|  |  |
| --- | --- |
|  |  |
| Заказчик: | ООО «Группа компаний «Иннотех» |
|  |  |
| Документ: | ТЕХНИЧЕСКОЕ ЗАДАНИЕСистема виртуальных ловушек  |
|  |  |
| Страниц: | 20 |
|  |  |
|  |

Содержание

[Перечень Сокращений и терминов 4](#_Toc172039968)

[1. Общие сведения 6](#_Toc172039969)

[1.1. Полное наименование Системы и ее условное обозначение 6](#_Toc172039970)

[1.2. Сведения о Заказчике и Исполнителе 6](#_Toc172039971)

[1.3. Границы проекта 6](#_Toc172039972)

[2. Назначение и цели создания системы 6](#_Toc172039973)

[2.1. Назначение системы 6](#_Toc172039974)

[2.2. Цели создания Системы 6](#_Toc172039975)

[2.3. Задачи Системы 6](#_Toc172039976)

[3. Требования к архитектуре системы 6](#_Toc172039977)

[3.1. Общие требования 6](#_Toc172039978)

[3.2. Требования к режимам функционирования системы 7](#_Toc172039979)

[3.3. Требования к диагностированию системы 7](#_Toc172039980)

[3.4. Требования к показателям назначения 7](#_Toc172039981)

[3.5. Требования к ролевой модели системы 8](#_Toc172039982)

[4. Функциональные требования к системе 8](#_Toc172039983)

4.1. Требования к структуре и функционированию Системы 8

[4.2. Требования к масштабированию Системы 8](#_Toc172039986)

[4.3. Требования к функциям, выполняемым системой 8](#_Toc172039993)

[5. Требования к информационной безопасности 15](#_Toc172040000)

[5.1. Требования по обеспечению информационной безопасности системы 15](#_Toc172040001)

[5.2. Регистрация значимых событий информационной безопасности 15](#_Toc172040002)

[5.3. Требования к защите информации от несанкционированного доступа 16](#_Toc172040003)

[6. Требования к составу и содержанию работ 16](#_Toc172040004)

[6.1. Этап 1. Поставка ПО и проектирование 16](#_Toc172040005)

[6.2. Этап 2. Пуско-наладочные работы 16](#_Toc172040006)

[6.3. Этап 3. Функциональное тестирование 17](#_Toc172040015)

[6.4. Этап 4. Опытная эксплуатация 17](#_Toc172040016)

[6.5. Этап 5. ПСИ 17](#_Toc172040017)

[7. Работы, выполняемые Заказчиком самостоятельно 17](#_Toc172040018)

[8. Порядок контроля и приемки результатов работ 17](#_Toc172040019)

[9. Требования к Исполнителю работ 18](#_Toc172040020)

[10. Требования к срокам выполнения работ 18](#_Toc172040021)

[11. Требования к документированию 19](#_Toc172040022)

[11.1. Требования к составу документации 19](#_Toc172040023)

Перечень Сокращений и терминов

В настоящем документе применены следующие сокращения и термины:

БД: База данных

ИБ: Информационная безопасность

ИС: Информационная система

ОС: Операционная система

ОЭ: Опытная эксплуатация

ПМИ: Программа и методика испытаний

ПНР: Пуско-наладочные работы

ПСИ: Приемо-сдаточные испытания

ПО: Программное обеспечение

Система: Система виртуальных ловушек

УЗ: Учетная запись

ФТ: Функциональное тестирование

AD: Microsoft Active Directory

MiTM: Технология, которая позволяет перехватывать, модифицировать, инспектировать поток трафика.

RDP: Remote Desktop Protocol. Протокол удаленного рабочего стола.

TTP: Тактики, техники и процедуры злоумышленников. (по матрице MITRE ATT&CK)

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IP: Internet Protocol

FTP: File Transfer Protocol

SFTP: Secure File Transfer Protocol

LDAP: Lightweight Directory Access Protocol

SMB: Server Message Block

SQL: Structured Query Language

SSH: Secure Shell

TCP: Transmission Control Protocol

FQDN: Fully qualified domain name

Syslog: System logging protocol

CEF: Common Event Format

TLS : Transport Layer Security

LLMNR: Link-Local Multicast Name Resolution

mDNS: Multicast Domain Name System

NBT-NS: NetBIOS over TCP/IP

SIEM: Система сбора и анализа событий ИБ

Инцидент ИБ: одно или несколько нежелательных или неожиданных событий ИБ, которые со значительной вероятностью указывают на компрометацию бизнес-процессов или реализованную угрозу ИБ.

Ловушка: эмулированные сервисы под управлением реальных операционных систем, развернутые с целью имитации легитимных активов.

Ложноположительное срабатывание: срабатывание системы информационной безопасности в отсутствии реального инцидента информационной безопасности (ошибка первого рода).

Приманка: объект (файл, А-запись, мета информация и т.п.), размещаемый на конечных узлах в инфраструктуре Компании, содержащий данные (ссылку на сервис, аутентификационные данные и т.п.) о ловушках.

Угроза ИБ: возможная причина нежелательного инцидента ИБ, который может нанести ущерб системе или организации.

Цифровой отпечаток: совокупность данных об устройстве, его компоненте или приложении (например, браузере), позволяющая однозначно идентифицировать его.

A-запись: адресная запись в системе доменных имен, определяющая соответствие между именем и IP-адресом.

SIEM: система, предназначенная для анализа в реальном времени событий информационной безопасности, исходящих от источников событий и создания уведомление о потенциальных инцидентах ИБ в соответствии с правилами корреляции.

1. Общие сведения

Настоящий документ определяет функциональные и технические требования к созданию Системы виртуальных ловушек.

* 1. Полное наименование Системы и ее условное обозначение

Полное наименование: Система виртуальных ловушек.

Краткое наименование: СВЛ, Система.

* 1. Сведения о Заказчике и Исполнителе

Заказчик – ООО «Группа компаний «Иннотех»

Исполнитель по проекту должен быть определен по результатам проведения конкурсных процедур.

* 1. Границы проекта

Информация о предприятиях, затрагиваемых в процессе разработки проекта, представлена в таблице Таблица 1.

1. Границы проекта

| № п.п. | Наименование предприятия | Адрес объекта |
| --- | --- | --- |
|  |  ООО «Группа компаний «Иннотех» |  123112, Город Москва, вн.тер.г. муниципальный округ Пресненский, наб Пресненская, д. 12, помещ. 9/60 |

1. Назначение и цели создания системы
	1. Назначение системы
2. Система предназначена для раннего обнаружения направленных атак на корпоративную сеть компании;
3. Принцип работы системы заключается в распространении ловушек и приманок в корпоративной сети компании и своевременном реагировании на инциденты ИБ, которые связаны с использованием злоумышленниками распространенных приманок и ловушек.
	1. Цели создания Системы

Целью создания и функционирования Системы является повышение эффективности системы обеспечения информационной безопасности путем раннего обнаружения направленных атак на корпоративную сеть.

* 1. Задачи Системы

Система решает следующие задачи:

* Обеспечение раннего обнаружения действий злоумышленника;
* Создание объектов, имитирующих активы инфраструктуры, для привлечения к ним внимания злоумышленников с целью раннего обнаружения;
* Выявление внутренних нарушителей с высоким уровнем привилегий, стремящихся нанести ущерб организации;
* Замедление движения злоумышленника внутри корпоративной сети, которое вызовет необходимость выполнений дополнительных действий и шагов, провоцируя на ошибку и обнаружение;
* Обеспечение оперативности оповещений о скомпрометированных активах;
* Снижение уровня ложных срабатываний применительно к инцидентам ИБ;
1. Требования к архитектуре системы
	1. Общие требования
		1. Все подсистемы Системы должны поддерживать развертывание в среде виртуализации;
		2. Все подсистемы Системы должны быть расположены в инфраструктуре Заказчика. Обрабатываемая в системе информация не должна передаваться за пределы инфраструктуры Заказчика;
		3. Все подсистемы должны поддерживать установку на:
* Microsoft Windows Server 2016 и выше;
* Astra Linux SE 1.6 и выше, с английской и русской локализацией систем;
* Debian 11 и выше;
	+ 1. Система не должна требовать установки агентского ПО на рабочие станции и сервера для распространения приманок;
		2. В Системе должна поддерживаться интеграция с доменными службами Microsoft Active Directory для аутентификации пользователей в системе;
		3. Система должна иметь возможность поддержки нескольких доменов Active Directory в рамках одного сервера управления;
		4. Система должна иметь возможность управления приманками не менее, чем на 5000 хостах;
		5. Подсистема управления Системой должна иметь возможность управления не менее, чем 200 подсистемами управления ловушек;
		6. Подсистема управления Системой должна иметь возможность управления не менее, чем 30 дочерними подсистемами управления;
		7. Система должна поддерживать специфику русского языка и русскоязычную морфологию, а также специфику английского языка и английскую морфологию при генерации приманок и ловушек;
		8. Требуемый в соответствии с настоящим документом функционал должен быть реализован в составе законченного комплекта ПО, не требовать доработки и/или разработки дополнительных программных средств с использованием API или иного дополнительного ПО;
		9. При реализации Системы должно применяться только лицензионное программное обеспечение.
	1. Требования к режимам функционирования системы

Система должна обеспечивать возможность работы в следующих режимах:

1. штатный режим (непрерывная круглосуточная работа). Режим, при котором Система работает без сбоев и выполняют обмен данными, Система реализует свою функциональность в полном объеме. Нормальный режим функционирования Системы должен рассчитываться исходя из формулы 24\*7\*365;
2. сервисный режим (для проведения обслуживания, реконфигурации и модернизации компонентов). Режим, при котором в Системе по запланированному графику проводится обслуживание, реконфигурация или обновление модулей. В данном режиме все модули Системы функционируют в полном объеме и обеспечивают информационный обмен между компонентами, не затронутыми работами на обновляемом модуле;
3. аварийный режим (в случае отсутствия связи между компонентами системы или с внешними сетями, для доступа к конфигурационной и архивной информации). Режим, при котором Система продолжает работу в случае выхода из строя одного из функциональных модулей. В данном режиме все модули Системы, кроме вышедшего из строя модуля, функционируют в полном объеме и обеспечивают информационный обмен между компонентами, не затронутыми сбоем вышедшего из строя модуля.
	1. Требования к диагностированию системы

Система должна предоставлять возможность диагностирования неисправностей любого из компонентов Системы и уведомления об этом администраторов Системы (ведения соответствующих журналов работы Системы, уведомлений).

* 1. Требования к показателям назначения

Система должна соответствовать требованиям в части показателей назначения, приведенным в таблице 244.

1. Требования к показателям назначения

| № п/п | Параметр | Значение |
| --- | --- | --- |
|  | Утилизация ЦП Системы, минимальная и максимальная (в пиках) | 40-70 % |
|  | Утилизация оперативной памяти, минимальная и максимальная (в пиках) | 40-70 % |
|  | Утилизация сетевых интерфейсов, минимальная и максимальная (в пиках) | 40-70 % |
|  | Утилизация системы хранения данных, минимальная и максимальная (в пиках) | 40-70 % |
|  | Количество администраторов, одновременно работающих с Системой  | 20 |
|  | Время отклика административных консолей  | 5 с |
|  | Нормальный режим функционирования Системы | 24\*7\*365 |

* 1. Требования к ролевой модели системы

Система должна поддерживать следующие роли пользователей системы:

* Администратор. Доступен весь функционал системы.
* Аналитик. Доступен полный функционал работы с инцидентами ИБ и просмотр на остальной функционал.
* Наблюдатель. Доступен только просмотр.
1. Функциональные требования к системе
	1. Требования к структуре и функционированию Системы
		1. Система должна быть реализована в виде программного обеспечения распределенной структуры и состоять из следующих модулей:
* единый централизованный модуль управления – подсистема управления Системой;
* распределенные модули размещения ловушек – подсистема управления ловушками;
* распределённые модули для управления приманками и ловушками на объектах распределенной инфраструктуры, которые будут устанавливаться на отдельные сервера – дочерняя подсистема управления.
	1. Требования к масштабированию Системы
		1. Система должна обладать возможностью горизонтального и вертикального масштабирования путем увеличения вычислительных мощностей и добавления дополнительных серверов в архитектуру;
		2. Система должна иметь возможность масштабирования путем подключения дополнительных подсистем управления ловушек без изменения архитектуры;
		3. Система должна поддерживать способность к увеличению функциональных возможностей путем наращивания числа функциональных блоков, выполняющих одни и те же задачи, без фундаментальной перестройки архитектуры или модели реализации
		4. Технические решения по созданию Системы должны предусматривать возможность ее дальнейшего развития и модернизации в соответствии с потребностями Заказчика.
	2. Требования к функциям, выполняемым системой
		1. Требования к подсистеме управления приманками
			1. Подсистема управления приманками должна иметь возможность обеспечивать на рабочих станциях и серверах функционирование приманок, включая: распространение, удаление, обновление, модификацию, мониторинг;
			2. Подсистема управления приманками должна обеспечивать автоматическое создание приманок из веб интерфейса Системы;
			3. Подсистема управления приманками должна предоставлять возможность автоматического создания индивидуального профиля приманок под каждый хост, в зависимости от используемого на нем системного и прикладного программного обеспечения;
			4. Система должна иметь возможность адаптивной генерации приманок в формате учетных записей на основе данных с LDAP-каталогов:
* Microsoft LDAP;
* IPA LDAP;
* OpenLDAP.
	+ - 1. Подсистема управления приманками должна иметь возможность адаптивной генерации приманок в формате учетных записей на основе данных с LDAP каталога;
			2. Подсистема управления приманками должна иметь возможность адаптивной генерации приманок в формате учетных записей на основе шаблона, заданного администратором Системы;
			3. Подсистема управления приманками должна иметь возможность выключения генерации приманок в формате учетных записей;
			4. Подсистема управления приманками должна иметь возможность генерации приманок в формате учетных записей в соответствии с предустановленными и определенными пользователем системы правилами наименования;
			5. Подсистема управления приманками должна иметь возможность выполнять поиск в доменах Active Directory неиспользуемых и отключенных учетных записей для их использования в качестве приманок в формате учетных записей;
			6. Подсистема управления приманками должна иметь возможность выполнять ротацию приманок на хостах с помощью конфигурации следующих параметров:
* Время жизни приманки на хосте;
* Время устаревания профиля с приманками;
* Время жизни профиля с приманками.
	+ - 1. Подсистема управления приманками должна иметь возможность генерации приманок в формате учетных записей с любым типом приманки, используя пароль, отличный от реального пароля в Active Directory;
			2. Подсистема управления приманками должна иметь аналитический механизм создания профилированных приманок в Active Directory: автоматическое заполнение атрибутов для AD приманок на основе анализа объектов в LDAP каталоге;
			3. Подсистема управления приманками должна иметь возможность автоматического комбинирования приманок в формате учетных записей и ложных целей в рамках заданных пользователем системы политик;
			4. Подсистема управления приманками должна поддерживать различные наборы приманок для рабочих станций под управлением всех следующих ОС:
* Windows;
* Linux;
* MacOS.
	+ - 1. Подсистема управления приманками должна поддерживать распространение приманок в инфраструктуре виртуальных рабочих столов и иметь настройки для конфигурирования под такую архитектуру;
			2. Подсистема управления приманками должна поддерживать распространение приманок в инфраструктуре удаленных рабочих столов (RDS) и корректно обрабатывать многопользовательские конечные хосты;
			3. Подсистема управления приманками должна обеспечивать создание, распространение и функционирование приманок, содержащих сохраненные данные подключения к следующим сетевым службам:
* сервисы удаленного доступа к файлам (SMB);
* сетевые файловые ресурсы (FTP, SFTP);
* веб-сервисы (HTTP, HTTPS);
* сервисы удаленного управления (SSH);
* службы удаленных рабочих столов (RDP);
* СУБД.

На рабочих станциях и серверах c ОС Microsoft Windows следующими способами:

* в Windows Credential Manager;
* в браузерах Mozilla Firefox, Google Chrome, Microsoft Internet Explorer и Edge;
* в файлах конфигурации службы подключения к удаленному рабочему столу Microsoft Windows (.rdp);
* в текстовых файлах;
* в реестре;
* в скриптах PowerShell;
* в конфигурационных файлах для подключения к СУБД;
* в виде сохраненных подключений к сетевым ресурсам;
* внедрение в память процесса Lsass.exe (в части распространения, обновления, модификации, мониторинга).

На рабочих станциях и серверах c ОС Linux и MacOS следующими способами:

* в скриптах bash (.sh);
* в виде истории SSH-, FTP-, HTTP-подключений;
* в виде истории команд терминала;
* в виде ключей SSH;
* в конфигурационных файлах для подключения к БД;
* в файлах.
	+ 1. Требования к подсистеме управления ловушками
			1. Подсистема управления ловушками должна поддерживать возможность установки стороннего ПО, поддерживаемого ОС, на котором установлен сам компонент;
			2. Подсистема управления ловушками должна обеспечивать функционирование средне-интерактивных и высоко-интерактивных ловушек, включая: включение, выключение, эмуляцию, обновление, модификацию, мониторинг, управление, контроль ловушек и эмулированных на них служб и протоколов;
			3. Подсистема управления ловушками должна иметь возможность автоматической генерации множества A-записей для каждого IP-адреса северов ловушек и дальнейшего их размещения на корпоративных DNS серверах организации для использования в качестве приманок;
			4. Подсистема управления ловушками должна генерировать PowerShell сценарии для автоматического заведения A-записей ловушек на DNS серверах;
			5. Подсистема управления ловушками должна иметь возможность загрузки DNS зоны инфраструктуры Заказчика с помощью csv файла для последующего автоматического анализа;
			6. Подсистема управления ловушками должна обеспечивать функционирование на ловушках следующих сетевых служб и протоколов:
* сервисы удаленного доступа к файлам (SMB) - доступ к его файловой системе;
* сетевые файловые ресурсы (FTP, SFTP);
* веб-сервисы (HTTP, HTTPS) - имитация страницы ввода логина и пароля с авторизацией с возможностью установки собственного шаблона;
* сервисы удаленного управления (SSH) с поддержкой логирования действий пользователей на данном типе ловушек с последующей передачей в карточку инцидента ИБ;
* службы удаленных рабочих столов (RDP и VNC);
* базы данных (PostrgeSQL, MongoDB, MSSQL, MySQL, Redis) с поддержкой логирования действий пользователей на данном типе ловушек с последующей передачей в карточку инцидента ИБ;
* протоколы управления сетевым оборудованием (SNMP и UPnP);
* протоколы управления IoT-устройствами (MQTT);
* протоколы удаленного доступа к каталогам (LDAP);
* сервисы SIP-телефонии.
	+ - 1. Подсистема управления ловушками должна обеспечивать функционирование на ловушках следующих сетевых служб и протоколов с уникальным цифровым отпечатком для конкретного устройства:
* Microsoft Windows 7/8/10;
* Microsoft Windows Server 2016;
* Ubuntu;
* CentOS;
* Debian;
* Сетевых устройств: Cisco ASA;
* Принтеров: HP;
* VOIP телефонов;
* Мобильных устройств.
	+ - 1. Подсистема управления ловушками должна обеспечивать возможность обнаружения MiTM-атаки на следующие протоколы:
* LLMNR;
* mDNS;
* NBT-NS;
* SMB.
	+ - 1. Подсистема управления ловушками должна иметь возможность назначать сервера-ловушки, которые будут обнаруживать MiTM-атаки;
			2. Подсистема управления ловушками должна иметь возможность автоматического включения и отключения эмулированных служб и протоколов согласно расписанию, заданному через веб-интерфейс подсистемы;
			3. Подсистема управления ловушками должна обеспечивать возможность создания каталогов с произвольным наименованием из веб-интерфейса, в том числе на русском языке для служб сервисов удаленного доступа к файлам и сетевым файловым ресурсам.
		1. Требования к подсистеме регистрации инцидентов ИБ
			1. Подсистема регистрации инцидентов ИБ должна отображать последовательность взаимодействия злоумышленника с ложной инфраструктурой в хронологическом порядке с указанием точного времени;
			2. Подсистема регистрации инцидентов ИБ должна иметь возможность отображения хостов, потенциально являющимися начальной точкой атаки;
			3. Подсистема регистрации инцидентов ИБ должна обеспечивать безагентным способом сбор событий ИБ: данные о захваченных злоумышленником хостах, источниках потенциально нежелательной активности;
			4. Подсистема регистрации инцидентов ИБ должна иметь возможность предоставлять подробную информацию о процессах, использующих ложные данные и инициирующих подключение к серверам-ловушкам;
			5. Подсистема регистрации инцидентов ИБ должна поддерживать интеграцию с почтовым сервером для оповещения об инцидентах ИБ по электронной почте;
			6. Подсистема регистрации инцидентов ИБ должна предоставлять возможности для отправки событий и/или инцидентов ИБ по протоколу Syslog;
			7. Подсистема регистрации инцидентов ИБ должна иметь возможности для интеграции с SIEM по протоколу Syslog с использованием формата CEF;
			8. Подсистема регистрации инцидентов ИБ должна поддерживать следующие форматы событий Syslog:
* RFC 5424;
* RFC 5425;
* RFC 3164.
	+ - 1. Подсистема регистрации инцидентов ИБ должна уметь отображать информацию о техниках и тактиках, используемых злоумышленником в рамках инцидента ИБ;
			2. Подсистема регистрации инцидентов ИБ должна иметь возможность регистрировать все попытки аутентификации при помощи приманок в формате учетных записей на реальных доменных узлах сети под управлением Active Directory;
			3. Подсистема регистрации инцидентов ИБ должна регистрировать все попытки аутентификации на подсистеме управления ловушками по всем типам сетевых служб и протоколов, поддерживаемых подсистемой управления ловушками;
			4. Подсистема регистрации инцидентов ИБ должна выявлять и регистрировать сетевое сканирование сетевых портов ловушек;
			5. При регистрации инцидента ИБ подсистема регистрации инцидентов ИБ должна определить:
* IP-адрес и/или FQDN узла сети, с которого осуществлялась попытка аутентификации или сетевого сканирования;
* IP-адрес и/или FQDN узла сети, на который осуществлялась попытка аутентификации или сетевого сканирования;
* учетную запись, использованную в момент события для попытки удаленного входа на сервер-ловушку;
* учетную запись, использованную в момент события для попытки удаленного входа на доменный хост;
* идентификатор события журналов Active Directory, на основе которого создано событие системы, при получении его с контроллеров домена;
* время события: попытки аутентификации или сетевого сканирования;
* сетевую службу и/или протокол, использованные для аутентификации или сетевого сканирования;
* Хост, на котором размещалась приманка с информацией об учетной записи, используемой для аутентификации.
	+ - 1. Подсистема регистрации инцидентов ИБ должна поддерживать автоматическую группировку событий в инциденты ИБ;
			2. Подсистема регистрации инцидентов ИБ должна иметь возможность исключения или удаления события и групп событий как ложноположительные срабатывания;
			3. Подсистема регистрации инцидентов ИБ должна иметь возможность добавлять комментарии к инцидентам ИБ;
			4. Подсистема регистрации инцидентов ИБ должна иметь возможность создавать исключения на основе инцидентов ИБ.
		1. Требования к дочерней подсистеме управления
			1. Дочерняя подсистема управления должна поддерживать подключение к локальной инфраструктуре на объектах распределенной инфраструктуры Заказчика следующих систем сбора событий аутентификации:
* Microsoft Active Directory;
* Windows Event Collector;
* Apache Kafka.
	+ - 1. Дочерняя подсистема управления должна поддерживать подключение к локальной DNS инфраструктуре на соответствующем объекте распределенной инфраструктуры Заказчика для автоматической генерации информации для ловушек и приманок;
			2. Дочерняя подсистема управления должна поддерживать распространение и ротацию приманок, которые развернуты на защищаемых рабочих станциях в соответствующем объекте распределенной инфраструктуры Заказчика;
			3. Дочерняя подсистема управления должна поддерживать сбор событий с подсистемы управления ловушками, которая развернута на соответствующем объекте распределенной инфраструктуры;
			4. Дочерняя подсистема управления должна поддерживать передачу собранных событий в подсистему управления Системой.
		1. Требования к подсистеме управления Системой
			1. Подсистема управления системой должна иметь возможность назначения политик распространения приманок на группы хостов;
			2. Подсистема управления системой должна иметь возможность назначения дочерней подсистемы управления;
			3. Подсистема управления системой должна иметь единый веб интерфейс для управления всеми подсистемами решения;
			4. Подсистема управления системой должна иметь возможность работы в скрытом режиме:
* не отображать логотипы вендора решения в подсистеме управления Системы;
* не отображать название вендора в подсистеме управления Системы.
	+ - 1. Подсистема управления системой должна поддерживать все следующие способы для распространения приманок, доступные через веб интерфейс решения:
* PsExec;
* PaExec;
* WinRM;
* SSH.

Сторонними средствами:

* Active Directory GPO;
* Microsoft Endpoint Manager;
* Ansible;
* Puppet;
* Jamf.
	+ - 1. Подсистема управления Системой должна поддерживать механизм периодического распространения и автоматического обновления приманок через Microsoft Endpoint Manager;
			2. Подсистема управления Системой должна поддерживать распространение приманок на Linux и MacOS с помощью учетной записи с приватным ключом, который можно указать в веб-интерфейсе подсистемы;
			3. Подсистема управления Системой должна иметь возможность конфигурации следующих параметров для распространения приманок:
* Механизм распространения по умолчанию: WinRM, PsExec, PaExec;
* Количество параллельных распространений;
* Возможность использовать Proxy по умолчанию;
* Возможность подключения TLS 1.2.
	+ - 1. Подсистема управления Системой должна иметь возможность конфигурации следующих параметров для распространения с помощью WinRM:
* Возможность использовать SSL;
* Выбор порта;
* Метод аутентификации.
	+ - 1. Подсистема управления Системой должна иметь возможность настройки распространения по расписанию по следующим параметрам:
* Периодичность;
* Время последнего распространения;
* Домены;
* Политики;
* Доступность хоста;
* По количеству приманок на хосте;
* Операционная система хоста.
	+ - 1. Подсистема управления системой должна иметь возможность генерировать PowerShell скрипты для распространения приманок сторонними средствами:
* Active Directory GPO;
* Microsoft Endpoint Manger.
	+ - 1. Подсистема управления системой должна иметь возможность генерировать исполняемый файл для распространения приманок на Linux и MacOS;
			2. Подсистема управления системой должна иметь возможность автоматического распространения приманок непосредственно из консоли на хостах под управлением:
* Windows;
* Linux;
* MacOS.
	+ - 1. Подсистема управления системой должна поддерживать механизмы распространения приманок в пользовательские профили без необходимости вызывать исполняемые файлы от имени этих пользователей;
			2. Подсистема управления системой должна иметь возможность автоматического распространения, удаления, обновления, модификации приманок в соответствии с расписанием и политиками;
			3. Подсистема управления системой должна поддерживать ролевую модель в такой мере достаточную, чтобы разделить пользователей системы на администраторов и пользователей;
			4. Подсистема управления системой должна иметь возможность управления привилегированными пользователями на конечных хостах:
* Проверка на соответствие наличия пользователей в административной группе согласно ролевой модели организации;
* Возможность удалить пользователей из администраторов, если это не соответствует ролевой модели.
	+ - 1. Подсистема управления системой должна иметь возможность интеграции со сторонними решениями по сбору событий аутентификации:
* Microsoft Active Directory;
* Windows Event Collector;
* Apache Kafka.
	+ - 1. Подсистема управления системой должна иметь возможность установки правил нормализации для событий, получаемых из сторонних систем, в формате для мониторинга действий пользователей;
			2. Подсистема управления системой должна поддерживать автоматическое удаление из веб-интерфейса и освобождение лицензии защищаемых рабочих станций, на которые пользователь не заходил более 90 дней;
			3. Подсистема управления системой должна поддерживать русскоязычный интерфейс;
			4. Подсистема управления системой должна иметь открытый API с документацией и иметь возможность доступа к встроенной документации и инструментам тестирования;
			5. Подсистема управления системой должна иметь возможность журналирования событий от источников аутентификации;
			6. Подсистема управления системой должна иметь возможность передавать регистрируемые в Системе события ИБ в SIEM;
			7. Подсистема управления системой должна иметь возможность включения детального журналирования событий с возможностью сохранения XML варианта события источника аутентификации в подсистеме;
			8. Подсистема управления системой должна иметь возможность журналирования событий создания исключений в Системе;
			9. Подсистема управления системой должна иметь возможность установки следующих уровней журналирования Системы:
* Trace;
* Debug;
* Error.
	+ - 1. Подсистема управления системой должна поддерживать следующие протоколы для шифрования коммуникаций между различными компонентами системы:
* TLS 1.2;
* TLS 1.3.
	+ - 1. Подсистема управления системой должна иметь возможность завершать сеансы пользователей;
			2. Подсистема управления системой должна поддерживать загрузку из веб-интерфейса защищаемых хостов, на которых пользователь не заходил более 90 дней;
			3. Подсистема управления системой должна поддерживать действие в веб-интерфейсе по сбросу Системы к состоянию чистой установки;
			4. Подсистема управления системой должна поддерживать действие в веб-интерфейсе по резервной копии всех настроек.
		1. Требования к подсистеме визуализации
			1. Подсистема визуализации должна поддерживать наличие панели визуализации с автоматическим обновлением данных по каждому представлению;
			2. Подсистема визуализации должна отображать количество распространенных приманок за период времени;
			3. Подсистема визуализации должна отображать количество приманок в среднем на одном хосте;
			4. Система должна отображать Топ-5 скомпрометированных учетных записей;
			5. Подсистема визуализации должна отображать график с количеством защищаемых хостов/доступных лицензий;
			6. Подсистема визуализации должна отображать график c инцидентами ИБ по времени;
			7. Подсистема визуализации должна отображать график c количеством техник, тактик и процедур, которые обнаружены системой;
			8. Подсистема визуализации должна отображать ленту событий с последними инцидентами ИБ с возможностью перехода из них в инцидент ИБ;
			9. Подсистема визуализации должна отображать график с событиями с разбивкой по протоколам.
1. Требования к информационной безопасности
	1. Требования по обеспечению информационной безопасности системы
		1. Система не предназначена для обработки информации, составляющей коммерческую тайну, и иной конфиденциальной информации, включая персональные данные.
		2. При реализации функций защиты информации системы должны использоваться встроенные средства защиты информации (входящие в состав среды виртуализации, операционных систем, прикладного программного обеспечения и СУБД) и наложенные (дополнительные) средства  защиты в случае невозможности реализации функций защиты информации встроенными средствами.
		3. Система должна обеспечивать возможность ролевого разграничения прав доступа пользователей и администраторов к информационным ресурсам в соответствии с разработанной матрицей доступа (+ другие требования в части подсистемы управления доступом.
		4. Система должна обеспечивать возможность мониторинга и протоколирования действий пользователей и администраторов при работе с функциями Системы.
		5. Система должна обеспечивать возможность контроля целостности, а также резервного копирования и восстановления информации.
		6. Требования по безопасности информации, предъявляемые к Системе, распространяются на все ее подсистемы и компоненты.
		7. В рамках проекта Исполнителем должен быть разработан раздел «Обеспечение информационной безопасности системы» документа «Пояснительная записка к техническому проекту (Техническое решение)».
		8. Раздел «Обеспечение информационной безопасности системы» должен описывать применяемые организационно-технические методы и средства защиты Системы.
	2. Регистрация значимых событий информационной безопасности

Для реализации функции регистрации и учета значимых событий информационной безопасности должны использоваться встроенные средства прикладных компонентов Системы.

Система должна аккумулировать регистрируемые события, сохраняя их в соответствующих таблицах базы данных и/или журналах.

Регистрации подлежат следующие события:

* регистрация попыток входа пользователей в Систему;
* регистрация изменений/назначений полномочий субъектов доступа и статуса объектов доступа;
* регистрация действий пользователей и администраторов в Системе;
* сбор, запись и хранение информации о событиях ИБ в течение установленного времени хранения.
	1. Требования к защите информации от несанкционированного доступа

В Системе должны быть реализованы следующие основные механизмы защиты информации от несанкционированного доступа:

* компоненты Системы, выполняющие функции управления, должны поддерживать возможность задания парольной политики для локальных учетных записей с административными правами.
* для информационного обмена между компонентами Системы должен использоваться протокол защищенной передачи данных TLS версии 1.2 или 1.3.

В Системе должна быть возможность предоставления пользователю доступа только к данным на основании назначенных данному пользователю ролей.

В Системе должна быть возможность предоставления пользователю доступа только к определенным подсистемам, данным, визуальным панелям на основании назначенных данному пользователю ролей.

В Системе должна быть сконфигурирована ролевая модель доступа ко всем компонентам, согласованная с Заказчиком на этапе реализации проекта.

1. Требования к составу и содержанию работ

Работы должны проводиться в 5 этапов:

1. Этап 1. Поставка ПО и проектирование.
2. Этап 2. Пуско-наладочные работы.
3. Этап 3. Функциональное тестирование.
4. Этап 4. Опытная эксплуатация Системы.
5. Этап 5. Приемо-сдаточные испытания.

* 1. Этап 1. Поставка ПО и проектирование

В рамках данного этапа Исполнителем должно быть выполнено следующее:

1. согласование с Заказчиком Технического решения;
2. разработка и согласование с Заказчиком технического проекта Системы для инфраструктуры Заказчика в составе: функциональная схема, схема структурная комплекса технических средств, описание комплекса технических средств и пояснительная записка к проекту;
3. разработка и согласование с Заказчиком Матрицы доступа;
4. передача прав на использование ПО на срок не менее 1 года, включая 12 месяцев технической поддержки от правообладателя.
	1. Этап 2. Пуско-наладочные работы

На данном этапе выполняется разворачивание и настройка Системы в инфраструктуре Заказчика, включая установку и настройку следующих ловушек и приманок:

1. распространение приманок на 5000 хостов (рабочие станции, серверы и т.д.);
2. установка серверов-ловушек в объеме не менее 6 штук;
3. установка и настройка MITM-агентов на серверах-ловушках.

 Объем устанавливаемых ловушек и приманок может быть изменен по согласованию с Заказчиком.

 В рамках данного этапа Исполнителем должно быть выполнено следующее:

1. согласование с Заказчиком требований к генерации приманок и ловушек;
2. установка ОС на виртуальные машины;
3. настройка сетевых интерфейсов на виртуальных машинах.
4. установка ПО на сервера;
5. первоначальная конфигурация системы, добавление в систему системных пользователей Microsoft Active Directory, настройка интеграции с доменом под управлением Microsoft Active Directory, интеграция с источниками событий Windows/Kafka, интеграция с DNS-сервером, интеграция с SIEM для передачи событий ИБ и инцидентов ИБ в SIEM;
6. интеграция серверов ловушек с сервером управления или коннектором;
7. создание и настройка политик, настройка их конфигураций, добавление учетных записей;
8. установка и настройка ловушек и приманок в инфраструктуре в объёме, согласованным с Заказчиком;
9. оформление акта «Акт завершения пуско-наладочных работ».

В рамках данного этапа Исполнителем также должны быть разработаны следующие документы:

1. руководство пользователя;
2. руководство администратора;
3. программа и методика испытаний;
4. программа проведения опытной эксплуатации.

Содержание и форма отчетных материалов согласовывается Заказчиком и Исполнителем.

Программа и методика испытаний должна содержать тест-кейсы, проверяющие соответствие Системы Техническому заданию и Техническому проекту.

* 1. Этап 3. Функциональное тестирование

В рамках данного этапа Исполнителем и Заказчиком должны быть проведено функциональное тестирование Системы. Испытания проводятся согласно документу ПМИ, разработанному на этапе 3. По результатам проведения функционального тестирования оформляются следующие документы:

1. протокол ФТ;
2. акт ввода Системы в опытную эксплуатацию.

Содержание и форма документов согласовывается на уровне специалистов Заказчика и Исполнителя.

* 1. Этап 4. Опытная эксплуатация

Опытная эксплуатация должна проводиться персоналом Заказчика при техническом сопровождении Исполнителя в соответствии с Программой проведения опытной эксплуатации.

Сроки и объем опытной эксплуатации Системы согласовываются Заказчиком и Исполнителем до начала опытной эксплуатации.

По результатам опытной эксплуатации Исполнителем должен быть оформлен протокол, утвержденный Заказчиком, с выводами и зафиксированными ошибками функционирования Системы.

В случае наличия отрицательных выводов и заключений по результатам опытной эксплуатации Исполнителем должна быть проведена доработка Системы по указанным в протоколе пунктам до проведения ПСИ (Этап 5).

* 1. Этап 5. ПСИ

В рамках данного этапа Исполнителем и Заказчиком должны быть проведены ПСИ Системы. Испытания проводятся согласно документу ПМИ, разработанному на этапе 3. По результатам проведения ПСИ оформляются следующие документы:

1. протокол ПСИ;
2. акт ввода Системы в промышленную эксплуатацию.

Содержание и форма документов согласовывается на уровне специалистов Заказчика и Исполнителя.

1. Работы, выполняемые Заказчиком самостоятельно

Заказчик предоставляет:

1. виртуальные машины для развертывания компонентов Системы;
2. лицензии на ОС, необходимых для развертывания компонентов Системы;
3. предоставление Исполнителю доступов, необходимых и достаточных для выполнения работ;
4. необходимые технические учетные записи для интеграции с AD.

Заказчик определяет и предоставляет перечень хостов для раскладки приманок.

1. Порядок контроля и приемки результатов работ

Состав и содержание работ должны соответствовать требованиям, представленным в настоящем Техническом задании.

Приемочные испытания Системы проводятся в соответствии с Программой и методикой испытаний.

Отчетные материалы, подтверждающие завершение работ каждого этапа описаны в Таблице 3.

Перечень разрабатываемых документов может быть пересмотрен по согласованию с Заказчиком.

Исполнитель информирует о разработке отчетных документов и направляет их в адрес Заказчика с сопроводительным письмом.

В случае наличия замечаний у Заказчика к полученным отчетным документам Исполнителя он письменно информирует его о таких замечаниях.

1. Требования к Исполнителю работ

Исполнитель должен иметь лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, включая следующий перечень работ и услуг:

1. контроль защищенности конфиденциальной информации от утечки по техническим каналам в: средствах и системах информатизации; технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается; помещениях со средствами (системами), подлежащими защите; защищаемых помещениях;
2. контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
3. проектирование в защищенном исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений.
4. Требования к срокам выполнения работ

Ниже в Таблице 3 приведены требования к срокам выполнения каждого этапа работ. Срок по каждому этапу указан с даты заключения договора. Этапы могут выполняться параллельно при наличии такой возможности и по согласованию с Заказчиком. Работы по первому этапу должны начаться с даты заключения договора.

1. Этапы и сроки работ

| **№ п/п** | **Наименование и содержание мероприятия** | **Срок работ** | **Документ, подтверждающий исполнение (Отчетные материалы)** |
| --- | --- | --- | --- |
|  | Этап 1. Поставка ПО и проектирование | 35 рабочих дней с даты заключения договора | * акт приема–передачи прав на ПО;
* технический проект в составе: функциональная схема, схема структурная комплекса технических средств, описание комплекса технических средств и пояснительная записка к техническому проекту;
* матрица доступа.
 |
|  | Этап 2. Пуско-наладочные работы | 50 рабочих дней с даты заключения договора | * руководство пользователя;
* руководство администратора;
* программа и методика испытаний;
* программа проведения опытной эксплуатации;
* акт завершения пуско-наладочных работ.
 |
|  | Этап 3. Функциональное тестирование | 55 рабочих дней с даты заключения договора | * протокол функционального тестирования;
* акт ввода Системы в опытную эксплуатацию.
 |
|  | Этап 4. Опытная эксплуатация | 65 рабочих дней с даты заключения договора | * протокол опытной эксплуатации.
 |
|  | Этап 5. ПСИ | 70 рабочих дней с даты заключения договора | * протокол приемочных испытаний;
* акт ввода Системы в промышленную эксплуатацию.
 |

1. Требования к документированию
	1. Требования к составу документации

По результатам реализации проекта Исполнитель должен разработать, согласовать и передать Заказчику документы в соответствии с Таблицей 4Таблица .

1. Перечень документации

| № п/п | Наименование документа | Тип документации |
| --- | --- | --- |
| 1. | Функциональная схемаСхема структурная комплекса технических средствОписание комплекса технических средствПояснительная записка к техническому проекту | Технический проект, русский |
| 2.  | Руководство администратора  | Эксплуатационная документация, русский |
| 3. | Руководство пользователя  | Эксплуатационная документация, русский |
| 4. | Программа и методика приемочных испытанийПрограмма проведения опытной эксплуатации | Рабочая документация, русский |
| 5. | Акт завершения пуско-наладочных работ Протокол ФТАкт ввода Системы в опытную эксплуатациюПротокол ОЭПротокол ПСИАкт ввода Системы в промышленную эксплуатацию | Рабочая документация, русский |

Комплект документации должен быть передан Исполнителем как на бумажных, так и на машинных носителях в службу эксплуатации Заказчика (на машинных носителях – в формате документов .docx, .xlsx, pptx.

Дополнительно для текстовых документов – в формате .pdf;

Для графических документов – в формате .vxdx, .vxdm.

Факт передачи документации фиксируется Актом передачи проектной документации.

Каждый документ является неотъемлемой частью процедуры передачи Системы на сопровождение. Без передачи всего комплекта документации Заказчику проект не может считаться завершенным.

1. Общие условия Договора и оплаты

Договор на поставку заключается по форме исполнителя с возможностью внесения правок со стороны ООО «ГК «Иннотех»

Условия поставки: Предпочтительнее в течение 14 дней с момента подписания договора. Участник может отразить свои условия поставки в КП.

Условия оплаты ПО: 100% постоплата в течение 30 календарных дней

Договор на выполнение работ заключается по форме исполнителя с возможностью внесения правок со стороны ООО «ГК «Иннотех»

Условия оплаты: 100% постоплата в течение 30 календарных дней, предпочтительно после выполнения всех этапов работ.

С Исполнителем в обязательном порядке подписывается NDA.