ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на проведение работ по внедрению и сопровождению системы защиты от сложных угроз Kaspersky Anti Targeted Attack Platform для АО «ФортеИнвест»

Москва, 2025

**Оглавление**

[1. ОБЩИЕ ПОЛОЖЕНИЯ 3](#_Toc202433219)

[2. НАЗНАЧЕНИЕ И ЦЕЛИ ПРОВЕДЕНИЯ РАБОТ 3](#_Toc202433220)

[3. МЕСТО ВНЕДРЕНИЯ РЕШЕНИЯ 3](#_Toc202433221)

[4. ТРЕБОВАНИЯ К РАБОТАМ 3](#_Toc202433222)

[5. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ 9](#_Toc202433223)

1. Общие положения

Настоящее техническое задание (далее – ТЗ) является исходным техническим документом для определения требований по внедрению и сопровождению системы защиты от сложных угроз Kaspersky Anti Targeted Attack Platform (далее – КАТА) для АО «ФортеИнвест» (далее – Заказчик).

Состав работ:

* Поставка лицензии в соответствии со спецификацией;
* Внедрение решения;
* Сопровождение решения;
* Мониторинг и реагирование на инциденты информационной безопасности с применением внедрённого решения КАТА.

Плановые сроки реализации работ по поставке и внедрению: в течение 90 дней с даты подписания договора.

Срок оказания услуг по сопровождению, мониторингу и реагированию на инциденты: в течение 1 года с даты внедрения решения.

1. Назначение и цели ПРОВЕДЕНИЯ РАБОТ

Целью внедрения решения является повышение уровня защищённости информационной инфраструктуры Заказчика от компьютерных атак. Внедряемое решение KATA и комплекс услуг по мониторингу должны обеспечивать защищённость информационной инфраструктуры Заказчика в соответствии с критериями, установленными в настоящем техническом задании.

1. МЕСТО ВНЕДРЕНИЯ РЕШЕНИЯ

Решение планируется к внедрению в информационной инфраструктуре Заказчика, размещённой:

* Российская Федерация, г. Москва, ул. Новослободская д. 41.
1. Требования к работам
	1. **Общие требования к проведению работ**

Работы реализуются по следующим направлениям:

* Поставка лицензии в соответствии со спецификацией;
* Внедрение решения;
* Сопровождение внедрённого решения;
* Мониторинг инцидентов информационной безопасности (далее – ИБ) с применением решения КАТА.
	+ 1. **Поставка лицензий**

Исполнитель должен осуществить поставку лицензий в соответствии с предоставленной в Таблице №1 спецификацией.

Таблица №1 «Спецификация поставляемых лицензий»

|  |  |  |
| --- | --- | --- |
| **Артикул** | **Наименование** | **Количество** |
| KL4692RAAFA | Kaspersky Anti Targeted Attack Platform Advanced Russian Edition. 1 - Instance 1 year Base Premium License  | 1 |
| KL4704RAXFA  | Kaspersky Anti Targeted Attack Platform EDR Agent Russian Edition. 2500-4999 Node 1 year Base Premium License – | 900 |

* + 1. **Внедрение решения**

 Исполнитель должен осуществить внедрение решения KATA в соответствии с указанными в настоящем ТЗ требованиями и составом работ.

Состав работ:

* Аудит инфраструктуры Заказчика;
* Разработка архитектуры внедрения;
* Внедрение решения в соответствии с Таблицей №2;
* Ввод решения в тестовую/опытную эксплуатацию;
* Реализация программы и методики испытаний (далее – ПМИ), проведение Киберучений в соответствии с Таблицей №3;
* Ввод решения в промышленную эксплуатацию.

Внедрение решения KATA включает в себя настройку до готовности к проведению Киберучений, указанных в настоящем техническом задании.

Таблица №2 «Состав работ по внедрению решения»

|  |  |  |
| --- | --- | --- |
| **№** | **Обозначение** | **Наименование и техническая характеристика** |
| 1 | - | Установка компонентов решения КАТА, проверка работоспособности |
| 2 | - | Установка и настройка компонента Sandbox |
| 3 | - | Подготовка и распространение агентов EDR |

Реализация ПМИ должна включать все проверки, рекомендованные производителем решения, но не ограничиваться ими.

Таблица №3 «Состав проверок по проведению Киберучений»

|  |  |  |
| --- | --- | --- |
| **name** | **TTP** | **test\_name** |
| **Windows** |  |  |
| OS Credential Dumping: LSASS Memory | T1003.001 | Dump LSASS.exe Memory using ProcDump |
| OS Credential Dumping: LSASS Memory | T1003.001 | Dump LSASS.exe Memory using direct system calls and API unhooking |
| OS Credential Dumping: LSASS Memory | T1003.001 | Dump LSASS.exe Memory using Windows Task Manager |
| Command and Scripting Interpreter: PowerShell | T1059.001 | Mimikatz |
| OS Credential Dumping: Security Account Manager | T1003.002 | Registry dump of SAM, creds, and secrets |
| OS Credential Dumping: DCSync | T1003.006 | DCSync (Active Directory) |
| Remote System Discovery | T1018 | Adfind - Enumerate Active Directory Computer Objects |
| Obfuscated Files or Information | T1027 | Obfuscated Command in PowerShell |
| HTML Smuggling | T1027.006 | HTML Smuggling Remote Payload |
| Network Service Scanning | T1046 | Port Scan Angry IP Scanner |
| Network Service Scanning | T1046 | Port Scan NMap for Windows |
| Exfiltration Over Alternative Protocol | T1048 | DNSExfiltration |
| Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | T1048.003 | Exfiltration Over Alternative Protocol - ICMP |
| Scheduled Task/Job: Scheduled Task | T1053.005 | Scheduled Task Executing Base64 Encoded Commands From Registry |
| Process Injection: Asynchronous Procedure Call | T1055.004 | Process Injection via C# |
| Process Injection: Process Hollowing | T1055.012 | Process Hollowing |
| Command and Scripting Interpreter: PowerShell | T1059.001 | Run BloodHound from local disk |
| Command and Scripting Interpreter: PowerShell | T1059.001 | Obfuscation Tests |
| Valid Accounts: Local Accounts | T1078.003 | Create local account with admin privileges |
| System Information Discovery | T1082 | System Information Discovery |
| System Information Discovery | T1082 | winPEAS |
| Ingress Tool Transfer | T1105 | certutil download (urlcache) |
| Ingress Tool Transfer | T1105 | Windows - BITSAdmin BITS Download |
| Brute Force: Password Spraying | T1110.003 | Password Spray all Domain Users |
| Network Share Discovery | T1135 | Network Share Discovery |
| Steal Web Session Cookie | T1539 | Steal Firefox and Chrome Cookies (Windows) |
| Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | T1547.001 | Reg Key Run |
| Credentials from Password Stores: Credentials from Web Browsers | T1555.003 | LaZagne - Credentials from Browser |
| Steal or Forge Kerberos Tickets: Kerberoasting | T1558.003 | Rubeus kerberoast |
| Steal or Forge Kerberos Tickets: AS-REP Roasting | T1558.004 | Rubeus asreproast |
| **Linux** |  |  |
| OS Credential Dumping: /etc/passwd and /etc/shadow | T1003.008 | Access /etc/{shadow,passwd} with a standard bin that's not cat |
| System Information Discovery | T1082 | List OS Information |
| Network Service Scanning | T1046 | Port Scan Nmap |
| Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | T1048.003 | Exfiltration Over Alternative Protocol - DNS |
| Scheduled Task/Job: Cron | T1053.003 | Cron - Add script to /var/spool/cron/crontabs/ folder |
| Command and Scripting Interpreter: Bash | T1059.004 | LinEnum tool execution |
| SSH Authorized Keys | T1098.004 | Modify SSH Authorized Keys |
| Brute Force: Password Guessing | T1110.001 | SUDO brute force  |
| Network Share Discovery | T1135 | Network Share Discovery - linux |
| Create Account: Local Account | T1136.001 | Create a new user in Linux with `root` UID and GID. |
| Create or Modify System Process: Systemd Service | T1543.002 | Create Systemd Service |
| Abuse Elevation Control Mechanism: Setuid and Setgid | T1548.001 | Set a SetUID flag on file |
| Event Triggered Execution: .bash\_profile and .bashrc | T1546.004 | Add command to .bashrc |
| Unsecured Credentials: Bash History | T1552.003 | Search Through Bash History |
| Unsecured Credentials: Private Keys | T1552.004 | Discover Private SSH Keys |

* + 1. **Сопровождение внедрённого решения**

В рамках сопровождения Исполнитель должен осуществлять следующие услуги:

* Восстановление работоспособности внедренного решения и ее компонентов;
* Консультации Заказчика по различным вопросам эксплуатации решения;
* Корректировка настроек и конфигураций решения;
* Консультации по развитию использования решения.
	+ 1. **Мониторинг и реагирование на инциденты информационной безопасности**

Услуги по мониторингу оказываются с использованием внедрённого решения КАТА.

Состав услуг по мониторингу:

* + Услуги по мониторингу инцидентов по гибридной модели;
	+ Развитие и модернизация решения.

Услуги по мониторингу инцидентов информационной безопасности по гибридной модели включают в себя:

* Мониторинг инцидентов и реагирование в строгом соответствии с параметрами оказания услуги (SLA) (Таблица № 4);
* Разбор инцидентов, фильтрация ложных срабатываний, установление первичных причин их возникновения;
* Разработка и предоставление рекомендаций по ликвидации последствий подтвержденных инцидентов;
* Предоставление отчетности по инцидентам и принятым мерам.

Таблица № 4 - Параметры оказания услуг по мониторингу

| **Название параметра** | **Значение параметра** |
| --- | --- |
| Аппаратные мощности для установки компонента сбора событий | Предоставляет Заказчик |
| Количество расследуемых инцидентов | Все критичные инциденты информационной безопасности |
| Разработка сценариев реагирования | Не более 3-х в квартал |
| Периодичность предоставления отчетности | 1 раз в квартал |
| **Мониторинг инцидентов ИБ** |
| Период предоставления услуг | 24\*7\*365 |
| Время регистрации инцидента ИБ | Высокая критичность | до 15 минут |
| Средняя критичность | до 15 минут |
| Низкая критичность | до 15 минут |
| Первичный анализ, проверка на false positive, формирование первичного отчета | Высокая критичность | до 2 часов |
| Средняя критичность | до 4 часов |
| Низкая критичность | до 8 часов |
| Расширенный анализ, разработка расширенных рекомендаций с анализом последствий и вектора атаки (в случае подтверждения инцидента) | Высокая критичность | до 12 часов |
| Средняя критичность | До 24 часов |
| Низкая критичность | до 30 часов |
| Разработка и отправка отчета по инциденту (в случае подтверждения инцидента) | Высокая критичность | До 6 часов |
| Средняя критичность | До 10 часов |
| Низкая критичность | До 14 часов |
| **Обеспечение доступности услуги** |
| Период обслуживания платформы | 24\*7\*365 |

Порядок оказания услуг по мониторингу и реагированию на инциденты информационной безопасности должен в себя включать:

• Выявление и регистрация всех инцидентов ИБ, зафиксированных внедренным решением;

• Первичная обработка выявленного инцидента ИБ: базовая диагностика (обработка ложных срабатываний сценария), уточнение критичности инцидента, исходя из данных, полученных при анализе. На основании предоставленной информации Заказчик вправе повысить или понизить критичность инцидента для изменения процесса его обработки;

• Анализ инцидента ИБ: установление причин и источника инцидента на основе информации, полученной в рамках работы внедренного решения, передача информации Заказчику.

• Информирование ответственного специалиста (группы) Заказчика о факте обнаружения инцидента в соответствии с SLA из Таблицы 4;

• Сбор и обработка дополнительной информации по запросу уполномоченных специалистов Заказчика в рамках расследования инцидентов;

• В рамках реализации услуг по мониторингу создаются сценарии реагирования для предоставления Заказчику согласно SLA в Таблице 4.

• Анализ событий, обрабатываемых центром мониторинга Исполнителя, для выявления аномалий, потенциально являющихся инцидентами, но не соответствующие текущим сценариям обнаружения инцидентов;

• Проверка индикаторов компрометации, получаемых Исполнителем в рамках информационного обмена с партнерами;

• Проверка критических индикаторов компрометации, получаемых Исполнителем в рамках взаимодействия с Заказчиком. Осуществляется по запросу.

 • Доработка существующих сценариев обнаружения инцидентов для снижения количества ложных срабатываний.

1. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ

Исполнитель (в том числе каждое юридическое и/или физическое лицо, выступающее на стороне одного участника) должен:

* не иметь задолженности по уплате налогов (сборов, пеней, налоговых санкций) в бюджеты всех уровней и обязательных платежей в государственные внебюджетные фонды;
* не находиться в процессе ликвидации;
* не быть признанным несостоятельным (банкротом);
* не иметь наложенного ареста на имущество, экономическая деятельность участника не должна быть приостановлена;
* не находиться в реестрах недобросовестных поставщиков.
* иметь действующую лицензию ФСТЭК России на деятельность:
* по технической защите конфиденциальной информации в области проектирования в защищенном исполнении средств и систем информации;
* по оказанию услуг контроля защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации,
* по оказанию услуг контроля защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* по мониторингу информационной безопасности средств и систем информатизации;
* по установке, монтажу, наладке, испытаний средств защиты информации.
* обладать опытом работы в области защиты информации не менее 5 лет;
* иметь не менее 5 штатных сотрудников с профильным образованием в области информационной безопасности;
* Для проведения Киберучения иметь сертифицированных социалистов по тестированию на проникновение:
1. Сертификат Offensive Security Web Expert (OSWE);
2. Сертификат Offensive Security Certified Professional (OSCP);
3. Сертификат Offensive Security Experienced Penetration Tester (OSEP);
4. Сертификат Offensive Security Certified Expert (OSCE).
* иметь подтверждённый опыт внедрения Kaspersky Anti Targeted Attack Platform – не менее 3-х проектов;
* иметь статус от компании Касперского - Extended Detection and Response;
* Иметь следующие сертификаты от компании Касперского:

|  |  |
| --- | --- |
| **Наименование сертификата** | **Количество сертифицированных инженеров** |
| Certified Professional: Kaspersky Symphony XDR Core (032.1.1) | Не менее 1-ого |
| Certified Professional: Kaspersky Secure Mail Gateway (036.2.1) | Не менее 1-ого |
| Certified Professional: KUMA (034.3.2) | Не менее 1-ого |
| Certified Professional: KATA Platform & EDR Expert (025.6) | Не менее 1-ого |
| Sales Specialist: Kaspersky Endpoint Security for Business (S02.12) | Не менее 1-ого |
| Certified Professional: Kaspersky Threat Intelligence Presales (P39.03) | Не менее 1-ого |
| Certified Professional: KATA Platform & EDR Expert (025.5) | Не менее 1-ого |
| Certified Professional: Kaspersky Industrial CyberSecurity (038.4) | Не менее 1-ого |
| Sales Specialist: Kaspersky Industrial CyberSecurity (S38.41) | Не менее 1-ого |
| Certified Professional: Kaspersky Security for Microsoft Exchange Server (003.90) | Не менее 1-ого |
| System Engineer Level 1.1 | Не менее 1-ого |
| System Engineer Level I | Не менее 1-ого |
| System Engineer: Kaspersky Security Center. Systems Management (009.12) | Не менее 1-ого |
| Certified Professional: Kaspersky Endpoint Security and Management (002.12.1) | Не менее 1-ого |

* обладать сертификатом соответствия системы менеджмента качества требованиям международного стандарта ISO 900l: 2015 (ГОСТ Р ИСО 9001-2015);
* иметь не менее 2-х штатных сотрудников, имеющих сертификат соответствия системы менеджмента качества требованиям международного стандарта ISO/IEC 9001:2015;
* обладать сертификатом соответствия системы менеджмента информационной безопасности в соответствии с требованиями международного стандарта ГОСТ Р ИСО/МЭК 270012006 (ISO/IEC 27001:2013);
* иметь не менее 3-х штатных сотрудников, имеющих сертификат соответствия аудитора ГОСТ Р ИСО/МЭК 27001 2006 (ISO/IEC 27001:2013).

**5.1 Требование к проектному управлению**

* Организация работ должна строиться таким образом, чтобы оптимизировать объем задействованных ресурсов со стороны Заказчика;
* Должен быть предложен ролевой состав проектной группы со стороны Исполнителя и Заказчика, а именно должны быть указаны лица, ответственные за управление проектом, разработку документации, проведение технических работ;

**5.2 Требования по обеспечению конфиденциальности выполнения работ**

Согласно действующему законодательству и нормативным документам, принятым у Заказчика, должны быть реализованы следующие меры по обеспечению конфиденциальности выполнения работ:

* Информация, полученная Исполнителем в процессе выполнения работ, не может быть передана третьим лицам без согласия Заказчика;
* Исполнитель должен обеспечивать безопасность передаваемой ему информации Заказчика.

**5.3 Дополнительные требования**

Материалы, полученные по результатам работ, должны быть подготовлены и оформлены на русском языке с использованием MS Office 2010/2016 (Word, Excel, PowerPoint).

Разрабатываемая документация должна быть представлена в электронном и бумажном видах в 1 экземпляре.