**ტექნიკური დავალება**

**საინფორმაციო უსაფრთხოების ინციდენტების მონიტორინგისა და მართვის სისტემის ტექნიკური აღწერა (SIEM)**

**მოთხოვნები SIEM-ის მიმართ**

სისტემა უნდა წარმოადგენდეს პროგრამულ პაკეტს. SIEM უნდა ახორციელებდეს მოვლენების შეგროვებას საკუთარი პროგრამული ხელსაწყოების (ე.წ. შემგროვებლების) მეშვეობით, სხვა მწარმოებლის რაიმე გადაწყვეტილების გამოყენების გარეშე. შემგროვებლის ამოცანას წარმოადგენს საინფორმაციო წყაროდან მოვლენების (LOG) შეგროვება, მათი ნორმალიზება შესაბამის ფორმატში ყველა საჭირო ველების მითითებითა (Source/Destination IP, Host, Username, Device Vendor და ა.შ.) და პირველადი მოვლენის სრული შემადგენლობის შენარჩუნებით მათი სისტემაში გადაცემა.

შემგროვებელს უნდა ჰქონდეთ მინიმუმ შემდეგი მეთოდების მხარდაჭერა:

* ტექსტური ფაილიდან წაკითხვა;
* WMI;
* Syslog;
* SNMP;
* ხდომილებების მონაცემთა ბაზიდან წაკითხვა JDBC ან ODBC დრაივერების მეშვეობით;
* XML;
* IP Flow (NetFlow, J-Flow);
* IPFIX;
* sFlow

შემგროვებელს უნდა ჰქონდეთ შემდეგი სისტემების მხარდაჭერა:

* სერვერული სისტემები - Microsoft Servers (Windows, AD, Exchange,), Linux , DNS & DHCP, VmWare ESXi
* ვებ სერვერები - Microsoft IIS, Apache და სხვები
* ქსელური მოწყობილობები - Cisco, Dell, Aruba, Fortinet, Palo Alto, CheckPoint, Barracuda, F5 და სხვები
* მონაცემთა ბაზები - Microsoft SQL, MySQL, Oracle და სხვები

**SIEM** სისტემების/მოდულების ფუნქციონალში უნდა შედიოდეს:

1. მოვლენების ანალიზი და კორელაცია რეალურ დროში (დაყოვნება არაუმეტეს 1წმ-მდე), შემდეგი პარამეტრებით:
* სისტემას უნდა შეეძლოს არანაკლებ 1000 მოვლენის წამში (EPS) მიღება და დამუშავება,

**SIEM**-ის ლიცენზირების მოდელი

შემოთავაზებული პროდუქტი უნდა წარმოადგენდეს ე.წ. მუდმივ ლიცენზიას(Perpetual License) ყოველწლიური განახლების ფუნქციით.

**მომწოებელმა უნდა უზრუნველყოს შემდეგი თანმდევი მომსახურება:**

1. SIEM სისტემის ინსტალაცია და კონფიგურაცია;
2. საინფორმაციო რესურსების მიერთება SIEM სისტემასთან;
3. კორელაციის პირველადი წესების ჩამოყალიბება და კონფიგურაცია;
4. პირველადი რეპორტების გენერაცია;
5. საგარანტიო და ტექნიკური მოსახურება ხელშეკრულების გაფორმებიდან 1 წლის განმავლობაში.

**საგარანტიო პირობები:**

* წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს მინიმუმ 1 წლიანი საგარანტიო მომსახურება მის ყველა კომპონენტზე;
* საგარანტიო მომსახურება უნდა ხორციელდებოდეს მომწოდებლის მიერ;
* წარმოდგენილ SIEM სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის მხარდაჭერა.
* პრეტენდენტს უნდა ქონდეს SIEM სისტემების დანერგვის გამოცდილება, რის შესაბამისადაც უნდა წარმოადგინოს ინფორმაცია რომლითაც დასტურდება, რომ ანალოგიური გადაწყვეტილება დანერგილი აქვს მინიმუმ სამ ორგანიზაციაში საქართველოს ტერიტორიაზე
* პრეტენდენტს უნდა ჰყავდეს შემოთავაზებული პროდუქტის, მწარმოებლის მიერ, სერტიფიცირებული მინიმუმ ერთი თანამშრომელი. დამადასტურებელ დოკუმენტად პრეტენდენტმა უნდა წარმოადგინოს მის თანამშრომელზე მწარმოებლის მიერ გაცემული სერტიფიკატი.

**შენიშვნა:**

ინფორმაცია ანგარიშსწორების პირობის შესახებ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ინფორმაცია მიწოდების ვადის შესახებ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

პრეტენდენტის ხელმოწერა: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_