Требования к системе защиты от целевых атакRequirements for Protection
Against Targeted Attacks

# Система защиты от целевых атак должна состоять из следующих подсистем:The system of protection against targeted attacks should consist of the following subsystems:

1. **Подсистема защиты сетевого трафика Network traffic protection subsystem**
* **мульти-протокольный модуль** **multi-protocol module**
* **модуль обнаружения вторжений и сетевых** **атак** **intrusion detection and network** **attack** **module**
1. **Подсистема защиты корпоративного почтового трафика Corporate mail traffic protection subsystem**

## Общие требования General requirements

1. Поддержка следующих форм-факторов: Support for the following form factors:
* ПАК ( hardware appliance ) PACK ( hardware appliance )
* в иртуальн ая машин а ( virtual appliance ) в среде VMware appliance ) in a VMware environment
* virtual Virtual appliance Appliance в at среде environment KVM KVM
1. Поддержка следующих режимов Support for the following modes: р абот ы:
* копией трафика в режиме SPAN SPAN traffic copy
* Работа с копией трафика в режиме TAP Work with a copy of traffic in TAP mode
* Работа с копией трафика в режиме ERSPAN Working with a copy of traffic in ERSPAN mode
1. Поддержка пропускной способности до 10 Гбит на один Bandwidth support up to 10 Gbit per one ПАКPACK
2. Поддержка пропускной способности Bandwidth support до 1 Гбит на up to 1 Gbit per virtual virtual appliance appliance
3. Поддержка внешних балансировщиков и сетевых брокеров для обработки потоков данных, превышающих возможности одного модуля ( F 5, A 10, Citrix , и др.) Support for external balancers and network brokers for processing data flows that exceed the capabilities of a single module ( F 5, A 10, Citrix , etc.)
4. Поддержка сброса TCP сессий (отправка TCP Support for resetting TCP sessions (sending TCP RST ) для выявленных подозрительных активностей RST ) for identified suspicious activities
5. Идентификация Identification соответствия matching протокола of the protocol порту the port
6. Работа с исключениями по типам протоколов Work with protocol type exceptions
7. Работа с исключениями по URL , доменам, контрольным суммам ( хешам ) Work with exceptions by URL , domains, checksums ( hashes )
8. Генерация PCAP для сетевого инцидента с привязкой к отдельным типам правил в целях улучшения детального расследования Generate PCAP for a network incident with specific types of rules in order to improve detailed investigation
9. Поддержка интегрированных песочниц (до 30 образов на одном ПАК ) Support for integrated sandboxes (up to 30 images on one PAK )
10. Поддержка внешних песочниц (кластерная модель до 10 нод ) Support for external sandboxes (cluster model up to 10 nodes )
11. Поддержка передачи инцидентов по syslog в формате CEF Support for incident transfer via syslog in CEF format
12. Поддержка передачи инцидентов по syslog в формате LEEF Support for transmitting incidents via syslog in LEEF format
13. Поддержка передачи инцидентов по e - mail Incident Support transmission by e - mail
14. Поддержка протокола SNMP для мониторинга SNMP protocol support for monitoring

## Требования к анализу Requirements for analysis

1. Идентификация запросов и о тветов для Identification of requests and requests for центров управления ботнетов ( C & C ) botnet control center (C & C)
2. Проверка репутации веб ресурсов при обращении к доменам и URL на основе уже известных или подозрительных данных / контента Checking the reputation of web resources when accessing domains and URLs based on already known or suspicious data / content
3. Идентификация рисков при обращении к новым и непроверенным доменам (без скоринга репутации) и URL Risk identification when accessing new and unverified domains (without reputation scoring ) and URL
4. Проверка легитимности мобильных приложений по репутационной базе Checking the legitimacy of mobile applications on the reputation database
5. Режим ретроспективного анализа URL по ранее сделанным откликам в CDN The mode of retrospective analysis of URLs from previously made responses in the CDN
6. Режим маркировки инцидентов для нерабочего времени суток (тегирование) Incident labeling mode for non-working day (tagging)
7. Возможности Opportunities выявления identify многовекторных multi-vector атак attacks
8. Возможности выявления активностей с использованием Tor Activity Detection Using Tor
9. Возможности выявления в трафике передачи зашифрованных ( запароленных ) объектов (архивов / документов) Possibilities of detecting encrypted ( password-protected ) objects (archives / documents) in traffic
10. Возможность вскрытия и проверки запароленных объектов по заранее подготовленной словарной базе The possibility of opening and checking password-protected objects in a prepared dictionary database
11. Наличие базовых механизмов корреляции, обеспечивающих выявление атаки по отдельным событиям, сопоставляя их ежесуточно The presence of basic correlation mechanisms that ensure the detection of attacks on individual events, comparing them daily
12. Идентификация атак на основе Network Network based attack identification Virus Virus Pattern в протоколе IP Pattern in IP
13. Идентификация атак на основе Network Network based attack identification Virus Virus Pattern в протоколе TCP Pattern in TCP
14. Идентификация атак на основе Network Network based attack identification Virus Virus Pattern в протоколе UDP Pattern in UDP protocol
15. Анализ DNS (идентификация рисков на уровне DNS - запросов / DNS - откликов ) DNS analysis (risk identification at the DNS level - requests / DNS - responses)
16. Идентификация атак и а нализ рисков в следующих протокол ах (как на уровне объектов / файлов , так и на уровне сетевы х активност ей ) : Identification of attacks and a nalysis of risks in the following protocol ah (both at the level of objects / files, and at the level of the network, the active s):
* ARP ARP
* DAMEWARE DAMEWARE
* DCE - RPC DCE - RPC
* DHCP / DHCPv6 DHCP / DHCPv6
* FTP (в том числе FTP (including откликов по протоколу FTP ) FTP responses )
* HTTP HTTP
* ICMP ICMP
* IGMP Igmp
* IMAP 4 IMAP 4
* IRC IRC
* KERBEROS KERBEROS
* LDAP Ldap
* MMS Mms
* POP3 Pop3
* SMTP SMTP
* SNMP SNMP
* SIP Sip
* RADIUS RADIUS
* RDP RDP
* RTMP RTMP
* RTSP / RDT - TCP RTSP / RDT - TCP
* RTSP / RDT - UDP RTSP / RDT - UDP
* RTSP / RTP - TCP RTSP / RTP - TCP
* RTSP / RTP - UDP RTSP / RTP - UDP
* TELNET Telnet
* TFTP Tftp
* VNC VNC
1. Идентификация атак при работе с СУБД MS Identification of attacks when working with MS SQL SQL
2. Идентификация атак при работе с СУБД MySQL Identification of attacks when working with MySQL
3. Идентификация атак при работе с СУБД ORACLE Identification of attacks when working with ORACLE DBMS
4. Идентификация атак при работе с СУБД PostrgreSQL Identification of attacks when working with PostrgreSQL DBMS
5. Идентификация атак в протоколе MODBUS - TCP в АСУТП системах Identification of attacks in the MODBUS - TCP protocol in process control systems
6. Идентификация атак в протоколе MODBUS - UDP в АСУТП системах Identification of attacks in the MODBUS - UDP protocol in process control systems
7. По ддержка следующих протокол ов / приложений для идентификации потенциального источника атаки (свыше 110-ти протоколов и приложений) : According to the following protocol dderzhka s / applications to identify potential attack source (over the 110 minute protocols and applications):
* AIM AIM
* Bittorrent Bittorrent
* Google Google Talk Talk
* RAT Radmin RAT Radmin
* RAT PCAnywhere RAT PCAnywhere
* Skype Skype
* Yahoo Yahoo Web Web Messenger Messenger
* и другие. other.

# Требования к подсистеме защиты сетевого трафика: Requirements for the network traffic protection subsystem:

# *модуль обнаружения вторжений и сетевых атак.* *intrusion detection module and network attacks.*

## Требования к платформе Platform requirements

1. Модуль обнаружения вторжений и сетевых атак должен быть построен на базе системы предотвращения вторжений ( IPS ). The intrusion detection module and network attacks must be built on the basis of an intrusion prevention system ( IPS ).
2. IPS IPS должна быть построена на базе специально разработанной платформы, включающей в себя схему логических элементов, программируемую в условиях эксплуатации ( FPGA ), встроенного коммутатора L 2 и двухплоскостной архитектуре (управление и данные) . should be built on the basis of a specially developed platform, which includes a logic element circuit programmable in operating conditions ( FPGA ), an integrated L 2 switch and a two-plane architecture (control and data) .
3. ОС, используемая в IPS , должна быть проприетарной и не построенной на базе стандартных (таких как Windows , Linux или иной Unix - подобной). The OS used in IPS should be proprietary and not built on the basis of standard ones (such as Windows , Linux or other Unix -like).
4. IPS должна обладать возможностью внесения трафика в доверенную зону и иметь режим bypass для него путем настройки правил, применяемых на аппаратном уровне . IPS should have the ability to add traffic to the trusted zone and have a bypass mode for it by setting the rules applied at the hardware level .
5. IPS должна поддерживать режим " IPS IPS must support IPS on on a a stick " на уровне ядра коммутатора посредством VLAN stick "at the switch core level via VLAN Translation , обеспечивая проверку трафика между VLAN без добавления дополнительных IPS в разрыве на каждый VLAN . Translation , providing verification of traffic between VLANs without adding additional IPS in the gap to each VLAN .

## Требования к отказоустойчивости Resiliency requirements

1. Поддержка Support отказоустойчивого fault tolerant решения (Active-Passive, Active-Active) solutions (Active-Passive, Active-Active)
2. IPS должен работать в сетевом окружении с ассиметричным трафиком с применением защиты фильтрами DV IPS should work in a network environment with asymmetric traffic using protection filters DV
3. HA не должен требовать синхронизации для работы HA should not require synchronization to work.
4. Решение IPS должно поддерживать модульность в контексте горячей замены, обеспечивая режим bypass для трафика даже в процессе замены модуля (пока он отключен на время процедур RMA ) The IPS solution must support modularity in the context of hot-swap, providing bypass mode for traffic even during module replacement (while it is disabled for the duration of the RMA procedures )
5. Решение IPS должно иметь два БП для работы The IPS solution must have two power supplies to operate.
6. Решение IPS должно быть масштабируемым и использовать агрегирование портов ( Link The IPS solution must be scalable and use port aggregation ( Link aggregation ), т.о . aggregation), the point O. чтобы IPS на 5Гб/с можно было превратить в 10Гб/сек устройство, добавив еще один модуль IPS на 5Гб/сек во второй порт so that IPS at 5GB / s can be turned into a 10GB / s device by adding another IPS module at 5GB / s to the second port
7. Решение IPS должно поддерживать режим Layer 2 Fallback для режима bypass трафика (даже в случае включенного энергопитания) на случай невосстановимой ошибки внутреннего ПО (например, повреждение микропрограммы, сбоев памяти и т.п.) The IPS solution must support Layer 2 Fallback mode for traffic bypass mode (even in the case of power on) in case of unrecoverable internal software errors (for example, firmware corruption, memory failures, etc.)
8. Решение IPS должно поддерживать Adaptive IPS solution must support Adaptive Filter Filter Configuration ( AFC ), что позволит сигнализировать или отключать неэффективный фильтр в случае повышенного уровня шума (ложноположительных срабатываний) Configuration ( AFC ), which will signal or disable an ineffective filter in case of high noise levels (false positives)
9. Решение IPS должно поддерживать обновление/перезагрузку ОС без помех, обеспечивая модернизацию ОС на IPS без The IPS solution should support OS update / reboot without interference, providing OS upgrades on IPS without простоев downtime на on сетевом networked уровне level
10. Решение IPS должно иметь возможности по масштабированию вплоть до 100Гб/сек The IPS solution should be able to scale up to 100GB / s.

## Регуляторские требования Regulatory requirements

1. Решение IPS должно быть сертифицировано по IPv 6 в Join IPS solution must be IPv 6 certified in Join Interoperability Interoperability Test Test Command ( JITC ) Command ( JITC )
2. Производитель решения IPS должен быть среди лидеров по найденному числу уязвимостей по последним данным Frost The manufacturer of the IPS solution should be among the leaders in the number of vulnerabilities found according to the latest Frost data. and and Sullivan Sullivan
3. Решение IPS должно обладать сертификатом CC IPS solution must have a CC certificate EAL 3+ EAL 3+
4. Решение IPS должно быть в числе рекомендованных продуктов по последнему отчёту NSS The IPS solution should be among the recommended products for the latest NSS report.
5. Решение IPS должно быть среди лидеров в Gartner IPS solution should be among the leaders in Gartner MQ Mq

## Требования к функциям защиты Security Feature Requirements

1. Движок NG NG engine IPS должен быть "умным" в достаточной степени, чтобы проверять трафик с привязкой к условиям ( if The IPS must be smart enough to inspect traffic with conditions ( if then then else ). else ). В случае подозрительности трафик направляется на анализ в DPI In case of suspicion, traffic is sent for analysis in DPI
2. Движок NG NG engine IPS должен блокировать опасный трафик без дополнительного анализа последовательных пакетов, когда пакеты в неизвестном трафике оказываются опасными IPS should block dangerous traffic without additional sequential packet analysis when packets in unknown traffic prove to be dangerous.
3. Решение IPS должно обеспечивать возможности предотвращения вторжений "из коробки", при этом около 20% активных фильтров должно быть в режиме блокировки по умолчанию The IPS solution should provide out-of-box intrusion prevention, with about 20% of active filters should be in blocking mode by default.
4. Фильтры IPS должны IPS filters must поддерживать support такие such режиме mode действий action как Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit и Quarantine as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine
5. Решение IPS должно поддерживать методы сигнатурного анализа, выявление аномалий протоколов, поиск уязвимостей для выявления атак и вредоносного трафика The IPS solution should support signature analysis methods, detect protocol anomalies, search for vulnerabilities to detect attacks and malicious traffic.
6. Фильтры IPS должны категоризироваться по следующим категориям для простоты управления: IPS filters should be categorized into the following categories for ease of management:

|  |
| --- |
| * Exploits Exploits
 |
| * Identity Theft/Phishing Identity Theft / Phishing
 |
| * Reconnaissance Reconnaissance
 |
| * Security Policy Security policy
 |
| * Spyware Spyware
 |
| * Virus Virus
 |
| * Vulnerabilities Vulnerabilities
 |
| * Network Equipment Network equipment
 |
| * Traffic Normalization Traffic Normalization
 |
| * Peer to Peer Peer to peer
 |
| * Internet Messaging Internet messaging
 |
| * Streaming Media Streaming media
 |

1. Решение IPS должно обладать возможностью гранулированного применения политики безопасности на основе следующих методов: The IPS solution should have the ability to granularly apply security policies based on the following methods:

|  |
| --- |
| * По устройствам IPS (все сегменты) By IPS devices (all segments)
 |
| * По физическим сегментам (однонаправленно и двунаправленно) By physical segments (unidirectional and bidirectional)
 |
| * По VLAN тэгам 802.1 Q (однонаправленно и двунаправленно) By VLAN Tag 802.1 Q (Unidirectional and Bidirectional)
 |
| * По диапазону IP адресов CIDR By CIDR IP Address Range
 |
| * По VLAN тэгам 802.1 Q и CIDR By VLAN Tag 802.1 Q and CIDR
 |
| * Политика МСЭ по профилю защиты ITU Security Profile Policy
 |

1. Наиболее известный метод защиты от уязвимостей нулевого дня - это фильтр с привязкой к конкретной уязвимости. The best-known method of protection against zero-day vulnerabilities is a filter with reference to a specific vulnerability. Решение IPS должно содержать примерно 40% подобных фильтров от общего их числа The IPS solution should contain approximately 40% of these filters of their total number.
2. (производитель должен показать, как было получено значение) (manufacturer must show how the value was obtained)
3. Решение IPS должно поддерживать возможность смягчения атак типа Denial The IPS solution must support the ability to mitigate Denial- type attacks. of of Service ( DoS / DDoS ) на основе SYN Service ( DoS / DDoS ) based on SYN floods floods
4. Решение IPS должно обеспечить лимитирование пропускной способности для контроля нежелательного трафика типа P 2 P , Online The IPS solution should provide bandwidth limiting to control unwanted traffic type P 2 P , Online Game , и т.п. Game , etc.
5. Решение IPS должно поддерживать проверку GTP для мобильных сетей GPRS /3 G IPS solution must support the GTP inspection Mobile GPRS / 3 G networks
6. Решение IPS должно иметь возможность использования репутационного сервиса (по IP адресам или DNS ) для блокировки трафика или "заранее известных плохих узлов" типа spyware , фишинга или C & C An IPS solution must be able to use a reputation service (by IP addresses or DNS ) to block traffic or “known bad sites” such as spyware , phishing or C & C
7. Решение IPS должно поддерживать опцию ' VLAN IPS solution must support the option ' VLAN Translation ' для обеспечения установки вне полосы пропускания (" on Translation 'to provide installation outside the bandwidth (" on a a stick "), но продолжать защищать весь трафик между VLAN таким же образом, как в случае установки в разрыве stick "), but continue to protect all traffic between VLANs in the same way as in the case of installation in a gap
8. Решение IPS должно иметь возможность конвертировать сигнатуры других вендоров (например, snort ) в свои фильтры The IPS solution should be able to convert the signatures of other vendors (for example, snort ) into their filters.
9. Решение IPS должно уметь контролировать заранее известные узлы, такие как spyware , C 2 серверы ( C & C ), спам и прочих в привязке к стране-источнику угрозы, типу и скорингу репутации The IPS solution should be able to control previously known sites, such as spyware , C 2 servers ( C & C ), spam and others in relation to the country of source of threat, type and reputation scoring

## Требования к обновлениям Update Requirements

1. Производитель IPS должен предоставить данные статуса Acknowledgement по Microsoft IPS manufacturer must provide data on the status of Microsoft Acknowledgement Security Security bulletin за последние 3 года, чтобы подтвердить лидерство по числу обнаруженных уязвимостей нулевого дня в продуктах Microsoft bulletin for the last 3 years, to confirm the leadership in the number of zero-day vulnerabilities found in Microsoft products
2. Решение IPS должно поддерживать обновления не менее одного раза в неделю. The IPS solution must support updates at least once a week.
3. Решение IPS должно содержать zero - day фильтры, получаемые в составе еженедельного пакета обновлений The IPS solution must contain zero - day filters received as part of the weekly update package.
4. Производитель IPS должен иметь портал с данным по global IPS manufacturer must have a portal with global data. threat threat intellgence , обеспечивающий мониторинг в реальном времени и статистику по угрозам и атакам, и обладающий следующими возможностями: Intellgence , which provides real-time monitoring and statistics on threats and attacks, and has the following features:

|  |
| --- |
| * Активности по атакам на базе стран и континентов Country and Continent Attack Activities
 |
| * Обеспечение детальности в режиме "сверху вниз" для оценки данных по усточнику угрозы и направлению передаваемых данных для каждого типа атаки Ensuring top-down detail for evaluating data on the threat source and the direction of the transmitted data for each type of attack.
 |
| * Обеспечение мониторинга и выделение недавно появившихся и растущих типов угроз Ensuring monitoring and highlighting newly emerging and growing types of threats
 |

## Требования к локальной системе управления Local Management System Requirements

1. Решение IPS должно поддерживать внеполосный порт ethernet для управления The IPS solution must support an out-of-band ethernet port to manage
2. Решение IPS должно поддерживать SSH 2/ Telnet и HTTPS / HTTP в качестве протоколов управления. The IPS solution should support SSH 2 / Telnet and HTTPS / HTTP as management protocols.
3. Решение IPS должно поддерживать SNMP и служебные MIB , которые могут быть подгружены из Enterprise The IPS solution must support SNMP and service MIBs that can be loaded from Enterprise Management Management Application , таких как HP Application such as HP Openview , MRTG , и т.п. Openview , MRTG , etc.
4. Решение IPS должно управляться локально и независимо (без центрального сервера управления) IPS solution must be managed locally and independently (without a central management server)
5. Решение IPS должно поддерживать отправку событий в формате sysylog , SNMP The IPS solution should support sending sysylog , SNMP events. Traps и без необходимости использования центрального сервера управления Traps and without the need for a central management server

## Требования к централизованной системе управления Requirements for a centralized management system

1. Решение IPS должно поддерживать использование единого сервера управления устройствами IPS IPS solution should support the use of a single IPS device management server.
2. Единый сервер управления должен быть на базе ПАК со встроенной ОС, установленной на заводе A single management server should be based on the PAK with an embedded OS installed at the factory
3. Единый сервер управления должен быть способным управлять набором устройств IPS числом до 25 A single management server must be able to manage a set of IPS devices up to 25
4. Единый сервер управления должен должен обеспечить обновление правил вручную, автоматически или по расписанию A single management server must provide manual update of rules manually or automatically.
5. Единый сервер управления должен должен распространять обновленные правила вручную, автоматически или по расписанию по различным устройствам IPS A single management server must distribute updated rules manually, automatically or according to a schedule across different IPS devices.
6. Единый сервер управления должен должен обеспечивать настраиваемую панель мониторинга ' At - a - glance - Dashboard ' для отображения статуса по трафику и угрозам A single management server should provide a custom dashboard ' At - a - glance - Dashboard ' to display traffic and threat status
7. Единый сервер управления должен служить центральной точкой обеспечения защиты по всем устройствам IPS на уровне политик, включая версионность, откат, резервирование настроек A single management server should serve as a central point of protection for all IPS devices at the policy level, including versioning, rollback, redundancy settings
8. Единый Single сервер server управления of management должен should обеспечивать provide детальную detailed отчетность , включая statements, including данные data по All Attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report for All Attacks, Specific & Top N attack , Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report
9. Единый сервер управления должен поддерживать генерацию отчетов вручную или по расписанию ( Ежедневно , Еженедельно , Ежемесячно и т.п .) A single management server must support the generation of reports manually or according to a schedule ( Daily , Weekly , Monthly , etc. )
10. Единый сервер управления должен поддерживать экспорт отчетов в форматы PDF , HTML , CSV , XML и т.п. A single management server must support exporting reports to PDF , HTML , CSV , XML , etc.
11. Единый сервер управления должен должен поддерживать архивацию и резервирование событий, а также их экспорт на NFS , SMB , SCP и sFTP A single management server must support archiving and reservation of events, as well as their export to NFS , SMB , SCP and sFTP
12. Единый сервер управления должен поддерживать настраиваемы q A single management server must support customizable q RBAC и включать по крайней мере 3 базовых уровня - SuperUser , Administrator и User RBAC and include at least 3 base levels - SuperUser , Administrator and User
13. Единый сервер управления должен поддерживать syslog A single management server must support syslog CEF для отправки событий в Arcsight CEF to send events to Arcsight
14. Единый сервер управления должен поддерживать Acitive A single management server must support Acitive Directory для корреляции ID пользователя Directory for user ID correlation
15. Единый сервер управления должен поддерживать сторонние сканеры VA ( Qualys , A single management server must support third-party VA scanners ( Qualys , Foundstone , Nessus ) для коррекции политик IPS Foundstone , Nessus ) for correcting IPS policies
16. Единый сервер управления должен поддерживать аналитику больших данных на уровне движка, чтобы обеспечить более быструю аналитику и генерацию отчётов A single management server must support big data analytics at the engine level to enable faster analytics and report generation.
17. Единый сервер управления должен поддерживать получение данных в режиме "сверху вниз" на уровне работы с отчётами (например, данные отчёта по top 10 атак за последний год) A single management server must support top-down data retrieval at the report level (for example, report data on top 10 attacks over the past year)
18. Единый сервер управления должен поддерживать панель мониторинга ' threat A single management server must support a ' threat ' dashboard. insights ', отражающую скоррелированные данные по тому, как много скомпрометированных ухлов , сколько собрано данных IOC , данные по интеграции со сторонними сканерами VA , а также информация по числу обнаруженных заранее раскрытых уязвимостей . insights ', reflecting the correlated data on how many compromised digits , how many IOC data is collected , data on integration with third-party VA scanners , as well as information on the number of detected vulnerabilities discovered in advance .

# Требования к п одсистем е з ащит ы корпоративного почт ового трафика Requirements for Protection of Corporate Mail

## Общие требования General requirements

1. Поддержка следующих форм-факторов: Support for the following form factors:
* ПАК ( hardware appliance ) PACK ( hardware appliance )
* virtual virtual appliance appliance в среде VMware in the VMware environment
1. Поддержка следующих режимов Support for the following modes р абот ы: ted s:
* р абота с копией трафика в режиме SPAN Started with a copy of the traffic in the SPAN mode
* р абота с копией трафика в режиме TAP Started with a copy of the traffic in the TAP mode
* р абота с копией трафика в режиме BCC Started with a copy of the traffic in the BCC mode
* р абота в режиме p Handling Mode MTA (режим логического разрыва с удержанием анализируемого объекта до вынесения вердикта ) MTA (logical discontinuity mode with retention of the analyzed object until a verdict is rendered )
1. Анализ почты с поддержкой протокола шифрования TLS Mail Analysis with TLS Encryption Protocol
2. Возможность отдельной настройки действий по уровням риска Ability to customize actions by risk level
3. Наличие карантина почты, доступного администратору (по всем угрозам) Availability of quarantine mail accessible to the administrator (for all threats)
4. Интеграция с Active Integration with Active Directory для административных задач Directory for administrative tasks
5. Привязка политик к пользователям в LDAP Linking policies to users in LDAP
6. Поддержка интегрированных песочниц (до 60 на одно устройство) Integrated sandbox support (up to 60 per device)
7. Поддержка внешних песочниц (кластерная модель до 10 нод ) Support for external sandboxes (cluster model up to 10 nodes )
8. Поддержка передачи инцидентов по syslog в формате CEF Support for incident transfer via syslog in CEF format
9. Поддержка передачи инцидентов по syslog в формате LEEF Support for transmitting incidents via syslog in LEEF format
10. Поддержка передачи инцидентов по e - mail Incident Support transmission by e - mail
11. Перезапись опасных ссылок внутри письма с перенаправлением на страницу с сообщением об опасности (на самом модуле или внутреннем портале организации) Rewriting dangerous links inside a letter with redirection to a page with a danger message (on the module itself or the organization’s internal portal)
12. Создание исключений по словам в URL (предотвращение нарушения работы маркетинговых рассылок) Creating word exceptions in a URL (preventing disruption of marketing newsletters)
13. Создание исключений по отправителям и получателям Creating exceptions by senders and recipients
14. Поддержка чёрных списков отправителей (адреса, домены, IP ) Supports blacklists of senders (addresses, domains, IP )
15. Создание исключений по словам в URL (защита от нарушения работы списков рассылок) Creating word exceptions in a URL (protection against disrupting mailing lists)
16. Поддержка внешних балансировщиков для построения отказоустойчивости Support external balancers for building fault tolerance
17. Поддержка Support протокола SNMP для SNMP protocol for мониторинга monitoring

## Требования к анализу Requirements for analysis

1. Поддержка контентной фильтрации по типам файлов, словам, размерам файлов Support for content filtering by file type, word, file size
2. Поддержка явного запрета запароленных объектов (архивов и документов) Support for explicit prohibition of password-protected objects (archives and documents)
3. Поддержка вскрытия запароленных архивов и документов ( Office , PDF ) по заранее подготовленной словарной базе Support for opening password-protected archives and documents ( Office , PDF ) according to a prepared dictionary base
4. Поддержка вскрытия запароленных архивов и документов ( Office , PDF ) путём автоматического извлечения пароля из тела письма и применения его к вложению (в т.ч . находящемуся в другом письме) Support for opening password-protected archives and documents ( Office , PDF ) by automatically extracting the password from the message body and applying it to the attachment ( including in another letter)
5. Поддержка вскрытия запароленных архивов и документов ( Office , PDF ) методом перебора паролей Support for opening password-protected archives and documents ( Office , PDF ) using password search
6. Поддержка блокировки писем по пороговым значениям Threshold blocking support
7. Возможность выявлять и блокировать вредоносный код в файлах, передаваемых по электронной почте пользователей The ability to detect and block malicious code in files transmitted by e-mail users
8. Предварительные проверки содержимого по репутационным базам до отправки в песочницу (файлы, ссылки) Preliminary checks of the contents of the reputation database before sending to the sandbox (files, links)
9. Механизм перезаписи ссылок с последующим анализом каждого нажатия на них пользователем с целью ретроспективной оценки компрометации целевых страниц средствами облачного Threat The mechanism of rewriting links with the subsequent analysis of each click on them by the user in order to retrospectively assess the compromise of landing pages by means of cloud Threat Intelligence Intelligence
10. Возможность принудительной (ручной) передачи писем для анализа The possibility of forced (manual) transmission of letters for analysis
11. Загрузка содержимого по ссылкам в письме и последующий его анализ Download content by reference in the letter and its subsequent analysis
12. Загрузка содержимого по ссылкам в письме с выдачей объекта через meta - refresh и последующий его анализ Downloading content from links in a letter with object output via meta - refresh and its subsequent analysis
13. Анализ ссылок внутри документов Office и PDF с лимитом не менее 20 ссылок на документ Link analysis inside Office and PDF documents with a limit of at least 20 document links
14. Поддержка песочниц для всех актуальных версий ОС для АРМ WinXP , Win 7, Win 8/8.1/ Win 10 (для всех версий 32/64 бита) Sandbox support for all current OS versions for AWS WinXP , Win 7, Win 8 / 8.1 / Win 10 (for all versions 32/64 bits)
15. Поддержка песочниц для всех актуальных версий ОС для серверов Win 2003, Win 2008, Win 2012, 2016 (64 бита) Sandbox support for all current OS versions for servers Win 2003, Win 2008, Win 2012, 2016 (64 bits)
16. Поддержка создания песочниц на основе собственных шаблонов ОС с прикладным ПО предприятия и возможностью автоматизированной проверки корректности подготавливаемого образа Support for creating sandboxes based on native OS templates with enterprise application software and the ability to automatically verify the correctness of a prepared image
17. Поддержка Support русскоязычных ОС в песочнице Russian-language OS in the sandbox
18. Использование уникальных активационных ключей для Windows , Office и базового ПО песочниц Using unique activation keys for Windows , Office and sandbox base software
19. Поддержка выхода песочниц в интернет через прокси Support for accessing sandboxes to the Internet through a proxy
20. Возможность расширения списка проверяемых типов файлов в песочницах за счет настраиваемого образа пользователем Ability to expand the list of checked file types in sandboxes due to a custom image by the user
21. Возможность расширения списка проверяемых типов файлов в песочницах за счет настраиваемого образа пользователем Ability to expand the list of checked file types in sandboxes due to a custom image by the user
22. Поддержка системы глобального списка «белых приложений» для снижения ложноположительных срабатываний при обработке в песочнице Support for the global list of "white applications" to reduce false positives during sandbox processing
23. Поддержка создания исключений по хэшам , IP , URL , доменам Support for creating exceptions by hashes , IP , URL , domains
24. Возможность детальной настройки критериев для передачи объектов на анализ в песочницах (комбинация протоколов, типов файлов, расширений файлов и прочее) The ability to fine-tune the criteria for transferring objects for analysis in sandboxes (a combination of protocols, file types, file extensions, etc.)
25. Возможность принудительной отправки определённых категорий файлов для анализа в песочницах Ability to force the sending of certain categories of files for analysis in sandboxes
26. Устойчивость к техникам обхода песочниц (в т.ч . по проверке окружения, MAC адресов и таймеров запуска и других механизмов) Resistance to sandbox bypass techniques ( including environmental testing, MAC addresses and launch timers and other mechanisms)
27. Поддержка полноценной симуляции в песочнице для не менее, чем 38 типов объектов ( exe , dll , swf , lnk , doc , xls , ppt , docx , xlsx , pptx , hwp , jtd , pdf , rtf , gul , jar , chm , cell , class , mov , vbs , xml , js , vbe , hwpx , jse , ps 1, hta , wsf , bat , cmd , pub , svg , htm , html , slk , iqy , url ) Full sandbox simulation support for at least 38 object types ( exe , dll , swf , lnk , doc , xls , ppt , docx , xlsx , pptx , hwp , jtd , pdf , rtf , gul , jar , chm , cell , class, mov, vbs, xml, js, vbe, hwpx, jse, ps 1, hta, wsf, bat, cmd , pub, svg, htm, html, slk, iqy, url)
28. Поддержка предварительной проверки для не менее, чем 155 типов объектов ( MS Pre-check support for at least 155 object types ( MS Winword , MS Winword , MS PowerPoint , FNT , MS PowerPoint , FNT , MS Excel , COM , ICO , EXE , SCR , SYS , CPL , DRV , VSD , VXX , OCX , GKS , PCX , CPIO , PPM , AR , ARC , WRT , CAL , BAT , INI , INF , ELF , TD 0, FLI , MAC , XML , HTM / HTML , AS , XDP , ASP , SBFT , PROJECT , ASF , QTM , MPG , PNG , PSP , TGA , PICT , AFC , AI , AIF , ANI , ATM , AVS , C 4 D , CDA , CHL , CMX , CST , DCR , DWD , DWG , IFF , ISU , LWO , MAUD , NEO , RA , RLA , SCENE , SCM , SDS , SFR , SRF , WMF , MBX , USRDEF , CUSDEF , GMS , CPT , WORDPRO , JGF , EPOC , PROCESS , DEX , MSEMF , BPL , UHA , HWP , WIM , ZLIP , XML , TTF , BMP , CLP , TERMINFO , CORE , GRP , JPG , SND , JAVA , PA - RISC Excel , COM , ICO , EXE , SCR , SYS , CPL , DRV , VSD , VXX , OCX , GKS , PCX , CPIO , PPM , AR , ARC , WRT , CAL , BAT , INI , INF , ELF , TD 0, FLI , MAC , XML , HTM / HTML , AS , XDP , ASP , SBFT , PROJECT , ASF , QTM , MPG , PNG , PSP , TGA , PICT , AFC , AI , AIF , ANI , ATM , AVS , C 4 D , CDA , CHL , CMX , CST , DCR , DWD , DWG , IFF , ISU , LWO , MAUD , NEO , RA , RLA , SCENE , SCM , SDS , SFR , SRF , WMF , MBX , USRDEF , CUSDEF , GMS , CPT , WORDPRO , JGF , EPOC , PROCESS , DEX , MSEMF , BPL , UHA , HWP , WIM , ZLIP , XML , TTF , BMP , CLP , TERMINFO , CORE , GRP , JPG , SND , JAVA , PA - RISC executables , C \_ LISP , HP \_ FONT , MMDF , S 800\_ EXE , S 800\_ SEXE , S 800\_ DEXE , S 800\_ SLIB , S 800\_ DLIB , PA \_ ROBJ , RIFF , MSP 1, MSP 2, CMF , TIFF , WP , RAS , PSD , MIDI , DWORD , MP 3, TLB , HLP , BND , BAK , RMF , TTC , SWF , CDR , SAVF , NSF , EPS , QXD , MDI , FLV , OPENDOC , FATBINARY , MACHO , PST , ONENOTE , XAR , DMG , ANDROID \_ CERT , ADB , CRD , FM , GIF , NLM , PS , RTF , NWPDF , NWHLP , NWUNI , VOC , PDF , MSO , SIT , YCODE , LNK )
29. Containers and archives support for opening and checking content inside the listed object types: MSI / MSM , LHA / LHARC , TAR / TGZ , RAR , ACE , XZ , 7 Z , AMG , TNEF , ISO , ARJ , GZ / GZIP , LZW , PKZIP , CAB , CHM , JAR , OFFICE 12, UUE , ADB , HQX , MIME , PDF , EML , LZH , MSG , SIS , BZ 2 / BZIP 2, BIN / MACBIN
30. Detection of 0- day exploits in document files
31. Sandbox threat identification support based on machine learning model data
32. Detailing the analysis results in the sandbox (report, pcap , screenshots, IOC , loaded additional components of malware)
33. Simulation of clicking links (including with redirections ) inside sandboxes with subsequent content analysis
34. Simulation of the transition on short links, followed by content analysis
35. Identifying threats in sandboxes based on Yara profiles
36. Construction of a coherent chain of events in the report for visual presentation of the results of the investigation
37. Access system на on RBAC based
38. Partial transfer of a part of cloud data to the enterprise infrastructure to reduce external calls during reputation checks (files, links)
39. The possibility of a detailed search for incidents across a wide range of parameters while maintaining the search query
40. Ability to save incident details (including reports, description, pcap )
41. Comparison of local incident results with Global Threat Intelligence data on demand
42. The ability to explicitly specify network areas and assets in the enterprise infrastructure for incident details

## Requirements for filtering spam

1. Support filtering mechanism ov :
* DKIM
* DMARC
* SPF
1. Support for anti-spam protection by source reputation
2. Signature based antispam support
3. Availability of personal quarantine mail available to users
4. Sending digests to withheld letters in personal quarantine

Preference will be given to those who have experience in implementation of offered solution in our Region or CIS



**Original text**

Contribute a better translation







**ორიგინალი რუსული ტექსტი:**

Решение IPS должно поддерживать модульность в контексте горячей замены, обеспечивая режим bypass для трафика даже в процессе замены модуля (пока он отключен на время процедур RMA )

თარგმანის უკეთესი ვარიანტის შეთავაზება