АЙТИБАСТИОН

РАМ-ПЛАТФОРМА СКДПУ НТ
ИНСТРУМЕНТЫ ПРЯМОГО И КОСВЕННОГО АНАЛИЗА ИНФРАСТРУКТУРЫ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

www.it-bastion.com

АЙТИБАСТИОН

Технологии

Люди – сотрудники

Процессы

Бюджет и его ~~безумное~~ разумное использование

Privileged Access Management (PAM)

Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз.

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

ЕДИНАЯ ТОЧКА ДОСТУПА

Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius)

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись видео и метаданных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д.

УПРАВЛЕНИЕ ПАРОЛЯМИ

Управление паролями целевых учетных записей без необходимости установки агентов на целевые устройства по настраиваемым политикам

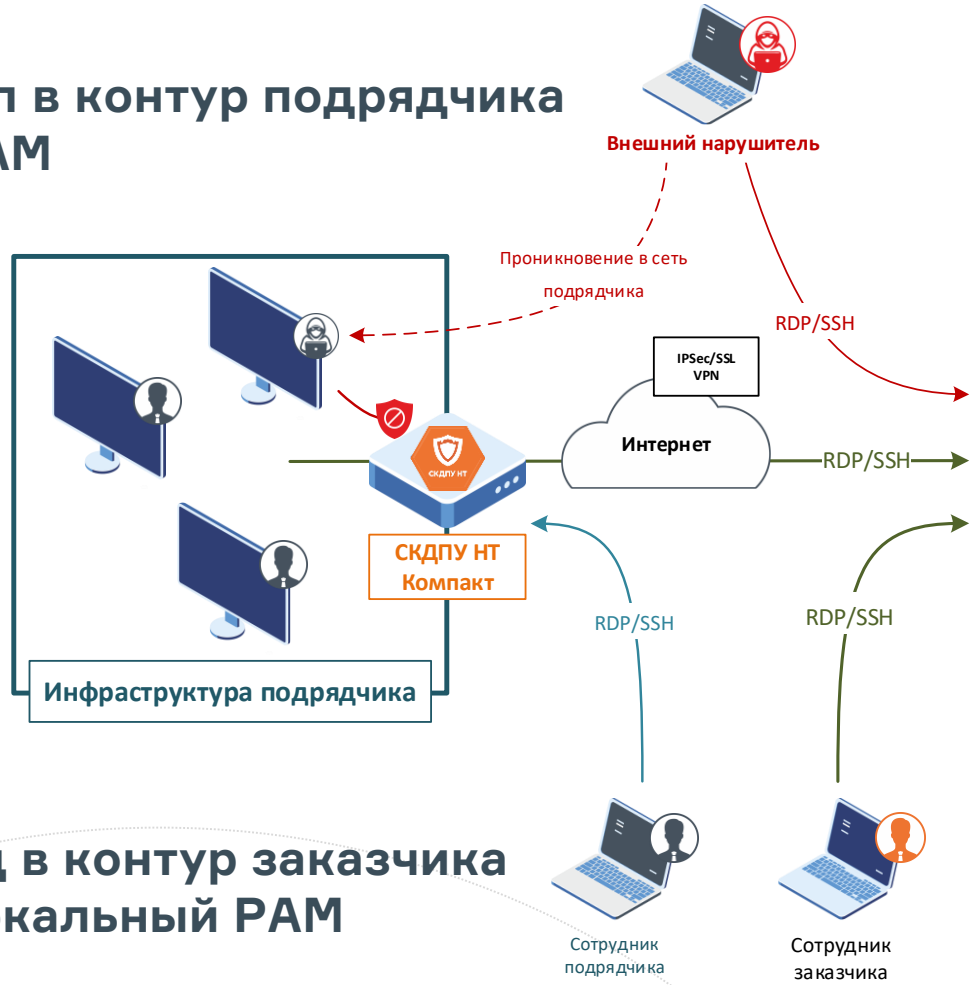
БЕЗ УСТАНОВКИ АГЕНТОВ

Подключение к ЦУ без необходимости установки агентов, особенно важна при подключении к объектам КИИ

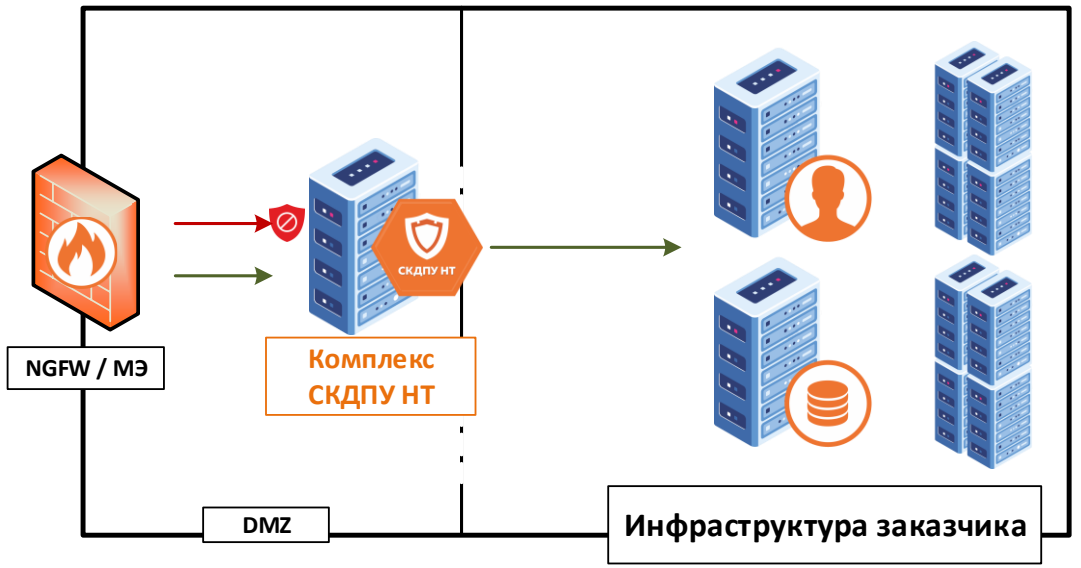
ЕДИНЫЙ КОНТРОЛИРУЕМЫЙ ДОСТУП В ЦЕПОЧКАХ ПОСТАВОК

АЙТИБАСТИОН

1. Доступ в контур подрядчика через PAM



2. Доступ в контур заказчика через PAM



3. Выход в контур заказчика через локальный PAM

- Защита сотрудников подрядчика
- Минимизация риска со стороны инсайдеров

www.it-bastion.com

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям без предоставления полного доступа с сокрытием УЗ от приложений.

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность не только контролировать сессию по её результату, но и видеть все действия в режиме реального времени. А в случае необходимости - блокировать сессию пользователя, предотвращая потенциальную угрозу.

РАБОТА ПО ЗАЯВКАМ С ВОЗМОЖНОСТЬЮ ПОДТВЕРЖДЕНИЯ ДОСТУПА

Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц.

КОНТРОЛЬ НА СТОРОНЕ ИС

Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

ЦЕНТРАЛИЗОВАННЫЙ АРХИВ ДАННЫХ ПО СЕССИЯМ

АЙТИБАСТИОН

Сессии: 1784, 10-03-2023

Добавить фильтры

Параметры запроса

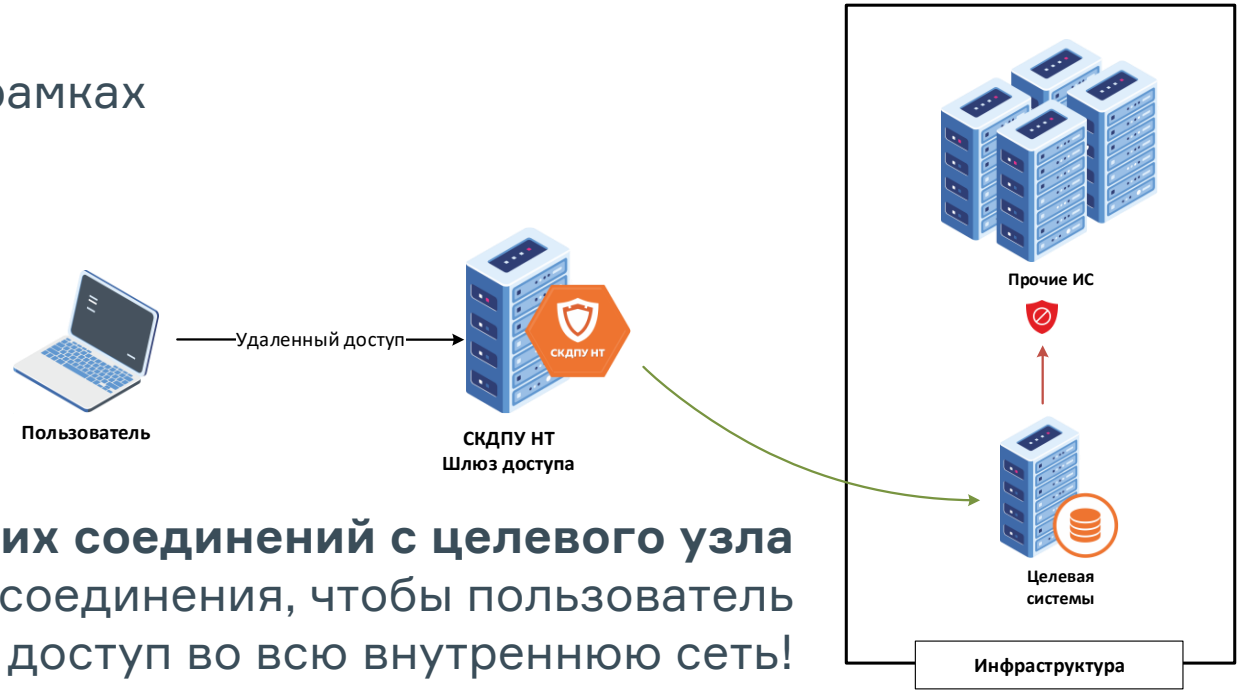
Тип	Старт	Продолжительность	Персона / Аккау				
RDP	09-03-2023 17:47:50	0:02:10	avs@avs16.local				
RDP	09-03-2023 16:36:21	0:01:22	avs@avs16.local				
SSH	09-03-2023 11:27:23	0:00:00	admin / wabadmi				
RDP	09-03-2023 11:14:29	0:00:21	admin / root				
SSH	09-03-2023 11:11:59	0:00:16	admin / wabadmi				
SSH	07-03-2023 16:07:17	0:00:02	portaltest@test.lo				
RDP	07-03-2023 15:12:53	0:00:21	abezboro / root				
SSH	07-03-2023 15:10:34	0:00:07	abezboro / ntadm				
SSH	07-03-2023 14:40:45	0:00:14	abezboro / ntadm				
RDP	07-03-2023 14:24:11	0:00:20	admin / root				
SSH	07-03-2023 14:23:19	0:00:16	abezboro / ntadm				
SSH	07-03-2023 14:15:35	0:00:06	abezboro / ntadm				
RDP	07-03-2023 14:13:40	0:00:11	abezboro / root	172.16.128.186	10.100.1.50	skdpu70	8

Дата и время записи	Тип события	Данные
09-03-2023 16:36:21	SERVER_CERTIFICATE_MATCH_SUCCESS	**description:** X.509 server certificate match
09-03-2023 16:36:21	CERTIFICATE_CHECK_SUCCESS	**description:** Connexion to server allowed
09-03-2023 16:36:22	SESSION_ESTABLISHED_SUCCESSFULLY	
09-03-2023 16:36:25	CB_COPYING_PASTING_DATA_TO_REMOTE_SESSION	**size:** 209 **format:** CF_TEXT(1)
09-03-2023 16:36:28	COMPLETED_PROCESS	**command_line:** C:\\Windows\\system32\\TSTheme.exe -Embedding
09-03-2023 16:36:28	INPUT_LANGUAGE	**display_name:** Russian (Russia) **identifier:** 0x0419
09-03-2023 16:36:28	KERBEROS_TICKET_CREATION	**client_name:** avs@AVS16.LOCAL **start_time:** 2023/03/09 16:33:11 **encryption_type:** AES256_CTS_HMAC_SHA1_96(18) **end_time:** 2023/03/10 02:33:11 **renew_time:** 2023/03/16 16:33:11 **flags:** [name_canonicalize | ok_as_delegate | pre_authent | renewable | forwardable](0x40a50000)

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ КОНТРОЛЯ ДОСТУПА

Блокировка запуска приложений

Можем запрещать запуск приложений в рамках сессий пользователей



Блокировка исходящих соединений с целевого узла

Блокируем заданные соединения, чтобы пользователь не имел доступ во всю внутреннюю сеть!

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

Создание и ведение профилирования пользователей. Анализ всех действий в разрезе «пользователь-цель-действие», машинное обучение и математические модели

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ

Предобработка, анализ и детектирование аномального поведения пользователей на основе профилирования и событий

ОТЧЕТЫ И СТАТИСТИКА

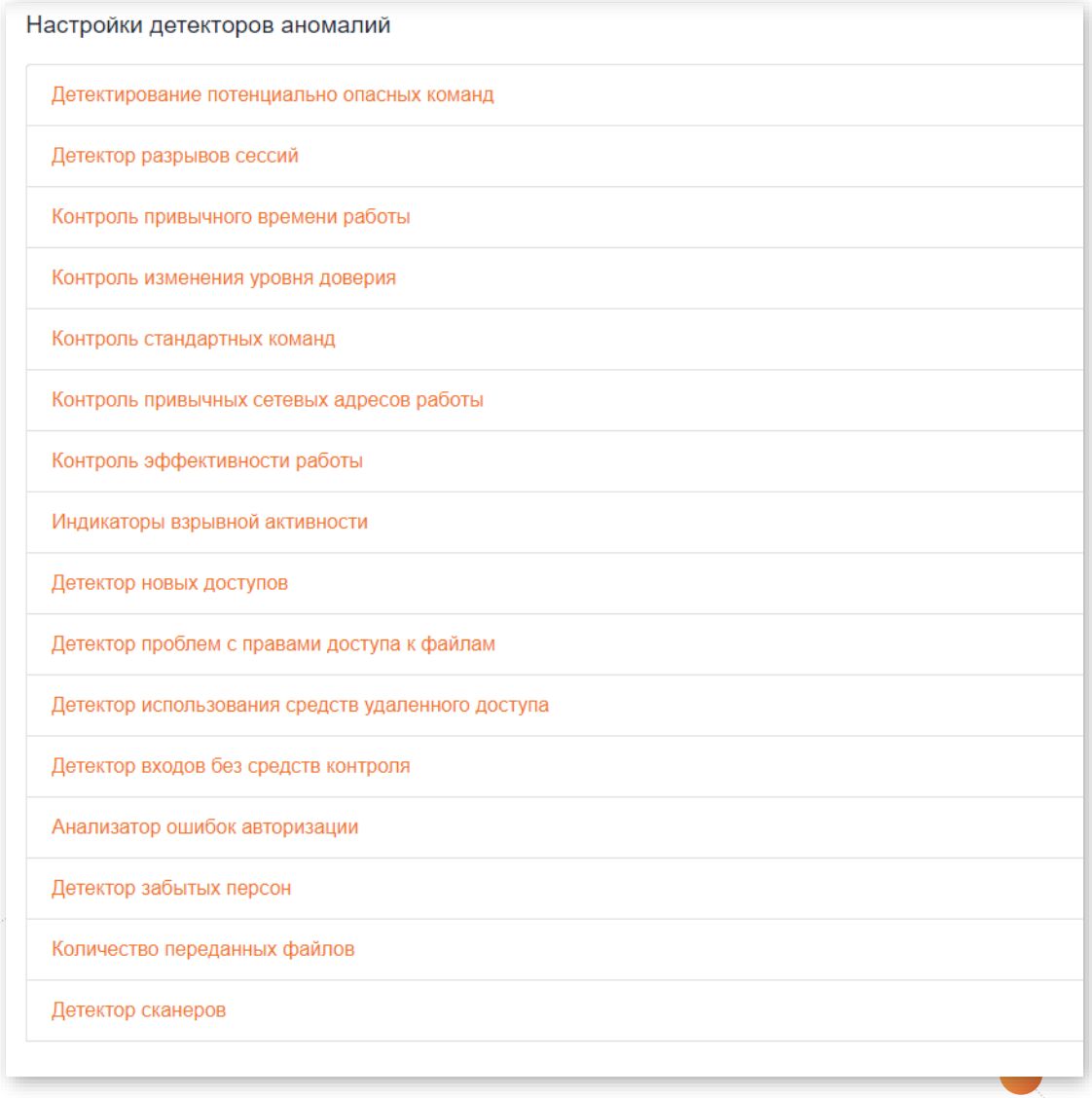
Обработка информации и её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей

ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВНИЕ

Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов

ОТ СБОРА СОБЫТИЙ К ПОИСКУ ИНЦИДЕНТОВ

АЙТИБАСТИОН

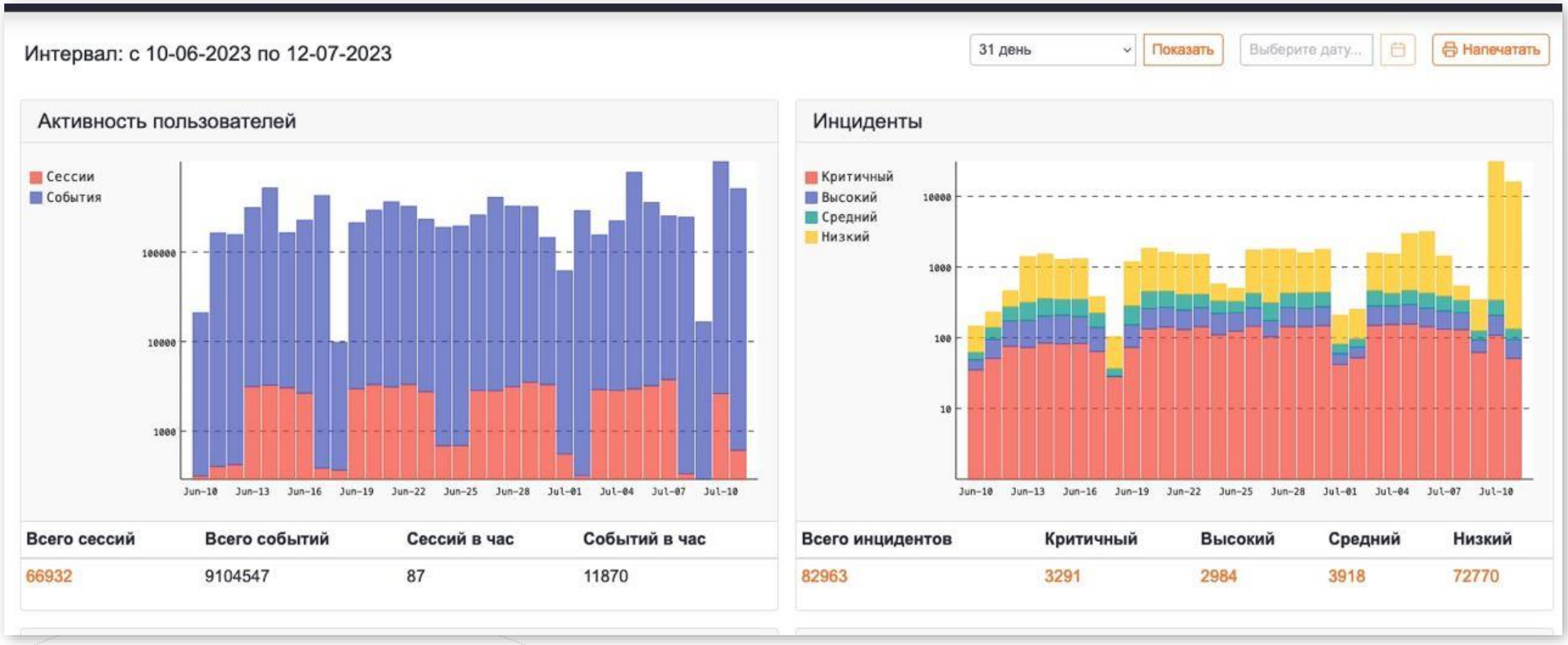


- **Детектирование аномалий** на основе статистических и математических моделей
- Детектор аномалий **«Анализ эффективности сессии»**
- Детектор аномалий **«Опасных команд»**
- Детектор аномалий **«Туннелей»**
- Детектор аномалий **«Забытых паролей»**

www.it-bastion.com

ЭКОНОМИЯ РЕСУРСОВ И РАСШИРЕННЫЙ АНАЛИЗ

АЙТИБАСТИОН



Всего сессий	Всего событий	Сессий в час	Событий в час
66932	9104547	87	11870

Всего инцидентов	Критичный	Высокий	Средний	Низкий
82963	3291	2984	3918	72770

Анализ «сырых событий» на стороне PAM и выдача в SIEM вердиктов по анализу событий, как следствие – экономия ресурсов для настройки и внедрения SIEM

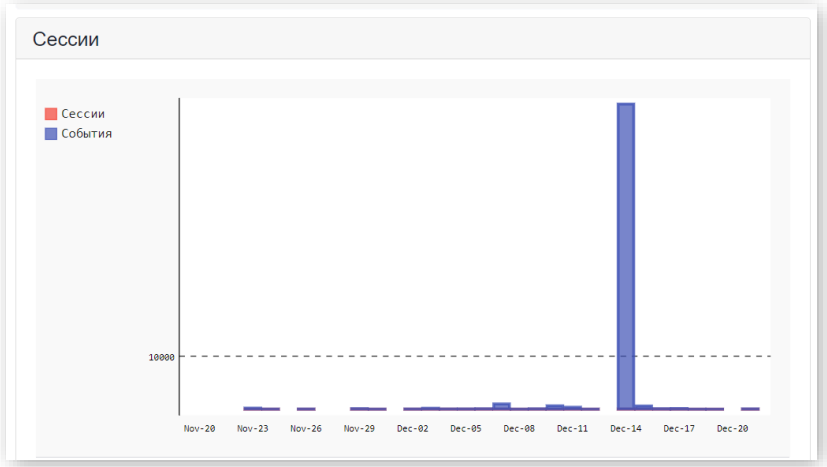
www.it-bastion.com

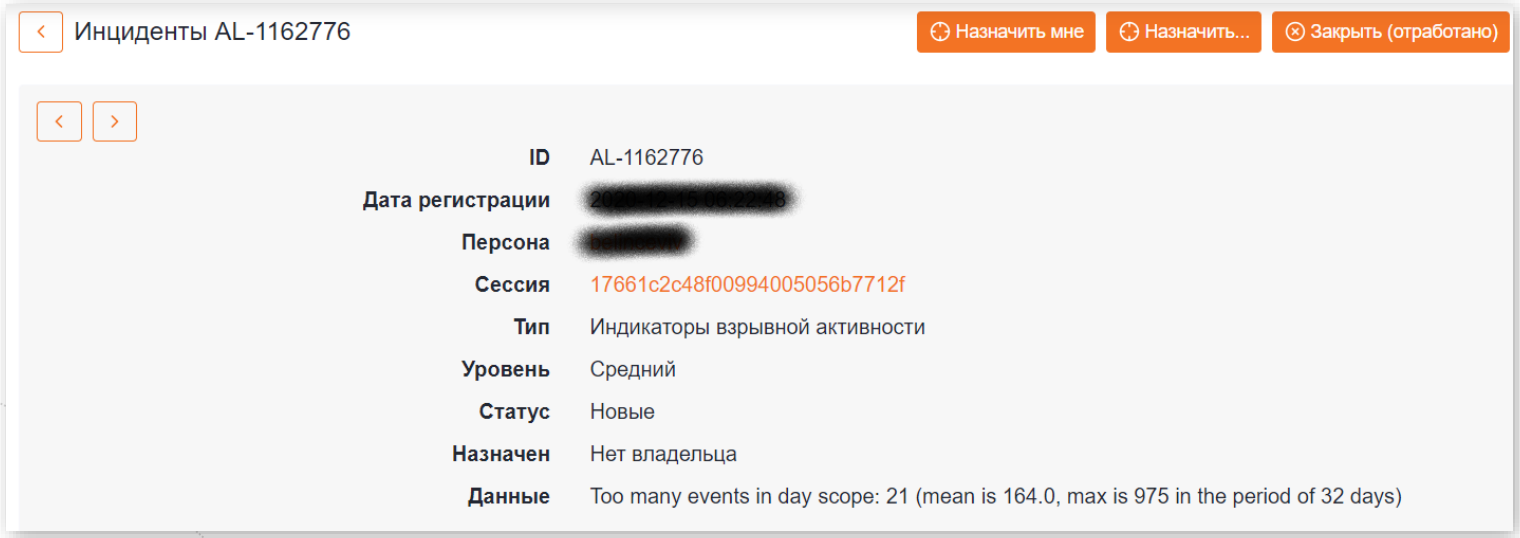
ПРИМЕР ВЗРЫВНОЙ АКТИВНОСТИ

АЙТИБАСТИОН

Варианты инцидента:

- Копирование данных из ИС
- Компрометация контура
- Аварии и критический инцидент





ПРИМЕР
ТУННЕЛИ И ПРЫЖКИ

АЙТИБАСТИОН

Дата регистрации	[redacted]
Персона	[redacted]
Сессия	177169a0150b4450005056b7712f
Тип	Туннели и прыжки
Уровень	Средний
Статус	Новые
Назначен	Нет владельца
Данные	Open Direct TCPIP Channel www.google.com:443

Подробности:

Дата и время записи	Тип события	Данные	
[redacted]	CHANNEL_EVENT	**data:**	Open Direct TCPIP Channel
		channel_id:	C0086
		dst:	www.google.com
		src_port:	53942
		dst_port:	443
		src:	127.0.0.1

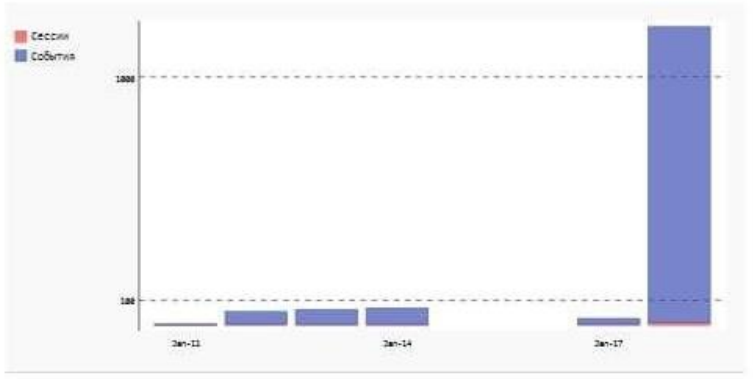
Цель [redacted]

7 дней

Избранное

Устройство:	[redacted]
IP-адрес цели:	[redacted]
Компонент:	SSH
Время последнего использования:	[redacted]

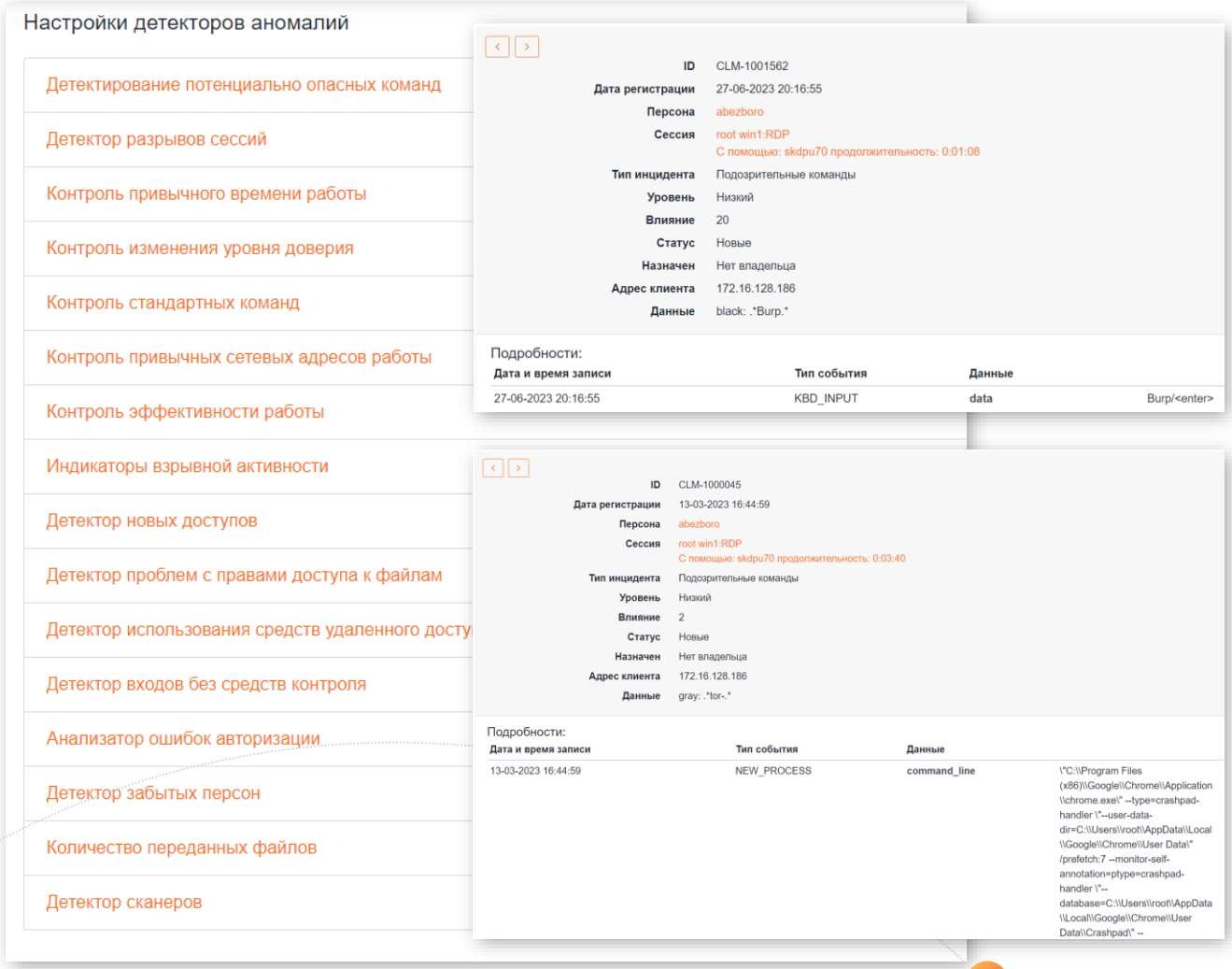
Сессии



www.it-bastion.com

ОТ ПОИСКА ИНЦИДЕНТОВ К РЕАГИРОВАНИЮ

АЙТИБАСТИОН



Индивидуальные модели реагирования

Подключение функций **реагирования на инциденты** и интеграция в единую систему реагирования

Взаимодействие с **SOAR/IRP**

```
do
incident=$(echo "${incident}" | base64 --decode)
session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
incident_id=$(echo "${incident}" | jq -r '.data.indent')
incident_link=$(echo "${incident}" | jq -r '.incident_link')

    if [ "$event_type" == "NEW_PROCESS" ]; then
        curl -k -X PUT \
    -H "X-Auth-Key: $xtoken" \
    -H "X-Auth-User: $xuser" \
    -H "Content-Type: application/json" \
    -d "{\"reason\":\"$incident_id\n$incident_link\"}" \
    "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
    fi
done
```

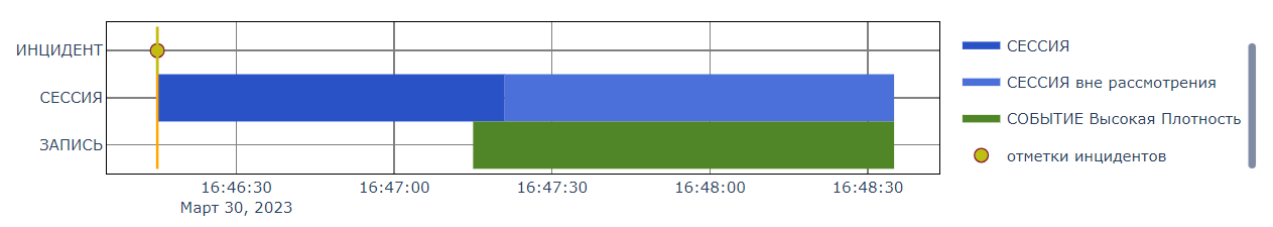
www.it-bastion.com

ПРАКТИКА РАССЛЕДОВАНИЯ НА ПРИМЕРЕ КОМПРОМЕТАЦИИ УЗ И УТЕЧКИ

АЙТИБАСТИОН

ID	eedc27123a22e61edb518fb3f5c9
Тип	RDP
Персона	p.ivan@pas.local
Адрес клиента	172.18.25.5
Старт	30-03-2023 16:46:15
Окончание	30-03-2023 16:48:35
Продолжительность	0:02:20
Цель	admin @ s_vdf-11.23.12.18 (11.23.12.18)
Шлюз	skdpu-03p
Видео	800×600 @ 25fps MPEG4
Инциденты	3

Старт сессии с нестандартного IP в необычное время



Дата и время записи	Тип события	Данные
30-03-2023 17:05:24	DRIVE_REDIRECTION_WRITE_EX	**sha256:** 19e037ddcd059235a5ce768c09b09426e8143da8867e7704e07a0f289a856281 **size:** 91452 **file_name:** D:/###Work/
30-03-2023 17:05:24	DRIVE_REDIRECTION_WRITE_EX	**sha256:** cf77028ca36aa3a046b779c77708deb1c23bf8602551994c6a362fe54947d76a **size:** 507918 **file_name:** D:/###Work/
30-03-2023 17:05:25	DRIVE_REDIRECTION_WRITE_EX	**sha256:** 2a7e251086b0729c8dd1071923ecd15a3d46860e4a0f74afc80066ff164e6284 **size:** 525794 **file_name:** D:/###Work/
:25	DRIVE_REDIRECTION_WRITE_EX	**sha256:** b4193f177542e1069852a5e86cd08fef6ef6fbffdb80e5c10985f681524cf508 **size:** 499078 **file_name:** D:/###Work/

Выгрузка большего количества файлов

ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента	Уровень	Влияние	Статус
TF-1000709	30-03-2023 16:46:15	p.ivan@pas.local	172.18.25.5	Необычное время работы	Низкий	10	Новые
SA-1000708	30-03-2023 16:46:15	p.ivan@pas.local	172.18.25.5	Сетевое расположение	Низкий	10	Новые
FT-1085414	30-03-2023 17:06:07	p.ivan@pas.local	172.18.25.5	Количество переданных файлов	Высокий	30	Новые

ИДЕНТИФИКАЦИЯ ВРЕДОНОСНОГО ПО И АТАК

АЙТИБАСТИОН

- Анализ запущенных процессов
- Сбор и накопление стандартных команд и процессов
- Детектирование аномалий

«В правилах стоял детект на типичные thread injection, и в случае выполнения тех или иных команд даже в фоновом режиме - сессия сотрудника обрывалась. Удалось задетектировать подобную вредоносную активность, расследовать её комплексом сзи и отозвать доступ к системам компании N.»

www.it-bastion.com

ЕДИНАЯ ДОПОЛНЯЕМАЯ КОНЦЕПЦИЯ РАБОТЫ РАМ-ПЛАТФОРМЫ СКДПУ НТ

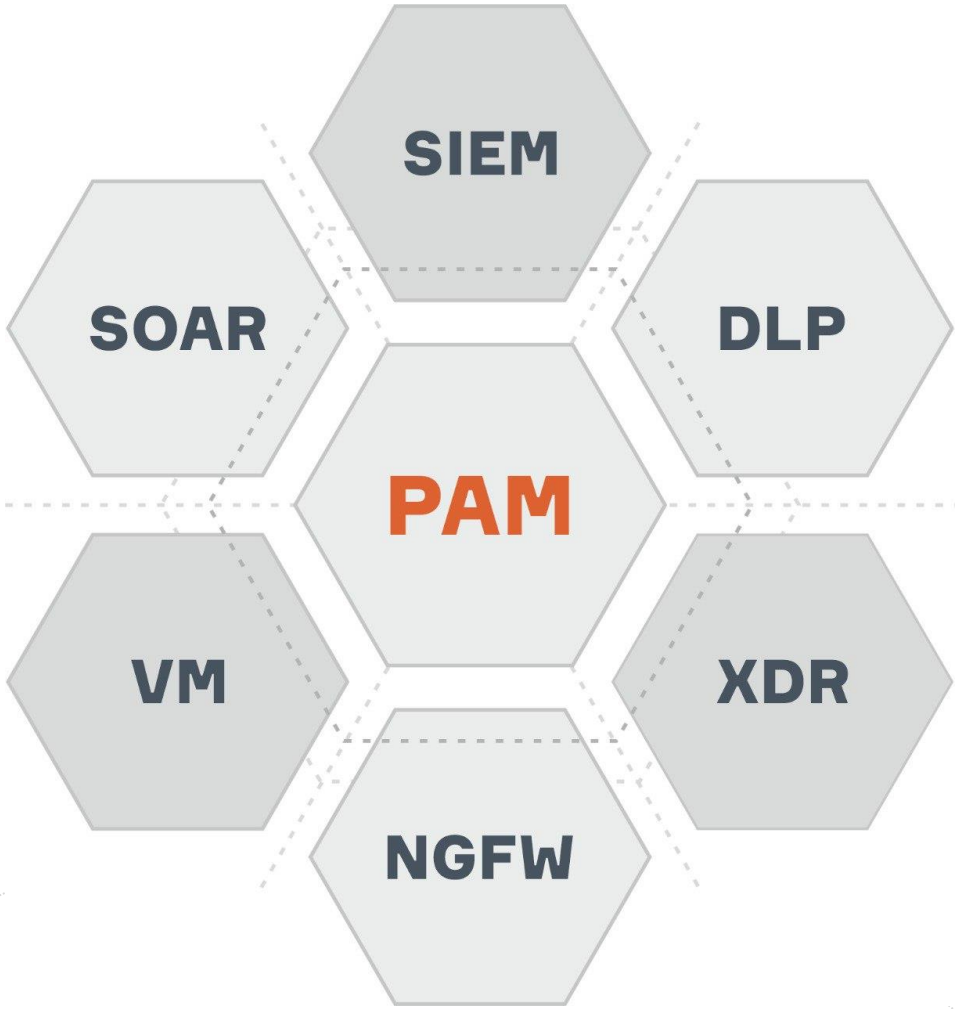
АЙТИБАСТИОН

Реализация концепции взаимодополняемых ИТ- и ИБ-систем, где каждая система предоставляет другой профильные данные, обогащая модель событий и предоставляя человеку максимально полный перечень данных для быстрого и точечного реагирования на инциденты.

1. Система обнаружения вторжений
2. Средства виртуализации и облачные сервисы
3. Многофакторная аутентификация
4. Отечественные ОС
5. IRP/SOAR
6. HoneyPot
7. SIEM-системы
8. Безопасные рабочие места, тонкие клиенты и т.п.
9. Криптошлюзы и VPN-туннели
10. Token и Smart Card
11. Межсетевые экраны
12. DLP*

СКДПУ НТ
РАМ-ПЛАТФОРМА

АЙТИБАСТИОН



Контроль и мониторинг доступа

Выявление инцидентов

Реагирование на инциденты

Кроссвендорная интеграция

Контроль доступа к информации

АЙТИБАСТИОН

Спасибо за внимание!

Константин Родин
Руководитель отдела
развития продуктов

k.rodin@it-bastion.com

it-bastion.com