Позитив Текнолоджиз Ведомственный центр

Версия 0.9

Руководство по установке

POSITIVE TECHNOLOGIES

Дата редакции документа: 28.03.2018

Содержание

1. О системе ПТ ВЦ

Позитив Текнолоджиз Ведомственный центр (далее также — ПТ ВЦ) предназначена для информационного взаимодействия с главным центром ГосСОПКА с целью обнаружения, предотвращения и ликвидации последствий компьютерных атак. С помощью ПТ ВЦ осуществляются:

- сбор данных об инцидентах;
- регистрация инцидентов путем создания заявок на их обработку;
- реагирование на инциденты (координация действий, определение причин, локализация инцидента, планирование мер по ликвидации последствий, контроль ликвидации последствий);
- обмен данными об инцидентах с главным центром ГосСОПКА;
- применение методических рекомендаций главного центра ГосСОПКА в процессе мониторинга информационной безопасности.

2. Аппаратные и программные требования

Все компоненты ПТ ВЦ разворачиваются на одном сервере, удовлетворяющем приведенным ниже аппаратным и программным требованиям.

Аппаратные требования для ПТ ВЦ

Таблица 1. Аппаратные требования к серверу для установки ПТ ВЦ

Компонент сервера	Минимальные требования
Центральный процессор	8 ядер с тактовой частотой 2,4 ГГц
Память (ОЗУ)	32 ГБ
Жесткий диск (ОС, компоненты)	2x600 ГБ, SAS, 10000 об/мин, RAID 1
Жесткий диск (локальная база данных)	2x600 ГБ, SAS, 10000 об/мин, RAID 1
Жесткий диск (хранилище артефактов инцидентов)	2x8 ТБ, SATA, RAID 1
Сетевой адаптер	1000 Мбит/с

Программные требования для ПТ ВЦ

- Microsoft Windows Server 2012 R2;
- Microsoft SQL Server 2014 Standart.

Аппаратные требования для PT MaxPatrol SIEM (MP Core)

Таблица 2. Аппаратные требования к серверу

Компонент сервера	Минимальное требование
Центральный процессор	6 ядер с тактовой частотой 2,4 ГГц
Память (ОЗУ)	32 ГБ
Сетевой адаптер	4 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Файловая система жестких дисков — NTFS. Для работы ОС и установки компонентов ПТ ВЦ — RAID 1 (10 000 об./мин.), не менее 100 ГБ. Для БД компонентов ПТ ВЦ — RAID 10 (7200 об./мин.), не менее 1,2 ТБ. Для хранилища событий MP SIEM Server — RAID 10 (7200 об./мин., не менее 6 дисков), не менее 1,2 ТБ

Программные требования для PT MaxPatrol SIEM (MP Core)

- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Google Chrome 63 (и выше).

3. Установка ПТ ВЦ

До начала установки убедитесь, что ваша система соответствует требованиям, предъявляемым к программному и аппаратному обеспечению (см. раздел 2).

► Чтобы установить ПТ ВЦ:

1. Скопируйте на сервер, где планируется развертывание ПТ ВЦ , в папку `c:\tmpMPX` следующие файлы, входящие в комплект поставки продукта:
   - `mp9certportal.nupkg`;
   - `csc-sopka.nupkg`;
   - `requestmanagementservice.nupkg`;
   - `deploy_csc.ps1`;
   - `CSC_Public`.
2. Распакуйте архивы.
3. Запустите Windows PowerShell от имени администратора.
4. В окне Windows PowerShell перейдите в каталог с распакованными архивами.

   ```
   cd c:\tmpMPX
   ```

5. Запустите установку ПТ ВЦ, указав IP-адрес сервера, логин и пароль администратора.

   ```
   deploy_csc.ps1 <ServerIP> <AdministratorUsername> <AdministratorPassword> CSC_Public FALSE
   TRUE TRUE
   ```

   ```
   deploy_internal.ps1 <ServerIP> none <AdministratorUsername> <AdministratorPassword>
   DepartmentCenter
   ```

Установка ПТ ВЦ завершена.

4. Удаление ПТ ВЦ

► Чтобы удалить ПТ ВЦ:

1. В панели управления выберите **Программы и компоненты**.
2. В списке установленных программ выберите MaxPatrolRMS и нажмите кнопку **Удалить**.

   Откроется окно мастера удаления MaxPatrolRMS.
3. Нажмите кнопку **Uninstall**.
4. Следуйте указаниям мастера.
5. Запустите диспетчер служб IIS.
6. В панели **Подключения** раскройте строку **Сайты**.
7. В контекстном меню службы **Cert_internal** выберите пункт **Deploy** → **Delete Web Site and Content** и подтвердите удаление сайта и контента.

Система ПТ ВЦ удалена.

5. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Заявки на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

5.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать заявки на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

5.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 20 3769 3606.
- США +1 857 208 7273.
- Италия +39 0 697631532.
- Швеция +46 8 121 111 86.
- Южная Корея +82 264 108 582.
- Россия +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданной заявке.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте заявку на портале support.ptsecurity.com. Заявка на портале, созданная и обновляемая по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

5.3. Время работы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся заявкам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

5.4. Как служба технической поддержки работает с заявками

При получении вашей заявки специалист службы технической поддержки классифицирует инцидент, указанный в заявке (присваивает инциденту тип и уровень значимости) и выполняет дальнейшие шаги по разрешению инцидента.

В этом разделе

5.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть заявку.

5.4.2. Типы инцидентов

Специалист технической поддержки относит инцидент в вашей заявке к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате

продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за инциденты, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

5.4.3. Время реакции на обращение и приоритизация инцидентов

Время реакции на ваше обращение рассчитывается как время с момента получения от вас информации по обращению до ответа специалиста технической поддержки с описанием дальнейших шагов по разрешению инцидента. Время реакции зависит от указанного вами уровня значимости инцидента (см. таблицу 3).

Время решения инцидента рассчитывается как время с момента регистрации обращения до ответа специалиста технической поддержки, ведущего к одному из вариантов решения инцидента (см. раздел 5.4.4).

Специалист технической поддержки может переопределять уровень значимости инцидента по приведенным ниже критериям. Значения сроков являются целевыми и подразумевают стремление и разумные усилия специалистов "Позитив Текнолоджиз" для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 3. Время реакции технической поддержки на обращение и решения инцидента

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту	Время решения инцидента
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку)	До 2 часов	До 2 рабочих дней

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту	Время решения инцидента
	либо оказывающие критическое влияние на бизнес		
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 4 часов	До 3 рабочих дней
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительное влияние на бизнес	До 8 часов	До 6 рабочих дней
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	До 10 рабочих дней

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки обращений).

5.4.4. Выполнение работ по заявке

По мере выполнения работ по вашей заявке специалист технической поддержки сообщает вам:

- о диагностике инцидента и ее результатах,
- поиске решения или возможности обойти причины возникновения инцидента,
- планировании и выпуске обновления продукта (если требуется для разрешения инцидента).

Если по итогам решения инцидента необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по заявке считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- инцидент диагностирован как дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- инцидент идентифицирован как вызванный программными продуктами или оборудованием сторонних производителей и не подпадающий под гарантийные обязательства по продукту;
- инцидент классифицирован как неподдерживаемый.

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com