Server	2
JBOSS Server	6
OpenVPN Server	1

Firewalls and Load Balancers

დასახელება	რაოდენობა
Cisco Firepower Firewall	3
CheckPoint Firewall	1
Citrix WAF	3

Cisco Routers

დასახელება	რაოდენობა
Router ASR 1001-X	4
Cisco R3945E	3
Cisco R3925E	1
Cisco R3925	1

სპეციალიზირებული აპარატურა

დასახელება	რაოდენობა
HSM	7
NYP Servers	2

- 1.4 არსებული Vulnerability scanner-ის კონფიგურაცია და საწარმო გარემოში გაშვება;
- 1.5 შემომავალი ხდომილებების ოპტიმიზაცია და მოთხოვნების თანახმად კორელაცია;
- 1.6 შემდეგი მოდულების ინსტალაცია და კონფიგურაცია:
 - ✓ User Behavior Analytics for Qradar -
<https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:UserBehaviorAnalytics>
 - ✓ IBM Security QRadar Network Visibility -
<https://exchange.xforce.ibmcloud.com/hub/extension/67f3b6c65131fc63a7e5ec5092d00050> ;
 - ✓ IBM QRadar Custom Properties for Symantec Endpoint Protection -
<https://exchange.xforce.ibmcloud.com/hub/extension/5b081018661ebd281c91a73736b4c9a6>;
 - ✓ IBM QRadar Custom Properties for Checkpoint -
<https://exchange.xforce.ibmcloud.com/hub/extension/2ab04201e22575e6b7323b8792d333e8> ;