Технологии Panda Adaptive Defense 360

Управляемое обнаружение,

Управляемое смягчение последствий

panda

Adaptive Defense 360

Содержание

1. Технологии и сервисы. Введение
2. Пакет технологий EPP
3. Сервис 100% классификации
4. Защита от эксплойтов приложений и атак Living-off-the-Land (LotL)
5. Сервис Threat Hunting
6. Сертификаты и награды

1. Технологии и сервисы в Panda Adaptive Defense 360.

Введение

Данный документ объясняет, как вместе работают **технологии и сервисы, интегрированные в Panda Adaptive Defense 360**. Отличительными факторами являются возможности обнаружение и реагирования на атаки (Endpoint Detection and Response, EDR), а также использование Искусственного интеллекта.

На следующем рисунке показано, где применяется каждая технология и техники, используемые для максимально быстрой блокировки противников, что позволяет предотвращать взлом конечных устройств, а также обнаруживать, сдерживать и реагировать на атаки прежде, чем они смогут причинить реальный ущерб.

Panda Adaptive Defense 360

Автоматические и управляемые сервисы	ПРЕДОТВРАЩЕНИЕ	ОБНАРУЖЕНИЕ	АКТИВНЫЙ ПОИСК	РАССЛЕДОВАНИЕ/ АНАЛИЗ	СДЕРЖИВАНИЕ/ ВОССТАНОВЛЕНИЕ	ПРОГНОЗ Избежать будущих атак
ИЗВЕСТНОЕ И НЕИЗВЕСТНОЕ ВРЕДОНОСНОЕ ПО	Традиционные EPP-технологии[1] Сервисы 100% классификации[2] Контроль приложений на основе рисков: режимы Lock/Hardening			Анализ инцидентов, Хронология событий	Запрет исполнения, управляемое лечение	Выводы анализа инцидентов Panda Patch Management Advanced Reporting tool Panda Data Control
ЭКСПЛОЙТЫ Мета-эксплойты, наборы эксплойтов, эксплойты в обращении	Предв. выполнение IoA эксплойтов в обращении[3]	Поведенческие IoA в памяти[4]	Сервис Threat Hunting & Investigation Service (THIS)[7] Передача новых IoA локальным агентам на конечных устройствах		Остановка процессов, изоляция конечных точек	
LIVIN-OFF-THE-LAND Вредоносная активность с высокой степенью достоверности	Предв. выполнение контекстных IoA (интерпретаторы, скрипты, внедрение shell-кодов)[5]	Поведенческие IoA с утилитами администрирования, скриптами и инъекцией shell-кода[6]			Запрет или блокировка выполнения	

Технологии и сервисы предотвращения, обнаружения и реагирования, интегрированные в Panda Adaptive Defense 360:

1. **Технологии защиты конечных устройств** (1).
2. **Управляемый сервис 100% классификации** (2), который классифицирует все приложения и бинарные файлы до и во время их выполнения для гарантии того, что могут запускаться только доверенные и надежные исполняемые файлы.
3. **Технологии обнаружения эксплойтов и техник атак Living-off-the-Land (LotL)** (3, 4, 5, 6). Техники LotL позволяют хакерам использовать на рабочих станциях и серверах уже существующие и легитимные приложения администрирования с двойным назначением, злоупотреблять ими и действовать незаметно для администратора.
4. **Управляемый сервис Threat Hunting** (7) как часть решения. Эксперты по безопасности обнаруживают новые техники LotL и включают эти новые обнаружения в локальные агенты на конечных устройствах.

2. Пакет технологий EPP

Пакет проактивных технологий EPP	Panda Adaptive Defense 360
Универсальные сигнатуры и эвристика	✓
Сравнение с облачной базой знаний Коллективный разум (Threat Intel)	✓
Поведенческий анализ и обнаружение IoA	✓
Файервол, IDS/IPS, инспектирование сетевых пакетов	✓
Анти-тампериng	✓
Контроль устройств	✓
Классификация и репутация URL	✓
Контроль приложений	✓
Антиспам, антифишинг, контент-фильтрация для серверов MS Exchange	✓
Защита ящика и интеллектуальное сканирование для серверов MS Exchange	✓
Оценка уязвимости и патчинг*	✓

*Panda Patch Management

Существует распространенное заблуждение о технологиях EPP, полагая, что они являются всего лишь традиционным и основанным на сигнатурах антивирусом, который можно заменить EDR-решением.

На самом деле, эти технологии, помимо сигнатурного анализа, сочетают в себе общие сигнатуры, эвристику, файервол, репутацию URL, поведенческий анализ и анализ индикаторов атак IoA, управление уязвимостями, контроль приложений и другие возможности, которые позволяют значительно снизить риски.

Эти превентивные технологии, если они работают вместе с EDR-решениями, предоставляют важные преимущества, среди которых:

- **Значительное снижение риска.** Им не нужно запускать файл для обнаружения вредоносных программ - им нужно только подключение к облаку
- **Очень низкий уровень ложных срабатываний.** Технологии EPP, способные защищать автономно, широко распространены на огромном количестве конечных устройств и настроены таким образом, чтобы минимизировать ложные срабатывания
- **Оптимизация производительности.** Они интегрированы и работают вместе во избежание избыточности и для снижения любого воздействия на производительность конечных устройств, которые они защищают.

3. Сервис 100% классификации.
Искусственный интеллект как прорывная инновация в безопасности

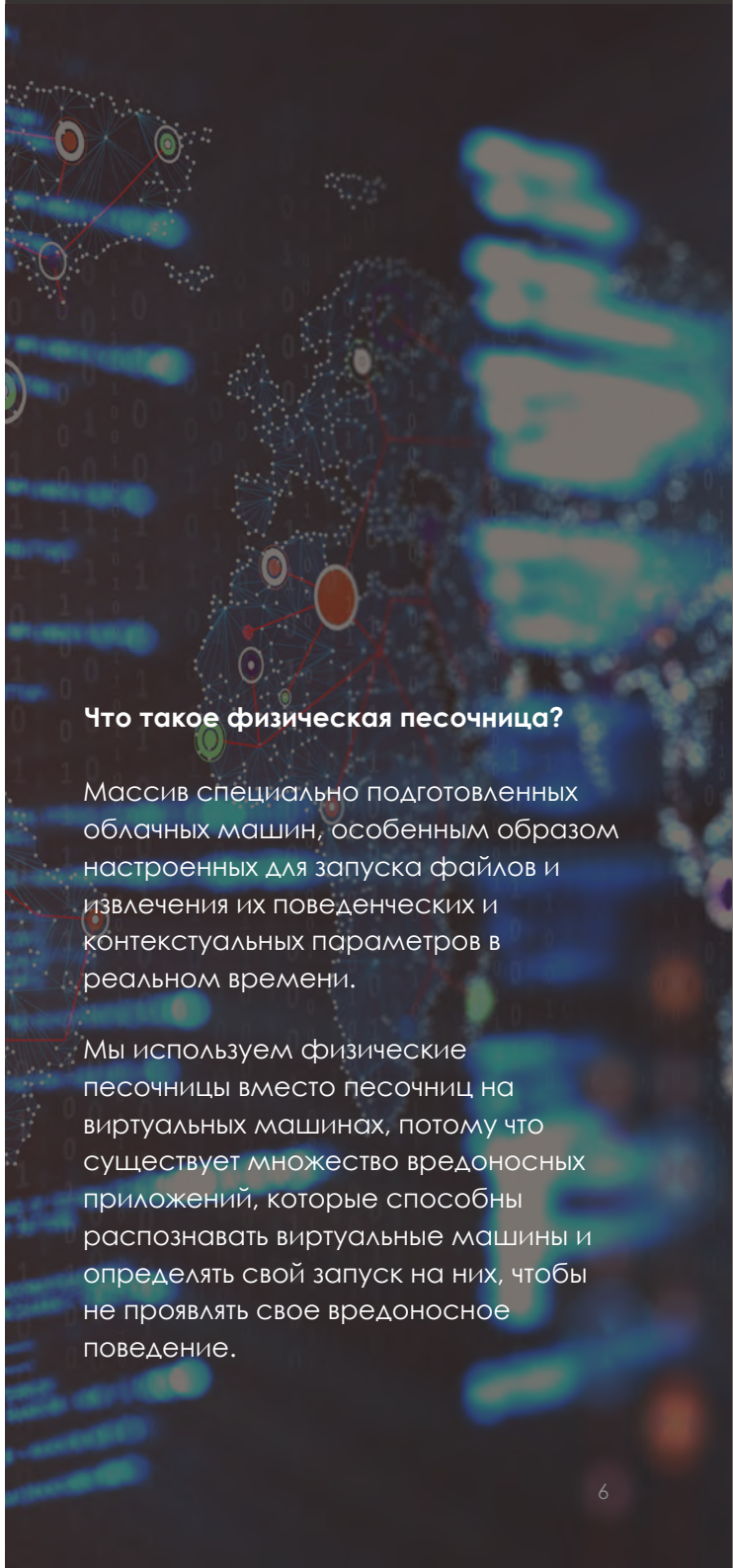
Управляемый сервис, включенный в состав лицензии на решения **Panda Adaptive Defense и Adaptive Defense 360**, классифицирует все исполняемые на каждой конечной точке процессы как вредоносные или надежные. Только надежным процессам разрешено запускаться. Поскольку это полностью автоматизированный сервис, он не требует каких-либо входных данных или действия со стороны конечного пользователя, службы безопасности или ИТ-отдела.

Сервис 100% классификации имеет три ключевых компонента:

1. **Непрерывный мониторинг активности конечных устройств из облачной платформы.**
   Активность каждого приложения на конечных устройствах вне зависимости от их природы отслеживается и отправляется в облако для ее непрерывной классификации. Таким образом, можно предотвратить выполнение вредоносных программ и даже сложных угроз, таких как атаки на цепочки поставок (Supply Chain Attack).

2. **Автоматизированная классификация на основе Искусственного интеллекта**
   Автоматизированные классификации выполняются в облачной системе Искусственного интеллекта, где выполняется массив различных ML-алгоритмов машинного обучения для обработки сотен статических, поведенческих и контекстных атрибутов в реальном времени. Эти атрибуты извлекаются из телеметрии защищаемой среды и из набора **физических песочниц**, в которой запускаются исполняемые файлы.

Сегодня уровень автоматизированной классификации составляет 99,98%, поэтому только 0,02% процессов требуют вмешательства наших экспертов. Таким образом, система классификации на основе Искусственного интеллекта самодостаточна, масштабируема для огромного объема файлов, работает в реальном времени и полностью не зависит от конечного пользователя.



Что такое физическая песочница?

Массив специально подготовленных облачных машин, особенным образом настроенных для запуска файлов и извлечения их поведенческих и контекстуальных параметров в реальном времени.

Мы используем физические песочницы вместо песочниц на виртуальных машинах, потому что существует множество вредоносных приложений, которые способны распознавать виртуальные машины и определять свой запуск на них, чтобы не проявлять свое вредоносное поведение.

3. **Контроль приложений на основе рисков.**

Относится к режимам работы агента защиты, запущенного на конечных устройствах. Существует два уровня защиты:

- **Режим Hardening:** по умолчанию запрещает запуск любого неизвестного приложения или бинарного файла, поступившего извне (скачивание из Интернета, электронная почта, съемный носитель, удаленные локации и пр.).
- **Режим Lock:** по умолчанию запрещает запуск любого неизвестного приложения или бинарного файла вне зависимости от его происхождения (из сети, на самом конечном устройстве или извне). Такой режим обеспечивает запуск только надежных процессов и приложений.

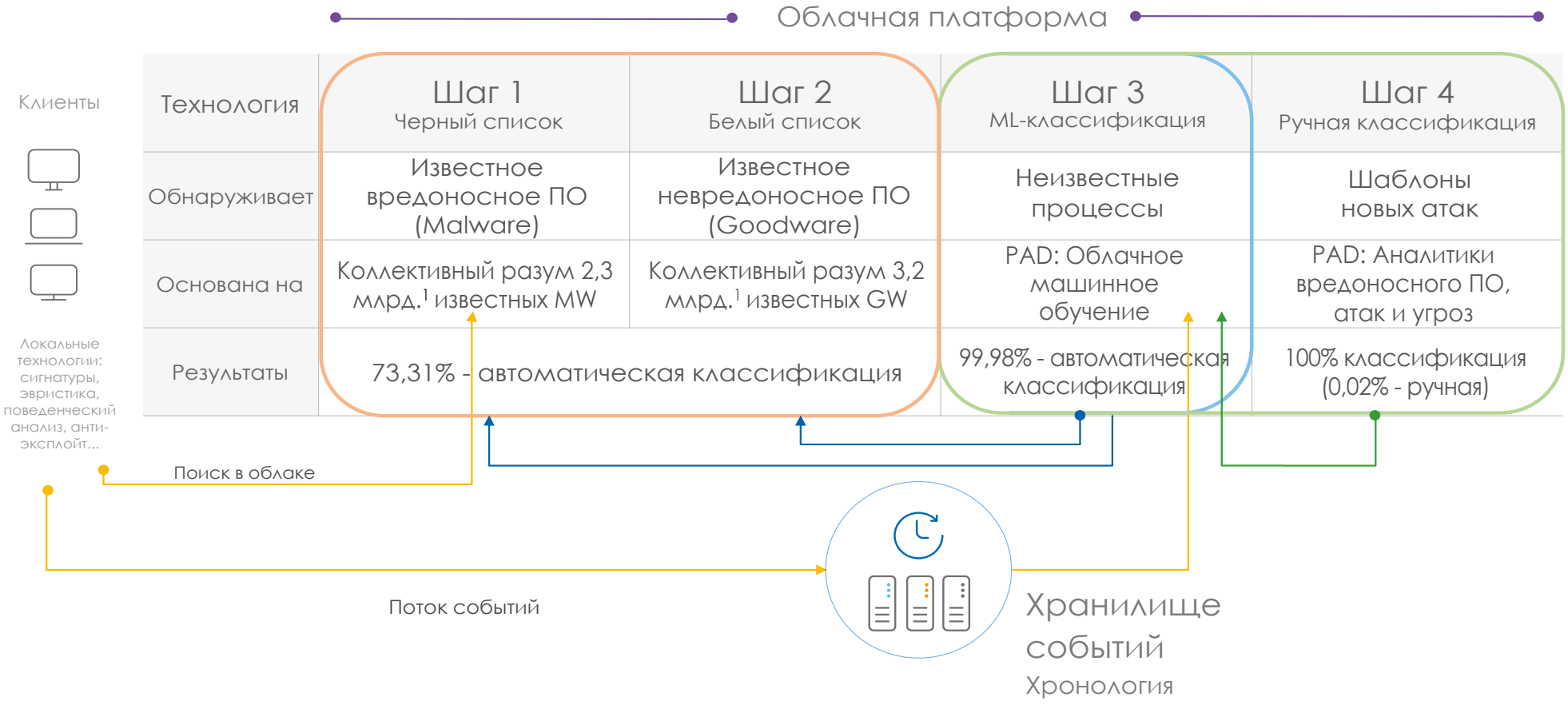
Коллективный разум Panda Security. Размещен на облачной платформе, является еще одним ключевым компонентом, обеспечивающим работу новой модели защиты и повышающим эффективность работы сервиса 100% классификации.

Коллективный разум представляет собой огромную базу знаний по всем надежным и вредоносным приложениям, бинарным файлам и другим файлам, содержащим интерпретируемый код.

Эта облачная база знаний непрерывно получает информацию из системы с искусственным интеллектом и от экспертов-аналитиков, и одновременно с этим непрерывно предоставляет требуемую информацию решениям и сервисам Panda Security перед запуском любых приложений.

- На следующем рисунке показано, как данные технологии легко работают вместе, осуществляя классификацию всех приложений, бинарных файлов и файлов с интерпретируемым кодом в режиме реального времени.

Как работает сервис 100% классификации



4. Защита от эксплойтов приложений и атак Living-off-the-Land (LotL)

Непрерывный мониторинг активностей на конечных устройствах позволяет агенту действовать в качестве сенсора и информировать облачную платформу не только о запускаемых файлах, но также и о контексте их выполнения (что произошло непосредственно перед запуском, какие пользователи пытаются запустить какие команды или приложения, какой генерируется сетевой трафик, к каким файлам с данными обращаются, какие параметры и пр.).

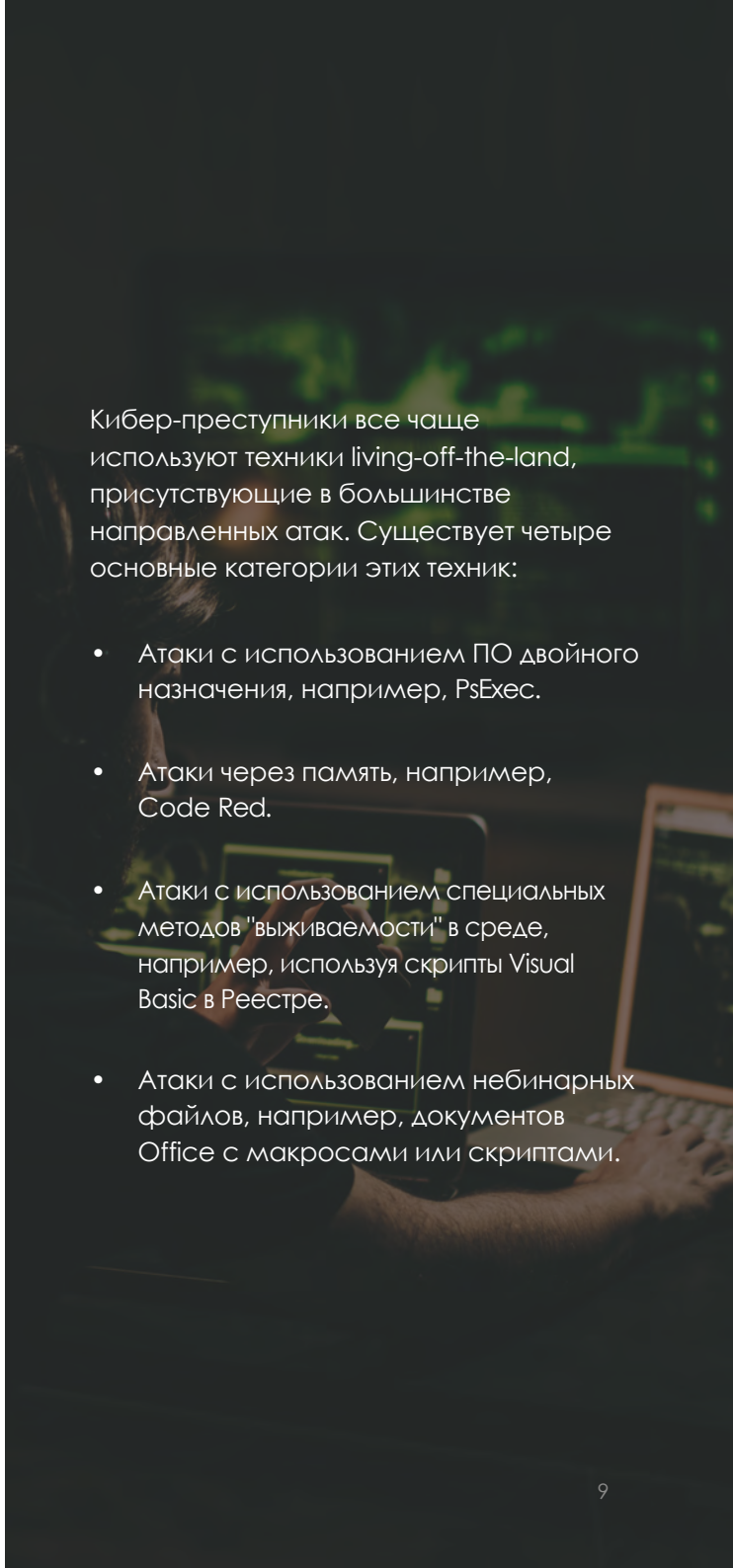
Это позволяет идентифицировать, в первую очередь на конечном устройстве, аномальное или подозрительное поведение и классифицировать их как индикаторы атаки (IoA) с высокой степенью достоверности и без ложных срабатываний.

IoA связаны с определенными фазами цепочки **Cyber Kill Chain** или с тактиками **MITRE ATT&CK framework**[2]:

- Первоначальный доступ
- Выполнение
- Закрепление
- Повышение привилегий
- Обход систем защиты
- Доступ к учетным данным
- Обнаружение
- Горизонтальное продвижение
- Сбор данных
- Команды и управление
- Извлечение данных
- Последствия

Обнаружение IoA прежде, чем данные будут извлечены (или зашифрованы в случае атак шифровальщика), - это очень эффективный механизм защиты, особенно против атак Living-off-the-Land (LotL), даже если конечные устройства к тому времени были скомпрометированы.

Panda Adaptive Defense и Panda Adaptive Defense 360 интегрируют в едином агенте защиты полный набор технологий для обнаружения IoA на различных этапах атаки. Не являясь статичными технологиями, они постоянно обновляются новыми шаблонами атак и техник, которые обнаруживаются с помощью сервиса Threat Hunting and Investigation Service (THIS).



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

- Атаки с использованием ПО двойного назначения, например, PsExec.
- Атаки через память, например, Code Red.
- Атаки с использованием специальных методов "выживаемости" в среде, например, используя скрипты Visual Basic в Реестре.
- Атаки с использованием небинарных файлов, например, документов Office с макросами или скриптами.

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

1. IoA эксплойтов в обращении

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

Кроме того, с помощью собственной технологии файервола "**Virtual Patching**" при мониторинге входящего трафика обнаруживаются и блокируются попытки эксплуатации уязвимостей.

Например, эта технология используется для идентификации и блокировки эксплойтов против уязвимости EternalBlue (атаки BlueKeep), когда в рамках RDP-сессии устанавливаются определенные соединения. Пока они не заблокированы, такие соединения позволяют хакеру удаленно выполнять код (RCE).

Технология виртуального патчинга обнаруживает такие соединения и автоматически их отклоняет. Обнаружения регистрируются в облаке и отображаются в веб-консоли Panda Adaptive Defense 360, позволяя администраторам немедленно принимать соответствующие меры.

Они могут в качестве меры сдерживания применять изменения конфигурации, например, активируя Network Level Authentication (NLA) или отключая несущественные службы RDP на конечных устройствах, или по возможности применяя патчи к системам, что в итоге эффективно сокращает поверхность атаки.

2. IoA для атак через память: динамическая анти-эксплойтная технология

Panda Adaptive Defense 360 содержит динамическую анти-эксплойтную технологию.

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

Динамическая анти-эксплойтная технология осуществляет мониторинг внутреннего поведения процессов в поисках аномалий. Она очень эффективна вне зависимости от используемого в атаке эксплойта, и она дополняется собственной технологией **анализа структуры памяти**, которая инспектирует сектор памяти в определенные моменты времени после того, как происходят определенные события или наблюдаются определенные модели поведения. Таким образом, можно обнаружить новые шаблоны атак различных типов.

Эти технологии могут эффективно защищать против **любого типа эксплойтов**, особенно от эксплойтов "нулевого дня", которые направлены на:

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

3. IoA для обнаружения атак Living-off-the-land и попыток злоупотребления инструментами администрирования.

Для обнаружения такого типа индикаторов коррелируются события скриптов, выполняемых интерпретаторами скриптов (Powershell, Visual Basic, Javascripts и т.д.), а также макросов/скриптов в документах MS Office, активностей WMI и пр. Также включены и другие индикаторы для запрета выполнения определенных процессов другими процессами, в зависимости от контекста, блокируя атаки без использования вредоносного ПО (malwareless attack) с помощью инструментов администрирования и командной строки. Кроме того, обнаруживаются некоторые другие атаки через память, например, обнаружение попыток внедрения кода в память без участия файлов на диске.

5. Сервис Threat Hunting:
Обнаруживая необнаруживаемое

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

Они управляют собственной облачной платформой для Threat Hunting и реагирования на инциденты, которая позволяет координировать работу аналитиков на уровнях L1, L2 и L3, а также "охотников" за угрозами и специалистов по реагированию на инциденты для минимизации среднего времени обнаружения (MTTD) и среднего времени реагирования (MTTR).

Аналитики также могут создавать новые правила, представляющие новые IoA. Эти достоверные индикаторы IoA могут передаваться на конечные устройства, как можно более оперативно защищая от хакеров, пытающихся обойти другие системы контроля с помощью таких техник как безфайловые техники, LotL и т.д.

Эти новые индикаторы атак являются результатом непрерывного процесса выявления субъектов угроз, использующего передовые методы анализа данных, нашу собственную базу знаний по угрозам и опыт наших аналитиков.

Этот сервис получает все возможные кибер-знания, которые мы усовершенствовали благодаря нашему многолетнему опыту исследования угроз, видимости динамики поведения приложений, пользователей и машин во времени более чем за 30 лет и нашему альянсу с такими международными организациями как Cyber Threat Alliance, где мы обмениваемся индикаторами угроз (IoA и IoC) и соответствующими мерами реагирования.

6. Сертификаты и награды

Panda Security регулярно принимает участие и получает награды в тестах защиты и производительности, проводимых независимыми лабораториями Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs. Panda Adaptive Defense получил сертификацию EAL2+ при его оценке по стандартам Common Criteria.

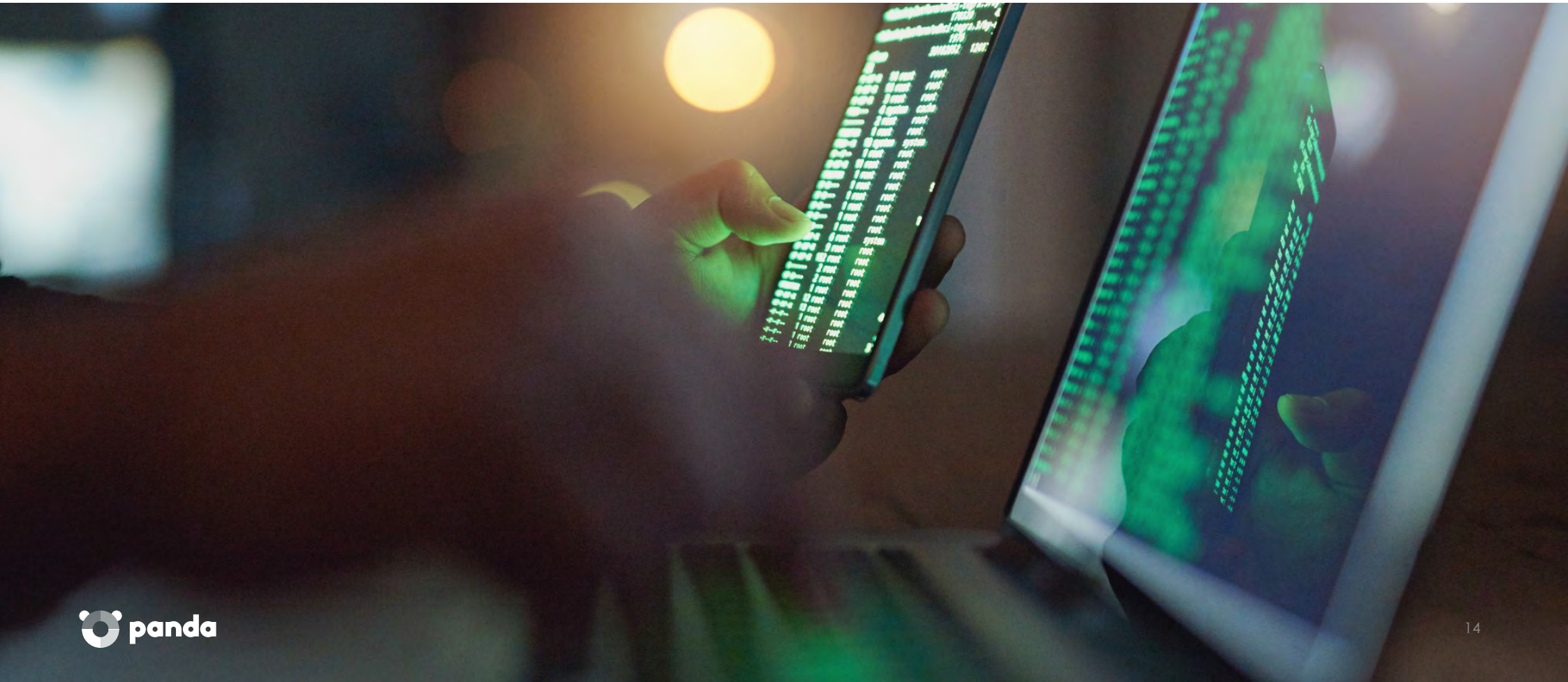
Panda Security получила статус "Визионарий" в Магическом квадранте Gartner для платформ защиты конечных точек (EPP) 2018.

ЧЛЕНСТВО

Примечания:

1. Атаки на цепочку поставок - это новая угроза, нацеленная на разработчиков и производителей ПО. Цель - получить доступ к исходным кодам, создать процессы или механизмы обновления, заразив легитимные приложения для распространения вредоносного ПО.

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



Подробнее:

www.cloudav.ru/enterprise/solutions/adaptive-defense-360/

Panda Adaptive Defense 360

Неограниченная видимость, абсолютный контроль