VULNERABILITY MANAGEMENT SOLUTION

გადაწყვეტილების და შესაბამისი მხარდაჭერის და განახლებების სერვისის შესყიდვის ტენდერი

საკონტაქტო ინფორმაცია

მარიამ ტაბატაძე

tenders@gc.ge

+995 577 331197

აბსტრაქტი

წინამდებარე დოკუმენტი მოიცავს, - სს ჯორჯიან ქარდის განცხადებას პროდუქტის შესყიდვის წინადადებების მოთხოვნის შესახებ. დოკუმეტი მოიცავს შესყიდვის პროცედურას, სადაც ორგანიზაციის მოთხოვნები შესაძლოა აღწერილი იყოს როგორც (ზოგადი) კონცეფტუალური პრინციპით, ისე ფუნქციური და შედეგზე ორიენტირებული სპეციფიკაციებით, - შედეგის მიღწევის კონკრეტული გზის (დეტალური ტექნიკური სპეციფიკაციების) მითითების გარეშე.

დეტალები

ტენდერის # 24 გამოცხადების თარიღი: 14.06.2024

დასრულების თარიღი: 21.06.2024 14:00:00

სარჩევი

[ტენდერში მონაწილეობის ინსტრუქცია: 2](#_Toc73369513)

[დავალებათა აღწერილობა 2](#_Toc73369514)

[სატენდერო მოთხოვნები 2](#_Toc73369515)

[თანდართული დოკუმენტაცია 3](#_Toc73369516)

[დანართი 1: ფასების ცხრილი 4](#_Toc73369517)

[დანართი 2: საბანკო რეკვიზიტები 5](#_Toc73369518)

[დანართი 3: გადაწყვეტილების მახასიათებლები 6](#_Toc73369519)

დანართი 3: გადაწყვეტილების მახასიათებლები 7

სს ჯორჯიან ქარდი (ს/კ 204396377) აცხადებს ტენდერს - უსაფრთხოების მოწყვლადობების სკანირების და მართვის გადაწყვეტილების და მასთან დაკავშირებული მხარდაჭერის და განახლებების გამოწერის - ე.წ. “Subscription” სერვისების შესყიდვაზე.

ტენდერში მონაწილეობის ინსტრუქცია:

* ტენდერის ფარგლებში პრეტენდენტებმა სისტემაში უნდა ატვირთონ სატენდერო მოთხოვნებით გათვალისწინებული დოკუმენტები;
* ტენდერის ეტაპზე დამატებითი ინფორმაციის მოპოვება ან დაზუსტება შესაძლებელია საკონტაქტო პირთან დაკავშირების საფუძველზე, - საწყის გვერდზე მითითებული ელექტრონული ფოსტის ან ტელეფონის საშუალებით;
* ტენდერის დასრულების შემდეგ სატენდერო კომისია განიხილავს შეთავაზებებს და გამოავლენს საუკეთესო პირობების მქონე მომწოდებელს;
* ტენდერში მონაწილემ უნდა წარმოადგინოს პროგრამული უზრუნველყოფის მომსახურების ჯამური ფასი;
* ტენდერში მონაწილემ უნდა წარმოადგინოს შემოთავაზებული პროდუქტის პრეზენტაციის და ე.წ. „datasheet“ ფაილები;
* სატენდერო წინადადება წარმოდგენილი უნდა იყოს ***აშშ დოლარში;***
* პრეტენდენტის მიერ ასატვირთი ყველა დოკუმენტი და ინფორმაცია დამოწმებული უნდა იყოს უფლებამოსილი პირის ხელმოწერითა და ბეჭდით;
* ტენდერში მონაწილეობის მისაღებად აუცილებელია ორგანიზაციამ წარმოადგინოს შემდეგი სავალდებულო დოკუმენტაცია:
  + შემოთავაზებული ფასების ცხრილი (**დანართი 1**);
  + საბანკო რეკვიზიტები (**დანართი 2**);
  + გადაწყვეტილების მახასიათებლები (ივსება მხოლოდ საჭიროების შემთხვევაში) (**დანართი 3**)
  + ამონაწერი სამეწარმეო რეესტრიდან;
  + MAF [Manufacturer Authorization Form] ფორმა, რომელსაც მწარმოებელი აძლევს პარტნიორ კომპანიებს (reseller) იმის დასტურად რომ ნამდვილად არიან მწარმოებლის მიერ აკრედიტირებული პარტნიორები;
* ტენდერის განმავლობაში პრეტენდენტს აქვს ვალდებულება მოთხოვნისამებრ წარმოადგინოს დამატებითი იურიდიული თუ ფინანსური დოკუმენტი;
* წარმოდგენილი წინადადება ძალაში უნდა იყოს მინიმუმ 90 კალენდარული დღის განმავლობაში;

დავალებათა აღწერილობა

შესასყიდი გადაწყვეტილების მახასიათებლების დეტალური აღწერა მოცემულია დანართი 3-ში.

სატენდერო მოთხოვნები

პრეტენდენტის წინააღმდეგ არ უნდა მიმდინარეობდეს გადახდისუუნარობის საქმის წარმოება და პრეტენდენტი არ უნდა იყოს ლიკვიდაციის / რეორგანიზაციის პროცესში.

პრეტენდენტ ორგანიზაციას უნდა ჰქონდეს შესაბამისი მომსახურების გაწევის მინიმუმ **3** (**სამი**) წლიანი გამოცდილება.

პრეტენდენტმა უნდა წარმოადგინოს კომპანიის საქმიანობის შესახებ ინფორმაცია, საქმიანობის მოკლე აღწერილობა (გამოცდილება, კლიენტების სია) და **მსგავსი ტიპის მომსახურების მინიმუმ ორი ხელშეკრულების წარმატებით დასრულების დამადასტურებელი დოკუმენტი (ხელშეკრულება და მიღება-ჩაბარების აქტი) რომელიც განხორციელებული უნდა იყოს ბოლო 5 (ხუთი) წლის განმავლობაში**;

პრეტენდენტმა MAF [Manufacturer Authorization Form] ფორმასთან ერთად, უნდა წარმოადგინოს პარტნიორობის დამადასტურებელი სხვა დოკუმენტებიც - ასეთის არსებობსი შემთხვევაში.

წინამდებარე ტენდერის გამოცხადება არ ავალდებულებს სს „ჯორჯიან ქარდ“-ს რომელიმე მონაწილესთან ხელშეკრულების გაფორმებას და ტენდერის ნებისმიერ ეტაპზე სს „ჯორჯიან ქარდი“ იტოვებს უფლებას რომ შეწყვიტოს ტენდერი.

თანდართული დოკუმენტაცია

* + დანართი 1: ფასების ცხრილი
  + დანართი 2: საბანკო რეკვიზიტები
  + დანართი 3: გადაწყვეტილების მახასიათებლები (ივსება მხოლოდ საჭიროების შემთხვევაში)

დანართი 1 - ფასების ცხრილი

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N** | **პროდუქტი/მომსახურების დასახელება** | **სპეციფიკაცია** | **რაოდენობა** | **მიწოდების ვადა** | **ღირებულება** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |
| **4** |  |  |  |  |  |

დანართი 2: საბანკო რეკვიზიტები

|  |  |
| --- | --- |
| ინფორმაცია პრეტენდენტი ორგანიზაციის შესახებ | |
| ორგანიზაციის დასახელება: |  |
| საიდენტიფიკაციო კოდი: |  |
| იურიდიული მისამართი: |  |
| ფაქტიური მისამართი: |  |
| ხელმძღვანელის სახელი და გვარი: |  |
| ხელმძღვანელის პირადი ნომერი: |  |
| ხელმძღვანელის ტელეფონის ნომერი: |  |
| საკონტაქტო პირის სახელი და გვარი: |  |
| საკონტაქტო პირის პირადი ნომერი: |  |
| საკონტაქტო ტელეფონი: |  |
| ელექტრონული ფოსტის მისამართი: |  |
| ვებ-გვერდი: |  |
| ბანკის დასახელება: |  |
| ბანკის კოდი: |  |
| ბანკის ანგარიშის ნომერი: |  |

დანართი 3: გადაწყვეტილების მახასიათებლები

შემოთავაზებული გადაწყვეტილება უნდა წარმოადგენდეს უსაფრთხოების მოწყვლადობების სკანირების და მართვის გადაწყვეტილებას და მასთან დაკავშირებულ მხარდაჭერის და განახლებების გამოწერის, ე.წ. “Subscription” სერვისს, რომელიც გამოყენებადი იქნება სულ მცირე ერთი წლის (12 თვე) ვადით.

გადაწყვეტილება უნდა აკმაყოფილებდეს ქვემოთ ჩამოთვლილ მოთხოვნებს და შესაბამისად შეფასდება შემდეგი კრიტერიუმებით:

**Requirements for Vulnerability Management Solution Acquisition**

**Core Requirements**

1. **Compliance Capabilities:**
   * **PCI DSS Compliance:** The solution must meet all requirements for vulnerability scanning as per PCI DSS (the solution must meet all scanning capabilities and requirements defined by PCI DSS v4.0).

**Note**: The bidder must demonstrate how the offered solution can address vulnerability scanning and management requirements defined by PCI DSS v4.0 by mapping the solution’s features to specific requirements from the standard.

* + **PCI 3DS Compliance:** The solution must adhere to the specific scanning and vulnerability management requirements outlined in PCI 3DS (the solution must meet all scanning capabilities and requirements defined by PCI 3DS v1.0).

**Note**: The bidder must demonstrate how the offered solution can address vulnerability scanning and management requirements defined by PCI 3DS v1.0 by mapping the solution’s features to specific requirements from the standard.

1. **Scanning Capabilities:**
   * **Authenticated Scanning:** The solution should support authenticated scanning to provide a comprehensive view of vulnerabilities within systems and applications.
   * **Web Application Scanning:** Must include capabilities for scanning web applications for common vulnerabilities (e.g., OWASP Top Ten).
   * **ASV Scanning:** The solution must be an Approved Scanning Vendor (ASV) and capable of performing ASV scans as required by PCI DSS.
2. **Configuration Auditing:**
   * **CIS Benchmark Auditing:** The solution should be capable of auditing configurations against CIS benchmarks.
   * **STIG Auditing:** Should support Security Technical Implementation Guide (STIG) auditing to ensure compliance with security standards.
3. **Asset Management:**
   * **Asset Inventory Capabilities:** The solution must provide robust asset inventory management to keep track of all assets within the organization.
   * **Asset Criticality Rating:** Ability to assign and manage criticality ratings for different assets to prioritize vulnerability management efforts.
   * **Vulnerability Criticality Rating:** The solution must have the capability to rate vulnerabilities based on industry standards and best practices.
   * **Combined Risk Scoring:** The solution must take into consideration the combination of asset criticality and vulnerability criticality to calculate a final risk rating.
4. **Risk Management:**
   * **Risk-Based Prioritization:** The solution should include risk-based vulnerability prioritization capabilities, helping to focus on vulnerabilities that pose the greatest risk to the organization.
5. **Reporting and Workflow:**
   * **Comprehensive Reporting:** Must provide detailed and customizable reports that can meet the needs of various stakeholders, including compliance reports for PCI DSS and PCI 3DS.
   * **Workflow Management:** Should have built-in workflow management capabilities or integrate with industry-standard systems like Jira for efficient vulnerability tracking and remediation.
6. **Deployment:**
   * **On-Premise Deployment:** The solution must support on-premise deployment capabilities and should not require inbound connections from untrusted zones, such as the internet, for its functionality.

**Additional Features and Capabilities**

1. **Integration Capabilities:**
   * **SIEM Integration:** Ability to integrate with Security Information and Event Management (SIEM) systems for enhanced threat intelligence and correlation.
   * **Ticketing Systems Integration:** Seamless integration with ticketing and workflow management systems like Jira, ServiceNow, etc., to streamline the vulnerability remediation process.
   * **Communication Channel Integration:** Support for integration with communication channels such as Slack to facilitate real-time collaboration and notification.
2. **Usability and Management:**
   * **User-Friendly Interface:** An intuitive and easy-to-navigate user interface to facilitate use by various teams.
   * **Automation:** Support for automation of routine tasks such as scheduling scans, report generation, and alerting to improve efficiency.
3. **Security and Scalability:**
   * **Data Security:** Ensure that the solution itself is secure and does not introduce vulnerabilities into the environment.
   * **Scalability:** The solution should be scalable to accommodate the growth of the organization and increasing number of assets.
4. **Advanced Features:**
   * **Client-Side Content Integrity Monitoring:** The solution must have the capability to detect changes on client-side public web pages by inventorying and monitoring the integrity of client-side scripts and other content. Reference solutions such as Akamai's Client-Side Protection & Compliance or Jscrambler's Webpage Integrity can be considered. This capability could be built-in, work as an additional functionality (e.g., a plugin), or the vulnerability management solution can be integrated with any of the aforementioned solutions.
   * **Machine Learning and AI:** Capabilities for leveraging machine learning and artificial intelligence to enhance vulnerability detection and prioritization.
   * **Threat Intelligence Integration:** Integration with threat intelligence feeds to provide context-aware vulnerability management.
5. **Support and Documentation:**
   * **Vendor Support:** Robust vendor support, including documentation, training, and a dedicated support team.
   * **Community and Updates:** Active community support and regular updates to address new vulnerabilities and compliance requirements.
   * **International Recognition:** The solution must be from an internationally recognized brand and be listed or recognized by reputable research authorities such as Gartner.
6. **Centralized Management and Intuitive Interface**
   * **Centralized Management Capabilities:** The solution must offer centralized management capabilities, allowing every module or feature to be managed from a single point, without the need for separate management panels for each module.
   * **Intuitive Interface:** The solution should provide an intuitive, easy-to-use interface to ensure that users can efficiently navigate and utilize all features and functionalities.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N** | **პროდუქტი/ მომსახურების დასახელება** | **სპეციფიკაცია** | **რაოდენობა** | **მიწოდების ვადა** | **პერიოდი** |
| 1 |  |  |  |  | მინიმუმ 1 წელი |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |