**Техническа спецификация по обособена позиция № 3 „Доставка на система за филтриране, проследяване и блокиране на Интернет трафик, система за управление на технически уязвимости и защитни стени за граничен слой“**

**1. Система от мрежови устройства за защита на интернет трафика – 2 броя**

| **Функционални изисквания на системата** | |
|---|---|
| REQ.1. | Системата чрез потребителски имена от Активната Директория следва да контролира достъпа до приложения на всеки един служител при достъпване на Интернет и вътрешните ресурси; |
| REQ.2. | Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти; |
| REQ.3. | Решението да предоставя защита от мрежови атаки чрез система за превенция (IPS); |
| REQ.4. | Системата да анализира съдържанието за наличие на зловреден код (AntiVirus и AntiSpyware); |
| REQ.5. | Системата да има възможност за анализ на непознати заплахи (Zero Day зловреден код) в защитена среда; |
| REQ.6. | Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране; |
| REQ.7. | Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи; |
| REQ.8. | Филтриране на уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мултикатегоризация на URL съгласно тип на съдържанието и риск; |
| REQ.9. | Решението трябва да предоставя възможност за идентифициране на ново регистрирани домейни и ограничаване на достъпа до тях; |
| REQ.10. | Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията; |
| REQ.11. | Декриптиране на SSL мрежова комуникация, която транспортира криптирани SMTP, IMAP, POP3, FTP, HTTP и други; |
| REQ.12. | Политиката за декриптиране трябва да има възможност да се настройва на база на URL или URL категория; |
| REQ.13. | Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv 1.1, TLSv1.2 ); |
| REQ.14. | Идентификация на приложенията на база съдържание (signatures) и стандартни портове, на които стандартно работят приложенията; |
| REQ.15. | Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата; |
| REQ.16. | Възможност за едновременно реализиране на различни видове архитектури Layer 2, Layer 3, TAP върху едно устройство; |

| | |
|---|---|
| REQ.17. | Възможност за изграждане на site-to-site VPN тунели на база IPSec и IKE стандартите; |
| REQ.18. | Възможност за QoS трафика според типа приложение потребител и/или URL категория; |
| REQ.19. | Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal; |
| REQ.20. | Ограничаване на корпоративни потребителни имена и пароли да бъдат използвани за външни за организацията ресурси (Dropbox, Google, Facebook, LinkedIn); |
| REQ.21. | Анализа на логовете и репортинг да се извършва от самото устройство с през неговия графичен интерфейс без да необходима инсталация на допълнителен софтуер; |
| REQ.22. | Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други; |
| REQ.23. | Генерираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други); |
| REQ.24. | Решението да предоставя възможност за надграждане чрез лиценз за защита на крайно клиентските машини и всички логове да се събират и анализират в защитена облачна среда на производителя; |
| REQ.25. | Решението да има механизъм за откриване и превенция на DNS Tunneling канали за комуникация.; |
| REQ.26. | Решението да може да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA)); |
| REQ.27. | Системата да има възможност за надграждане с допълнителен лиценз за реализация на софтуерно дефинирана мрежа (SD-WAN); |
| REQ.28. | Системата да има възможност за надграждане с допълнителен лиценз, чрез който да осъществява отдалечен защитен достъп от телефони и таблети (с операционни системи iOS, Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка; |
| **Хардуерни гранични устройства** | |
| REQ.29. | Минимална пропускателна способност с активирана функция за идентификация на приложенията - 6.4 Gbps |
| REQ.30. | Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/ AntiMalware / URL / Firewall / Application Control - 3.0 Gbps |
| REQ.31. | Минимална производителност за IPsec VPN - 3.0 Gbps |
| REQ.32. | Минимален брой TCP сесии - 1 800 000 |
| REQ.33. | Минимален брой нови сесии в секунда - 80 000 |
| REQ.34. | Разпознати и поддържани приложения (минимум) - 3 200 |
| REQ.35. | Да разполага с минимум 12x10/100/1000 Base-T ports |
| REQ.36. | Да предоставя възможност за надграждане с допълнителни минимум 8 x 10Gbit/s SFP+ |

| | |
|---|---|
| REQ.37. | Режими на работа на интерфейсите - L2, L3, Tap, Transparent |
| REQ.38. | Да поддържа следните машрутизиращи протоколи<br>• OSPFv2/v3, BGP with graceful restart<br>• RIP<br>• static routing<br>• Policy-based forwarding<br>• Point-to-Point Protocol over Ethernet (PPPoE)<br>• Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 Bidirectional Forwarding Detection (BFD) |
| REQ.39. | Минимални изисквания към IPSec имплементацията - Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 |
| REQ.40. | Минимален брой едновременни SSL VPN потребителя включени в системата - 1800 SSL VPN потребителя |
| REQ.41. | Минимален брой IPSec Site-to-Site VPN - 3000 отдалечени точки |
| REQ.42. | Устройството да поддържа минимум 10 виртуални таблици за маршрутизация |
| REQ.43. | Минимален брой поддържани VLAN - 4,094 броя IEEE 802.1q VLAN маркера (tags), конфигурируеми за всеки интерфейс и общо за устройството |
| REQ.44. | Да поддържа интернет протокол версия 6 (IPv6) |
| REQ.45. | Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието |
| REQ.46. | Системата следва да декриптира и инспектира SSL |
| REQ.47. | Управлението на канала (QoS) следва да е налично и приложимо за всяко идентифицирано приложение |
| REQ.48. | Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление |
| REQ.49. | Режим на надеждност - Active-Passive, Active/Active |
| REQ.50. | Минимален брой интерфейси за управление 1 x 10/100/1000 out-of-band management port, 2 x 10/100/1000 интерфейси за отказоустойчивост, 1 x RJ-45 конзолен порт |
| REQ.51. | Да бъдат предназначени за вграждане в 19‘‘ шкаф с максимален размер 2U |
| REQ.52. | Да поддържат резервирано захранване - 100-240VAC, (50-60Hz) |
| **Гаранция и поддръжка:** | |
| REQ.53. | Срок на хардуерната гаранция - минимум 5 (пет) години. |
| REQ.54. | Срок на техническа поддръжка – минимум 5 (пет) години. |

| | |
|---|---|
| REQ.55. | Получаване на нови версии на софтуера - минимум 5 (пет) години. |

**2. Устройства за филтриране, проследяване и балансиране на трафик – 2 броя специализирани физически устройства за балансиране на трафик, защита на уеб приложения (Web Application Firewall), защита на приложно програмни интерфейси (API) и контрол на достъпа до приложения със следните технически изисквания към всяко едно от устройствата**

| **Функционални изисквания на системата** | |
|---|---|
| REQ.56. | Устройството да има следната минимална производителност за балансиране на трафика:<br>• 11M HTTP заявки в секунда Layer 4;<br>• 1.7M заявки в секунда Layer 7<br>• 32Gbps пропускателна способност Layer 7<br>• 38M едновременни конекции Layer 4<br>• 58Gbps пропускателна способност Layer 4 |
| REQ.57. | Устройството да включва минимум следните методи за балансиране на трафика:<br>• Round Robin;<br>• Ratio (server/node), Ratio (session), Ratio service (IP + Port)<br>• Dynamic Ratio (server/node), Dynamic Ratio service (IP + Port);<br>• Least Connections (server/node), Least Connections service (IP + Port);<br>• Weighted Least Connection<br>• Least Sessions |
| REQ.58. | Устройството да включва функционалност за наблюдение на състоянието на сървърите към услугата, която балансира на база TCP, UDP, SMTP, DNS, FTP, SIP, Gateway, HTTP, HTTPS, ICMP, IMAP, POP3, LDAP, MSSQL, MySQL и Oracle за да разпределя заявките само до наличните сървъри. |
| REQ.59. | Устройството да включва функционалност (Persistence) за изпращане на заявките от един потребител към един и същи сървър в мрежата на база на:<br>• Sourse IP;<br>• Destination IP;<br>• Cookies;<br>• Hash;<br>• SIP;<br>• SSL; |
| REQ.60. | Устройството да включва функционалност за балансиране на услуги на ниво DNS между географски отдалечени Active/Active центрове за данни посредством следните методи:<br>• Round Robin;<br>• Availability;<br>• Ratio;<br>• Dynamic Ratio;<br>• Least Connections; |

| | |
|---|---|
| | • IP Geolocation;<br>• CPU;<br>• Round trip time;<br>• Hops;<br>• Complation rate;<br>• QoS;<br>• Kilobytes per second; |
| REQ.61. | Устройството да включва функционалност за DNS сървър, DNS SEC, DNS защитна стена с механизми за предотвратяване на DDoS атаки на ниво DNS. |
| REQ.62. | Устройството да включва функционалност за BGP, OSPF, IS-IS, RIPv2, виртуални домейни за маршрутизация и статична маршрутизация |
| REQ.63. | Устройството да включва достъп до актуална база с репутация на IP адреси с цел управление/ограничаване на достъпа до услугите от IP адреси с лоша репутация. |
| REQ.64. | Устройството да включва функционалност за защита на Web приложения (Web Application Firewall, WAF) със следните функционалности:<br>• Защита от атаки насочени към приложния слой - Layer 7;<br>• Защита и предотвратяване на OWASP Top 10 атаки;<br>• Откриване и смекчаване на L7 DoS/DDoS атаки;<br>• Защита и смекчаване на L7 DoS/DDoS атаки на база на поведение и аномалии в трафика.<br>• Защита и смекчаване на Brute force атаки;<br>• Защита и смекчаване на Heavy URLs атаки;<br>• Блокиране на заявки на база геолокация;<br>• Device Fingerprinting;<br>• Защита от Web Scraping;<br>• Разпознаване и защита от злонамерени ботове<br>• DAST (Dynamic Application Security Testing) интеграция |
| REQ.65. | Устройството да включва функционалност за защита на приложно-програмни интерфейси - API Security. |
| REQ.66. | Устройството да включва следните интерфейсни портове:<br>• минимум 1 бр. порт за управление<br>• минимум 8 бр. 10GbE SFP+ порта. Да бъдат предвидени минимум 4 броя 10Gb SFP+ SR приемо-предавателни модули за свързване към инфраструктурата.<br>• минимум 4 бр. 40GbE QSFP+ порта |
| REQ.67. | Устройството да включва два резервирани захранващи модула. |
| REQ.68. | Устройството да е с размер не повече от 1U и да се достави окомплектовано с необходимите компоненти за вграждане в стандартен шкаф 19”. |
| REQ.69. | Устройството да бъде окомплектовано с необходимите захранващи и конзолни кабели. |
| REQ.70. | Устройството да има минимум един 4 ядрен процесор |
| REQ.71. | Устройството да е с инсталирана памет не по-малко от 48GB |
| REQ.72. | Устройството да бъдат окомплектовано с минимум един SSD диск . |

| | |
|---|---|
| REQ.73. | Устройството да включва функционалност за разделяне на минимум 8 виртуални устройства/контекста; |
| REQ.74. | Устройството да включва функционалност за хардуерна компресия с капацитет минимум 18 Gbit/s. |
| REQ.75. | Устройството да може да работи в конфигурации за висока наличност (клъстер) в режими: Активен/Активен, Активен/Пасивен и възможност за поддръжка на повече от 2 устройства в клъстър конфигурация; |
| REQ.76. | Устройството да позволява бъдещо разширение с функционалност за изграждане на клъстер с устройствата за балансиране, централизирано декриптиране, пренасочване и повторно криптиране на трафик описани в точка 3 на техническото задание. |
| REQ.77. | Устройството да има хардуерен offload на SSL и TLS минимум 20Gbps и поддръжка на минимум 32K TPS RSA (2K ключове) |
| REQ.78. | Устройството да поддържа SNMP. |
| REQ.79. | Устройството да поддържа IPv4, IPv6; |
| REQ.80. | Устройството да поддържа конфигуриране и управление през API интерфейс; |
| REQ.81. | Администрацията на операционната система на устройството следва да допуска дефиниране на различни роли за различните типове потребители. |
| REQ.82. | Устройството следва да предоставя възможност за генериране на справки и мониторинг в следните направления:<br>• Да рапортува за наличност на услугите и участващите в тях сървъри/апликации.<br>• Да рапортува за натовареността на различните услугите и сървъри/апликации в тях.<br>• Да рапортува относно консумирания трафик.<br>• Устройството следва да предоставя опции за дефиниране на dashboard за администратор с цел бързо извеждане на актуалните рапорти и мониторинг. |
| REQ.83. | Устройството да има Full Proxy Architecture; |
| REQ.84. | Устройството да включва функционалност за регистрация на много услуги с една автентикация Single sign-on (SSO) с поддръжка на стандарт SAML 2.0. |
| REQ.85. | Устройството да включва функционалност за реализиране на SSL VPN свързаност на минимум 500 потребителя и възможност за бъдещо разширение на SSL VPN потребителите. |
| REQ.86. | Устройството да включва функционалност за L3/L4 защитна стена, разпознаване на аномалии на ниво протокол и механизми за предотвратяване на DDoS атаки на ниво L3/L4. |
| REQ.87. | Устройството да позволява бъдещо разширение с функционалност за декриптиране и пращане на трафика към трети устройства като защитни стени от следващо поколение (NGFW), системи за превенция на атаките (IPS), системи за контрол и защита на данните (DLP) |
| REQ.88. | Устройството да позволява бъдещо разширение с функционалност за защита и криптиране на потребителските имена и пароли в Web портали. Без да е необходима инсталация на агент на крайно клиентската машина. |
| REQ.89. | Устройството да е с включена стандартна гаранционна поддръжка от производителя за срок не по-малък от 60 месеца, която да позволява софтуерни обновления до по-нова версия. Да се включат всички необходими лицензи и софтуерни обновявания на сигнатурите за всички функционалности за срок не по-малък от 60 месеца. |
| **Гаранция и поддръжка:** | |

| | |
|---|---|
| REQ.90. | Срок на хардуерната гаранция - минимум 5 (пет) години. |
| REQ.91. | Срок на техническа поддържка – минимум 5 (пет) години. |
| REQ.92. | Получаване на нови версии на софтуера - минимум 5 (пет) години. |

**3. Устройства за филтриране, проследяване и балансиране на трафик – 2 броя специализирани физически устройства за балансиране, централизирано декриптиране, пренасочване и повторно криптиране на трафик със следните технически изисквания към всяко едно от устройствата.**

| **Функционални изисквания на системата** | |
|---|---|
| REQ.93. | Устройството да има следната минимална производителност за балансиране на трафика:<br>• 2M HTTP заявки в секунда Layer 4;<br>• 1M заявки в секунда Layer 7<br>• 20Gbps пропускателна способност Layer 7 и Layer 4<br>• 25M едновременни конекции Layer 4 |
| REQ.94. | Устройството да включва минимум следните методи за балансиране на трафика:<br>• Round Robin;<br>• Ratio (server/node), Ratio (session), Ratio service (IP + Port)<br>• Dynamic Ratio (server/node), Dynamic Ratio service (IP + Port);<br>• Least Connections (server/node), Least Connections service (IP + Port);<br>• Weighted Least Connection<br>• Least Sessions |
| REQ.95. | Устройството да включва функционалност за наблюдение на състоянието на сървърите към услугата, която балансира на база TCP, UDP, SMTP, DNS, FTP, SIP, Gateway, HTTP, HTTPS, ICMP, IMAP, POP3, LDAP, MSSQL, MySQL и Oracle за да разпределя заявките само до наличните сървъри. |
| REQ.96. | Устройството да включва функционалност (Persistence) за изпращане на заявките от един потребител към един и същи сървър в мрежата на база на:<br>• Sourse IP;<br>• Destination IP;<br>• Cookies;<br>• Hash;<br>• SIP;<br>• SSL; |
| REQ.97. | Устройството да включва функционалност за централизирано терминиране, декриптиране, пренасочване на трафика към трети устройства като защитни стени от следващо поколение (NGFW), системи за превенция на атаките (IPS), системи за контрол и защита на данните (DLP) и повторно криптиране на SSL/TLS трафик с поддръжка на следните режими и топологии: |

| | |
|---|---|
| | • Създаване на политики за препращане на декриптирания трафик SSL/TLS за проверка и инспекция към устройство/решение или верига от устройства/решения на трети производители;<br>• Създаване на политики за пропускане на трафик насочен към услуги съдържащи чувствителни лични данни, като банкови или здравни услуги;<br>• Повторно криптиране на входящия и изходящ SSL/TLS трафик след преминаването на проверка през веригата от устройства/решения за сигурност на трети производители;<br>• Inbound Layer 2/3<br>• Outbound L2<br>• Outbound explicit proxy<br>• Outbound transparent proxy<br>• Inline Layer 3<br>• Inline Layer 2<br>• ICAP services<br>• Receive-only<br>• TAP Services |
| REQ.98. | Устройството да включва следните интерфейсни портове:<br>• минимум 1 бр. порт за управление.<br>• минимум 8 бр. 1GbE SFP порта.<br>• минимум 4 бр. 10GbE SFP+ порта. Да бъдат предвидени минимум 2 броя 10Gb SFP+ SR приемо-предавателни модули за свързване към инфраструктурата |
| REQ.99. | Устройството да включва два резервирани захранващи модула. |
| REQ.100. | Устройството да е с размер не повече от 1U и да се достави окомплектовано с необходимите компоненти за вграждане в стандартен шкаф 19”. |
| REQ.101. | Устройството да бъде окомплектовано с необходимите захранващи и конзолни кабели. |
| REQ.102. | Устройството да има минимум един 4 ядрен процесор |
| REQ.103. | Устройството да е с инсталирана памет не по-малко от 32GB |
| REQ.104. | Устройството да бъдат окомплектовано с минимум един твърд диск с размер не по-малък от 400GB. |
| REQ.105. | Устройството да включва функционалност за хардуерна компресия с капацитет минимум 10 Gbit/s. |
| REQ.106. | Устройството да може да работи в конфигурации за висока наличност (клъстер) в режими: Активен/Активен, Активен/Пасивен и възможност за поддръжка на повече от 2 устройства в клъстър конфигурация; |
| REQ.107. | Устройството да позволява бъдещо разширение с функционалност за изграждане на клъстер с устройствата за балансиране на трафик, защита на уеб приложения (Web Application Firewall), защита на приложно програмни интерфейси (API) и контрол на достъпа до приложения описани в точка 2 на техническото задание. |
| REQ.108. | Устройството да има хардуерен offload на SSL и TLS минимум 14Gbps и поддръжка на минимум 18K TPS RSA (2K ключове) |
| REQ.109. | Устройството да поддържа SNMP. |

| | |
|---|---|
| REQ.110. | Устройството да поддържа IPv4, IPv6; |
| REQ.111. | Устройството да поддържа конфигуриране и управление през API интерфейс; |
| REQ.112. | Администрацията на операционната система на устройството следва да допуска дефиниране на различни роли за различните типове потребители. |
| REQ.113. | Устройството следва да предоставя възможност за генериране на справки и мониторинг в следните направления:<br>• Да рапортува за наличност на услугите и участващите в тях сървъри/апликации.<br>• Да рапортува за натовареността на различните услугите и сървъри/апликации в тях.<br>• Да рапортува относно консумирания трафик.<br>• Устройството следва да предоставя опции за дефиниране на dashboard за администратор с цел бързо извеждане на актуалните рапорти и мониторинг. |
| REQ.114. | Устройството да има Full Proxy Architecture; |
| REQ.115. | Устройството да позволява бъдещо разширение с функционалност за регистрация на много услуги с една автентикация Single sign-on (SSO) с поддръжка на стандарт SAML 2.0. |
| REQ.116. | Устройството да позволява бъдещо разширение с функционалност за реализиране на SSL VPN. |
| REQ.117. | Устройството да позволява бъдещо разширение с функционалност за L3/L4 защитна стена, разпознаване на аномалии на ниво протокол и механизми за предотвратяване на DDoS атаки на ниво L3/L4. |
| REQ.118. | Устройството да позволява бъдещо разширение с функционалност за балансиране на услуги на ниво DNS между географски отдалечени Active/Active центрове за данни. |
| REQ.119. | Устройството да позволява бъдещо разширение с функционалност за защита на Web приложения (Web Application Firewall, WAF). |
| REQ.120. | Устройството да позволява бъдещо разширение с функционалност за защита на приложно-програмни интерфейси - API Security. |
| REQ.121. | Устройството да позволява бъдещо разширение с функционалност за DNS сървър, DNS SEC, DNS защитна стена с механизми за предотвратяване на DDoS атаки на ниво DNS. |
| **Гаранция и поддръжка:** | |
| REQ.122. | Срок на хардуерната гаранция - минимум 5 (пет) години. |
| REQ.123. | Срок на техническа поддръжка – минимум 5 (пет) години. |
| REQ.124. | Получаване на нови версии на софтуера - минимум 5 (пет) години. |

**4. Софтуер за сканиране и управление на уязвимости с капацитет за 8000 информационни активи**

| **Функционални изисквания на системата** | |
|---|---|
| REQ.125. | Предложеното решение за сканиране и управление на уязвимости трябва да бъде изпълняван от програмен код инсталиран на място (във вътрешната мрежа на организацията) за нуждите на минимум 8000 информационни активи (assets). |

| | |
|---|---|
| REQ.126. | Решението трябва да сканира системи/устройства с IP адреси за актуални уязвимости в информационната сигурност. |
| REQ.127. | Решението да предоставя възможност за сканиране без необходимост от инсталиране на агент върху крайното устройство. |
| REQ.128. | Предложеното решение да бъде с 64 битова архитектура и да може да се инсталира на минимум следните платформи:<br>• Ubuntu Linux 14.04 LTS<br>• Ubuntu Linux 16.04 LTS<br>• Ubuntu Linux 18.04 LTS<br>• Microsoft Windows Server 2008 R2<br>• Microsoft Windows Server 2012 R2<br>• Microsoft Windows Server 2016<br>• Microsoft Windows 8.1<br>• Microsoft Windows 7 SP1+<br>• Red Hat Enterprise Linux Server 6<br>• Red Hat Enterprise Linux Server 7<br>• CentOS 7<br>• Oracle Linux 7<br>• Virtual Machines on VMware Player 6 or later, VMware Workstation 9 or later, VMware Fusion 8 or later, VMware vCenter 5.5, 6.0 and VMware ESXi 5.5, 6.0 |
| REQ.129. | Предложеното решение трябва да използва централна конзола за управление на всички инсталирани скенери, като предоставя обобщени данни за сканирането и потребителският достъп, без да се изискват допълнителни модули или софтуер. |
| REQ.130. | Решението трябва да поддържа интеграция с Active Directory, Kerberos или LDAP съвместима директория. |
| REQ.131. | Решението да не причинява смущения в работата на мрежата и устройството по време на сканирането. |
| REQ.132. | Решението е необходимо да идентифицира OS, инсталирания софтуер, активни услуги, състояние на портове ICMP TCP/UDP, използвани протоколи, конфигурации, зловреден софтуер, експлойти, потребители и групи от потребители. |
| REQ.133. | Решението трябва да прилага автоматични актуализации на съдържанието, без да се налага рестартиране, което да позволява на потребителите да изпълняват сканиране с най-новото покритие веднага, без прекъсване на работата. |
| REQ.134. | Решението за управление на уязвимостите, трябва да има възможност за директна интеграция с виртуални платформи VMware, което да осигурява виртуално динамично проследяване на активи. Чрез тази директна връзка, решението автоматично да оценява виртуалните активи за актуална информация за риска за състоянието. |
| REQ.135. | Решението трябва да поддържа планирани сканирания, които да са повторяеми през определени времеви прозорци и интервали. |

| | |
|---|---|
| REQ.136. | Решението трябва да осигурява двупосочен API. Като използването на API не трябва да изисква допълнителни такси или закупуване на допълнителен софтуер. |
| REQ.137. | Решението трябва да има способността да сканира Хеш стойности, за да идентифицира повторното използване на един и същ тип парола в различни системи. |
| REQ.138. | Системата трябва автоматично да открива и маркира нови потребители, устройства и уязвимости веднага щом се появят в мрежата. |
| REQ.139. | Решението трябва да идентифицира известни заплахи и набори от зловреден софтуер, свързани с вече открити уязвимости. |
| REQ.140. | Решението трябва да осигурява пълно покритие на категориите на „OWASP Top Ten“. |
| REQ.141. | Решението трябва да сканира WEB 2.0 технологиите, включително AJAX, ASP .NET 2.0 и Flash базирани сайтове. |
| REQ.142. | Решението трябва да има способността да приоритизира заплахите и да покаже най-бързия път към възстановяване. |
| REQ.143. | Решението да осигурява една точка на управление за всички отчети, независимо от това къде се извършват сканирането в мрежата, без това да налага закупуването на допълнителни модули или софтуер. |
| REQ.144. | Решението да предоставя следните възможности за отчитане: HTML, PDF, CSV, XML, Email |
| REQ.145. | Решението трябва да включва като минимум, следните типове отчети:<br>• Executive reports<br>• Trending reports<br>• Baseline reports<br>• Vulnerability reports<br>• Asset reports |
| REQ.146. | Решението трябва да може да оцени всяка открита заплаха, вирус или слабост чрез оценка на риска между 1 – 1000 като филтрира и покаже на анализатора най-критичните заплахи. |
| REQ.147. | Решението трябва да поддържа интеграция с технология за тестване на сигурността на информационни системи с цел симулиране на действителни атаки и тестване на защитата, с утвърждаване на резултатите от скенера за уязвимост, като използва автоматизиран процес със затворен цикъл. |
| REQ.148. | Решението трябва да има възможност за интеграция със специализираните физически устройства за балансиране на трафик, защита на уеб приложения (Web Application Firewall), защита на приложно програмни интерфейси (API) и контрол на достъпа до приложения. |
| REQ.149. | Решението трябва да има възможност чрез добавяне на допълнителен лиценз да бъде надградено и предостави достъп до облачна среда за събиране на логове и анализ на поведение. (SIEM & UEBA) |
| **Гаранция и поддръжка:** | |
| REQ.150. | Срок на хардуерната гаранция - минимум 5 (пет) години. |
| REQ.151. | Срок на техническа поддържка – минимум 5 (пет) години. |
| REQ.152. | Получаване на нови версии на софтуера - минимум 5 (пет) години. |