Технологии Panda Adaptive Defense 360

Мощное обнаружение, Надежное сдерживание

panda
a WatchGuard brand

Panda Adaptive Defense 360

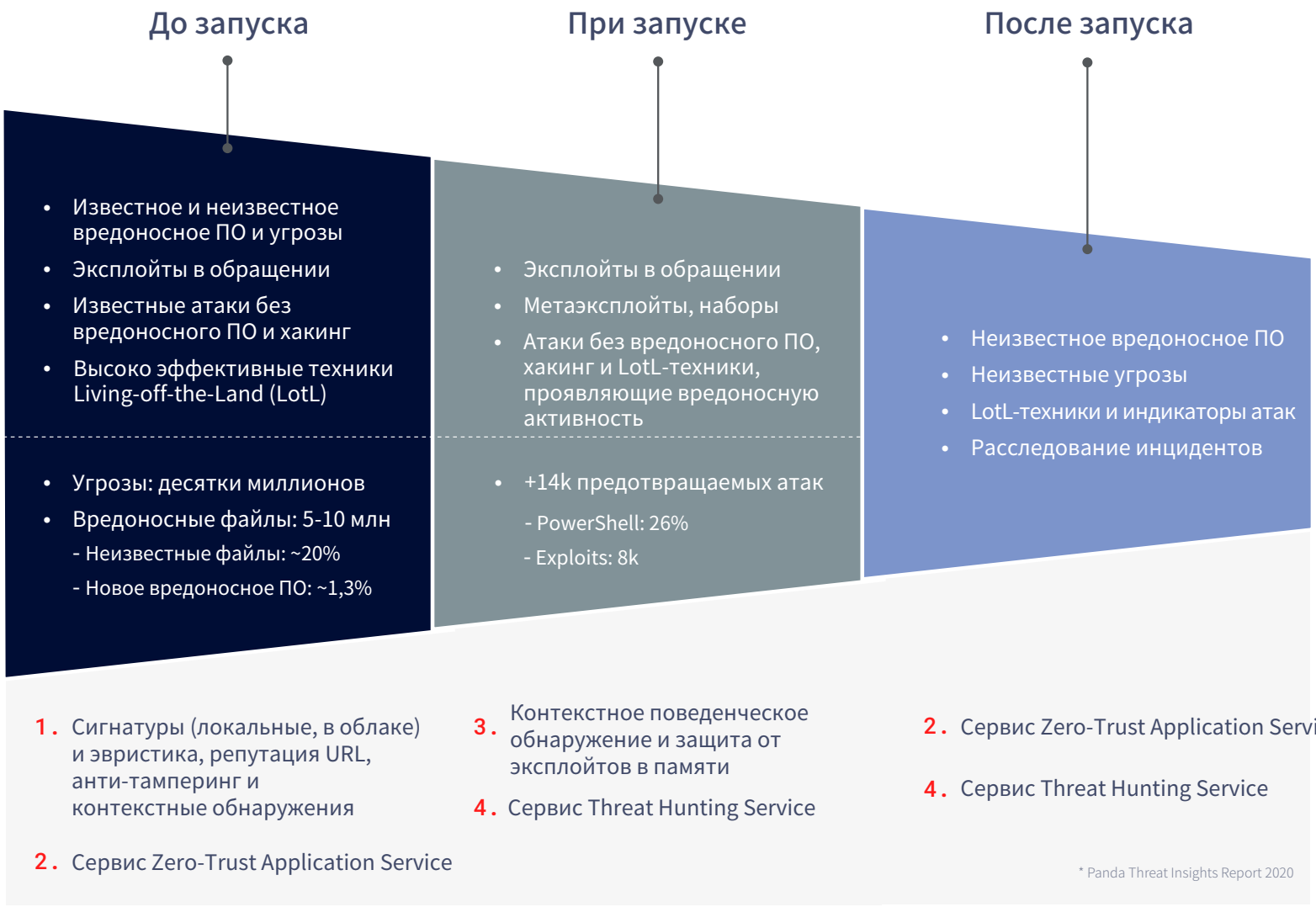
Содержание

Технологии и сервисы в Panda Adaptive Defense 360

Введение

Документ объясняет, как работают вместе **технологии и сервисы, интегрированные в Panda Adaptive Defense 360**. Отличительными факторами являются возможности обнаружения атак на конечные устройства и реагирование на них (Endpoint Detection and Response, EDR), а также использование технологий Искусственного интеллекта (ИИ).

На следующем рисунке показано, где работает каждая технология, и какие техники используются для максимально быстрой блокировки злоумышленников, предотвращая компрометацию конечных устройств и обнаруживая, сдерживая и реагируя на кибер-преступников прежде, чем они смогут причинить ущерб.



Основные группы технологий и сервисов предотвращения, обнаружения и реагирования, интегрированные в Panda Adaptive Defense 360:

1. **Полный набор технологий Panda для защиты конечных устройств**
2. **Сервис Zero-Trust Application Service**
3. **Контекстные поведенческие обнаружения и защита от эксплойтов в памяти**
4. **Сервис Threat Hunting Service**

Далее мы рассмотрим, как они работают вместе для обеспечения **более высокого уровня защиты с минимальными усилиями**.

1. Полный набор технологий защиты устройств (EPP)

Набор проактивных технологий EPP	Panda Adaptive Defense 360
Универсальные сигнатуры и эвристика	✓
Облачные знания Коллективного разума (Threat Intelligence)	✓
Поведенческий анализ и обнаружение индикаторов атак IoA	✓
Файервол, обнаружение (IDS) и предотвращение вторжений (IPS), инспектирование сетевых пакетов	✓
Анти-тампering	✓
Контроль устройств	✓
Репутация URL	✓
Контроль приложений	✓
Антиспам, антифишинг, фильтрация контента для серверов MS Exchange	✓
Защита почтового ящика и интеллектуальная проверка серверов MS Exchange	✓
Оценка уязвимости и управление патчами*	✓

*Panda Patch Management

На рынке существует распространенное заблуждение относительно EPP-технологий, полагая, что они являются всего лишь традиционными, основанными на сигнатурах антивирусами, и что они могут быть заменены EDR-решением.

На самом деле эти технологии, помимо сигнатурного анализа, объединяют в себе общие сигнатуры, эвристику, файервол, репутацию URL, контекстное обнаружение, управление уязвимостями, контроль приложений и другие возможности, которые могут значительно снизить риск.

Эти превентивные технологии, которые работают совместно с EDR-решениями, предоставляют важные преимущества, среди них:

- **Значительное снижение уровня риска.** Им не нужно запускать файл для обнаружения вредоносного ПО. Им нужно только подключение к облаку.
- **Очень низкий уровень ложных срабатываний.** EPP-технологии, которые могут защищать автономно, широко распространены на огромном количестве конечных устройств, и они настроены таким образом, чтобы свести к минимуму ложные срабатывания.
- **Оптимизация производительности.** Эти технологии интегрированы между собой и работают вместе, чтобы избежать избыточности и минимизировать любое влияние на производительность конечных устройств, которые они защищают.

2. Сервис Zero-Trust Application

Искусственный интеллект (ИИ) как прорывная инновация в безопасности

Управляемый сервис включен как часть лицензии на **Panda Adaptive Defense и Adaptive Defense 360**. Этот сервис классифицирует любой процесс как вредоносный или доверенный прежде, чем на каждом конечном устройстве разрешить запуск только доверенных процессов. Т.к. это полностью автоматизированный сервис, он не требует от конечного пользователя или сотрудников ИБ в компании каких-либо вводных данных или принятия решения.

Сервис Zero-Trust Application Service имеет три ключевых компонента:

1. **Непрерывный мониторинг активности конечного устройства из облачной платформы**

   Отслеживается активность каждого приложения на конечных устройствах, независимо от его природы, и данные мониторинга отправляются в облако для непрерывной классификации процессов.

   Таким образом, можно предотвратить выполнение вредоносных программ и даже сложных угроз, таких как атаки на цепочки поставок.

2. **Автоматизированная ИИ-классификация**

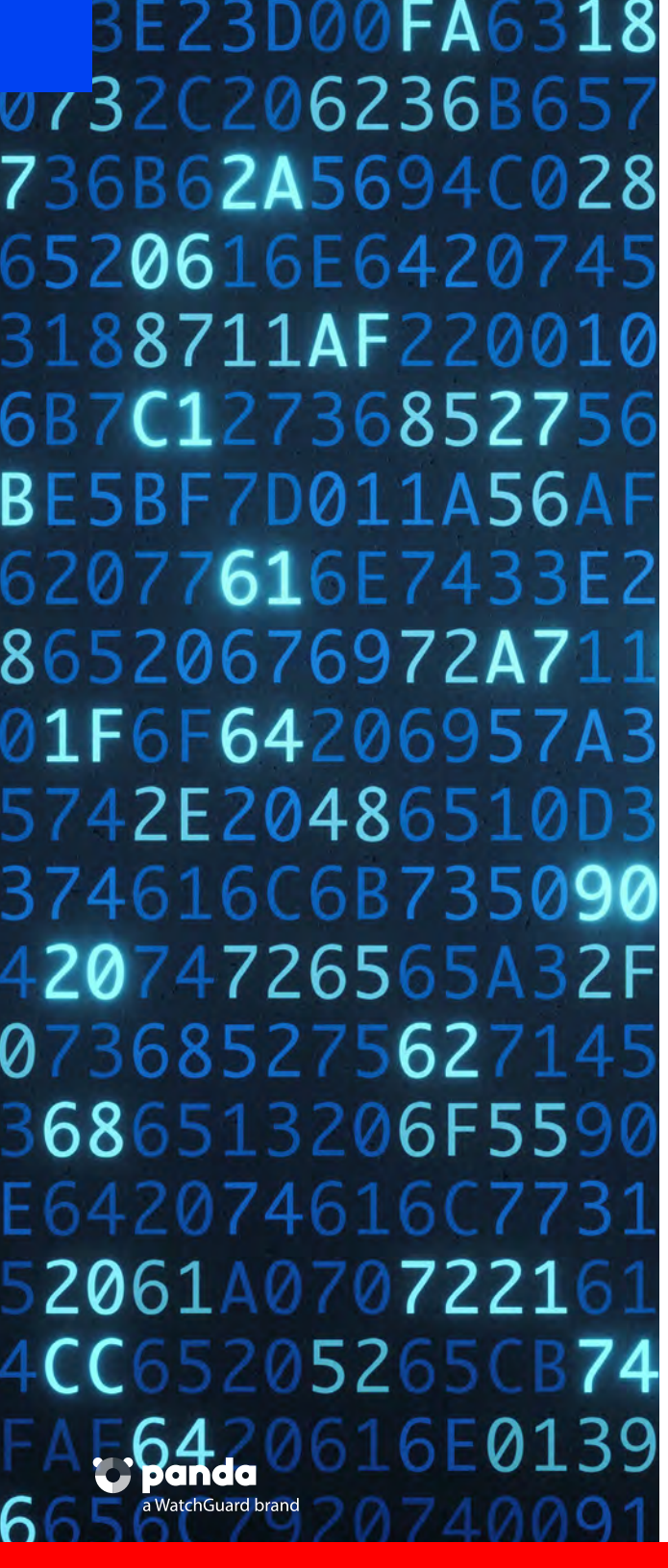
   Автоматизированные классификации выполняются в облачной ИИ-системе, где выполняется массив многочисленных алгоритмов машинного обучения (ML), обрабатывающих сотни статичных, поведенческих и контекстных параметров в реальном времени. Параметры извлекаются из телеметрии защищаемого окружения и набора **физических песочниц,** в которых "детонируют" исполняемые файлы.

Сегодня уровень автоматизированный классификации равен 99,98%, так что только 0,02% процессов требуют вмешательство наших экспертов. ИИ-система классификации является самодостаточной, масштабируемой до больших объемов файлов, работающей в реальном времени и не зависящей от любых вводных данных со стороны конечного пользователя.

Что такое физическая песочница?

Массив облачных пользовательских машин, специально настроенных для "детонации" файлов и извлечения их поведенческих и контекстных параметров в реальном времени.

Мы используем физические песочницы вместо песочниц на виртуальных машинах, потому что существует множество вредоносных приложений, которые способны обнаруживать свой запуск внутри виртуальной машины, скрывая свое вредоносное поведение.



panda
a WatchGuard brand

3. **Контроль приложений на основе уровня риска**

Связан с режимами работы агента защиты, запущенного на конечных устройствах. Есть два уровня защиты:

- **Режим Hardening:** по умолчанию запрещает запуск любого неизвестного приложения или бинарного файла, поступившего извне (скачивание из Интернета, почта, съемные носители, удаленные устройства и пр.).
- **Режим Lock:** по умолчанию запрещает запуск любого неизвестного приложения или бинарного файла вне зависимости от его происхождения (из сети, с самого конечного устройства или извне). Обеспечивает запуск только доверенных (надежных) процессов.

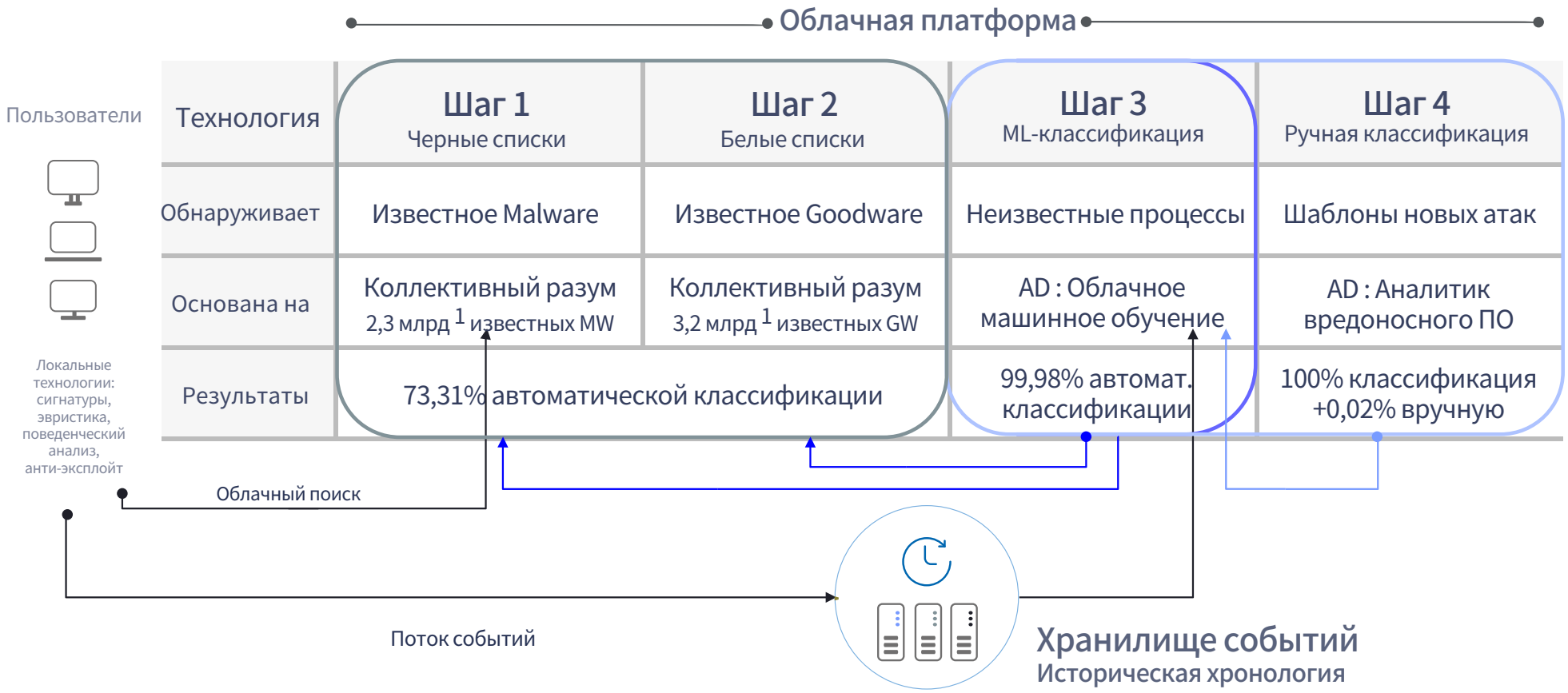
Коллективный разум Panda Security. Размещенный на облачной платформе, это еще один ключевой компонент, который позволяет работать новой модели защиты, повышающей эффективность работы сервиса Zero-Trust Application Service.

Коллективный разум представляет собой консолидированное и инкрементное хранилище всех приложений, бинарных файлов и других файлов, содержащих интерпретируемый код (доверенные и вредоносные).

Это облачное хранилище постоянно пополняется данными из системы Искусственного интеллекта и от экспертов-аналитиков, а его содержимое постоянно запрашивается решениями и сервисами Panda Security перед запуском любого процесса.

- На следующем рисунке показано, как технологии в указанном наборе органично работают вместе, позволяя классифицировать все приложения, бинарные файлы и файлы с интерпретируемым кодом в режиме реального времени.

Как работает сервис Zero-Trust Application Service



3. Контекстное поведенческое обнаружение и защита от эксплойтов в памяти

Непрерывный мониторинг активности на конечных устройствах позволяет агенту работать в качестве сенсора и информировать облачную платформу не только о запускаемых файлах, но также и контексте их запуска (что происходит прямо перед этим, какие пользователи пытаются запускать какую команду или приложение, какой генерируется сетевой трафик, к каким файлам с данными осуществляется доступ, параметры и т.д.).

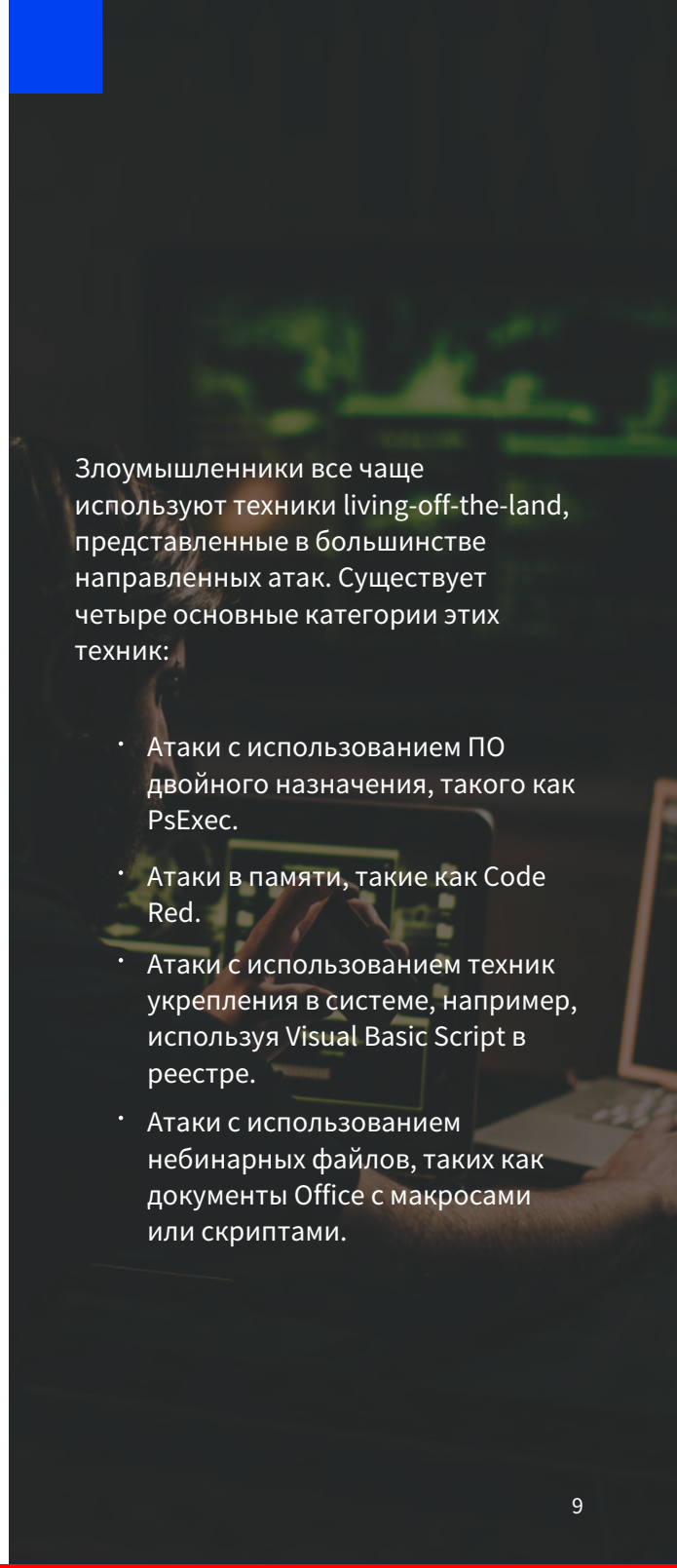
Это позволяет идентифицировать, прежде всего на конечном устройстве, аномальное поведение или подозрительную активность, а также классифицировать их как индикаторы атаки (IoA) с высокой степенью достоверности и без ложных срабатываний.

Во многих случаях IoA связаны с конкретными фазами цепочки **Cyber Kill Chain** или с тактиками **MITRE ATT&CK framework**[1]:

- Первоначальный доступ
- Выполнение
- Укрепление в системе
- Повышение прав
- Обход защиты
- Доступ к учетным данным
- Обнаружение
- Горизонтальное перемещение
- Сбор
- Командование и управление
- Эксфильтрация данных
- Последствия

Обнаружение IoA до момента извлечения данных (или их шифрования в случае с атакой шифровальщика) - это очень эффективный механизм защиты, особенно против атак типа Living-off-the-Land (LotL), даже если конечные устройства уже могут быть скомпрометированы.

Panda Adaptive Defense и Panda Adaptive Defense 360 в рамках единого агента защиты интегрируют полный набор технологий для обнаружения IoA на различных этапах атаки. Отнюдь не являясь статичными технологиями, они постоянно пополняются шаблонами и техниками новых атак, которые обнаруживаются в рамках сервиса Threat Hunting and Investigation Service (THIS).



Злоумышленники все чаще используют техники living-off-the-land, представленные в большинстве направленных атак. Существует четыре основные категории этих техник:

- Атаки с использованием ПО двойного назначения, такого как PsExec.
- Атаки в памяти, такие как Code Red.
- Атаки с использованием техник укрепления в системе, например, используя Visual Basic Script в реестре.
- Атаки с использованием небинарных файлов, таких как документы Office с макросами или скриптами.

Среди многочисленных индикаторов атаки, которые обнаруживает агент, мы выделяем следующие категории:

1. IoA эксплойтов в обращении

С помощью этих поведенческих и контекстных IoA, эксплойты в обращении, как и наборы эксплойтов, обнаруживаются и блокируются до их выполнения, закрывая злоумышленникам один из основных векторов проникновения.

Кроме того, собственная файервольная технология **виртуального патчинга обнаруживает и блокирует попытки использования уязвимостей за счет мониторинга входящего трафика**.

Например, эта технология используется для идентификации и блокировки эксплойтов против уязвимости BlueKeep, в которой устанавливаются определенные соединения через RDP-сессию. Эти соединения, если они не заблокированы, позволяют хакеру удаленно выполнять код (RCE).

Технология виртуального патчинга обнаруживает такие соединения и автоматически их отклоняет. Обнаружения записываются в облако и показываются в веб-консоли Panda Adaptive Defense 360, что позволяет администраторам немедленно принимать соответствующие меры.

В качестве меры сдерживания они могут применять изменения конфигурации, например, активируя Network Level Authentication (NLA), отключая различные несущественные RDP-сервисы на конечных устройствах или по возможности применяя в системах патчи, что в итоге позволяет эффективно сокращать поверхность атаки.

2. IoA в памяти: динамическая технология защиты от эксплойтов

Panda Adaptive Defense 360 содержит динамическую защиту от эксплойтов.

Эта технология, интегрированная в Panda Adaptive Defense 360, не зависит от технологий в EMET корпорации Microsoft, и она не основана на каком-либо морфологическом анализе файлов, на дополнительных техниках защиты от эксплойтов, не охватываемых в Windows (ASR, EP, EAF и т.д.) или на определенных обнаружениях против известных уязвимостей. Этих техник недостаточно, чтобы остановить атаки, направленные против уязвимостей нулевого дня.

Динамическая технология защиты от эксплойтов отслеживает внутреннее поведение процессов, осуществляя поиск аномалий. Это очень эффективно, вне зависимости от эксплойта, используемого в атаке, и все это дополняется проприетарным **анализом структуры памяти**, которая проверяет раздел памяти в определенные моменты времени после возникновения ряда определенных событий или при проявлении определенных моделей поведения. Таким образом, могут быть обнаружены шаблоны новых атак различных типов.

Эти технологии могут эффективно защищать от любого типа эксплойта, особенно от неизвестных эксплойтов нулевого дня:

- **Уязвимости в веб-браузерах:** Internet Explorer, Firefox, Chrome, Opera и другие.
- **Распространенные приложения,** часто используемые в направленных атаках (Java, Adobe Reader, Adobe Flash, Microsoft Office, мультимедиа-плейеры и т.д.).
- **Уязвимости в неподдерживаемых операционных системах**, таких как Windows XP и другие.

3. Индикаторы IoA для обнаружения атак типа Living-off-the-Land и вредоносного использования административных инструментов

Для обнаружения такого типа индикаторов атак, сопоставляются события скриптов, выполненных интерпретаторами скриптов (Powershell, Visual Basic, Javascripts и др.), макросы/скрипты в MS Office, активность WMI и пр.

Включены и другие индикаторы для запрета выполнения определенных процессов над другими процессами, и в зависимости от контекста, блокируя атаки без вредоносного ПО (malwareless attack), использующие инструменты администрирования и командную строку. Также обнаруживаются некоторые другие атаки в памяти, такие как обнаружение внедрения кода в памяти без файлов на диске.

4. Сервис Threat Hunting Service

Раскрывая необнаруживаемое

Сервис Threat Hunting and Investigation Service, включенный в Panda Adaptive Defense и Panda Adaptive Defense 360, полностью управляется аналитиками компании Panda Security.

Они используют собственную облачную платформу для поиска угроз и реагирования на инциденты, позволяющую координировать работу аналитиков на всех уровнях (L1, L2 и L3), а также хантеров и специалистов по реагированию на инциденты для минимизации MTTD и MTTR (среднее время обнаружения и среднее время реагирования).

Аналитики могут также создавать новые правила, представляющие новые индикаторы атак IoA. Эти высоконадежные IoA могут быть переданы на конечные устройства, как можно скорее защищая их от злоумышленников, обходящих другие системы контроля с помощью таких техник как безфайловые атаки, LotL и другие.

Эти новые индикаторы атак - результат непрерывного процесса выявления субъектов угроз, в котором задействованы передовая аналитика данных, наш собственный анализ угроз и опыт наших аналитиков.

Данный сервис вобрал в себя все кибер-знания, которые мы совершенствуем благодаря нашему многолетнему опыту исследования угроз, исторической видимости на базе знаний поведения приложений, пользователей и машин на протяжении более 30 лет, а также сотрудничеству с такими международными организациями как Cyber Threat Alliance, где мы обмениваемся индикаторами атак или компрометаций и их соответствующими мерами реагирования.

Сертификаты и награды

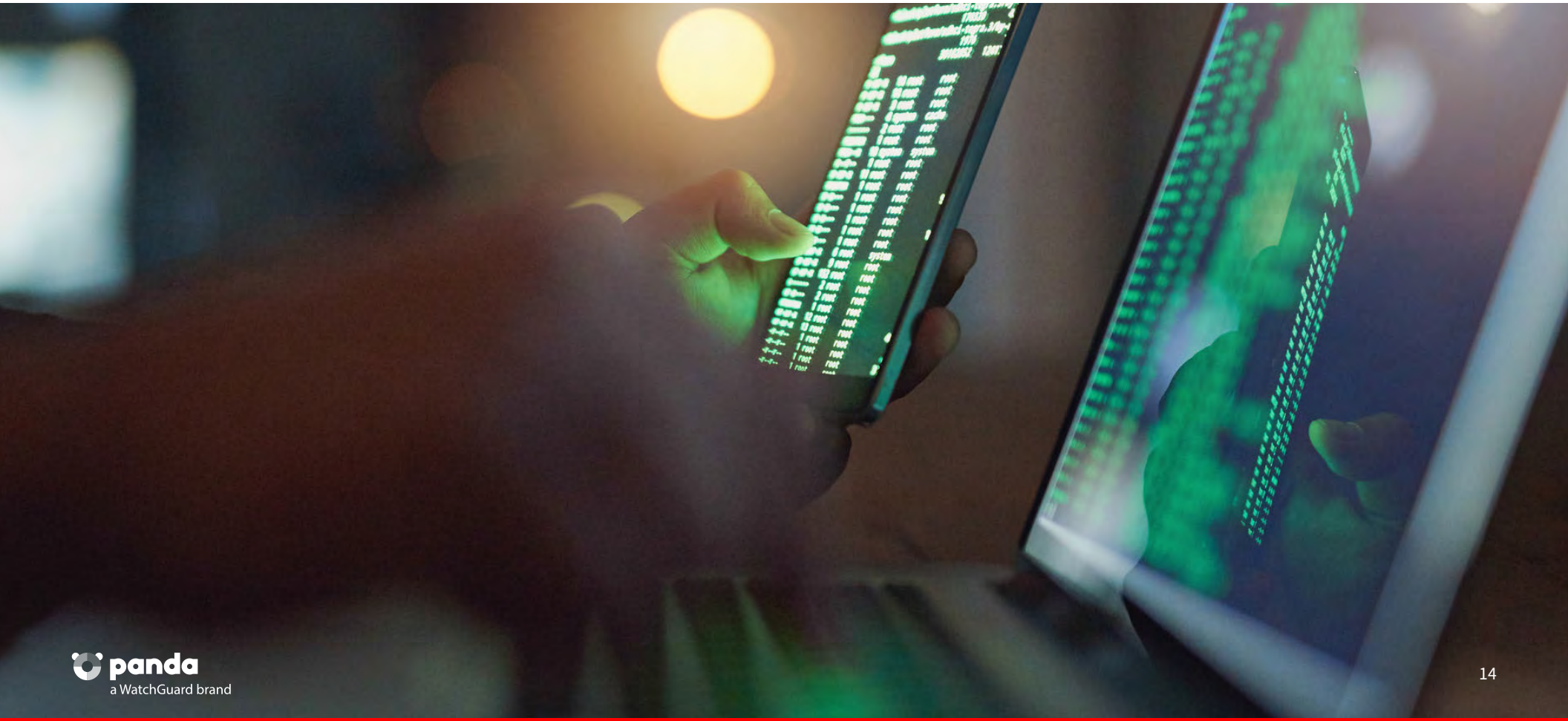
Panda Security регулярно принимает участие в сравнительных анализах и получает награды за защиту и производительность от Virus Bulletin, AV-Comparatives, AV-Test и NSS Labs. Panda Adaptive Defense получил сертификацию EAL2+ при оценке на соответствие стандартам Common Criteria.

ЧЛЕН АЛЬЯНСА

Примечания

1. Атаки на цепочку поставок - это новая угроза, нацеленная на разработчиков и поставщиков ПО. Цель - получить доступ к исходным кодам, создать процессы или механизмы обновления для заражения легитимных приложений с целью распространения вредоносного ПО.

2. MITRE ATT&CK Framework: **https://attack.mitre.org/**



Panda Adaptive Defense 360

Неограниченная видимость, абсолютный контроль

РОССИЯ И СНГ +7 495 1059451 ДРУГИЕ СТРАНЫ +1.206.613.0895 www.watchguard.com | pandasecurity.com