

Positive Technologies и Центр мониторинга SOCRAT – непрерывная безопасность как современный метод защиты информации

- **Виктор Еременко**
Лидер продуктовой практики NAD, Positive Technologies
- **Александр Кирий**
Руководитель центра мониторинга SOCRAT, КСБ-СОФТ
- **Дмитрий Чирков**
Руководитель регионального направления, КСБ-СОФТ





Время вебинара ~1 час



Обменивайтесь сообщениями
во вкладке «Чат»



Запись вебинара направим
всем участникам на указанный
при регистрации e-mail
в течение 2-3 рабочих дней



Задавайте вопросы во вкладке
«Вопросы»



Среди заданных вами вопросов, каждый
Эксперт выберет лучший, на его взгляд, вопрос,
и мы наградим 2-х авторов фирменным мерчем!

КСБ-СОФТ

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий



Входим в ГК «Кейсистемс»



Лицензиат ФСТЭК России
Лицензиат ФСБ России

Проекты компании курируют опытные ИБ-специалисты, аккредитованные по международным сертификациям OSCP, CISM, CGEIT и CISA.

80+

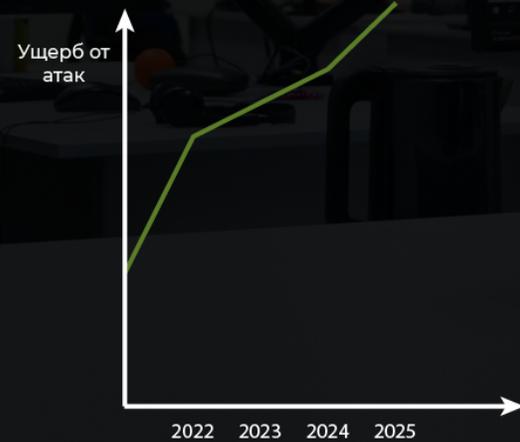
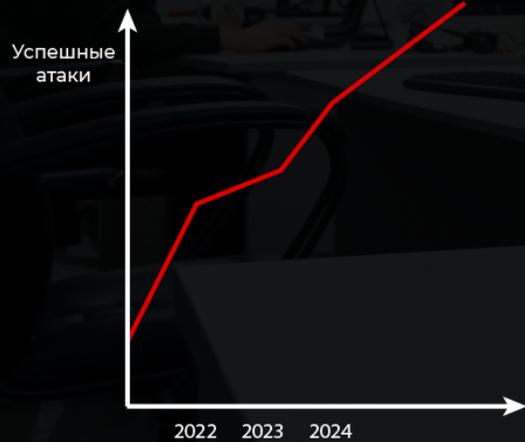
регионов
внедрения

4000+

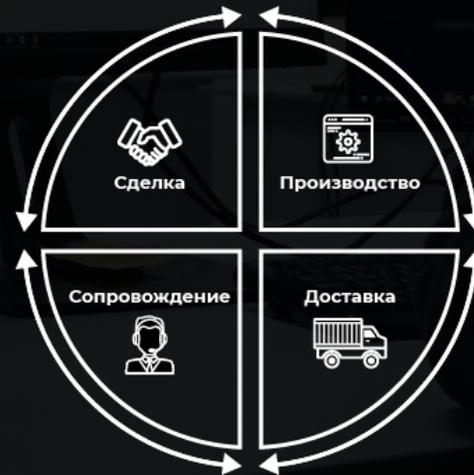
реализованных
проектов

Информационная безопасность остается актуальной

Рост количества успешных атак



Смещение целей атак в сторону нарушения бизнес-процессов



Почему безопасность должна быть непрерывной?

Общее направление в части изменения НПА в сторону выстраивание процессов



Постоянно появляются новые угрозы безопасности



Естественная деградация инфраструктуры и системы защиты (неподдерживаемые вендором версии ПО и ОС, устаревшие СЗИ, неактуальные базы, текущие средства защиты не защищают от современных атак)



Какие процессы необходимы?

06

ИТ



- Периодическая инвентаризация (актуализация и учет активов сети)
- Обновление версий ПО и ОС (особенно установка пакетов безопасности)
- Проверка корректности бэкапирования критичной информации

И другие

ИБ



- Управление уязвимостями
- Мониторинг и реагирование на инциденты ИБ
- Повышение осведомленности сотрудников

И другие

Какие процессы необходимы?

07



PT NAD

Система анализа трафика (NTA) для выявления атак



MaxPatrol VM

Система нового поколения для управления уязвимостями



MaxPatrol SIEM

Выявление инцидентов ИБ в реальном времени

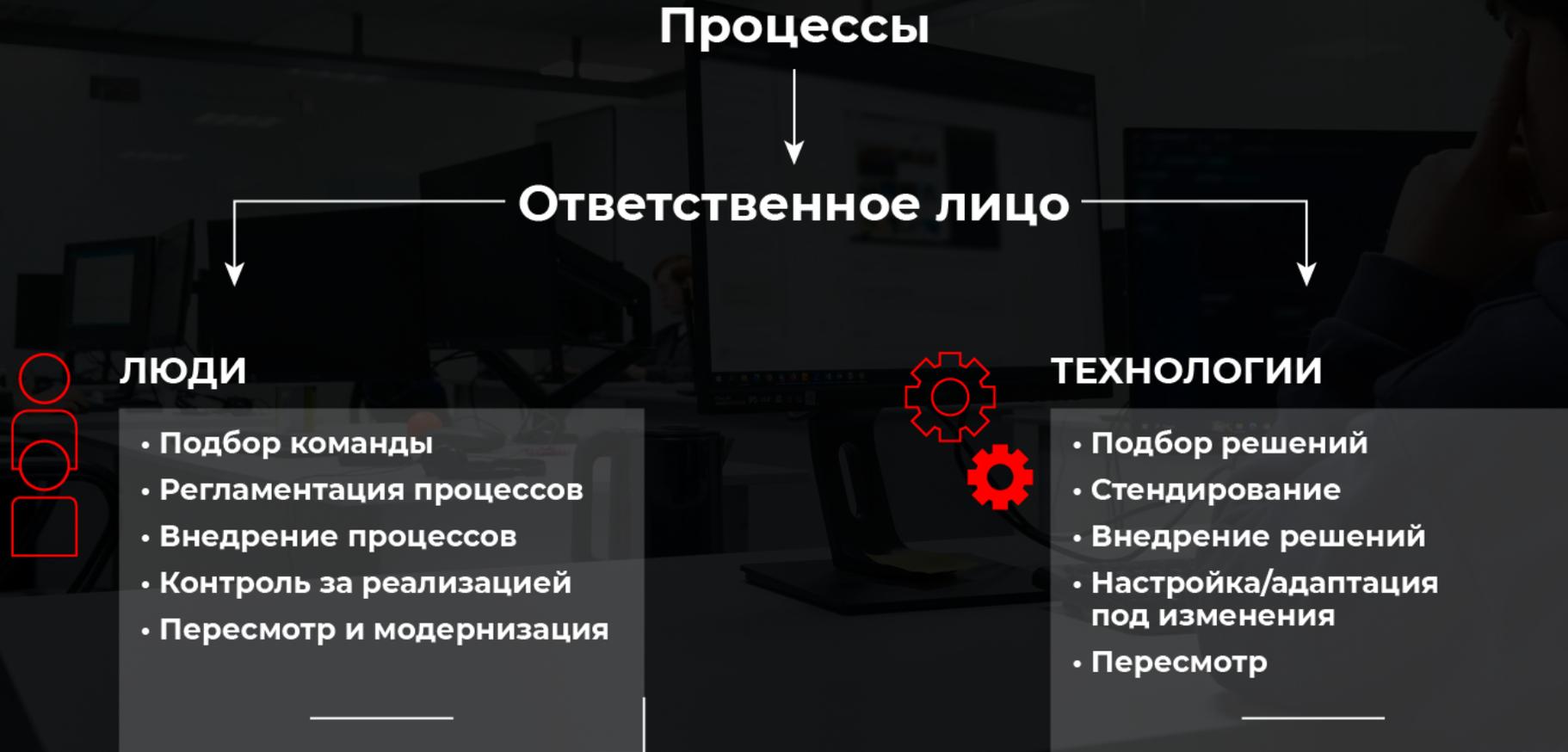


MaxPatrol EDR

Защитит конечные точки от сложных и целевых атак во всех популярных ОС, включая российские

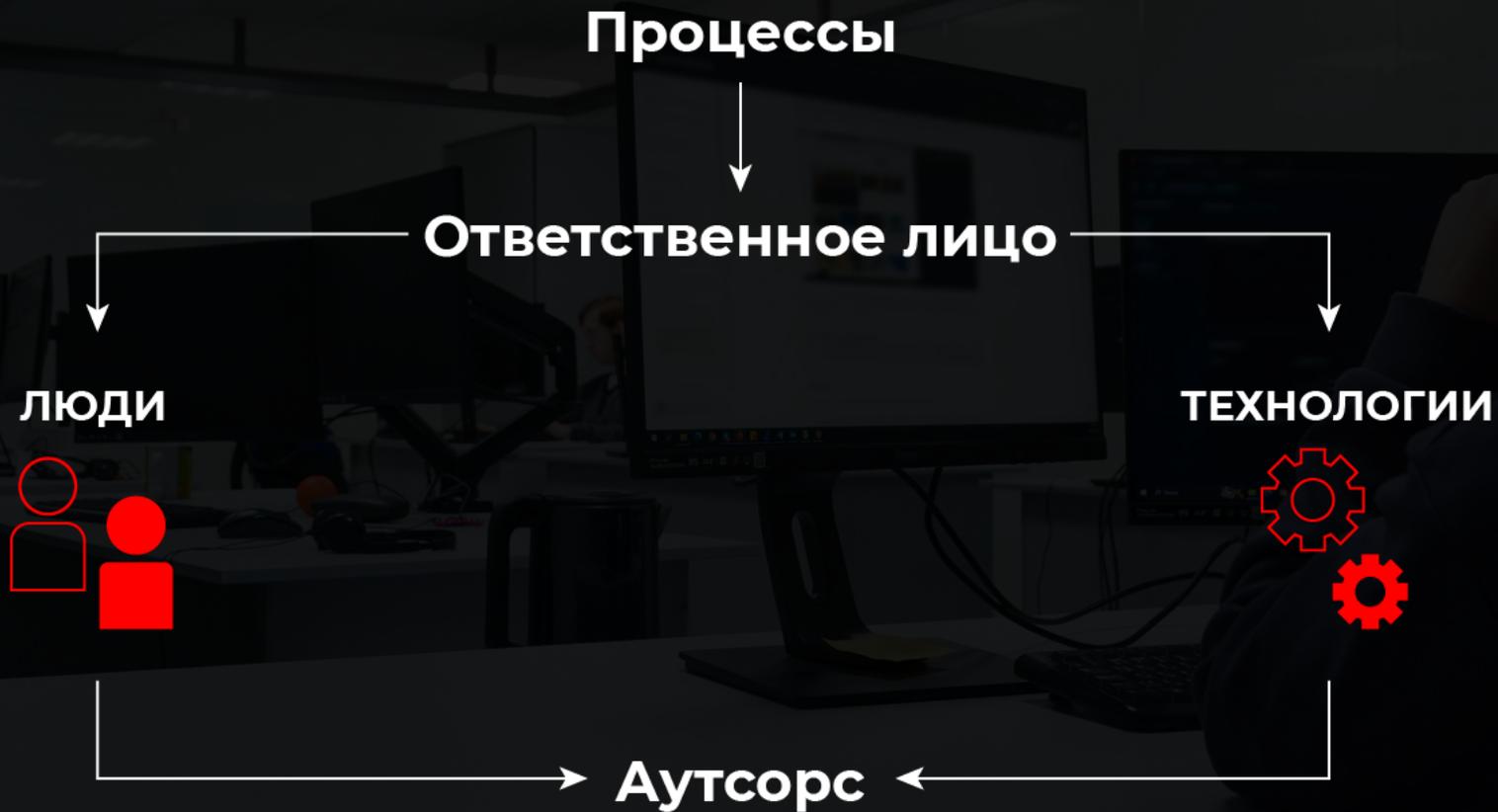
Как организовать процессы?

08



Как организовать процессы?

09



SOC
RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА

10

Режим работы **24x7**

Корпоративный
центром **ГосСОПКА**

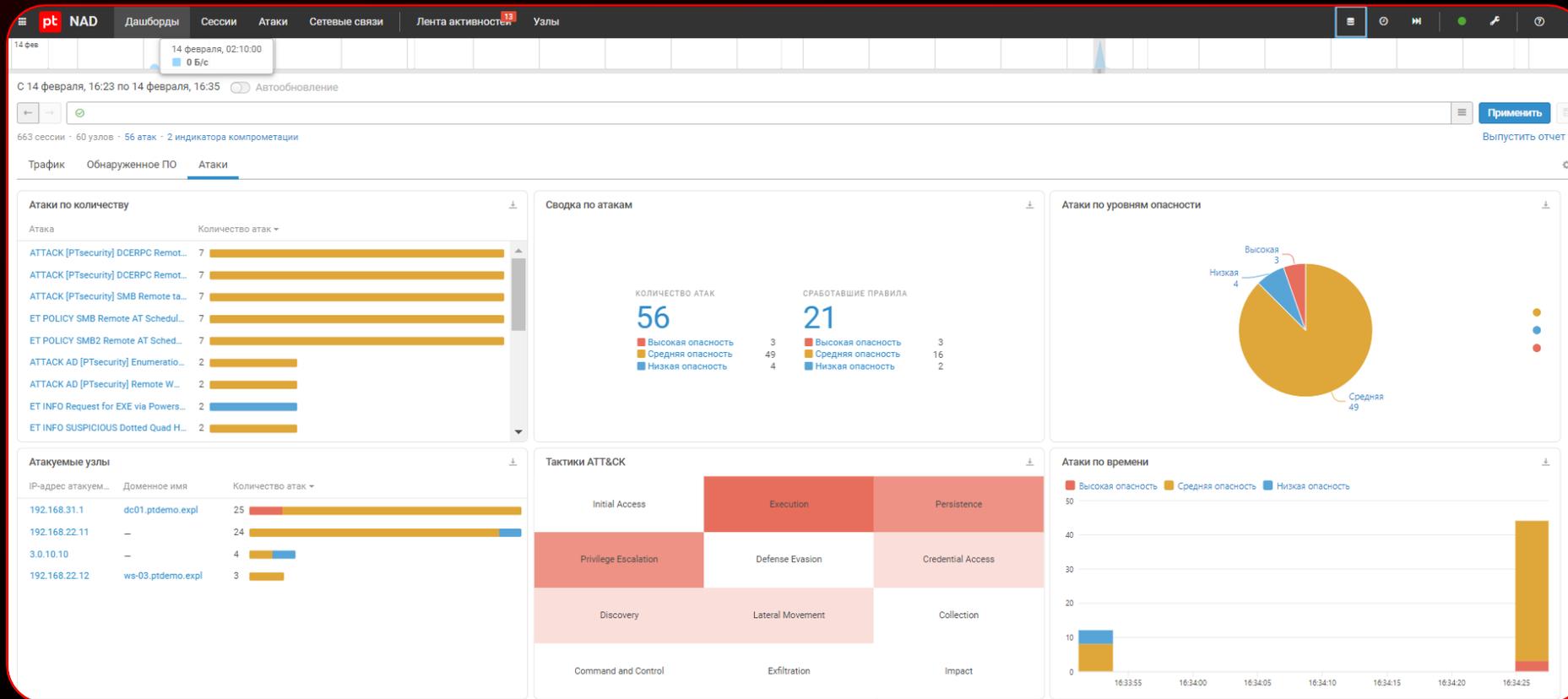
Инвентаризация
Анализ Уязвимостей
Тестирование на проникновение

Пакетная система предоставления
услуг (выбор только необходимого)

Год создания: **2020**

PT Network Attack Discovery

Система поведенческого анализа сетевого трафика для обнаружения скрытых кибератак
 Точно обнаруживает действия злоумышленников в сети, упрощает расследование инцидентов и помогает в проактивном поиске угроз



Варианты подключения PT NAD к сети



¹Брокер сетевых пакетов, TAP-устройства, коммутаторы (SPAN, GRE, ERSPAN).

²Брокер сетевых пакетов, vTAP (виртуальный TAP), виртуальные коммутаторы (GRE, ERSPAN).

Как работает PT NAD



Методы анализа трафика

Классический

Сигнатурный анализ

Репутационные списки

Интеграция с PT Sandbox

Глубокая экспертиза

Обнаружение новых активов

Экспертные модули

Детектирование приложений и сервисов

ML

Пользовательские правила профилирования

Анализ зашифрованного трафика

Поиск DGA-доменов

Какие техники MITRE ATT&CK выявляет PT NAD

| Разведка | Персональный доступ | Выполнение | Закрепление | Повышение привилегий | Предотвращение обнаружения | Получение учетных данных | Изучение | Перемещение внутри периметра | Сбор данных | Организация управления | Эксплоатация данных | Деструктивное воздействие |
|--|---|---|--|---|--|---|---|---|--|---|---|---|
| T1592 Сбор информации об атакуемых узлах (1/4) + | T1078 Существующие учетные записи (3/4) + | T1047 Инструментарий управления Windows (2/5) + | T1053 Запланированная задача (задание) (2/5) + | T1053 Запланированная задача (задание) (2/5) + | T1027 Обслуживаемые файлы или данные (1/7) + | T1003 Получение дампа учетных данных (5/8) + | T1007 Изучение системных служб (1/2) + | T1021 Службы удаленного доступа (8/7) + | T1039 Данные с общих сетевых дисков (1/2) + | T1008 Резервные каналы (4/4) + | T1029 Передача по расписанию (1/2) + | T1459 Остановка службы (1/2) + |
| T1595 Активное сканирование (2/2) + | T1133 Внешние службы удаленного доступа (1/2) + | T1053 Запланированная задача (задание) (2/5) + | T1078 Существующие учетные записи (2/4) + | T1068 Эксплуатация уязвимостей для повышения привилегий (2/4) + | T1070 Устранение индикаторов (1/9) + | T1100 Метод перебора (2/4) + | T1012 Запросы к реестру (1/2) + | T1072 Средства развертывания ПО (1/2) + | T1557 «Злоумышленник посередине» (1/2) + | T1071 Протокол прикладного уровня (4/4) + | T1041 Эксплоатация по каналу управления (1/2) + | T1459 Нисанционированное использование ресурсов (1/2) + |
| T1598 Фишинг с целью сбора сведений (1/2) + | T1189 Теневая (drive-by) компрометация (1/2) + | T1089 Интерпретаторы командной строки и сценариев (5/9) + | T1133 Внешние службы удаленного доступа (1/2) + | T1078 Существующие учетные записи (2/4) + | T1187 Принудительная аутентификация (1/2) + | T1187 Принудительная аутентификация (1/2) + | T1016 Изучение конфигурации сети (1/2) + | T1080 Заражение общего содержимого (1/2) + | T1402 Данные из репозитория конфигураций (1/2) + | T1090 Прокси-сервер (3/4) + | T1048 Эксплоатация по альтернативному протоколу (1/2) + | |
| | T1190 Недостатки в общедоступном приложении (1/2) + | T1072 Средства развертывания ПО (1/2) + | T1136 Создание учетной записи (1/2) + | T1484 Изменение доменной политики (1/2) + | T1112 Изменение реестра (1/2) + | T1212 Эксплуатация уязвимостей для получения учетных данных (1/2) + | T1018 Изучение удаленных систем (1/2) + | T1210 Эксплуатация уязвимостей в удаленных службах (1/2) + | | T1098 Протоколы (кроме прикладного уровня) (2/2) + | T1567 Эксплоатация через веб-службу (2/2) + | |
| | T1199 Доверительные отношения (1/2) + | T1003 Эксплуатация уязвимостей в клиентском ПО (1/2) + | T1197 Задания BITS (1/2) + | T1543 Создание или изменение системных процессов (1/4) + | T1197 Задания BITS (1/2) + | T1552 Незащищенные учетные данные (1/8) + | T1046 Изучение сетевых служб (1/2) + | T1180 Использование альтернативных суоностей для аутентификации (2/4) + | | T1102 Веб-служба (2/2) + | | |
| | T1200 Подключение дополнительных устройств (1/2) + | T1004 Выполнение с участием пользователя (2/2) + | T1205 Передача управляющих сигналов в трафике (1/2) + | T1546 Выполнение по событию (1/6) + | T1205 Передача управляющих сигналов в трафике (1/2) + | T1557 «Злоумышленник посередине» (1/2) + | T1049 Изучение сетевых подключений (1/2) + | T1570 Передача инструментов внутри периметра (1/2) + | | T1104 Отдельный канал для каждого этапа (1/2) + | | |
| | T1568 Фишинг (2/2) + | T1589 Микропроцессное взаимодействие (1/2) + | T1505 Компонент серверного ПО (2/5) + | | T1207 Поддельный контроллер домена (1/2) + | T1568 Кража или подделка билетов Kerberos (1/4) + | T1069 Изучение групп разрешений (1/2) + | | | T1105 Передача инструментов из внешней сети (1/2) + | | |
| | | T1569 Системные службы (1/2) + | T1542 Загрузка раннее ОС (1/5) + | | T1216 Выполнение через системный сценарий (1/1) + | T1649 Кража или подделка сертификатов аутентификации (1/4) + | T1082 Изучение систем (1/2) + | | | T1132 Кодирование данных (1/2) + | | |
| | | | T1543 Создание или изменение системных процессов (1/4) + | | T1207 Поддельный контроллер домена (1/2) + | | T1082 Изучение систем (1/2) + | | | T1205 Передача управляющих сигналов в трафике (1/2) + | | |
| | | | T1546 Выполнение по событию (1/6) + | | T1218 Выполнение с помощью системных бинарных файлов (2/2) + | | T1083 Изучение файлов и каталогов (1/2) + | | | T1219 ПО для удаленного доступа (1/2) + | | |
| | | | | | T1221 Внедрение в шаблоны (1/2) + | | T1087 Изучение учетных записей (1/4) + | | | T1568 Динамическое разрешение (1/2) + | | |
| | | | | | T1484 Изменение доменной политики (1/2) + | | T1124 Изучение системного времени (1/2) + | | | T1571 Нестандартный порт (1/2) + | | |
| | | | | | T1542 Загрузка раннее ОС (1/5) + | | T1138 Изучение общих сетевых ресурсов (1/2) + | | | T1572 Туннелирование протокола (1/2) + | | |



Подробнее о том, какие техники покрывает PT NAD и как он их выявляет:

mitre.ptsecurity.com

Выявляет 180 техник и тактик атакующих, включая хакерский инструментарий и модифицированное вредоносное ПО

Сценарии использования



Сетевые связи

The screenshot displays the PT NAD interface for network connections. The top navigation bar includes "Дашборды", "Сессии", "Атаки", "Сетевые связи", "Лента активностей", and "Узлы". The main area shows a network graph with nodes and connections. A tooltip for the connection between 10.125.124.26 and 10.158.3.2 is open, showing attack details.

Network Statistics: 244 узла · 55 клиентов · 198 серверов

Максимум показываемых связей: 15

Connection: 10.125.124.26 → 10.158.3.2

| Атаки | |
|---|---|
| Название | TOOLS [PTsecurity] SSF Tunneling tool over SSL |
| Опасность | Высокая |
| Класс | Exploitation attributes |
| Количество | 8 |
| Название | |
| TOOLS [PTsecurity] Sliver C2 HTTP Polling (Base64gzip) | |

Network Nodes and Connections:

- 10.125.124.5
- 10.158.3.2
- 10.125.124.26 → 10.158.3.2
- 192.168.53.1
- 192.168.31.222
- 192.168.64.65
- 192.168.55.21
- 192.168.22.99
- 192.168.23.12
- 192.168.23.13
- 192.168.23.1
- 192.168.55.16
- 192.168.64.17
- 169.254.19.165
- 239.255.255.250
- dc01.ptdemo.expl
- ex-01.ptdemo.expl
- dhcp.ptdemo.expl

Результативность



BDU:2024-08422



BDU:2024-08421

 НОВОСТИ

Positive Technologies помогла
устранить 0-day уязвимости
в российской ВКС-системе
VINTEO

18 НОЯБРЯ 2024

Детектирование хакерского инструментария

The image shows a screenshot of the PT NAD (Network Activity Detector) interface. The main window displays a list of detection rules under the heading "TOOLS [PTsecurity] Mythic C2 SMB Transport Response". The interface is divided into several sections:

- TOOLS [PTsecurity] Mythic C2 SMB Transport Response**: The main title of the tool set.
- Параметры правила**: Rule parameters section.
- Исключения**: Exclusions section.
- Обнаруживаемая атака**: Detected attack section.

Two specific rule details are shown in overlapping windows:

- Использование Cobalt Strike**: Shows "Общие сведения" (General information) and "Описание и рекомендации" (Description and recommendations).
- Использование Brute Ratel**: Shows "Общие сведения" (General information) and "Описание и рекомендации" (Description and recommendations).

Использование Brute Ratel - Общие сведения

| | | | |
|-----------|---|---------------|-------------------------|
| Состояние | <input checked="" type="checkbox"/> Включено | Идентификатор | brute_ratel |
| Название | Использование Brute Ratel | Ревизия | 1 от 18 мая 2023, 21:30 |
| Тип | Системное | | |
| Опасность | ■ Средняя ▾ | | |

Использование Brute Ratel - Описание и рекомендации

Описание

Обнаружена активность Brute Ratel — фреймворка для постэксплуатации зараженных систем. Brute Ratel позволяет злоумышленникам взаимодействовать со скомпрометированными узлами, выполнять на них команды и осуществлять продвижение внутри инфраструктуры. Для этого в Brute Ratel используются специальные агенты, называемые «барсуками» (badgers). PT NAD обнаруживает «барсуков» по периодическим HTTP-запросам к управляющему серверу (C2), используемому для взаимодействия, получения команд и предоставления отчета о результатах их выполнения. Периодичность запросов может быть разной, но, как правило, находится в диапазоне от 30 секунд до нескольких минут. Для предотвращения обнаружения запросы могут маскироваться, например, под запросы JavaScript-библиотек или запросы к криптографической инфраструктуре.

Рекомендации

Чтобы понять, является ли активность легитимной, изучите данные в блоках «Сервер» и «Клиенты». Отправляли ли перечисленные клиенты подобные запросы на указанный узел ранее? Поищите и проанализируйте сессии по доменным именам из поля HTTP-заголовка Host. Являются ли указанные в этом поле домены известными? Наконец, уделите внимание срабатываниям других правил на трафик сессий, в которых участвовали указанные клиенты.

Детектирование коннекта с C2



The image displays three overlapping screenshots of the PT NAD (Network Activity Detector) interface, illustrating the configuration and detection of a connection to a C2 server.

Top Screenshot: TOOLS [PTsecurity] LocaltoNet Active Tunnel

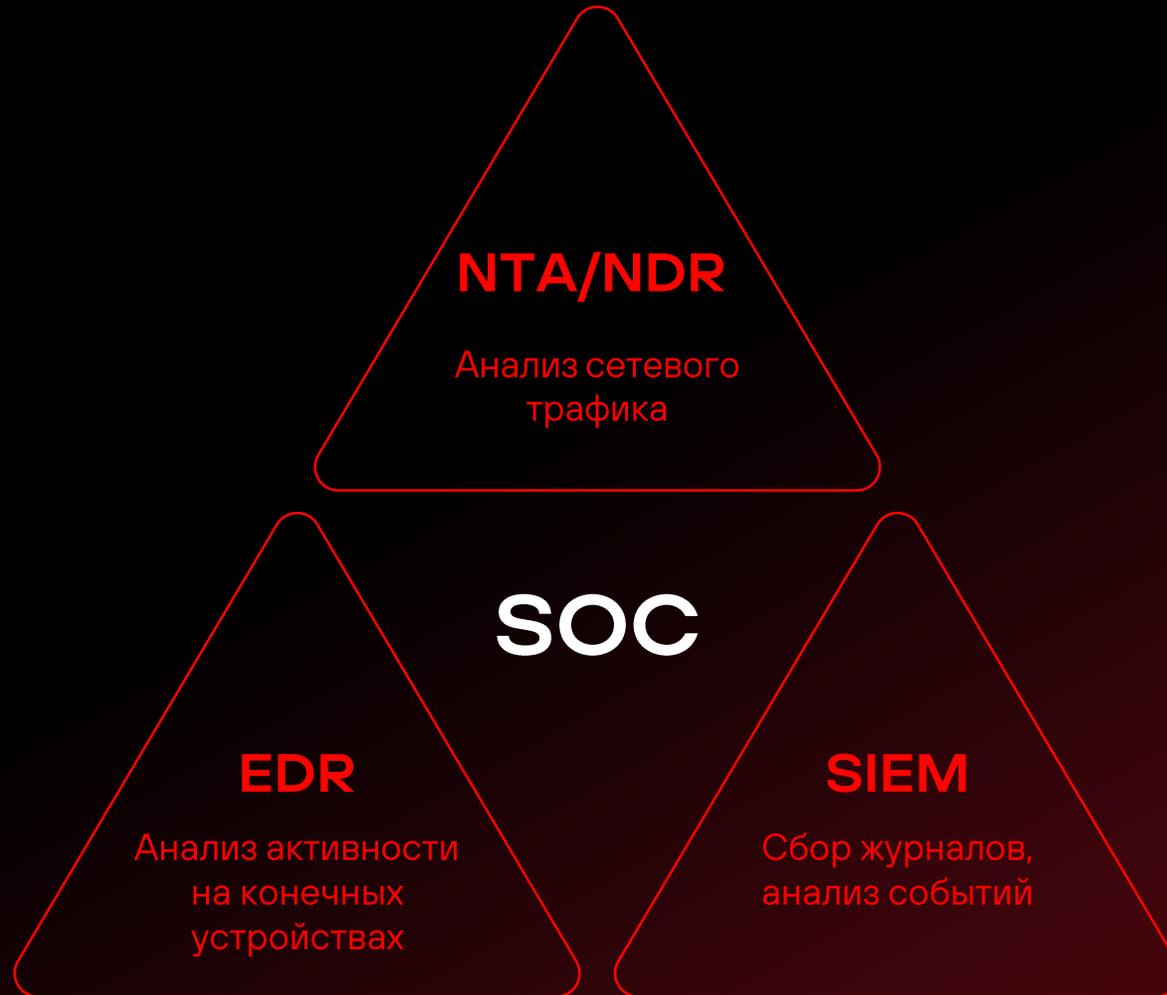
- Navigation: Дашборды, Сессии, Атаки, Сетевые связи, Лента активностей (1), Узлы
- Left sidebar: Параметры правила, Исключения, Обнаруживаемая атака
- Right panel: Параметры правила
- State: Состояние Включено
- SID: SID

Middle Screenshot: TOOLS [PTsecurity] gsocket client activity

- Navigation: Дашборды, Сессии, Атаки, Сетевые связи, Лента активностей (1), Узлы
- Left sidebar: Параметры правила, Исключения, Обнаруживаемая атака

Bottom Screenshot: TOOLS [PTsecurity] Chisel http tunnel tool connection

- Navigation: Дашборды, Сессии, Атаки, Сетевые связи, Лента активностей (2), Узлы
- Left sidebar: Параметры правила, Исключения, Обнаруживаемая атака
- Right panel: Параметры правила
- State: Состояние Включено
- Name: Название TOOLS [PTsecurity] Chisel http tunnel tool connection
- Class: Класс Exploitation attributes
- Severity: Опасность ■ Высокая
- Action: Действие Alert
- Protocol: Протокол tcp
- Source: Откуда any : any
- Destination: Куда any : any
- Metadata: SID 10004438, Ревизия 3, Вендор PTSecurity, Обновлено 12 ноября 2024, 15:59



С ЧЕГО НАЧАТЬ?



ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг **SOCRAT**

Мониторинг: **8x5**

Время реагирования – **24 часа** с момента обнаружения

Ограниченный состав подключаемых ресурсов

Длительность пилота – **1 месяц**



Демостенд



Пилот



Серверы



Консультации

■ positive technologies

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить **PT NAD**



PT NAD

Система анализа трафика (NTA) для выявления атак

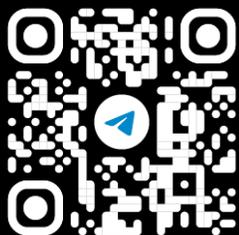
РАБОТАЙТЕ С НАМИ!



ksb-soft.ru



info@ksb-soft.ru



Телеграм-канал
«Мнение Интегратора»



8 800 3333-872



Подкаст
«Голос Интегратора»



428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9