

Коммерческое предложение по внедрению Серчинформ SIEM

1. Предлагаемое решение

1.1. Назначение

Серчинформ SIEM— приложение, предназначенное для сбора и автоматического анализа событий различных корпоративных систем с целью выявления угроз и нарушений политик информационной безопасности. Источниками событий для Серчинформ SIEM могут являться журналы Active Directory, Windows Event Log, базы данных, антивирусы, почтовые сервера, сетевые устройства, приложения и др.

Система позволяет работать не только со стандартными событиями (вход в систему, удаление учётной записи, назначение прав доступа и др.), но и по настроенным правилам автоматически выявлять потенциально опасные цепочки таких событий. Правила формирования взаимосвязи между событиями предустановлены в систему и обладают возможностью гибкой настройки.

1.2. Схема работы

Коннекторы Серчинформ SIEM в реальном времени осуществляют сбор данных и их анализ:

- 1CConnector осуществляет чтение событий журналов регистрации 1С;
- 1C TechlogConnector осуществляет чтение событий технологических журналов 1С;
- ABSCConnector осуществляет чтение событий журналов ошибок автоматизированной банковской системы (АБС);
- ADMonitoringConnector отслеживает изменения атрибутов и объектов Active Directory.
- CheckPointConnector обеспечивает сбор событий межсетевого экрана CheckPoint.
- CiscoConnector обеспечивает сбор событий сетевых устройств Cisco.
- CustomConnector обеспечивает сбор данных в соответствии с инструкциями скрипта PowerShell.
- CWACConnector осуществляет чтение событий журналов 1С и контрольно-весовых аппаратов.
- DeviceConnector обеспечивает чтение базы данных DeviceController, которая содержит информацию о файлах, копируемых на подключаемые внешние устройства и запускаемых с них.
- DHCPConnector осуществляет чтение логов на DHCP-сервере посредством выполнения на нем PowerShell скриптов.
- DominoConnector осуществляет чтение логов почтового сервера IBM Domino.
- DrWebConnector осуществляет подключение к базам данных антивируса Dr.Web и чтение их записей.
- ESETConnector осуществляет сбор событий антивирусного программного обеспечения ESET.
- ExchangeConnector обеспечивает чтение логов почтового сервера Exchange.
- FileConnector осуществляет вычитку базы данных FileController, которая содержит файловую активность пользователей.
- FortigateConnector обеспечивает сбор событий устройства комплексной сетевой безопасности FortiGate.
- GPOConnector отслеживает изменения в настройках объектов групповых политик.
- KavEventConnector осуществляет подключение к базе данных Kaspersky и чтение ее записей.
- LinuxConnector осуществляет сбор событий ОС Linux, веб-сервера Apache, почтового сервера Postfix и FTP-сервера Very Secure FTP Daemon.
- McAfeeConnector осуществляет подключение к базе данных McAfee и чтение ее записей.
- NetFlowConnector осуществляет получение событий о сетевом трафике по протоколу

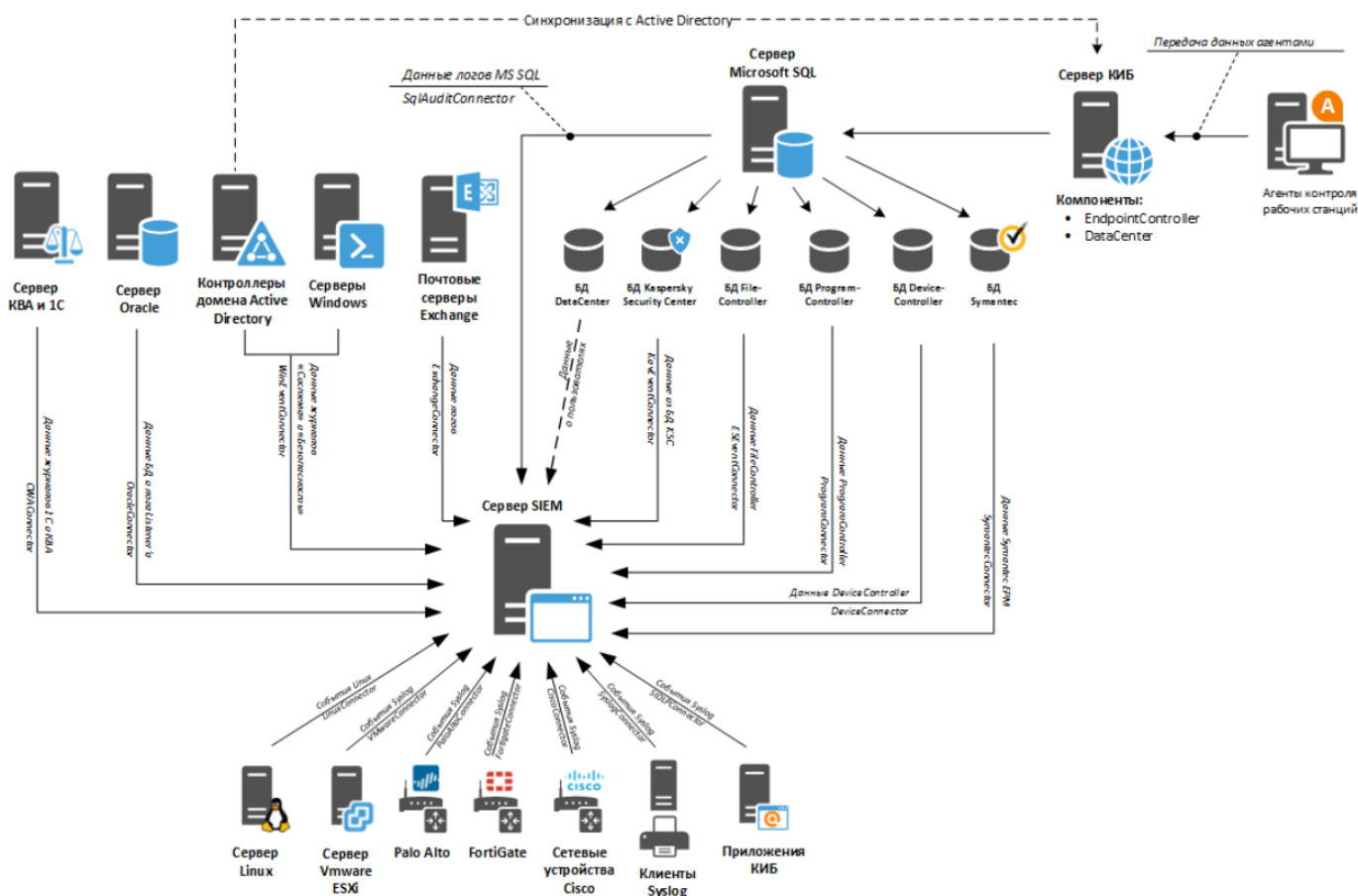
NetFlow от различных сетевых устройств.

- OracleConnector обеспечивает чтение таблиц баз данных и логов OracleListener.
- PaloAltoConnector обеспечивает сбор событий межсетевого экрана PaloAlto.
- PostgreSQLConnector осуществляет чтение SQL-запросов PostgreSQL из журналов Windows «Приложения».
- ProgramConnector осуществляет сбор информации об активности пользователей, подключаясь к базам данных ProgramController.
- SIDLPConnector обеспечивает сбор событий приложений КИБ.
- SqlAuditConnector обеспечивает чтение SQL-запросов Microsoft SQL из журналов Windows «Приложения».
- SymantecConnector осуществляет подключение к базе данных Symantec EPM и чтение ее записей.
- SyslogConnector осуществляет сбор событий Syslog.
- VMwareConnector обеспечивает сбор событий VMware ESXi.
- WinEventConnector отвечает за вычитку и анализ журнала Windows Event Log контроллеров доменов и серверов Windows, а также по протоколу LDAP производит вычитку и анализ информации об учётных записях.

В консоли Серчинформ SIEM создаются и настраиваются правила анализа, применяемые к перехваченным событиям. Список доменных пользователей в автоматическом режиме поступает от сервера DataCenter.

Если при анализе событий было выявлено нарушение, Серчинформ SIEM сохраняет инцидент в собственную базу данных под управлением MongoDB и оповещает сотрудника службы информационной безопасности по электронной почте.

Консоль администрирования Серчинформ SIEM позволяет строить отчёты по зафиксированным инцидентам, а также экспортировать выбранные события в файл.



2. Стоимость и специальные предложения

Стоимость лицензий приведены в Российских рублях (НДС не облагается на основании пп. 26 п. 2 ст. 149 Налогового кодекса Российской Федерации).

2.1. Общая стоимость Серчинформ SIEM на указанное число лицензий

| № п/п | Наименование программного обеспечения | Единица измерения | Количество лицензий | Стоимость за единицу | Сумма |
|---------------------|---------------------------------------|-------------------|---------------------|----------------------|---------------------|
| 1 | Серчинформ SIEM | шт. | 144 | 19 004,50 | 2 736 648,00 |
| Внедрение * | | | | | 273 665,00 |
| Общая сумма: | | | | | 3 010 313,00 |

*в том числе НДС 20%

2.2. Лицензирование

Неисключительное право на использование Серчинформ SIEM предоставляется до окончания срока действия исключительных прав на ПО (бессрочная лицензия).

В Серчинформ SIEM в качестве основной единицы лицензирования определён «Сетевой узел». «Сетевой узел» (не путать с «Источник данных») – физическое или виртуальное устройство с собственной ОС, однозначно идентифицируемое по имени хоста/IP-адресу.

Примеры сетевых узлов: серверы, компьютеры, коммутационное оборудование, виртуальные машины и пр.

Необходимое количество лицензий определяется как сумма **всех** сетевых узлов, с которых будет получать данные Серчинформ SIEM.

2.3. Условия гарантийного обслуживания и технической поддержки

Пользователям лицензионного программного обеспечения Серчинформ SIEM оказывается гарантийное обслуживание сроком на 1 год. По истечении данного срока услуги по технической поддержке осуществляются на основании отдельно заключаемого договора. Стоимость оказания услуг ТП и получение обновлений составляет:

1. При оплате в течение 3 месяцев с момента истечения первого года использования ПО либо любого последующего оплаченного периода – 30% от стоимости всех приобретенных пользователем лицензий на ПО, скорректированной с учетом цен на ПО, установленных лицензиатом на момент продления поддержки;

2. При оплате по истечении 3 месяцев с момента истечения первого года использования ПО либо любого последующего оплаченного периода – 50% от стоимости всех приобретенных пользователем лицензий на ПО, скорректированной с учетом цен на ПО, установленных лицензиатом на момент продления поддержки.

В рамках технической поддержки Продукта пользователям предоставляется: право использования новых версий Продукта, техническое сопровождение Продукта.

Информация, приведенная в данном Коммерческом предложении, не подлежит разглашению третьим лицам.

Дата составления документа: 26.02.2024.

Коммерческое предложение действительно в течение 30 дней.