



SECURITY CAPSULE

SIEM

ПЕРВАЯ ОТЕЧЕСТВЕННАЯ

О КОМПАНИИ



Компания ООО «Иновационные Технологии в Бизнесе» основана в октябре 2009 года.

Цель бизнеса: оказание полного спектра услуг по защите информации, начиная

от проектирования систем защиты информации заканчивая установкой и настройкой средств защиты с последующей аттестацией информационной системы по требованиям защиты информации.

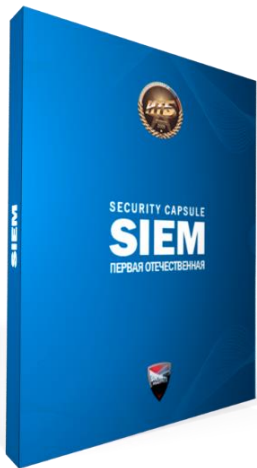


**ЛИЦЕНЗИАТ
ФСТЭК России**



**ЛИЦЕНЗИАТ
ФСБ России**

SECURITY CAPSULE SIEM



Система мониторинга и корреляции событий информационной безопасности.

Российская разработка, внедряемая с 2009 года.

Импортозамещающее решение, учитывающее потребности Государства и Бизнеса.

Соответствует требованиям регуляторов ФСТЭК России, ФСБ России.

Security Capsule SIEM совместима с Российскими операционными системами, средствами защиты информации, а также базами данных.

СЕРТИФИКАТЫ И СВИДЕТЕЛЬСТВА



Сертификат
Федеральной службы по
техническому и
экспортному контролю

№ 4735 от 01 ноября 2023 года
Требования доверия(5), ТУ.



Запись в едином
реестре российских
программ для
электронных вычислительных
машин и баз данных №1139 от
14 июня 2016 года.

ПРИМЕНЕНИЕ

Security Capsule SIEM может применяться в составе:

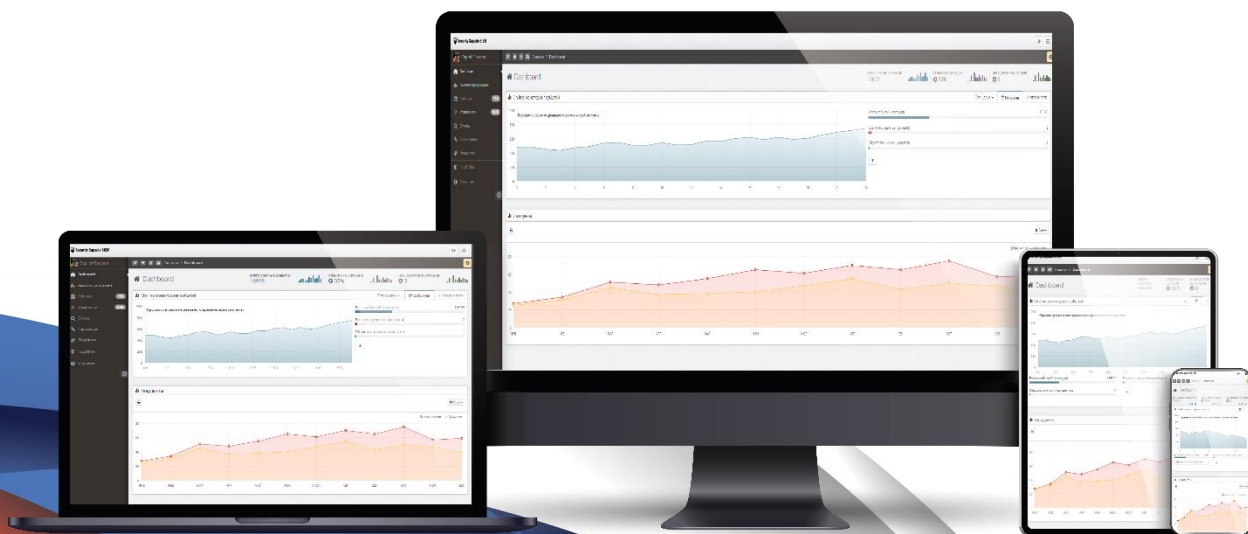
- Государственных информационных систем (ГИС)
- Информационных систем персональных данных (ИСПДн)
- Значимых объектов критической информационной инфраструктуры (КИИ)
- Автоматизированных систем управления технологическими процессами (АСУ ТП)
- Систем обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

ДОСТОИНСТВА

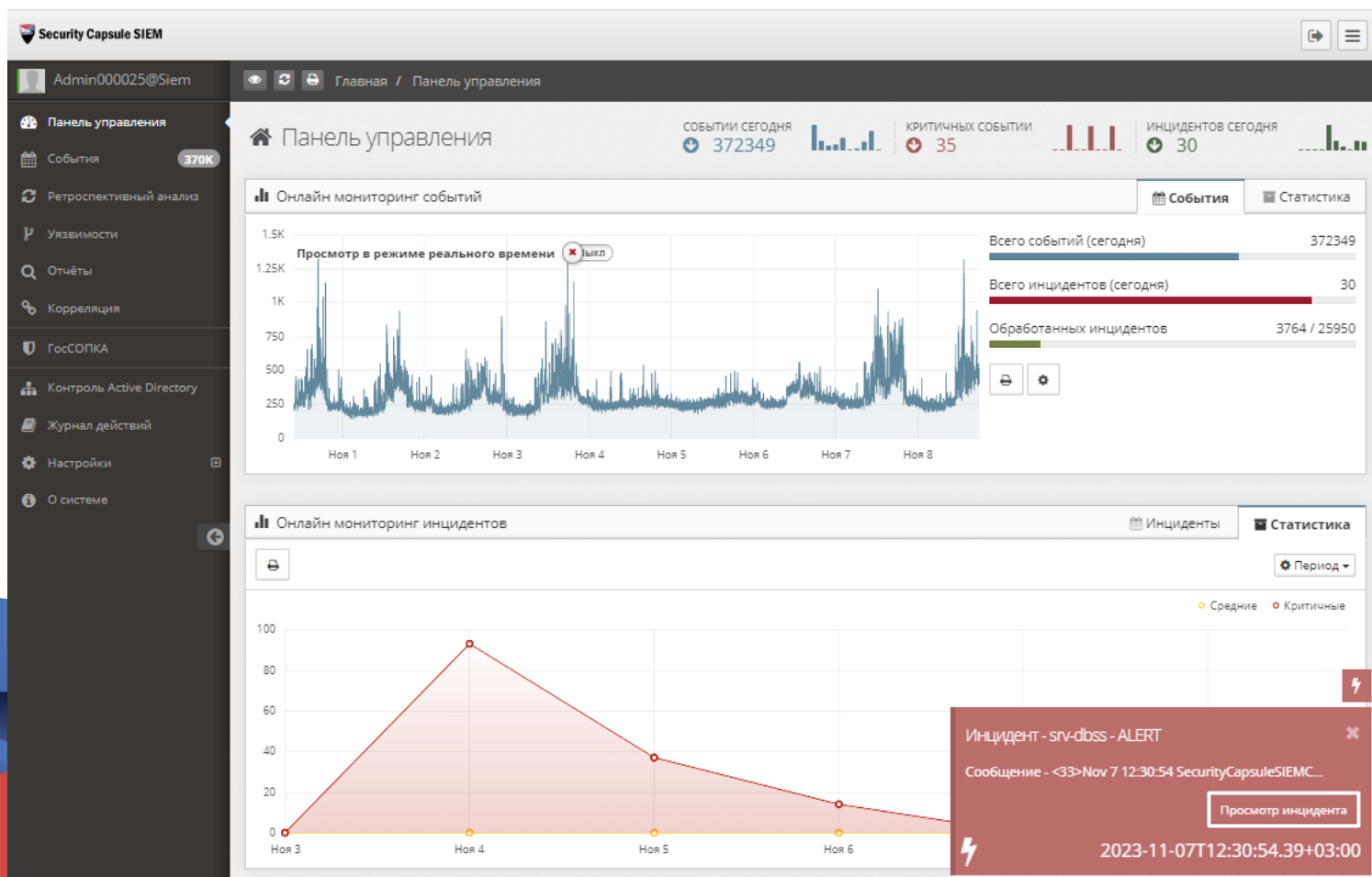
- Соответствие требованиям ФСТЭК России и ФСБ России
- Бессрочные лицензии или Срочные (подписка) от 6 месяцев
- Более 1000 предустановленных правил корреляции
- Ретроспективный анализ событий
- Техническая поддержка (24\7 и 9\5)
- Отправка уведомлений об инцидентах в НКЦКИ
- Доработка на основе опыта пользователей
- Бесплатный обучающий on-line курс
- Выявление атак с применением тактик модели MITRE ATT&CK, а также техник, атакующих по матрице ATT&CK

ИНТЕРФЕЙС

В Security Capsule SIEM интуитивно понятный, адаптивный web-интерфейс. Реализована ролевая модель разграничения прав доступа, а также логирование действий пользователей в системе.



ПРИМЕР: Интерфейс



ПОСТАВКА



Security Capsule SIEM поставляться как в виде модулей так и в формате all-in-one.

Типовые варианты поставки:

- Передача неисключительных прав на программные модули
- Программно-аппаратный комплекс с предустановленными компонентами Security Capsule SIEM

КОМПЛЕКТ ПОСТАВКИ

В базовый комплект поставки Security Capsule SIEM входит:

- Модуль сбора событий
- Модуль нормализации
- Модуль корреляции
- Модуль хранения
- Консоль

Дополнительно поставляемые модули:

- Модуль ГосСОПКА

SECURITY CAPSULE SIEM: Модуль сбора событий



Security Capsule SIEM: Модуль сбора событий – осуществляет сбор событий от источников

данных (АРМ, сервер, коммутационное оборудование, ПО\СЗИ).

Благодаря увеличению количества модулей сбора событий возможна реализация территориально распределенной топологии.

ПРИМЕР: RAW событие

```
<188>1831512: Cisco_Kernel_itb: 1831533: 4d20h: %SEC_LOGIN-4-  
LOGIN_FAILED: Login failed [user: siem] [Source: 192.168.1.6] [localport:  
22] [Reason: Login Authentication Failed] at 13:42:55 MSK Tue Mar 7 2023
```

SECURITY CAPSULE SIEM: Модуль нормализации



Security Capsule SIEM: Модуль нормализации - осуществляет преобразование поступающих от


источников данных из неоднородного формата к структурированному.

Настройка правил нормализации осуществляется на этапе пуско-наладки и не требует дополнительных трудозатрат со стороны специалистов Заказчика.

ПРИМЕР: Нормализованное событие

i Событие - 64072a8302d94f300a5184b4 ✕

Id	64072a8302d94f300a5184b4
sys	_gateway
time	07.03.2023 15:13:55
time_rcvd	07.03.2023 15:13:55
msg	<188>1831512: Cisco_Kernel_itb: 1831533: 4d20h: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: siem] [Source: 192.168.1.6] [localport: 22] [Reason: Login Authentication Failed] at 13:42:55 MSK Tue Mar 7 2023
syslog_fac	23
syslog_sever	4
syslog_tag	1831512:
procid	1831512
pid	-
level	WARN
Критичность	Средняя

 ✕ Закрыть

SECURITY CAPSULE SIEM: Модуль корреляции



Security Capsule SIEM Модуль корреляции – с целью выявления инцидентов осуществляет

анализ событий как в режиме реального времени, так и в ретроспективе.

Предусмотрена возможность создавать свои и вносить изменения в уже существующие правила корреляции.

Настройка правил корреляции осуществляется на этапе пуско-наладки и не требует дополнительных трудозатрат со стороны специалистов Заказчика.

ПРИМЕР: Корреляция инцидента

Событие - 64106e5902d94f300a931bef

Id	64106e5902d94f300a931bef
sys	_gateway
time	14.03.2023 15:53:45
time_rcvd	14.03.2023 15:53:45
msg	<188>5425921: Cisco %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: siem] [Source: 192.168.1.6] [localport: 22] [Reason: Authentication Failed]
syslog_fac	23
syslog_sever	4

Событие - 64106e6402d94f300a931c51

Id	64106e6402d94f300a931c51
sys	_gateway
time	14.03.2023 15:53:56
time_rcvd	14.03.2023 15:53:56
msg	<188>5426009: Cisco %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: siem] [Source: 192.168.1.6] [localport: 22] [Reason: Authentication Failed]

Событие - 64106eb602d94f300a931f8b

Id	64106eb602d94f300a931f8b
sys	_gateway
time	14.03.2023 15:55:18
time_rcvd	14.03.2023 15:55:18
msg	<188>5426772: Cisco_Kernel_itb: 5426826: 1w4d: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: siem] [Source: 192.168.1.6] [localport: 22] [Reason: Login Authentication Failed] at 14:24:20 MSK Tue Mar 14 2023
syslog_fac	23
syslog_sever	4
syslog_tag	5426772:
procid	5426772
pid	-
level	WARN
Критичность	Средняя

Закреть

Инцидент - 64106eb602d94f300a931f8c

Описание

В системе, с применением правила корреляции был зарегистрирован инцидент (Критичность - **Высокая**): "[cisco-ios] Ошибка входа. Brute Force"

Расследование инцидента

Управление инцидентом

Подробнее: SID - 5001686
Тип класса - Unsuccessful User Privilege Gain
Приоритет - 1
Критичность - **Высокая**
src_ip - 192.168.1.6
dst_ip - 192.168.1.1

Сообщение: <33>Mar 14 15:55:18 SecurityCapsuleSIEMCorrelator[43117]: [1:5001686:11] [cisco-ios] Ошибка входа. Brute Force [Classification: Unsuccessful User Privilege Gain] [Priority: 1] [Program: 5426772] {UDP} 192.168.1.6:22 [] -> 192.168.1.1:514 [] - <188>5426772: Cisco_Kernel_itb: 5426826: 1w4d: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: siem] [Source: 192.168.1.6] [localport: 22] [Reason: Login Authentication Failed] at 14:24:20 MSK Tue Mar 14 2023

Закреть

SECURITY CAPSULE SIEM: Модуль хранения



Security Capsule SIEM Модуль хранения - база данных raw событий, нормализованных

событий, инцидентов, а также иных системных данных.

Технические характеристики оборудования зависят от объемов и сроков хранения информации о событиях, инцидентах и оцениваются на этапе обследования объекта информатизации Заказчика.

SECURITY CAPSULE SIEM: MITRE ATT&CK

Матрица MITRE ATT&CK описывает тактики и техники, целевых атак, применяемые различными киберпреступными группами.

Security Capsule SIEM позволяет выявлять техники к следующим тактикам:

TA0001: Первоначальный доступ

TA0002: Выполнение

TA0003: Закрепление

TA0004: Повышение привилегий

TA0005: Предотвращение обнаружения

TA0006: Получение учетных данных

TA0007: Изучение

TA0008: Перемещение внутри периметра

TA0009: Сбор данных

TA0011: Организация управления

TA0010: Эксфильтрация данных

TA0040: Деструктивное воздействие

TA0042: Подготовка ресурсов

TA0043: Разведка

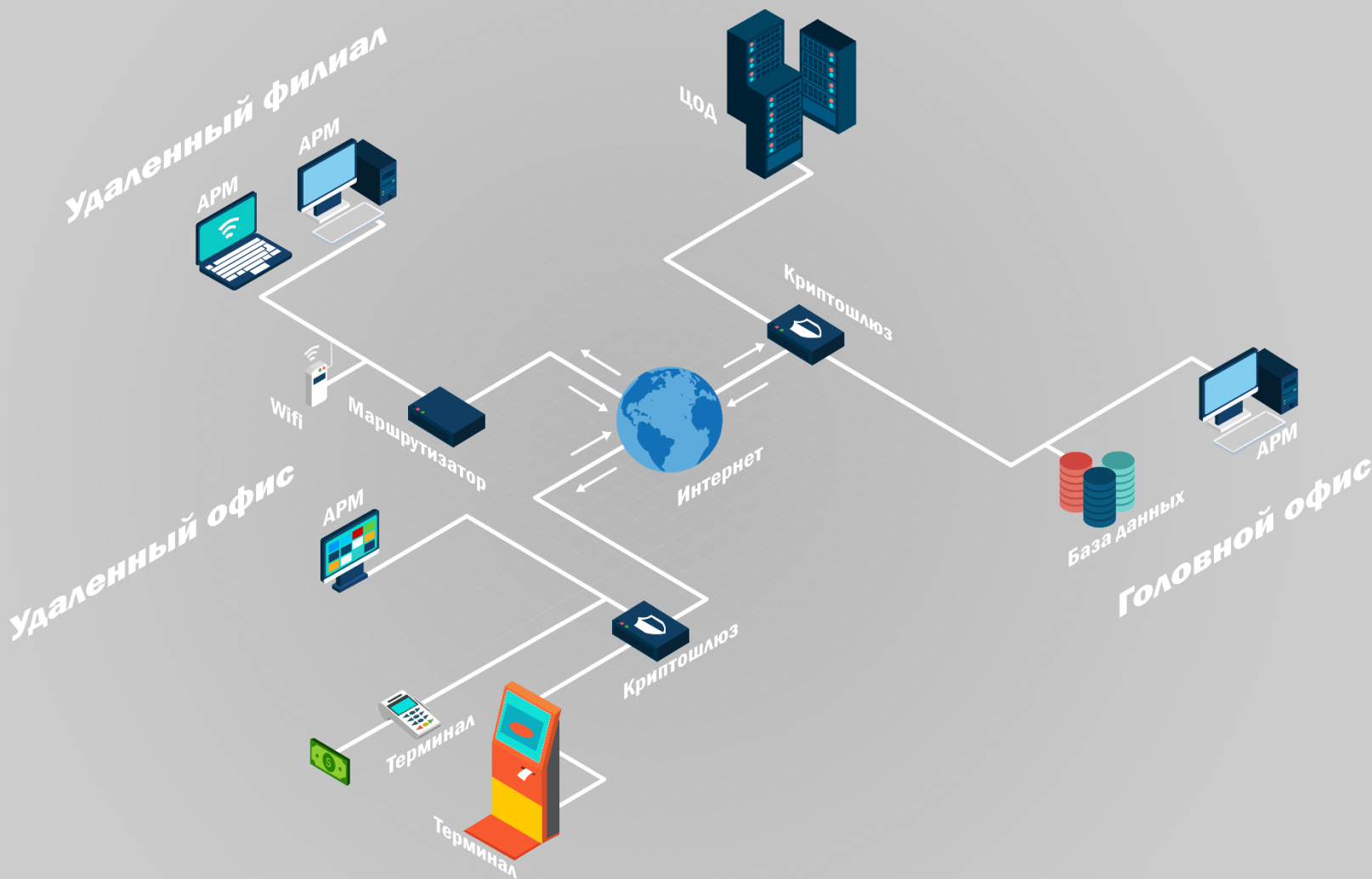
ВНЕДРЕНИЕ

Внедрение делится на четыре этапа:

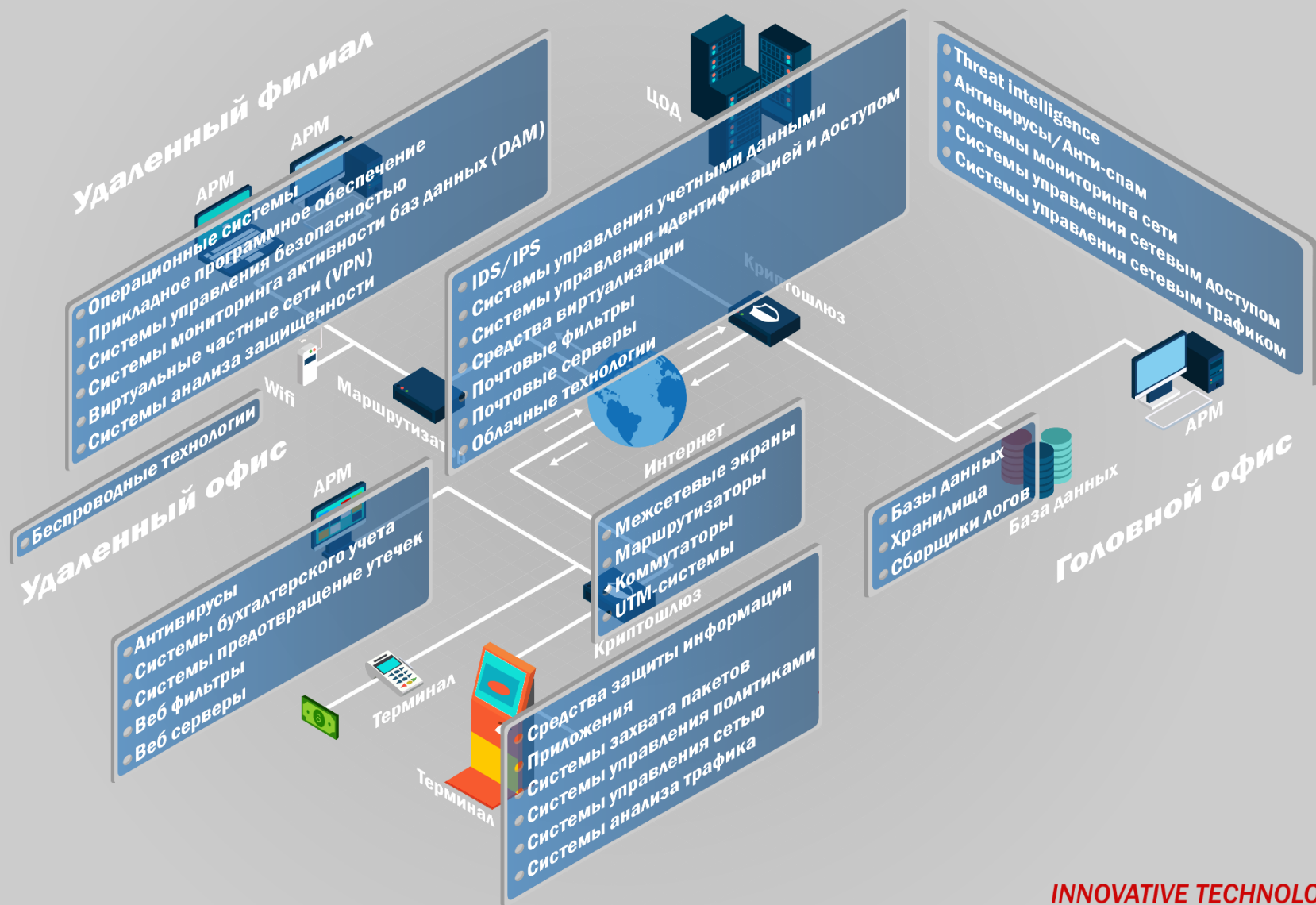
- Этап 1 – Обследование
- Этап 2 – Идентификация источников
- Этап 3 – Установка модулей
- Этап 4 – Настройка

Внедрение, в том числе настройка модулей Security Capsule SIEM осуществляется специалистами компании.

ВНЕДРЕНИЕ – ЭТАП 1. Обследование



ВНЕДРЕНИЕ – ЭТАП 2. Идентификация источников

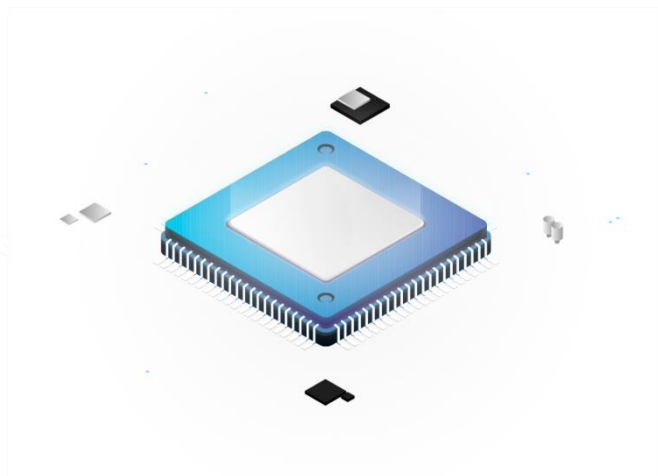


ОБЪЕКТЫ МОНИТОРИНГА

Security Capsule SIEM поддерживает сбор событий более чем от 40 типов источников, как программных так и программно-аппаратных не ограничиваясь при этом только средствами защиты информации.

Написание нестандартных коннекторов к источникам данных осуществляется на этапе пуско-наладки и не требует дополнительных трудозатрат со стороны специалистов Заказчика.

КОРРЕЛЯЦИЯ



Security Capsule SIEM имеет мощное корреляционное ядро, интуитивный интерфейс и гибкий мастер создания правил корреляции.

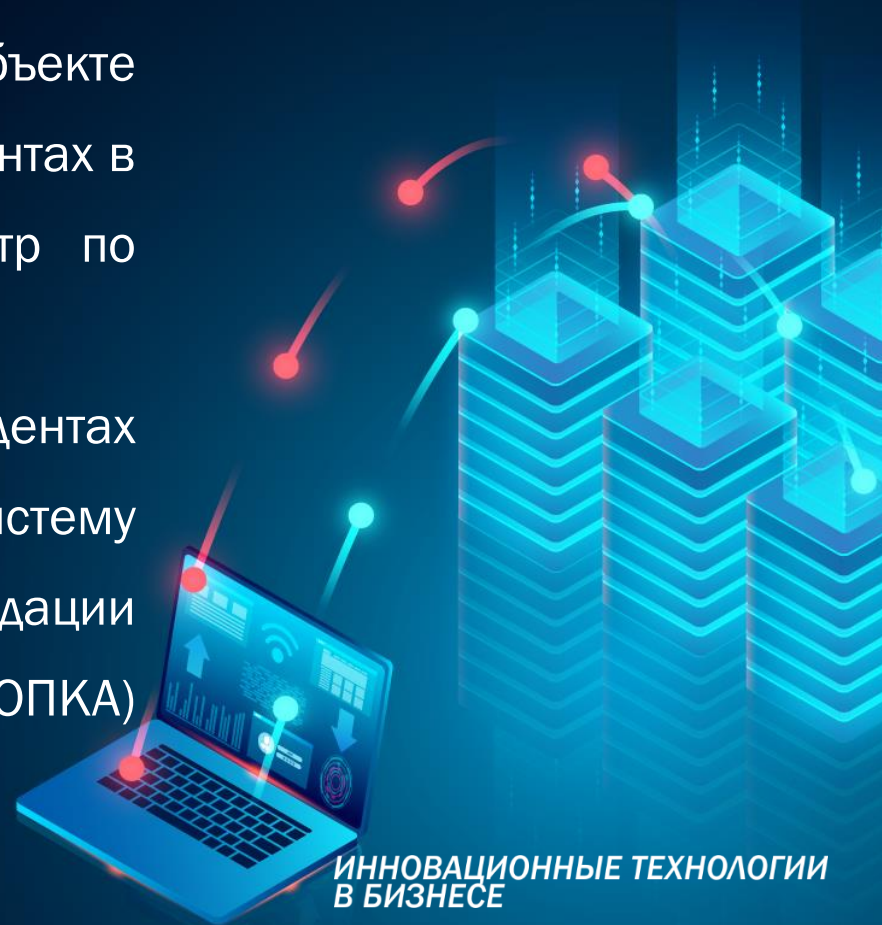
В Security Capsule SIEM предустановлено более 1000 правил корреляции.

База данных правил корреляции регулярно обновляется по мере выявления новых сценариев компрометации.

ВЗАИМОДЕЙСТВИЕ С НКЦКИ

В Security Capsule SIEM реализован модуль «ГосСОПКА», обеспечивающий возможность полуавтоматической отправки уведомлений о зафиксированных на объекте информатизации компьютерных инцидентах в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

Уведомления о компьютерных инцидентах направляются в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) по определенному НКЦКИ регламенту.



ОТЧЕТНОСТЬ

В системе реализован удобный механизм формирования отчетов, с возможностью сохранения собственных профилей.

The screenshot displays the Security Capsule SIEM reporting interface, which includes several key components:

- Еженедельный отчет (Weekly Report):** A bar chart showing events for the last 15 days, with a summary table below it.
- Линейный график событий критичные и средние (Line Chart of Critical and Average Events):** A line chart showing trends for critical and average events over a 15-day period.
- Инциденты (Incidents):** A list of security incidents with details such as date, time, message, and severity.
- Онлайн мониторинг событий (Online Event Monitoring):** A real-time event monitoring chart.
- Сводная статистика за день (Daily Summary Statistics):** A bar chart showing daily event counts and critical incidents.
- Топ 3 - Инцидентов (Top 3 Incidents):** A list of the most frequent incident types.

Summary Table Data:

	Сумма	Среднее
Всего (период 1 \ 15 дней)	7825284	521686
Средние (период 1 \ 15 дней)	46498	3100
Критичные (период 1 \ 15 дней)	16954	1130
Всего (период 2 \ 15 дней)	7806008	520401
Средние (период 2 \ 15 дней)	47991	3199
Критичные (период 2 \ 15 дней)	15579	1039
Средние (разница)	-1493	-99
Критичные (разница)	1375	91
Средние %	97	97
Критичные %	109	109

Incident List Data:

Дата и время	Сообщение	Тип класса	Критичность
09.11.2023 14:49:07	<33>Nov 9 14:49:07 SecurityCapsuleSIEMCorrelator[24701]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator	Successful Administrator Privilege Gain	Высокая
09.11.2023 14:49:07	<33>Nov 9 14:49:07 SecurityCapsuleSIEMCorrelator[24701]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator	Successful Administrator Privilege Gain	Высокая
09.11.2023 14:49:04	<33>Nov 9 14:49:04 SecurityCapsuleSIEMCorrelator[24369]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/service SecurityCapsuleSIEMCorrelator restart	Successful Administrator Privilege Gain	Высокая
09.11.2023 14:49:04	<33>Nov 9 14:49:04 SecurityCapsuleSIEMCorrelator[24369]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/service SecurityCapsuleSIEMCorrelator restart	Successful Administrator Privilege Gain	Высокая
09.11.2023 14:48:03	<33>Nov 9 14:48:03 SecurityCapsuleSIEMCorrelator[24369]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator	Successful Administrator Privilege Gain	Высокая
09.11.2023 14:48:01	<33>Nov 9 14:48:01 SecurityCapsuleSIEMCorrelator[21124]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator restart	Successful Administrator Privilege Gain	Высокая
09.11.2023 14:48:01	<33>Nov 9 14:48:01 SecurityCapsuleSIEMCorrelator[21124]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator	Successful Administrator Privilege Gain	Высокая
08.11.2023 15:54:14	<33>Nov 8 15:54:14 SecurityCapsuleSIEMCorrelator[20828]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/service SecurityCapsuleSIEMCorrelator restart	Successful Administrator Privilege Gain	Высокая
08.11.2023 15:54:14	<33>Nov 8 15:54:14 SecurityCapsuleSIEMCorrelator[20828]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator	Successful Administrator Privilege Gain	Высокая
08.11.2023 15:52:41	<33>Nov 8 15:52:41 SecurityCapsuleSIEMCorrelator[20828]: [1:5000133:9] [SU] SUDO получены привилегии ROOT [Classification: Successful Administrator Privilege Gain] [Priority: 1] [Program: sudo] (UDP) 127.0.0.1:514 [] -> 127.0.0.1:514 [] - root: TTY=unknown: PWD=/root : USER=root : COMMAND=/sbin/pidof SecurityCapsuleSIEMCorrelator	Successful Administrator Privilege Gain	Высокая

Daily Summary Statistics (13.11.2023):

Событий за сегодня	Событий средней критичности	Критичных событий	Инцидентов
274737	1933	2217	0

Top 3 - Incidents:

#	Название	Класс	Количество
2	"[ClSCO-IOS] успешный вход"	successful-admin	174
7	"[SU] SUDO получены привилегии ROOT"	successful-admin	45
8	"[ADLoca] Не верный пароль"	unsuccessful-admin	61

СПАСИБО ЗА ВНИМАНИЕ!



Руководитель проекта:

Графов Сергей Александрович

Почта: sag@itb.spb.ru

Телефон: +7 (911) 920-09-87

Мы в соц. сетях:



[/itb_spb/](#)



[/с/ИнновационныеТехнологиииБизнесе](#)



[/profile/14089663908?lr=2](#)

Контакты

По общим вопросам:

manager@itb.spb.ru

Обучение:

learning@itb.spb.ru

Техническая поддержка:

support@itb.spb.ru



Подписывайтесь на канал t.me/ttl_news, чтобы первыми узнавать о новостях и эксклюзивных материалах по информационной безопасности