Техническое задание

на поставку программно-аппаратного комплекса Positive Technologies Sandbox для анализа сетевого трафика и выявления атак

1. **Общие требования**
   1. Поставка должна включать в себя программно-аппаратный комплекс (далее – ПАК) Positive Technologies Sandbox со всеми сопутствующими подписками на сервисы безопасности и технической поддержкой от производителя 24х7 сроком на 36 месяцев согласно следующей спецификации:

|  |  |  |
| --- | --- | --- |
| **Positive Technologies Sandbox** | | |
| PRT-SBX-AIO-500-M36 | Программное обеспечение Система статического и ди-намического анализа для выявления вредоносных объектов Positive Technologies Sandbox. Конфигурация PT Sandbox All-in-One, до 500 почтовых ящиков, до 500 Мбит/с, обновления в течение 3 (трех) лет | 2 |
| PRT-SBX-AIO-1000-M36 | Программное обеспечение Система статического и ди-намического анализа для выявления вредоносных объ-ектов Positive Technologies Sandbox. Конфигурация PT Sandbox All-in-One, до 1000 почтовых ящиков, до 1 Гбит/с, обновления в течение 3 (трех) лет | 1 |
| **PT Network Attack Discovery** | | |
| **Базовые лицензии** | | |
| PRT-NAD-BASE-2-M36 | Программное обеспечение Positive Technologies Net-work Attack Discovery. Базовая лицензия на 2 Гбит/с, обновления в течение 3 (трех) лет | 1 |
| **Инфраструктурные ли-цензии** | | |
| PRT-NAD-SRV-M36 | Программное обеспечение Positive Technologies Net-work Attack Discovery. Компонент Network Attack Discovery Server, обновления в течение 3 (трех) лет | 1 |
| PRT-NAD-CAP-1000-M36 | Программное обеспечение Positive Technologies Net-work Attack Discovery. Компонент Network Attack Discovery Capturer, до 1 000 Мбит/с, обновления в тече-ние 3 (трех) лет | 2 |
| **Серверное оборудование** | | |
| PowerEdge R650 Server [PowerEdge R650 - SRV 1] |  | 2 |
|  | PowerEdge R650 Server | 1 |
| 4x3.5 Front Storage | 1 |
| SAS/SATA Backplane | 1 |
| 2x2.5 Rear Storage | 1 |
| Trusted Platform Module 2.0 V3 | 1 |
| 3.5" Chassis with up to 4 Hard Drives (SAS/SATA), 2x2.5" Rear Hard Drives (SAS/SATA), 1 PCIe Slot, 2 CPU | 1 |
| Intel Xeon Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933 | 1 |
| Intel Xeon Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933 | 1 |
| Additional Processor Selected | 1 |
| Heatsink for 2 CPU configuration (CPU less than or equal to 165W) | 1 |
| Performance Optimized | 1 |
| 3200MT/s RDIMMs | 1 |
| RAID 1 | 1 |
| PERC H355 Controller Front | 1 |
| Front PERC Mechanical Parts, front load | 1 |
| Power Saving BIOS Settings | 1 |
| iDRAC9, Express 15G | 1 |
| 4 High Performance Fans for 2 CPU | 1 |
| Dual, Hot-plug, Power Supply Redundant (1+1), 800W, Mixed Mode, NAF | 1 |
| Riser Config 2, Half Length, Low Profile, 1 x16 Slot | 1 |
| PowerEdge R650 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM, Ti | 1 |
| Intel i350 Quad Port 1GbE BASE-T, OCP NIC 3.0 | 1 |
| No Quick Sync | 1 |
| iDRAC,Factory Generated Password | 1 |
| iDRAC Group Manager, Disabled | 1 |
| Standard Bezel | 1 |
| Luggage Tray x4 Chassis, R650 | 1 |
| BOSS-S2 controller card + with 2 M.2 240GB (RAID 1) | 1 |
| BOSS Cables and Bracket for R650 | 1 |
| Cable Management Arm | 1 |
| ReadyRails Sliding Rails Without Cable Management Arm or Strain Relief Bar | 1 |
| PowerEdge R650 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) | 1 |
| R650 Ship 4x3.5, 10x2.5, 8x2.5 NVMe | 1 |
| PowerEdge R650 Non BIS Marking | 1 |
| PowerEdge R650 CCC Marking, No CE Marking | 1 |
| Enterprise Order - EMEA. | 1 |
| No Installation Service Selected (Contact Sales Rep for more details) | 1 |
| 16GB RDIMM, 3200MT/s, Dual Rank | 8 |
| 4TB Hard Drive SATA 6Gbps 7.2K 512n 3.5in Hot-Plug | 2 |
| 960GB SSD vSAS Mixed Use 12Gbps 512e 2.5in Hot-Plug,Flex Bay ,AG Drive SED, 3DWPD | 2 |
| C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord | 2 |
| UEFI BIOS Boot Mode with GPT Partition | 1 |
| No Operating System | 1 |
| No Media Required | 1 |
| Parts Only Warranty 12 Months | 1 |
| ProSupport and Next Business Day Onsite Service Extension, 24 Month(s) | 1 |
| ProSupport and Next Business Day Onsite Service Initial, 12 Month(s) | 1 |
| Asset Tag - ProSupport (Website, barcode, Onboard MacAddress) | 1 |
| Configuration Services, Standard ISG System Report, Deliver Via Email | 1 |
| Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM) | 1 |
| PowerEdge R750 Server [PowerEdge R750 - SRV 2] |  | 1 |
|  | PowerEdge R750 Server | 1 |
|  | 3.5 Chassis | 1 |
|  | SAS/SATA Backplane | 1 |
|  | 4x2.5 Rear Storage | 1 |
|  | No GPU Enablement | 1 |
|  | Trusted Platform Module 2.0 V3 | 1 |
|  | 3.5" Chassis with up to 12 HDDs (SAS/SATA), 4x2.5" Rear HDDs (SAS/SATA), Adapater PERC | 1 |
|  | Intel Xeon Gold 5320 2.2G, 26C/52T, 11.2GT/s, 39M Cache, Turbo, HT (185W) DDR4-2933 | 1 |
|  | Intel Xeon Gold 5320 2.2G, 26C/52T, 11.2GT/s, 39M Cache, Turbo, HT (185W) DDR4-2933 | 1 |
|  | Additional Processor Selected | 1 |
|  | Heatsink for 2 CPU configuration (CPU greater than or equal to 165W) | 1 |
|  | Performance Optimized | 1 |
|  | 3200MT/s RDIMMs | 1 |
|  | Unconfigured RAID | 1 |
|  | PERC H755 Adapter, Low Profile | 1 |
|  | Power Saving Dell Active Power Controller | 1 |
|  | iDRAC9, Express 15G | 1 |
|  | High Performance Fan x6 | 1 |
|  | Power Supply 800W RDNT D, Mixed Mode | 1 |
|  | Riser Config 5, 2x8, 2x16 slots | 1 |
|  | R750 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM, Ti | 1 |
|  | Intel X710 Dual Port 10GbE SFP+, OCP NIC 3.0 | 1 |
|  | No Quick Sync | 1 |
|  | iDRAC,Factory Generated Password | 1 |
|  | iDRAC Group Manager, Disabled | 1 |
|  | PowerEdge 2U Standard Bezel | 1 |
|  | Dell EMC Luggage Tag | 1 |
|  | BOSS-S2 controller card + with 2 M.2 240GB (RAID 1) | 1 |
|  | BOSS Cables and Bracket for R750 (4x2.5" Rear) | 1 |
|  | ReadyRails Sliding Rails | 1 |
|  | Cable Management Arm, 2U | 1 |
|  | Fan Foam, HDD 2U | 1 |
|  | PowerEdge R750 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) | 1 |
|  | PowerEdge R750 Shipping Material | 1 |
|  | PowerEdge INMETRO Label, BCC | 1 |
|  | PowerEdge R750 CE, CCC, Marking | 1 |
|  | Enterprise Order - EMEA. | 1 |
|  | No Installation Service Selected (Contact Sales Rep for more details) | 1 |
|  | 16GB RDIMM, 3200MT/s, Dual Rank | 12 |
|  | 4TB Hard Drive SATA 6Gbps 7.2K 512n 3.5in Hot-Plug | 4 |
|  | 960GB SSD vSAS Mixed Use 12Gbps 512e 2.5in Hot-Plug,Flex Bay ,AG Drive SED, 3DWPD | 4 |
|  | C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord | 2 |
|  | Intel Ethernet i350 Quad Port 1GbE BASE-T Adapter, PCIe Full Height, V2, FIRMWARE RESTRICTIONS APPLY | 1 |
|  | Dell EMC PowerEdge SFP+ SR Optic 10GbE 850nm | 2 |
|  | UEFI BIOS Boot Mode with GPT Partition | 1 |
|  | No Operating System | 1 |
|  | No Media Required | 1 |
|  | No Systems Documentation, No OpenManage DVD Kit | 1 |
|  | Parts Only Warranty 12 Months | 1 |
|  | ProSupport and Next Business Day Onsite Service Extension, 24 Month(s) | 1 |
|  | ProSupport and Next Business Day Onsite Service Initial, 12 Month(s) | 1 |
|  | Asset Tag - ProSupport (Website, barcode, Onboard MacAddress) | 1 |
|  | Configuration Services, Standard ISG System Report, Deliver Via Email | 1 |
|  | Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM) | 1 |
| PowerEdge R650 Server [PowerEdge R650 - Sensor\_1Gb] |  | 2 |
|  | PowerEdge R650 Server | 1 |
|  | 4x3.5 Front Storage | 1 |
|  | SAS/SATA Backplane | 1 |
|  | No Rear Storage | 1 |
|  | Trusted Platform Module 2.0 V3 | 1 |
|  | 3.5" Chassis with up to 4 Hard Drives (SAS/SATA), 3 PCIe Slots, 2 CPU | 1 |
|  | Intel Xeon Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933 | 1 |
|  | Intel Xeon Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933 | 1 |
|  | Additional Processor Selected | 1 |
|  | Heatsink for 2 CPU configuration (CPU less than or equal to 165W) | 1 |
|  | Performance Optimized | 1 |
|  | 3200MT/s RDIMMs | 1 |
|  | No RAID | 1 |
|  | PERC H355 Controller Front | 1 |
|  | Front PERC Mechanical Parts, front load | 1 |
|  | Power Saving BIOS Settings | 1 |
|  | iDRAC9, Express 15G | 1 |
|  | 4 High Performance Fans for 2 CPU | 1 |
|  | Dual, Fully Redundant(1+1), Hot-Plug Power Supply,1100W MM(100-240Vac) Titanium | 1 |
|  | Riser Config 0, 2CPU, Half Length, Low Profile, 3 x16 Slots, SW GPU Capable | 1 |
|  | PowerEdge R650 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM, Ti | 1 |
|  | Intel X710-T4L Quad Port 10GbE BASE-T, OCP NIC 3.0 | 1 |
|  | No Quick Sync | 1 |
|  | iDRAC,Factory Generated Password | 1 |
|  | iDRAC Group Manager, Disabled | 1 |
|  | Standard Bezel | 1 |
|  | Luggage Tray x4 Chassis, R650 | 1 |
|  | BOSS-S2 controller card + with 2 M.2 240GB (RAID 1) | 1 |
|  | BOSS Cables and Bracket for R650 | 1 |
|  | Cable Management Arm | 1 |
|  | ReadyRails Sliding Rails Without Cable Management Arm or Strain Relief Bar | 1 |
|  | PowerEdge R650 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) | 1 |
|  | R650 Ship 4x3.5, 10x2.5, 8x2.5 NVMe | 1 |
|  | PowerEdge R650 Non BIS Marking | 1 |
|  | PowerEdge R650 CE, CCC, Marking | 1 |
|  | Enterprise Order - EMEA. | 1 |
|  | No Installation Service Selected (Contact Sales Rep for more details) | 1 |
|  | 16GB RDIMM, 3200MT/s, Dual Rank | 4 |
|  | 4TB 7.2K RPM NLSAS ISE 12Gbps 512n 3.5in Hard Drive | 4 |
|  | C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord | 2 |
|  | Intel Ethernet i350 Quad Port 1GbE BASE-T Adapter, PCIe Low Profile, V2, FIRMWARE RESTRICTIONS APPLY | 1 |
|  | UEFI BIOS Boot Mode with GPT Partition | 1 |
|  | No Operating System | 1 |
|  | No Media Required | 1 |
|  | Parts Only Warranty 12 Months | 1 |
|  | ProSupport and Next Business Day Onsite Service Extension, 24 Month(s) | 1 |
|  | ProSupport and Next Business Day Onsite Service Initial, 12 Month(s) | 1 |
|  | Asset Tag - ProSupport (Website, barcode, Onboard MacAddress) | 1 |
|  | Configuration Services, Standard ISG System Report, Deliver Via Email | 1 |
|  | Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM) | 1 |
| PowerEdge R750 Server [PowerEdge R750 - Sensor\_5Gb] |  | 1 |
|  | PowerEdge R750 Server | 1 |
|  | 3.5 Chassis | 1 |
|  | SAS/SATA Backplane | 1 |
|  | No Rear Storage | 1 |
|  | No GPU Enablement | 1 |
|  | Trusted Platform Module 2.0 V3 | 1 |
|  | 3.5" Chassis with up to 12 Hard Drives (SAS/SATA) with Adapter PERC | 1 |
|  | Intel Xeon Gold 5320 2.2G, 26C/52T, 11.2GT/s, 39M Cache, Turbo, HT (185W) DDR4-2933 | 1 |
|  | Intel Xeon Gold 5320 2.2G, 26C/52T, 11.2GT/s, 39M Cache, Turbo, HT (185W) DDR4-2933 | 1 |
|  | Additional Processor Selected | 1 |
|  | Heatsink for 2 CPU configuration (CPU greater than or equal to 165W) | 1 |
|  | Performance Optimized | 1 |
|  | 3200MT/s RDIMMs | 1 |
|  | Unconfigured RAID | 1 |
|  | PERC H755 Adapter Full Height | 1 |
|  | Power Saving Dell Active Power Controller | 1 |
|  | iDRAC9, Express 15G | 1 |
|  | High Performance Fan x6 | 1 |
|  | Dual, Hot-Plug, Power Supply, 1100W MM (100-240Vac) Titanium, Redundant (1+1) | 1 |
|  | Riser Config 0, 4x8 slots | 1 |
|  | R750 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM, Ti | 1 |
|  | Intel X710 Dual Port 10GbE SFP+, OCP NIC 3.0 | 1 |
|  | No Quick Sync | 1 |
|  | iDRAC,Factory Generated Password | 1 |
|  | iDRAC Group Manager, Disabled | 1 |
|  | PowerEdge 2U Standard Bezel | 1 |
|  | Dell EMC Luggage Tag | 1 |
|  | BOSS-S2 controller card + with 2 M.2 240GB (RAID 1) | 1 |
|  | BOSS Cables and Bracket for R750 (Riser 1) | 1 |
|  | ReadyRails Sliding Rails | 1 |
|  | Cable Management Arm, 2U | 1 |
|  | Fan Foam, HDD 2U | 1 |
|  | PowerEdge R750 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) | 1 |
|  | PowerEdge R750 Shipping Material | 1 |
|  | PowerEdge INMETRO Label, BCC | 1 |
|  | PowerEdge R750 CE, CCC, Marking | 1 |
|  | Enterprise Order - EMEA. | 1 |
|  | No Installation Service Selected (Contact Sales Rep for more details) | 1 |
|  | 16GB RDIMM, 3200MT/s, Dual Rank | 8 |
|  | 4TB 7.2K RPM NLSAS ISE 12Gbps 512n 3.5in Hard Drive | 8 |
|  | C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord | 2 |
|  | Intel Ethernet i350 Quad Port 1GbE BASE-T Adapter, PCIe Full Height, V2, FIRMWARE RESTRICTIONS APPLY | 1 |
|  | Dell EMC PowerEdge SFP+ SR Optic 10GbE 850nm | 2 |
|  | UEFI BIOS Boot Mode with GPT Partition | 1 |
|  | No Operating System | 1 |
|  | No Media Required | 1 |
|  | No Systems Documentation, No OpenManage DVD Kit | 1 |
|  | Parts Only Warranty 12 Months | 1 |
|  | ProSupport and Next Business Day Onsite Service Extension, 24 Month(s) | 1 |
|  | ProSupport and Next Business Day Onsite Service Initial, 12 Month(s) | 1 |
|  | Asset Tag - ProSupport (Website, barcode, Onboard MacAddress) | 1 |
|  | Configuration Services, Standard ISG System Report, Deliver Via Email | 1 |
|  | Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM) | 1 |
| PowerEdge R750 Server [PowerEdge R750 - Core] |  | 2 |
|  | PowerEdge R750 Server | 1 |
|  | 2.5 Chassis | 1 |
|  | SAS/SATA Backplane | 1 |
|  | No Rear Storage | 1 |
|  | No GPU Enablement | 1 |
|  | Trusted Platform Module 2.0 V3 | 1 |
|  | 2.5" Chassis with up to 16 SAS/SATA Drives, MAX IO | 1 |
|  | Intel Xeon Gold 5320 2.2G, 26C/52T, 11.2GT/s, 39M Cache, Turbo, HT (185W) DDR4-2933 | 1 |
|  | Intel Xeon Gold 5320 2.2G, 26C/52T, 11.2GT/s, 39M Cache, Turbo, HT (185W) DDR4-2933 | 1 |
|  | Additional Processor Selected | 1 |
|  | Heatsink for 2 CPU with GPU configuration | 1 |
|  | Performance Optimized | 1 |
|  | 3200MT/s RDIMMs | 1 |
|  | Unconfigured RAID | 1 |
|  | PERC H755 SAS Front | 1 |
|  | Front PERC Mechanical Parts, rear load | 1 |
|  | Power Saving Dell Active Power Controller | 1 |
|  | iDRAC9, Express 15G | 1 |
|  | Standard Fan x6 | 1 |
|  | Dual, Hot-Plug, Power Supply, 1100W MM (100-240Vac) Titanium, Redundant (1+1) | 1 |
|  | Riser Config 4, Full Length, 6x16 slots, MAX IO, SW GPU Capable | 1 |
|  | R750 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM, Ti | 1 |
|  | Intel X710 Dual Port 10GbE SFP+, OCP NIC 3.0 | 1 |
|  | No Quick Sync | 1 |
|  | iDRAC,Factory Generated Password | 1 |
|  | iDRAC Group Manager, Disabled | 1 |
|  | PowerEdge 2U Standard Bezel | 1 |
|  | Dell EMC Luggage Tag | 1 |
|  | BOSS-S2 controller card + with 2 M.2 240GB (RAID 1) | 1 |
|  | BOSS Cables and Bracket for R750 (Riser 1) | 1 |
|  | ReadyRails Sliding Rails | 1 |
|  | Cable Management Arm, 2U | 1 |
|  | PowerEdge R750 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) | 1 |
|  | PowerEdge R750 Shipping Material | 1 |
|  | PowerEdge INMETRO Label, BCC | 1 |
|  | PowerEdge R750 CE, CCC, Marking | 1 |
|  | Enterprise Order - EMEA. | 1 |
|  | No Installation Service Selected (Contact Sales Rep for more details) | 1 |
|  | 32GB RDIMM, 3200MT/s, Dual Rank 16Gb BASE x8 | 8 |
|  | 3.84TB SSD SAS RI 24Gbps 512e 2.5in Hot-Plug 1WPD, AG Drive | 9 |
|  | C13 to C14, PDU Style, 10 AMP, 6.5 Feet (2m), Power Cord | 2 |
|  | Intel Ethernet i350 Quad Port 1GbE BASE-T Adapter, PCIe Full Height, V2, FIRMWARE RESTRICTIONS APPLY | 1 |
|  | Dell EMC PowerEdge SFP+ SR Optic 10GbE 850nm | 2 |
|  | UEFI BIOS Boot Mode with GPT Partition | 1 |
|  | No Operating System | 1 |
|  | No Media Required | 1 |
|  | No Systems Documentation, No OpenManage DVD Kit | 1 |
|  | Parts Only Warranty 12 Months | 1 |
|  | ProSupport and Next Business Day Onsite Service Extension, 24 Month(s) | 1 |
|  | ProSupport and Next Business Day Onsite Service Initial, 12 Month(s) | 1 |
|  | Asset Tag - ProSupport (Website, barcode, Onboard MacAddress) | 1 |
|  | Configuration Services, Standard ISG System Report, Deliver Via Email | 1 |
|  | Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM) | 1 |

* 1. Поставляемый ПАК должен устанавливаться на площадке Заказчика.
  2. Все поставляемое оборудование должно быть новым, не бывшим в употреблении, в заводской упаковке и полной комплектации в соответствии с моделями, указанными в спецификации выше.
  3. Условия оплаты - по умолчанию 50% предоплата, 50 после подписания актов выполненных работ;
  4. Локальная техническая поддержка – 3 года.
  5. Срок поставки оборудования – 70 рабочих дней с даты подписания договора.
  6. Срок оказания Поставщиком услуг по установке и настройке поставляемого оборудования – 30 рабочих дней с даты поставки оборудования.
  7. Готовность подписать договор - по умолчанию 10 календарных дней с момента объявления победителя.

1. Требуемые функциональные, технические, качественные и эксплуатационные характеристики программно-аппаратного комплекса Positive Technologies Sandbox**.**
   1. В состав Системы должны входить следующие подсистемы:

* подсистема статического анализа - обеспечивает проверку файлов на основе антивирусных решений нескольких производителей, а также проверку на основе экспертных правил;
* подсистема поведенческого анализа - обеспечивает поведенческий анализ файлов в изолированной виртуальной среде;
* подсистема хранения - обеспечивает хранение поступивших на проверку файлов, а также результатов проверки;
* подсистема управления - предоставляет возможность настройки и работы с системой через пользовательский интерфейс;
* подсистема обновления - предоставляет возможность обновления данных, антивирусных баз, экспертных правил, образов виртуальных машин и программного обеспечения Системы.

### Требования к способам и средствам связи для информационного обмена между компонентами Системы

* Взаимодействие между компонентами Системы должно осуществляться на основе унифицированного информационного способа взаимодействия с использованием стека протоколов TCP/IP и технологии канального уровня Ethernet.
* Данные, предаваемые подсистемой управления на пользовательский интерфейс, должны быть защищены при помощи HTTPS с использованием SSL‑сертификата.

### Требования к характеристикам взаимосвязей создаваемой Системы со смежными системами

#### - система многоуровневой защиты от вредоносного контента должна иметь возможность интеграции с LDAP-серверами на базе Microsoft Active Directory для интеграции с внешними системами аутентификации и бесшовного соотнесения ролей пользователей Системы с ролями Microsoft Active Directory в рамках обеспечения единого входа в Систему (SSO);

* внешней IAM-системой PT Management and Configuration — для интеграции с внешними системами и подключения к Системе в рамках обеспечения единого входа в Систему (SSO);
* межсетевыми экранами уровня приложений, системами обнаружения и предотвращения вторжений или другими системами, поддерживающими протокол ICAP, для проверки файлов, обнаруживаемых этими системами в сетевом трафике, в режиме реального времени;
* системой глубокого анализа сетевого трафика PT Network Attack Discovery — для проверки файлов из захватываемого сетевого трафика в режиме реального времени;
* системой электронной почты - для реализации одного или нескольких взаимодействий: самостоятельной отправки пользователями файлов на проверку с целью получения вердикта по проведенной проверке; автоматической проверки файлов и ссылок, содержащихся в электронных письмах, на наличие ВПО; реализации защиты системы путем блокирования электронных писем и содержащихся в них файлов и ссылок на файлы;
* файловыми серверами для проверки файлов на общих файловых ресурсах;
* системой регистрации событий и выявления инцидентов информационной безопасности (системой класса SIEM) - для передачи сведений об обнаруженных угрозах;
* cистемой сбора и анализа индикаторов компрометации и киберугроз PT CybSI для передачи данных об обнаруженных опасных и потенциально опасных объектах;
* прочими внешними системами централизованного сбора событий (syslog-серверы) для передачи результатов проверки;
* системой точного времени ЛВС Заказчика — для обеспечения единых меток даты/времени.

#### Взаимодействие с внешними LDAP-серверами должно осуществляться по протоколам LDAP или LDAPS.

#### Взаимодействие с системой регистрации событий и выявления инцидентов информационной безопасности должно осуществляться по протоколу syslog.

#### Взаимодействие с файловыми серверами (папкой-шлюзом) должно осуществляться по протоколам SMB версии не ниже 2.1 (SMB 2.1) и (или) NFS версии не ниже 3 (NFSv3).

#### Взаимодействие с внешними системами для передачи результатов проверки должно осуществляться по протоколу syslog.

#### Взаимодействие с межсетевыми экранами уровня приложений, системами обнаружения и предотвращения вторжений или другими системами, поддерживающими протокол ICAP, должно осуществляться по ICAP (RFC 3507).

#### Взаимодействие с системой точного времени ЛВС Заказчика должно осуществляться на основе протокола NTP.

#### система многоуровневой защиты от вредоносного контента должна иметь указанные режимы функционирования:

* штатный - режим функционирования Системы, при котором поддерживается выполнение всех заявленных функций;
* технологический - режим функционирования для проведения регламентных работ по обслуживанию, реконфигурации и модернизации Системы;
* аварийный - режим функционирования при обнаружении сбоев и отказов в работе Системы, ее отдельных подсистем или поддерживающей инфраструктуры.
  1. Требования по обеспечению надежности
* Система должна поддерживать возможность работы в режиме отказоустойчивого кластера.

### Требования по диагностированию системы

* система многоуровневой защиты от вредоносного контента должна осуществлять самодиагностику и оповещение пользователя о сбоях в своей работе.

## Требования к функциям (задачам), выполняемым Системой

### Общие требования

#### Должен поддерживаться анализ:

* файлов (для проведения статического и (или) поведенческого анализа);
* ссылок на файлы (с возможностью загрузки файла по ссылке (при его наличии) для последующего статического и (или) поведенческого анализа).

#### Должны поддерживаться следующие варианты загрузки объектов для анализа (далее также источники объектов для анализа):

* загрузка файлов и ссылок вручную пользователями в Систему через графический веб-интерфейс;
* отправка файлов пользователями на выделенный почтовый адрес Системы;
* получение файлов, прикрепленных к электронным письмам, посредством направления копий писем в Систему или посредством встраивания Системы в почтовый транспорт;
* получение (извлечение) файлов из сетевого трафика (включая веб-трафик) другими средствами и системами, интегрированными с Системой с использованием протокола ICAP;
* получение файлов из сетевых папок общего доступа (анализ файлов в заданной входной папке и перемещение файлов в зависимости от вердикта в выходную папку или в карантин);
* получение файлов через API из других систем;
* загрузка файлов в рамках автоматической повторной проверки из постоянного хранилища (при их наличии в хранилище) в соответствии с заданными условиями проверки.

#### Должна обеспечиваться возможность извлечения файлов из архивов следующих форматов: RAR, 7z, ZIP, Tar, MSI, CAB и ISO.

#### Должен поддерживаться подбор паролей из текстового тела письма для распаковки архивов во вложении письма.

#### Должно обеспечиваться распаковывание вложенных архивов до настраиваемого уровня.

#### Должно обеспечиваться распаковывание сжатых файлов следующих форматов:

* .gz (gzip);
* .z (compress);
* .bz2 (bzip2);
* .lz, .lzma (LZMA);
* .xz (LZMA2).

#### Должна предоставляться возможность отнесения нераспакованных зашифрованных архивов и архивов с превышенной глубиной распаковки к потенциально опасным объектам.

#### Должны поддерживаться черный и белый списки файлов, поступающих на проверку, для исключения файлов из проверки на основе их хеш-сумм (белый список) или автоматического признания файлов опасными (черный список). Черный и белый списки должны срабатывать независимо от результатов проверки.

#### Должны поддерживаться следующие форматы сообщений электронной почты:

* application/CDFV2-corrupt (Outlook MSG);
* message/partial, message/rfc822, multipart/mixed, multipart/alternative, multipart/related (Eml Message).

#### Должна предоставляться возможность блокировки электронных писем при интеграции Системы с почтовым сервером, с возможностью помещения заблокированных писем размером не более 1 ГБ в карантин.

#### Должна предоставляться возможность блокировки объектов, определенных как «потенциально опасные» при работе со следующими источниками:

* системы электронной почты для которых реализовано встраивание Системы в почтовый транспорт (почтовый сервер с установленным агентом, почтовый сервер в режиме фильтрации);
* сетевыми папками общего доступа (источники типа папка-шлюз);
* ICAP-серверами.

#### Должна предоставляться возможность выбора параметров блокировки опасных и потенциально объектов при использовании источников типа «почтовый сервер с установленным агентом, почтовый сервер в режиме фильтрации»:

* всего сообщения;
* опасного содержимого.

#### Должен быть реализован встроенный механизм Anti-Evasion для защиты от техник обхода замкнутых сред предварительного выполнения программ (песочниц).

### Требования к подсистеме статического анализа

#### Должна поддерживаться предварительная, комплексная и многопоточная проверка загруженных файлов на наличие ВПО с использованием следующих средств проверки:

* антивирусного решения ClamAV;
* правил PT ESC.

#### Должна обеспечиваться возможность дополнения (при наличии соответствующих лицензий) набора антивирусных движков следующими решениями:

* Dr.Web Server Security Suite;
* Avast Core Security;
* Kaspersky Web Traffic Security;
* Symantec Protection Engine for Network Attached Storage.

#### Должно обеспечиваться формирование результата проверки, содержащего следующую информацию:

* уровень опасности файла (опасный, потенциально опасный, чистый);
* метаданные файла (наименование, размер);
* хеш-суммы файла, рассчитанные по алгоритмам SHA-1, SHA-2, MD5;
* итоговый результат проверки (обнаружено ВПО, обнаружено потенциально нежелательное ПО, угроз не обнаружено);
* тип вредоносного ПО, определенный каждым из антивирусных решений;
* оценка уровня опасности от каждого из антивирусных решений (опасный, потенциально опасный, угроз не обнаружено), с применением которого проводилось сканирование;
* наличие файла в черном или белом списке;
* версия антивирусных решений, с применением которых проводилось сканирование;
* дата обновления антивирусных баз.

#### Должна обеспечиваться проверка артефактов (файлов), полученных из подсистемы поведенческого анализа.

#### Должна обеспечиваться возможность проверки документов Microsoft Office Word, Microsoft Office Excel, Microsoft Office PowerPoint форматов xls, xlsb, xlsm, xlsx, xltm, xltx, potx, ppam, ppsx, ppt, pptm, pptx, doc, docm, docx на наличие макросов и OLE-объектов.

#### Должна поддерживаться возможность автоматического присвоения статуса «потенциальное опасный» для:

* зашифрованных файлов;
* файлов, содержащих макросы;
* файлов, содержащих OLE-объекты.

### Требования к подсистеме поведенческого анализа

#### Должен выполняться поведенческий анализ, включающий:

* запуск файлов (процессов), имеющих расширения (форматы), описанные в Приложении А, в виртуальной изолированной среде и анализ их поведения;
* выполнение интернет-запросов из изолированной среды.

#### Должны поддерживаться следующие операционные системы, используемые для анализа файлов в изолированной среде:

* Microsoft Windows 7 x64/x86;
* Microsoft Windows 8.1 Update 1 x64;
* Microsoft Windows 10 x64;
* Microsoft Windows Server 2016;
* Microsoft Windows Server 2019;
* Astra Linux Common Edition 2.12.45 «Орел»;
* РЕД ОС 7.3.2 «Муром».

#### Должно обеспечиваться автоматическое масштабирование количества виртуальных машин (изолированных сред) для анализа файлов в зависимости от ресурсов, предусмотренных на этапе технического проектирования (см. раздел 5).

#### Должен быть реализован анализ загруженных файлов на основе заданных правил поведения для обнаружения следующих действий, выполняемых объектом:

* создание файлов;
* запуск процессов;
* создание системных заданий;
* выполнение интернет-запросов;
* обращения к файлам-приманкам, процессам-приманкам и данным из буфера обмена;
* изменения в системном реестре.

#### Должна обеспечиваться возможность выявления буткитов.

#### Должно быть реализовано формирование результата проверки, содержащего следующую информацию:

* журнал событий в изолированной среде (в исходном и нормализованном виде);
* артефакты, созданные в процессе проведения проверки в изолированной среде;
* копию сетевого трафика;
* видеозапись поведения файла.

#### Должно обеспечиваться построение графа, отражающего поведение загруженных файлов в изолированной среде в процессе проведения поведенческого анализа, и отображение его в графическом веб-интерфейсе, реализуемом подсистемой управления.

#### Должно обеспечиваться построение дерева созданных в процессе поведенческого анализа артефактов (файлов, дампов памяти, ссылок).

#### Должен быть реализован сбор дампов памяти процессов при поведенческом анализе и возможность проведения постобработки этих дампов методом статического анализа на основе предустановленных разработчиком Системы правил экспертного анализа.

#### Должно осуществляться кэширование результатов проверки: одинаковые файлы (при совпадении параметров источников проверки), отправленные пользователями на проверку с помощью подсистемы поведенческого анализа, не должны проверяться повторно в течение установленного промежутка времени.

#### Должна предоставляться возможность ведения видеозаписи рабочего стола ОС изолированной среды, на которой должны фиксироваться запуск исполняемого файла и действия, производимые этим файлом.

#### Должно обеспечиваться машинное обучение Системы по результатам поведенческого анализа файлов.

#### Должна поддерживаться возможность включения автоматического выбора виртуальных изолированных сред для конкретных типов файлов, поступающих от источников.

#### Должна поддерживаться настройка параметров проверки при автоматическом выборе виртуальных сред для объектов, поступающих от конкретных источников, в том числе уполномоченный пользователь должен иметь возможность задания:

* типов файлов, проверяемых в изолированной среде с конкретной операционной системой;
* продолжительности наблюдения за файлом;
* необходимость записи видео при проверке файла.

#### Должна поддерживаться возможность включения автоматической остановки выполнения задания на проверку при обнаружении опасных или потенциально опасных файлов.

### Требования к подсистеме хранения

#### Должно обеспечиваться защищенное от неавторизованного доступа хранение:

* образов виртуальных машин, используемых подсистемой поведенческого анализа;
* объектов (файлов, ссылок), собранных (полученных) для анализа;
* результатов проверок;
* объектов, в отношении которых проведен анализ (в том числе для проведения ретроспективного анализа) в хранилище просканированных объектов;
* писем, включая вложенные объекты, помещенных в карантин.

#### Должно обеспечиваться хранение следующих данных о проверенных объектах:

* метаданные проверяемых писем, файлов, ссылок (например, наименования, сведения о размере файла, MIME-тип файла, текст ссылки, сведения об исходной ссылке, сведения о перенаправлении, сведения о наличии ссылки в других объектах, сведения об источнике (адресанте), сведения о наличии копий и теневых копий письма, наличие темы и др.);
* значения хеш-сумм проверяемых файлов;
* дата и время сканирования каждого объекта;
* информация об антивирусах, с помощью которых производилась статическая проверка объекта (имя, версия ядра, версия антивирусной базы, дата обновления антивирусной базы, результат сканирования);
* сведения об артефактах, созданных в процессе поведенческого анализа;
* сессионные трассы (журнал событий — необработанный список событий в простом текстовом формате; журнал нормализованных событий — событий, приведенных к единому виду, пригодному для дальнейшего анализа (в формате JSON); список скоррелированных событий — нормализованных событий, проанализированных с помощью правил корреляции для нахождения закономерностей и выявления опасного и потенциально опасного поведения (в формате JSON); копии сетевого трафика в формате PCAP);
* дампы памяти процессов.

#### Должна обеспечиваться возможность выгрузки данных, перечисленных в п. 4.2.4.2. При выгрузке (скачивании) должны поддерживаться следующие методы сжатия:

* application/gzip (Gzip);
* application/x-compress (Z).

#### Должно обеспечиваться ведение базы знаний по загруженным объектам с привязкой к вынесенным вердиктам.

#### Должно обеспечиваться выполнение следующих действий с просканированными файлами:

* выгрузка (скачивание);
* просмотр истории сканирования.

#### Должно обеспечиваться помещение любых файлов, выгружаемых (скачиваемых) пользователем из хранилища просканированных файлов, в ZIP-архивы с паролем *infected*.

#### Должна поддерживаться возможность поиска объектов в хранилище просканированных объектов.

#### Должна обеспечиваться возможность ограничения объема хранилищ и ротации данных в хранилищах.

### Требования к подсистеме управления

#### Должен предоставляться графический веб-интерфейс, обеспечивающий:

* доступ к функциям системы на основе прав пользователей или их ролей;
* информирование уполномоченных пользователей о состоянии всех подсистем, входящих в состав Системы, и работоспособности Системы;
* отображение результатов работы Системы (подсистем) в виде текстовых и графических материалов (для подсистем статического и поведенческого анализа), а также видеоматериалов (для подсистемы поведенческого анализа).

#### Должна обеспечиваться идентификация, аутентификация и авторизация зарегистрированных пользователей Системы на основе учетных записей.

#### Должна обеспечиваться реализация ролевой модели управления доступом к функциям Системы.

#### Должна обеспечиваться возможность управления (включая создание и изменение) учетными записями пользователей Системы:

* логинами и паролями;
* ролями;
* методами аутентификации (локальная база или LDAP-аутентификация).

#### Должно обеспечиваться бесшовное соотнесение ролей пользователей Системы с ролями Microsoft Active Directory.

#### Должна обеспечиваться возможность генерации пользовательских паролей.

#### Должна обеспечиваться возможность блокировки учетной записи пользователя в Системе.

#### Должна поддерживаться возможность включения анонимной проверки файлов (статический анализ) от незарегистрированных (анонимных) пользователей через веб-интерфейс.

#### Должен поддерживаться выбор ОС изолированной среды для проведения поведенческого анализа.

#### Должна обеспечиваться возможность добавления, изменения, отключения, удаления источников объектов для проверки.

#### Должна предоставляться возможность включения (отключения) сканирования ссылок, поступающих от источников для проверки.

#### Должна обеспечиваться возможность просмотра списка ссылок, не прошедших сканирование.

#### Должна предоставляться возможность выбора (из предустановленного списка) типов файлов от источников для проверки, для которых необходимо проводить поведенческий анализ.

#### Должна обеспечиваться возможность управления средствами проверки (антивирусными движками, встроенным набором правил PT ESC), в том числе включение, отключение.

#### Должна поддерживаться возможность настройки параметров отправки данных в PT Cybsi.

#### Должна поддерживаться возможность управления очередью поведенческого анализа (просмотр, очистка).

#### Должна обеспечиваться возможность задания словаря паролей для анализа архивов, защищенных паролем.

#### Должна обеспечиваться возможность задания паролей для архивов, отправляемых на проверку, при включенной проверке файлов от незарегистрированных (анонимных) пользователей.

#### Должна обеспечиваться возможность сохранения на АРМ пользователя, прошедшего аутентификацию в Системе, результатов поведенческого анализа файлов:

* журнала событий в изолированной среде (в исходном и нормализованном виде);
* созданных артефактов;
* копии сетевого трафика.

#### Должна обеспечиваться возможность формирования и копирования ссылки на конкретную страницу с результатами проверки объектов.

#### Должна обеспечиваться возможность выгрузки отчета по конкретному заданию на проверку файла.

#### Должна обеспечиваться возможность выгрузки отчета о работе Системы в формате CSV с информацией об отображаемых объектах и результатами проверок объектов.

#### Должна поддерживаться возможность выгрузки файлов журналов состояния Системы, в том числе:

* полностью;
* за определенный период.

#### Должна поддерживаться возможность отправки уведомлений по электронной почте об обнаружении опасных и потенциально опасных файлов:

* уполномоченному пользователю;
* отправителю;
* получателю.

#### Должна обеспечиваться возможность управления параметрами отправки уведомлений об обнаружении опасных и потенциально опасных файлов, в том числе:

* включением и отключением отправки уведомлений;
* минимальным уровнем опасности файлов, при которых отправляются уведомления:

1. потенциально опасные;
2. опасные.

### Требования к подсистеме обновления

#### Должна обеспечиваться возможность автоматического обновления программного обеспечения входящего в состав Системы (включая образы виртуальных машин).

#### Должна обеспечиваться возможность автоматизированного (запускаемого в ручном режиме) обновления программного обеспечения входящего в состав Системы (включая образы виртуальных машин).

#### Должна обеспечиваться возможность автоматического обновления баз антивирусных решений и экспертных правил.

1. **Требования к потенциальному Поставщику**
   1. Потенциальный Поставщик должен предоставить на конкурс авторизационное письмо от производителя **Positive Technologies** о том, что имеет право на продажу решения и оказание услуг локальной технической поддержки на территории Республики Казахстан.
   2. В рамках поставки потенциальный Поставщик должен произвести все необходимые работы по установке и настройке поставляемого решения, в соответствии с международными стандартами информационной безопасности и внутренними нормативными правилами на территории Заказчика.
   3. У потенциального Поставщика должно быть в штате не менее 2-х сертифицированных производителем специалистов, с опытом работы не менее 1 года. Квалификация специалиста должна быть подтверждена сертификатами.
   4. Потенциальный Поставщик должен оказывать локальную техническую поддержку 24х7 путем принятия обращений от Заказчика по телефону или по электронной почте (email) в течение 36 месяцев с даты ввода оборудования в промышленную эксплуатацию.