Платформа кибербезопасности Trend Vision One. От оценки рисков до реагирования на угрозы.

Alexander Djuraev

SE, Trend Micro

RISK TO RESILIENCE
– WORLD TOUR –

TREND MICRO

Кибербезопасность: актуальные задачи и сложности

Эволюция злоумышленников

Киберпреступник

Вымогательства и компрометация деловой электронной почты растут

Рост преступности из-за экономического кризиса

Повышение специализации, нацеленности, персонализации

Взлом преступников полицией

Поддержка на гос. уровне

Саботаж, шпионаж, кража интеллектуальной собственности

Укрывание преступников

Получение прибыли (С. Корея)

Для вашего бизнеса это актуальные угрозы?

Инсайдеры

Экономический кризис ведет к нарушению правил

Обиженные сотрудники мстят работодателю

Киберпреступники платят инсайдерам

Эволюция киберугроз

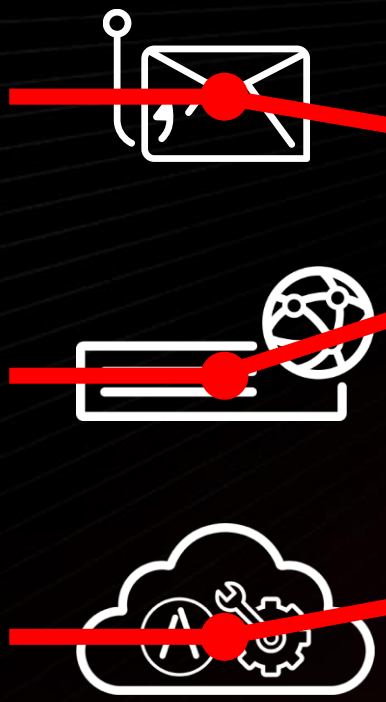
Первичный доступ → Боковое перемещение → Ущерб

Более быстрые и специализированные атаки

Более правдоподобный фишинг

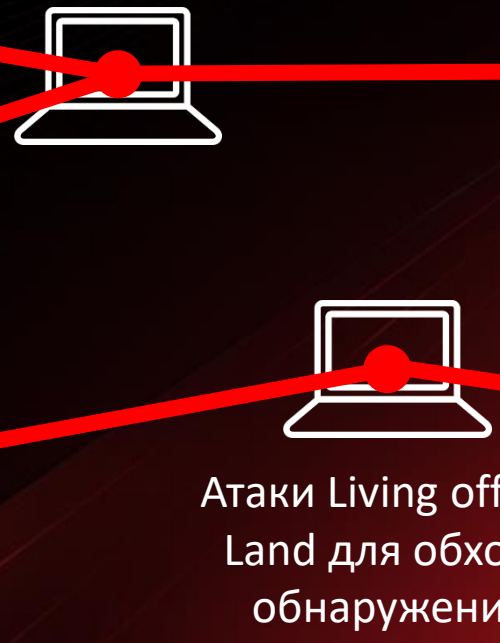
Быстрая эксплуатация уязвимостей

Атака через открытое ПО и цепочки поставок



Хакеры учатся обходить EDR

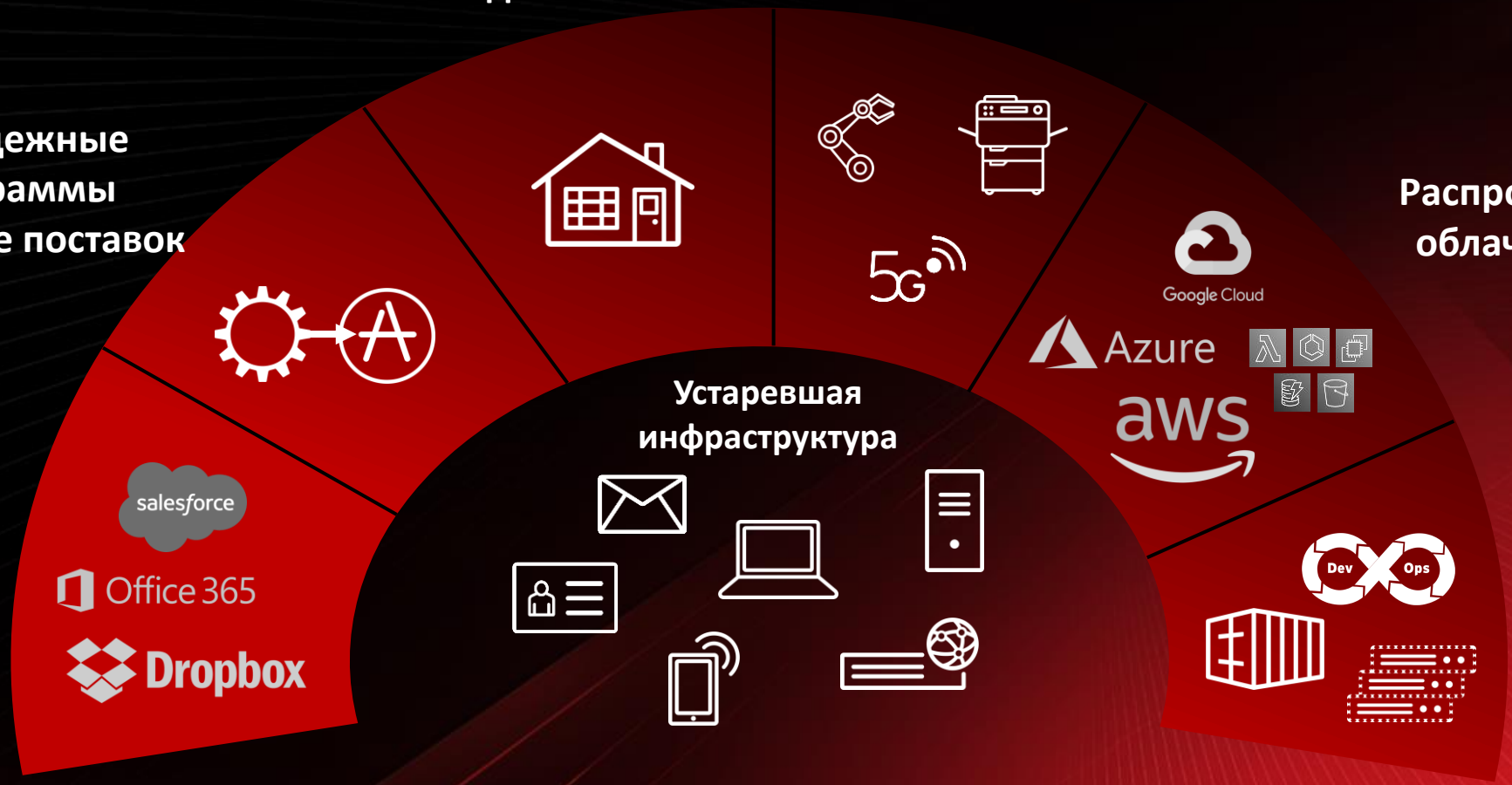
Атаки Living off the Land для обхода обнаружения (PowerShell и т. д.)



Улучшенное шифрование

Кража и вымогательство, не только шифрование

Поверхность атаки



Высокая нагрузка на специалистов по кибербезопасности

Усталость от оповещений

Недостаток навыков

Разрозненные инструменты

Слабая приоритизация

Поиск баланса при разработке

Разработчики

«Я хочу быстро поставлять новые функции».
«Система безопасности не сочетается с моими инструментами».

Специалисты по ИБ

«Я должен защитить бизнес от угроз».
«Я не знаю, чем занимаются разработчики».

RISK TO RESILIENCE
WORLD TOUR

TREND MICRO

Кибербезопасность быстро развивается

Проблемы традиционного подхода

Защита

Разрозненность

Слепые зоны

Слабая приоритизация

Обнаружение

Разрозненность

Избыток оповещений

Быстрые атаки

Реагирование

Разрозненность

Медлительность

Слабая автоматизация

Проактивный подход для уменьшения поверхности атаки

Оценка

Обнаружение активов

Оценка рисков

Приоритизация

Защита

Обзор всей платформы

Хорошая видимость

Приоритизация для критических активов

Обнаружение

Многоуровневый XDR

Приоритизация оповещений

Быстрое обнаружение

Реагирование

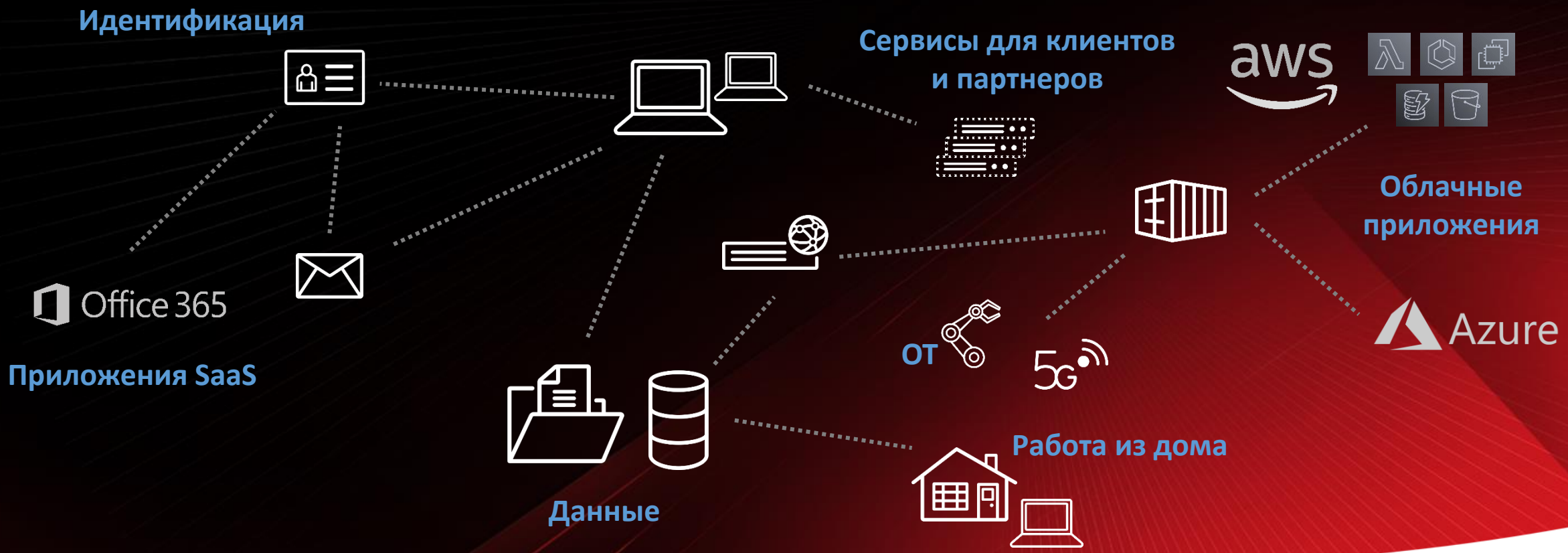
Централизация

Автоматизация

Поддержка ручного управления

Улучшенная видимость

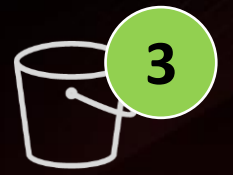
Уровень безопасности и действия по всем типам активов



Оценка рисков для расстановки приоритетов

Высокий риск компрометации, ограниченные права доступа

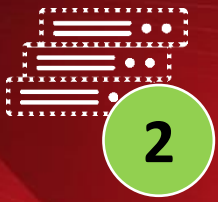
Уязвимый API



Дампинг учетных данных

Активно эксплуатируемая уязвимость на устройстве с выходом в Интернет

Активно эксплуатируемая уязвимость



Контроллер домена с неправильной конфигурацией безопасности

Хранилище с неправильной конфигурацией

Замедление атак

Управление поверхностью атаки

Оценка рисков и проактивное уменьшение поверхности атаки

Платформа защиты облачных приложений (CNAPP)

Интеграция безопасности в процесс разработки, обеспечивающая безопасность приложений до их запуска.

Нулевое доверие (Zero Trust)

«Никогда не доверяй, всегда проверяй»

Создать больше препятствий для атакующих и сделать их видимыми для обнаружения

Ускорение обнаружения и реагирования

БЫЛО: аналитики SOC получают много оповещений от SIEM без контекста и тратят время на их изучение.

Идентификация

Обнаружение и реагирование для конечных устройств (EDR)

Платформа для защиты облачных рабочих сред (CWPP)

Обнаружение угроз в сети и реагирование на них (NDR)

Предотвращение утечки данных (DLP)

Ускорение обнаружения и реагирования

СТАЛО: система расширенного обнаружения и реагирования (XDR) помогает расставить приоритеты.

Обнаружение в разных системах

Приоритизация на основе рисков

Автоматизированное восстановление

Управляемое обнаружение и реагирование

Оценка эффективности системы безопасности

Время обнаружения

Раннее обнаружение техник,
тактики и процедур

Симуляция атак

Использование симуляции взлома и атаки для более точной оценки эффективности мер безопасности

Red Teaming

Посмотрите на свою систему безопасности с точки зрения злоумышленников

Подход на основе платформы

Консолидация вендоров

Консолидируйте количество инструментов безопасности и вендоров для упрощения операций по обеспечению безопасности и закупок

Снижение затрат и сложности

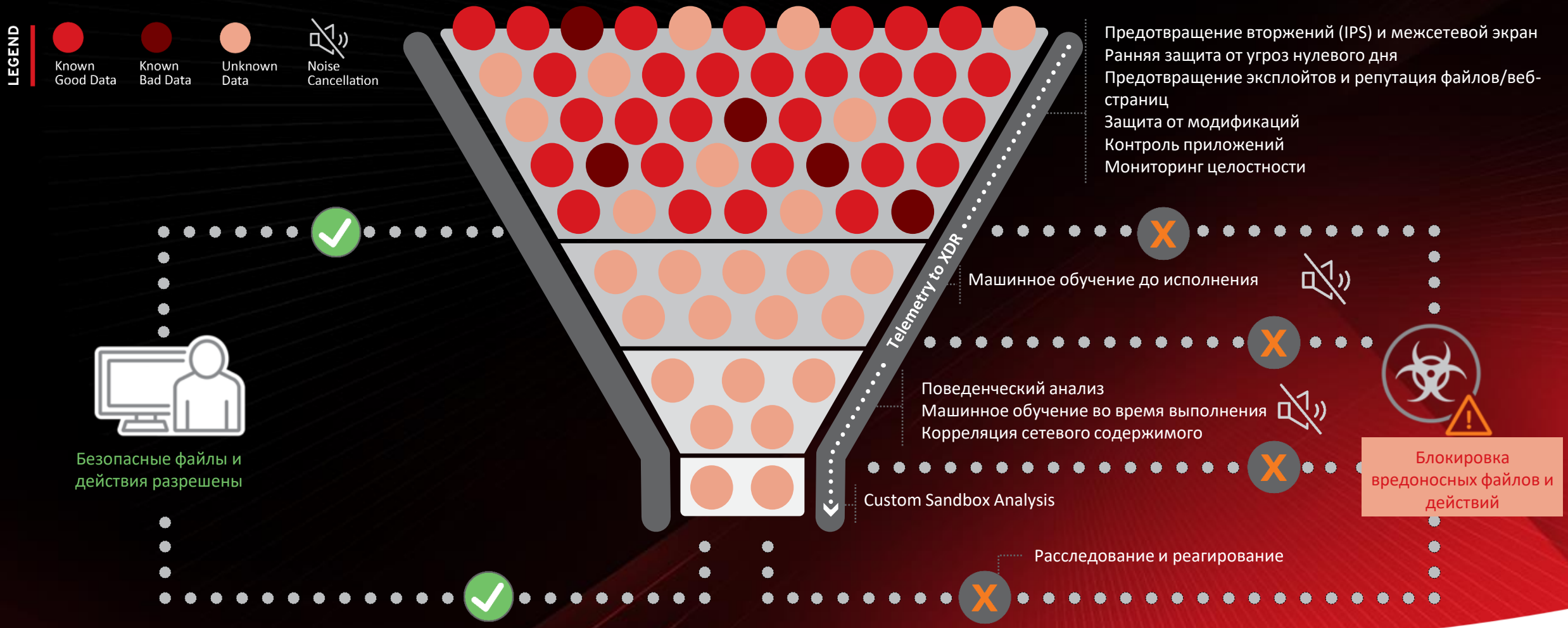
Используйте комплексные платформы по безопасности вместо точечных решений

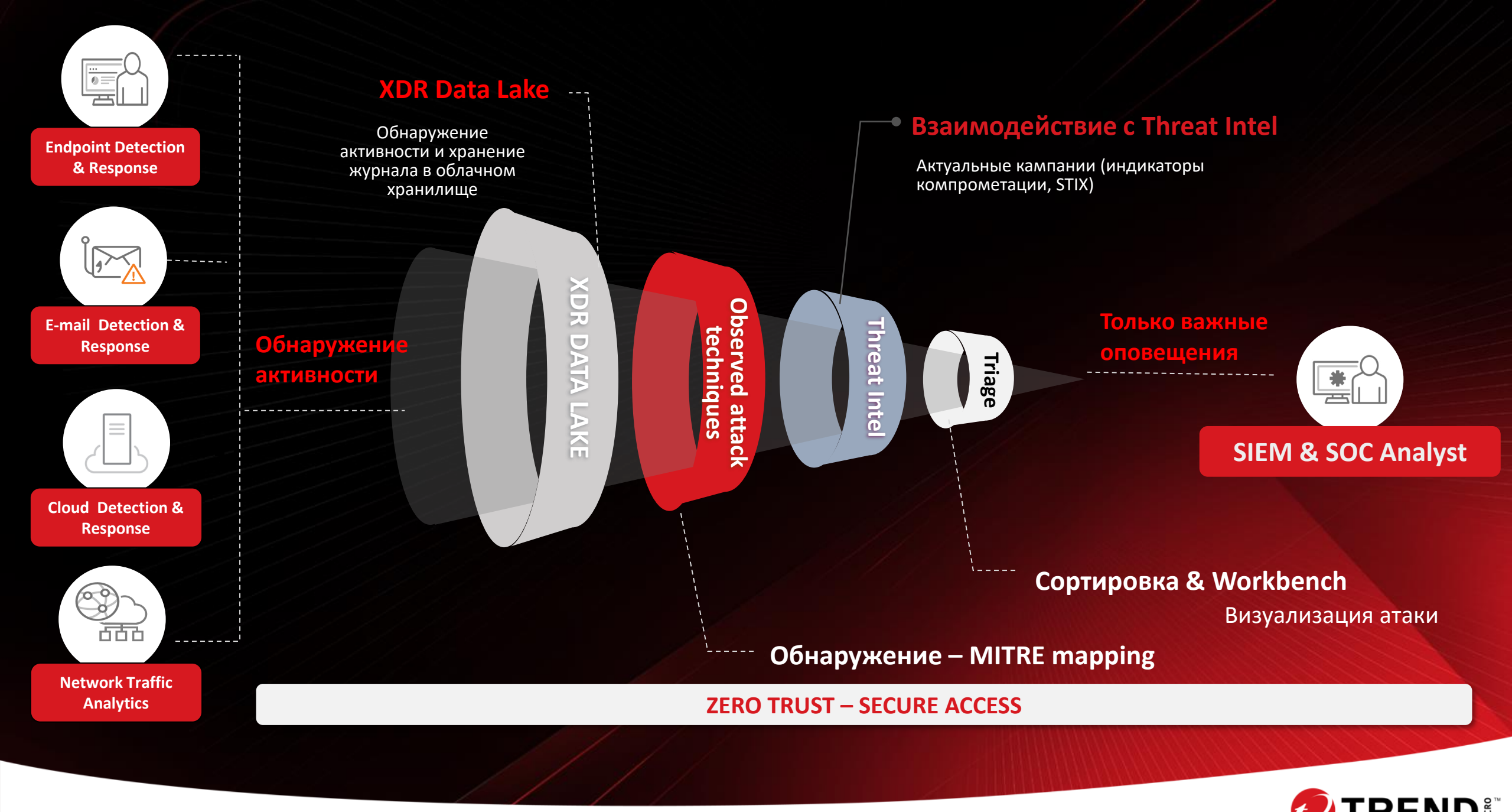
Соблюдение требований

Требования к конфиденциальности и надежности данных растут — средства безопасности должны соответствовать растущим потребностям


Attack Surface Risk Management
Discover Attack Surface • Assess Risk • Mitigate Risk
TREND MICRO
Zero Trust Architecture
User & Identity
Endpoints & Servers
Email
Cloud Infra
Applications
Code Repo
Data
Network
5G
ICS/OT
Managed Services
Ecosystem Integration
IT Infra Operations
Endpoint & Email Security
Network Security
SOC Operations
XDR
ASM
Cloud Operations
CNAPP
Hybrid Cloud Security
Core Services
Security Engines | Open API | AI/ML | Big Data Analytics
Global Threat Intelligence
Attack Surface Intelligence | Zero Day Initiative | Threat Research

Интеллектуальная многоуровневая система безопасности обеспечивает максимальную защиту




Endpoint Detection & Response
E-mail Detection & Response
Cloud Detection & Response
Network Traffic Analytics
XDR Data Lake
Обнаружение активности и хранение журнала в облачном хранилище
Взаимодействие с Threat Intel
Актуальные кампании (индикаторы компрометации, STIX)
Обнаружение активности
XDR DATA LAKE
Observed attack techniques
Threat Intel
Triage
Только важные оповещения
SIEM & SOC Analyst
Сортировка & Workbench
Визуализация атаки
Обнаружение – MITRE mapping
ZERO TRUST – SECURE ACCESS

Высокая достоверность обнаружения без перегрузки оповещения

Based on a real company with
1000 devices in a 7-day period

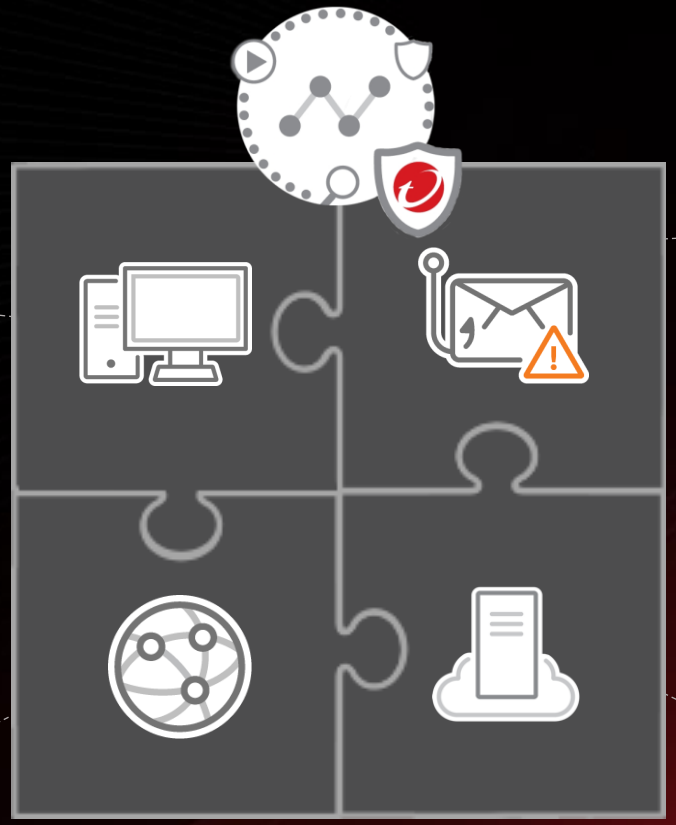
Каждый уровень добавляет значение

ENDPOINT - большинство атак затрагивают устройства пользователей

- Поиск угроз, скрытые в телеметрии конечных точек
- Что произошло на конечном устройстве? Как она распространилась?

СЕТЬ - выявление слепых зон EDR (неуправляемые; устаревшие, IoT, IIoT).

- Как злоумышленник перемещается по организации?
- Как угроза передается?



EMAIL- 94% вредоносных программ

Кто еще получил это письмо или аналогичную угрозу?

- Интеграция API для внутреннего просмотра
- Есть ли скомпрометированные учетные записи, отправляющие внутренние фишинговые письма?

CLOUD/WORKLOADS/CONTAINERS - критически важны для бизнес-операций.

- Коррелирует данные с большего количества средств контроля безопасности, чем обычные EDR, что позволяет решениям рассказать более полную историю.
- Что произошло на сервере**?**

Зачем распространять XDR на конечные точки?

Большинство атак взаимодействует с корпоративными конечными точками в течение жизненного цикла нарушения

Обнаружение: Аналитики безопасности находят угрозы, скрытые среди телеметрии конечных точек. IOC sweeping

Расследование: Что произошло в конечной точке? Как она распространилась? Какие тактики/техники используются?

Реагирование: Изоляция, остановка процесса, удаление/восстановление файлов

Дальнейшая работа с другими слоями XDR:

- Где возникла угроза?
- Где еще эта угроза присутствует в моей сети, рабочих нагрузках, электронной почте?

Зачем распространять XDR на электронную почту?

Источник заражения вредоносным ПО

Источник: Отчет Verizon о расследованиях утечек данных, май 2019 года

Обнаружение: Есть ли скомпрометированные учетные записи, рассылающие внутренние фишинговые письма? Индикаторы компрометации прочесывают почтовые ящики

Расследование: Кто еще получил это письмо/угрозу?

Реагирование: Карантин, удаление

Зачем распространять XDR на серверы?

Log Inspection Alert

Possible attack on the SSH Server (or version gathering)
Source: 3.211.84.114

Оповещения не рассказывают всей истории

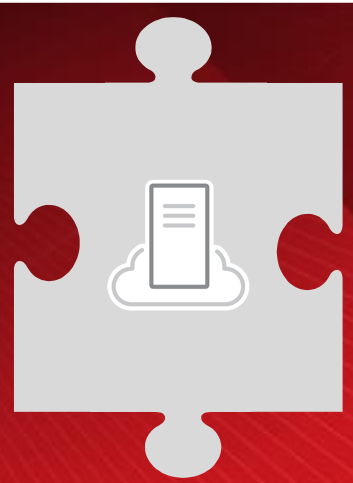
- Скорее всего, это один шаг из многих...
- Какова общая картина?
- Был ли злоумышленник успешен?

Обнаружение: Высокоточные обнаружения, соотнесенные с различными средствами контроля безопасности и мероприятиями, чтобы рассказать всю историю в целом. IOC sweeping

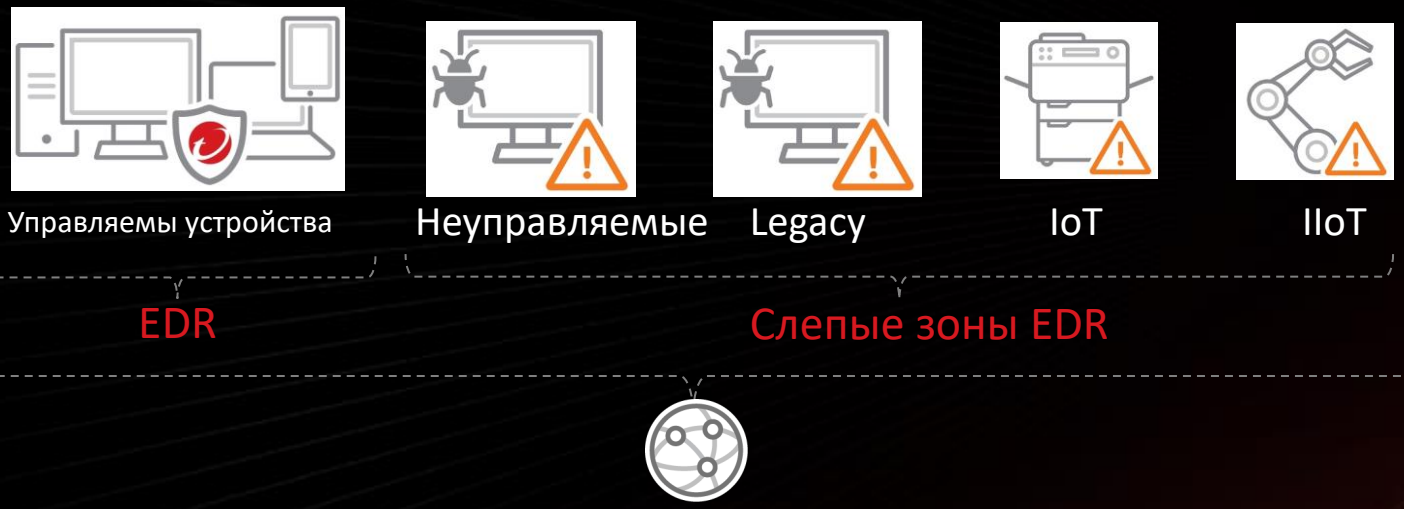
Расследование: Полная видимость активности помогает ответить на вопросы: что произошло внутри рабочей нагрузки? Как она распространилась?

Данные о активности:

- Активность учетной записи пользователя
- Процессы
- Выполненные команды
- Сетевые подключения
- Созданные/полученные файлы
- Модификации реестра

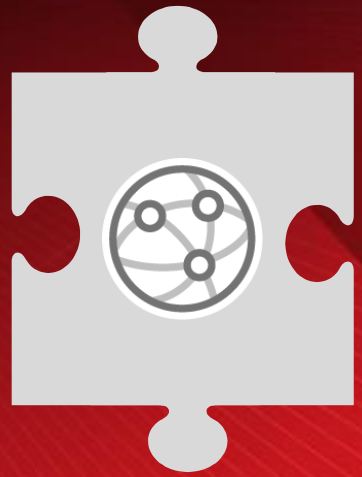


Зачем распространять XDR на вашу сеть?



Данные о активности:

- Поток трафика
- Периметральные и боковые подключения
- Подозрительное поведение трафика



Обнаружение: Видеть всю сеть, включая "мертвые зоны" EDR. Аналитика обнаруживает сложные угрозы. IOC sweeping.

Расследование: Как передается информация об угрозе? Как злоумышленник перемещается по организации?

Реагирование: Block host, block URL

Преимущества XDR:
быстрое и точное обнаружение сложных угроз и реагирование на них

Вызовы, стоящие перед командой SOC

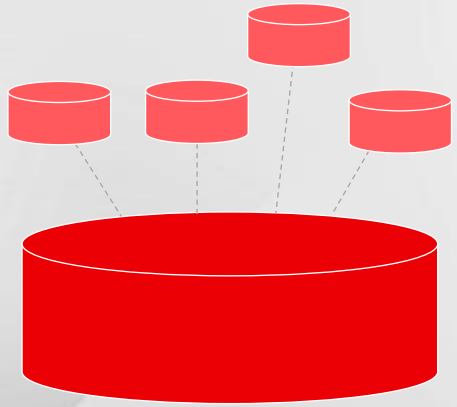
Сложный ландшафт угроз

Избыток оповещений

Ограниченная и фрагментированная видимость

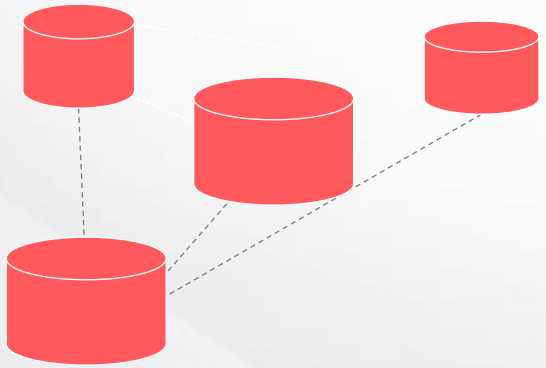
Разные подходы к XDR

Открытый



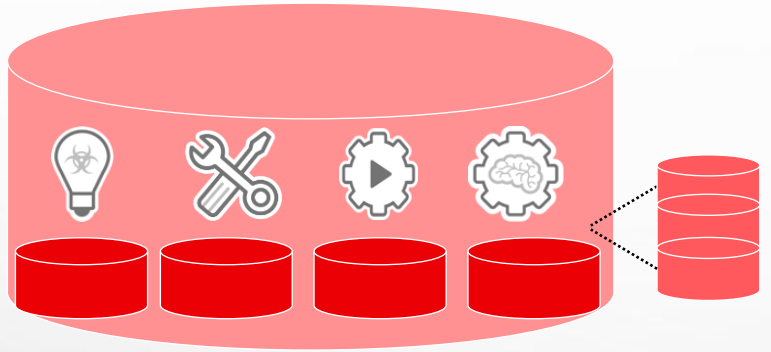
Полагается на интеграцию с сторонними производителями для сбора многоуровневой телеметрии и реализации реагирования

Нативный



Интегрируется с другими инструментами безопасности из собственного портфеля для сбора телеметрии и реализации реагирования

Гибридный



Специально созданная архитектура: Коррелированное обнаружение, интегрированные расследования, многоуровневое реагирование по всем векторам безопасности в тандеме с интеграцией сторонних производителей и API.

Trend Vision One XDR

Extended Detection & Response (XDR)

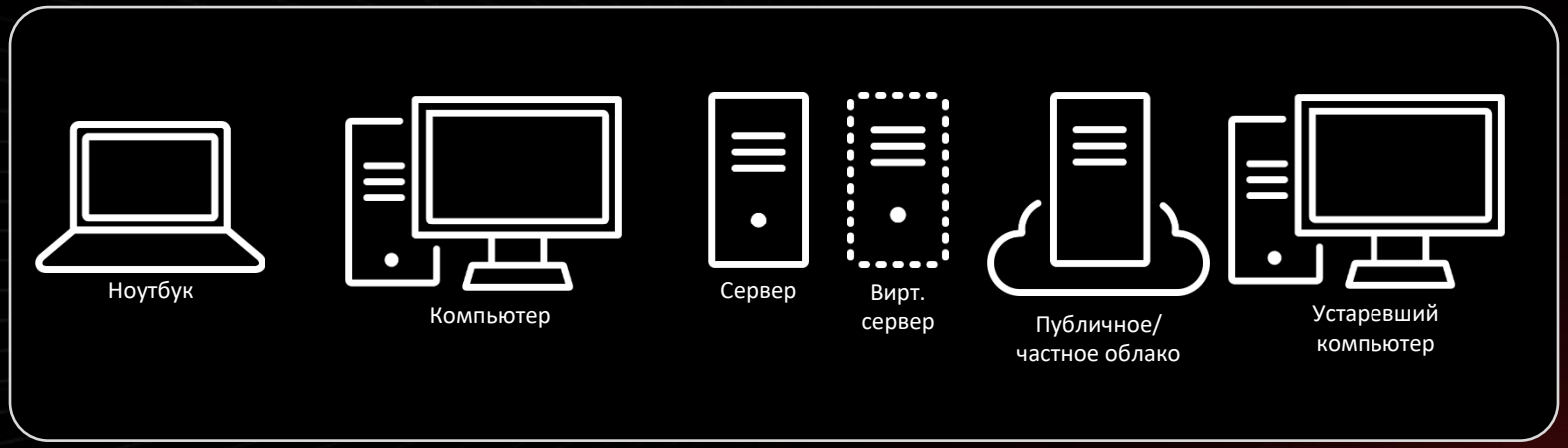
Сценарии

Криминалистика и реагирование

- Идентификация
- Данные
- ОТ/ИКТ
- Сеть
- Облако
- Эл. почта
- Конечное устройство
- Сторонние решения

Самый широкий охват сенсорами на рынке

Trend Vision One Endpoint Security



Централизованный мониторинг развернутых конечных устройств: версии, конфигурации, состояние работоспособности и т. д.

Единое управление и поддержка разных операционных систем

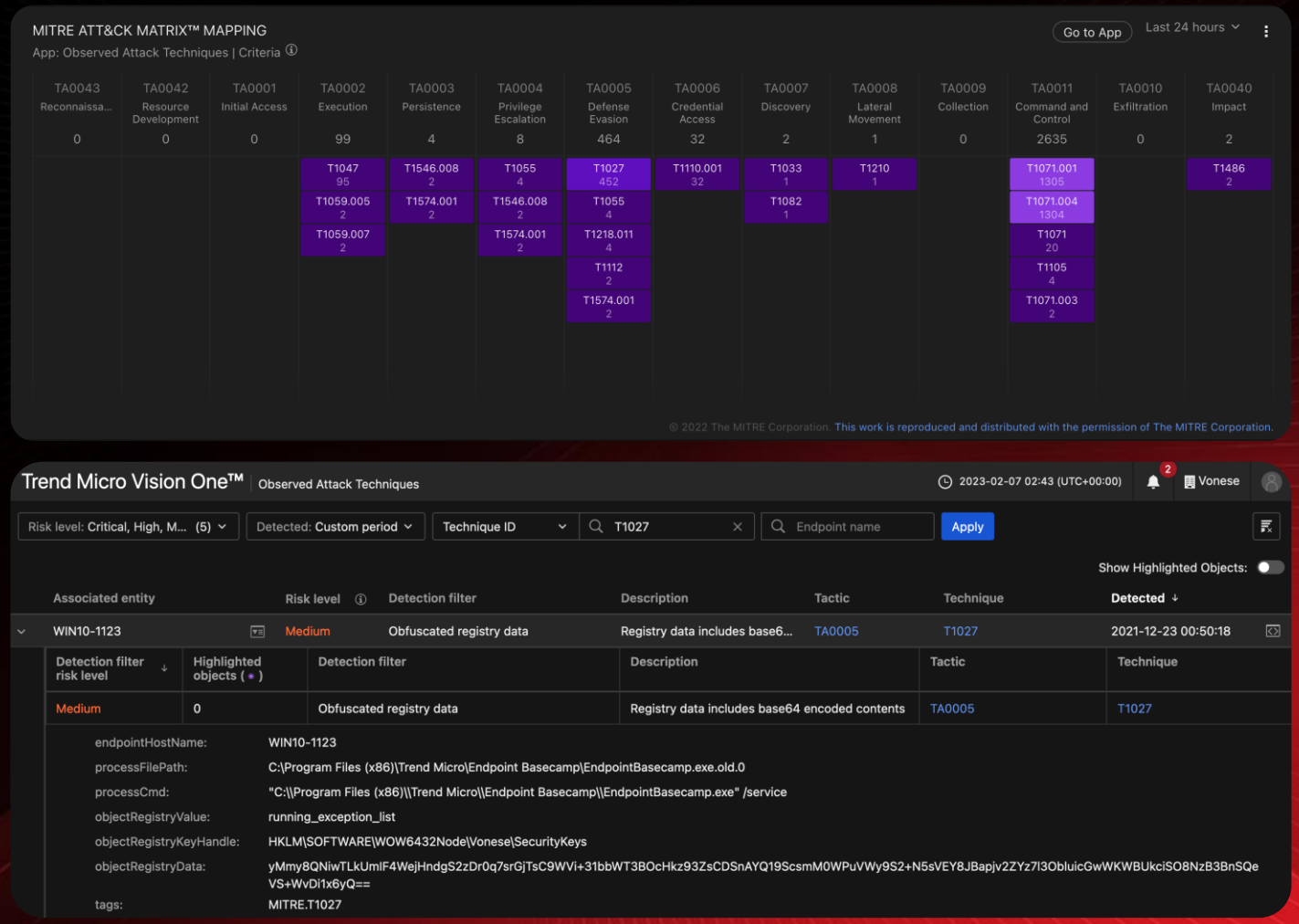
Интегрированные рабочие процессы SecOps: Применение мер по смягчению последствий; применение настроек политики...

Защита, оптимизированная под тип конечного устройства

Единая платформа для развертывания и управления EPP и EDR/XDR

Интеграция с базой знаний MITRE ATT&CK

Благодаря интеграции с базой знаний MITRE ATT&CK специалисты по ИБ говорят на одном языке



Модели обнаружения объединяют множество правил и фильтров с использованием различных методов анализа, включая суммирование данных и машинное обучение

Detection Models | Exceptions

Severity: Critical | Applicable products: All products | Status: All | Last updated: All

Severity	Model	Description	Applicable products
Critical	Potential Locky Ransomware Encryption	A file with filename similar to ransomware locky encryption has been found.	Trend Micro Apex One as a Service, Trend Cloud One - Endpoint & Workload Security, Endpoint Sensor
Critical	BlackByte Ransom Note Creation	BlackByte Ransom Note Created in the System	Trend Micro Apex One as a Service, Trend Cloud One - Endpoint & Workload Security, Endpoint Sensor
Critical	Ransom Note Detection (Real-time Scan)	Ransom Note Detection found on the system by Real time Scan	Trend Micro Apex One as a Service, Trend Cloud One - Endpoint & Workload Security, Trend Micro Apex Central, Trend Micro Deep Security Software, Trend Micro Deep Discovery Inspector

Работа по всем векторам безопасности для снижения уровня изолированности и обнаружения, расследования и реагирования на подозрительное поведение, вредоносные программы, программы-вымогатели, атаки с нарушением работы и другие критические атаки.

Summary

Possible Account Compromise Sign-In Activity Found - New application and device OS

Multiple indicators shows the account is compromised including sign-in from new application and device OS, sign-in IP is rarely seen in previous activity.

Score:	53
Impact scope:	3 1
Last seen:	2022-02-13T09:51:08Z
Automated responses:	3 tasks

Highlights

Possible Account Compromise Sign-In Activity Found - New application and device OS

Account Compromise Report (3 indicators found)

Technique: T1078.004 - Valid Accounts. Cloud Accounts

2020-02-13T09:51:08Z

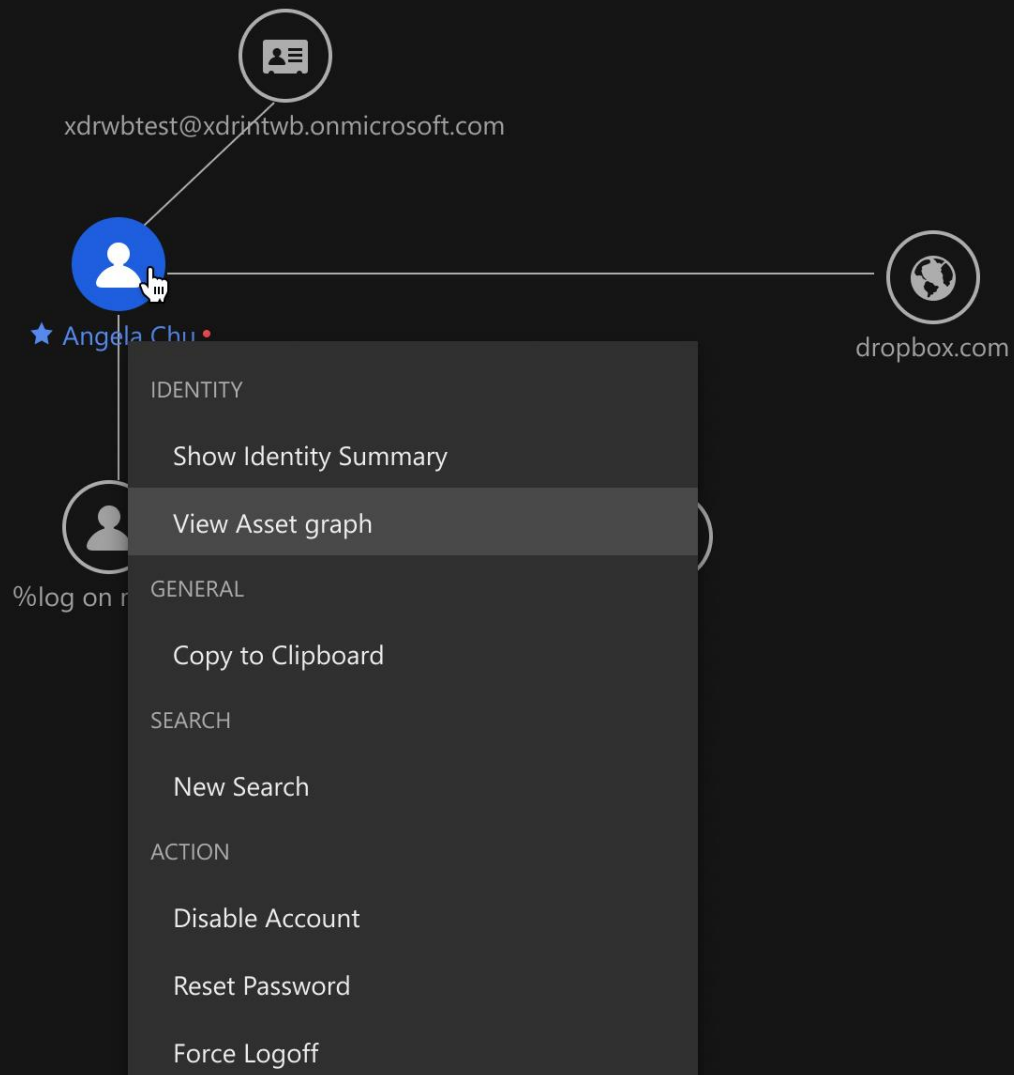
(Angela Chu) angela_chu@example.com
Sr. Staff Engineer | SPN
Risk level: High

(cloudapp) dropbox.com

(mailbox) xdrwbtest@xdrintwb.onmicrosoft.com

(sam_account) -

xdrwbtest@xdrintsb.onmicrosoft.com



Alerts (3) | Incident Timeline | Impact Scope (5) | Highlighted Objects (16)

Связывание отдельных точек событий во времени с одной первопричиной

64

Score

Demo - Possible Cobalt Strike Connection (3).

Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Key attack techniques: T1071.001, T1071.004, T1071

Created
Last up

Status: All | Created: All | Model: All | Workbench ID, Endpc

Score ↓	Workbench ID	Model	Model severity
75	WB-9439-20230312-00000	Demo - Possible Cobalt Strike Connection	High
75	WB-9439-20230313-00000	Demo - Possible Cobalt Strike Connection	High
75	WB-9439-20230314-00000	Demo - Possible Cobalt Strike Connection	High

Trend Vision One™ | Search

2023-03-14 09:36 (UTC-05:00)

99+

Open Guide | View History

Создание сложных строк запросов для точного определения данных или объектов в вашей системе, которые вы хотите исследовать

Search Method: Email Activity Data

mailMsgSubject: Email Demo AND mailUrlsRealLink:winshipway

Last 30 da

2023-02-12 10:45:04 - 2023

DATA GROUPING

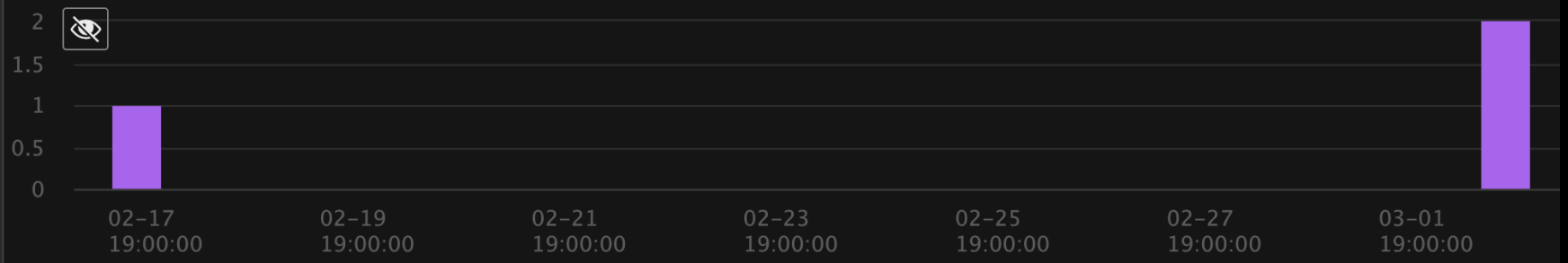
EMAIL ACTIVITY DATA

Matched Events: 3

- tags
- filterRiskLevel
- pname
- mailFromAddresses
- mailMsgId
- mailSenderIp
- mailbox
- mailSourceDomain
- customFilterTags
- customFilterRiskLevel

SEARCH RESULTS OBTAINED 100% DATA (3 EVENTS)

Query More



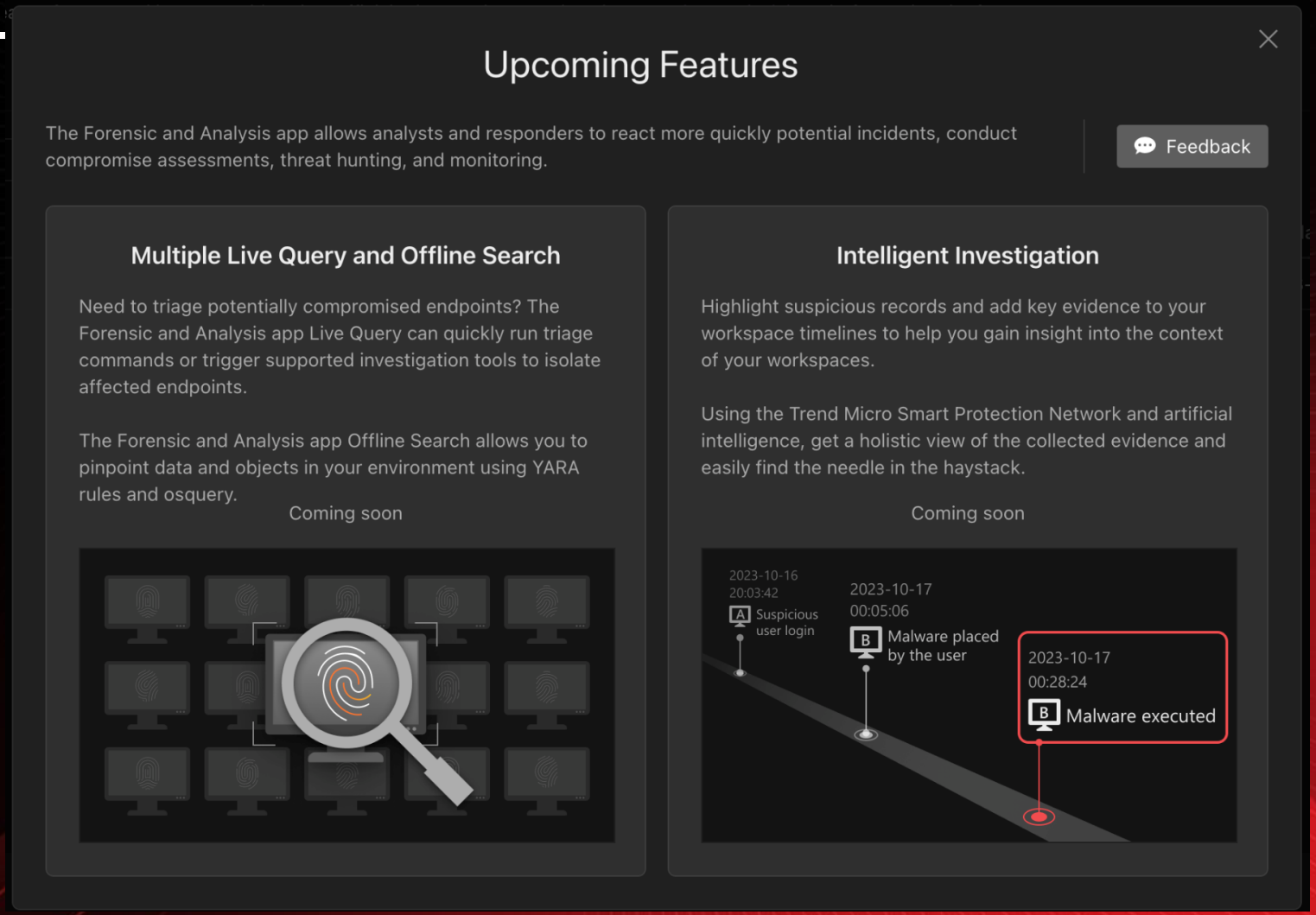
Profile: Defa

Logged	
2023-03-03 11:07:53	tags: XSAE.MA-01-002-VAR1 - First Email to Company from Newborn Sender - Varian - First Email to Company from Newborn Sender - Variant 2,mitrev9.t1566,mitrev9.t156 7-4eff-9e0d-571345c49b7d | filterRiskLevel: low | orgId: 55a5b510-8d3f-11e9-a3c
2023-03-03 11:07:45	tags: XSAE.MA-01-002-VAR1 - First Email to Company from Newborn Sender - Varian - First Email to Company from Newborn Sender - Variant 2,mitrev9.t1566,mitrev9.t156 51-4b5a-a04c-d8907171b823 | filterRiskLevel: low | pname: 742 - Trend Micro Ema

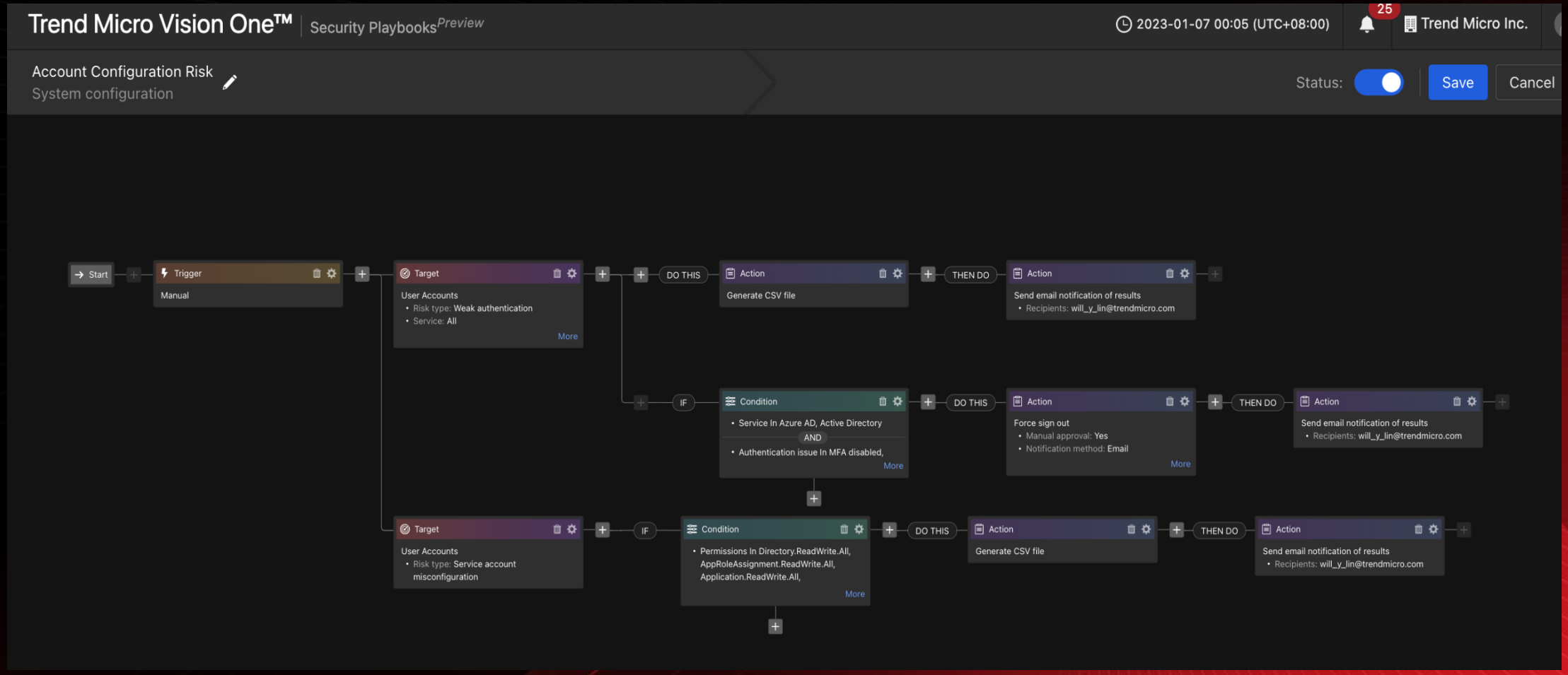
Криминалистика и реагирование

Инструменты и рабочие процессы для расширенного расследования критических инцидентов:

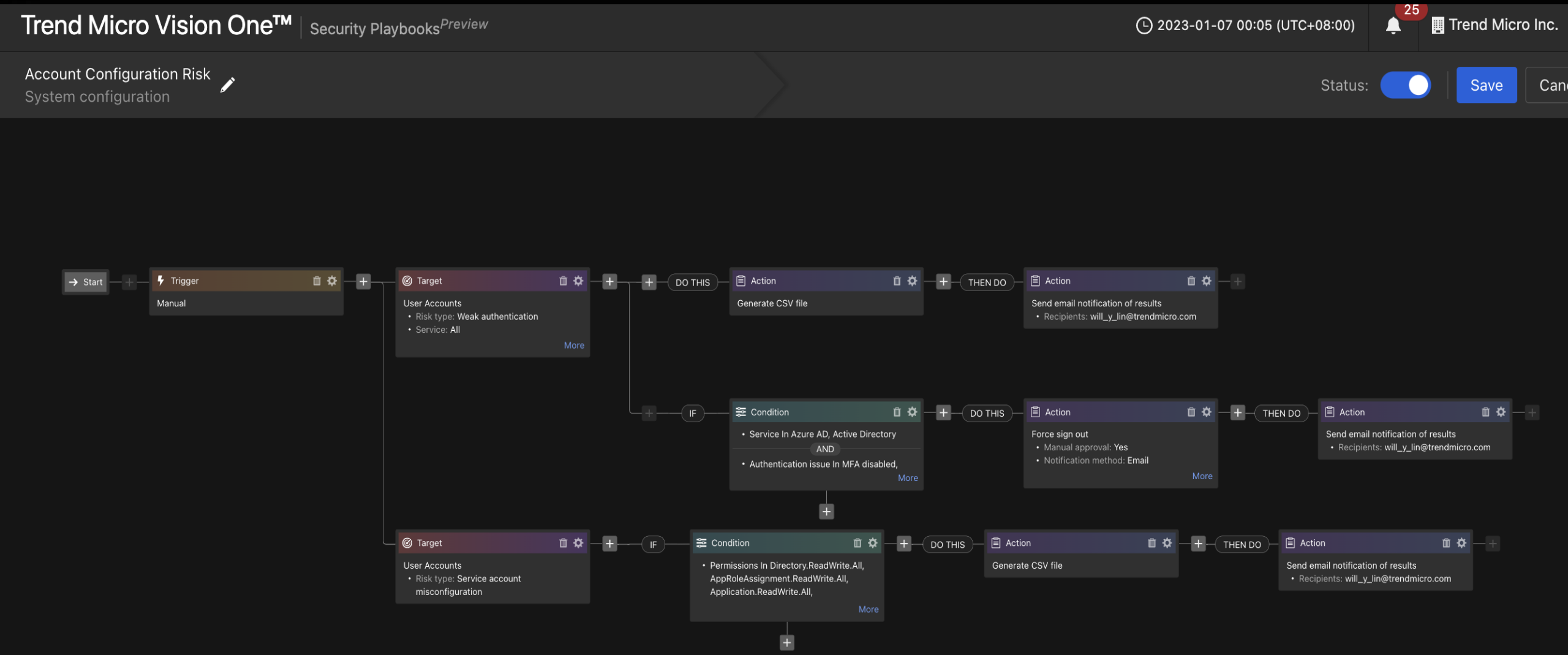
- Сбор доказательств
- Threat Intelligence
- Оперативный штаб
- Расследование в реальном времени
- Подробная хронология



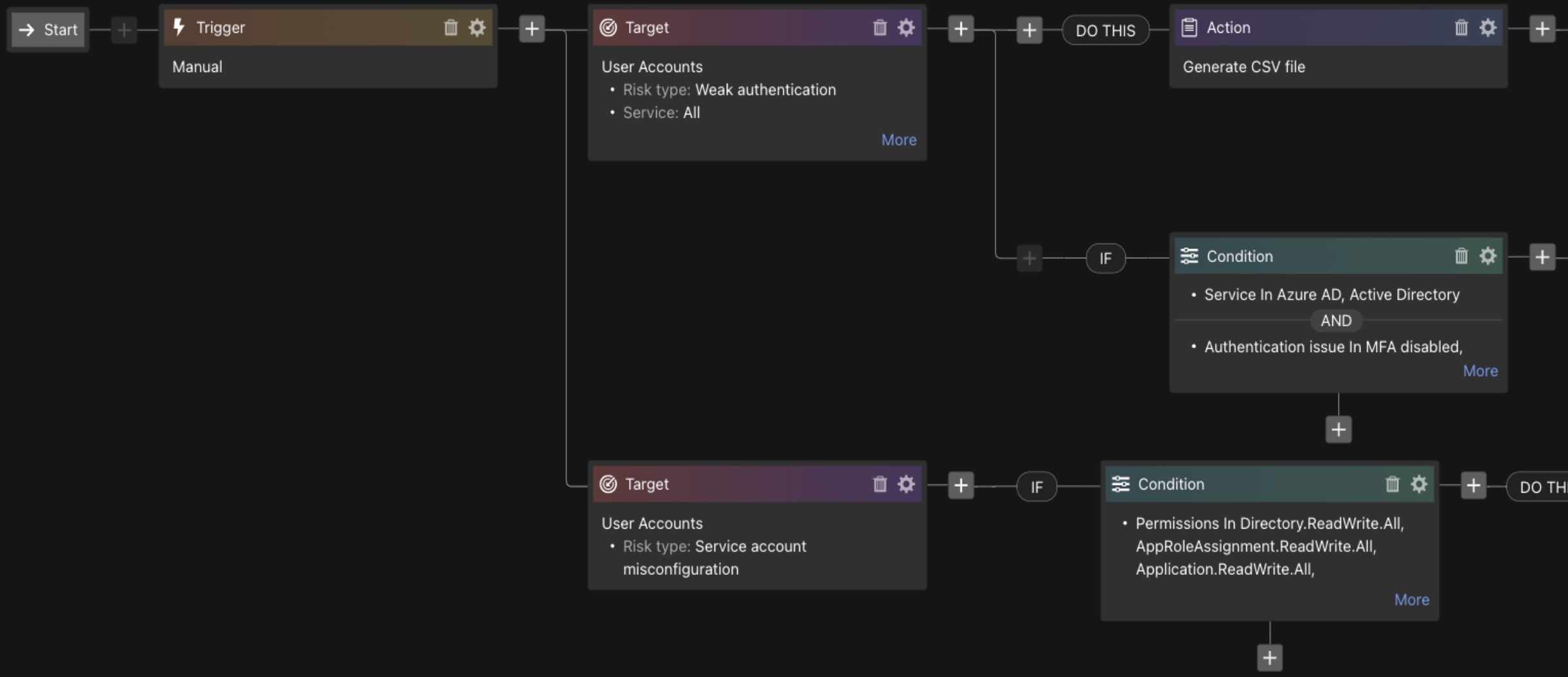
Автоматизация и оркестрация реагирования на угрозы



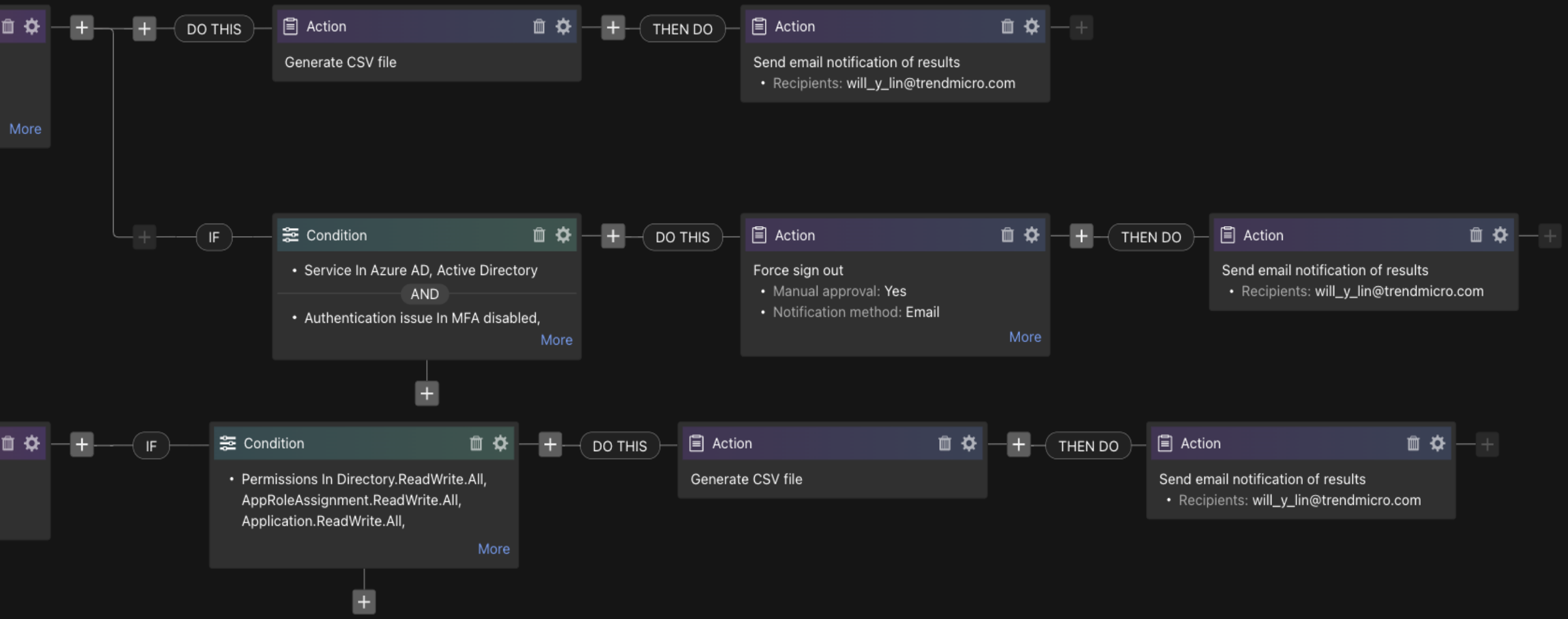
Автоматизация и оркестрация реагирования на угрозы



Автоматизация и оркестрация реагирования на угрозы



Автоматизация и оркестрация реагирования на угрозы



Managed Detection and Response

Круглосуточный мониторинг и обнаружение

Непрерывный мониторинг оповещений, корреляция и расстановка приоритетов с использованием автоматизации и аналитики. Проактивное сканнирование по конечным устройствам, серверам, сетям и эл. почте

Быстрое расследование и исправление

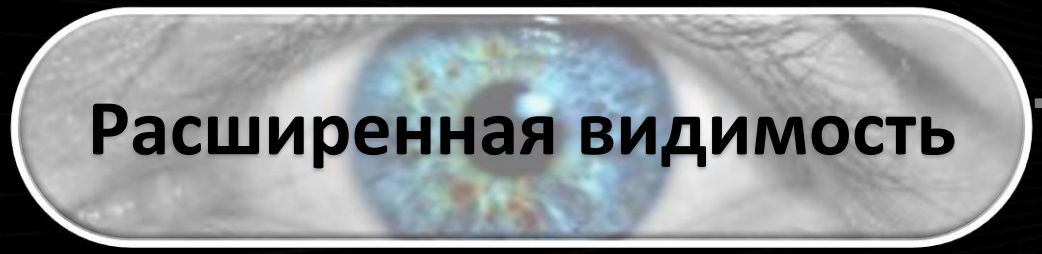
Всесторонний анализ и подробный план реагирования с удаленным реагированием с помощью продуктов Trend Micro

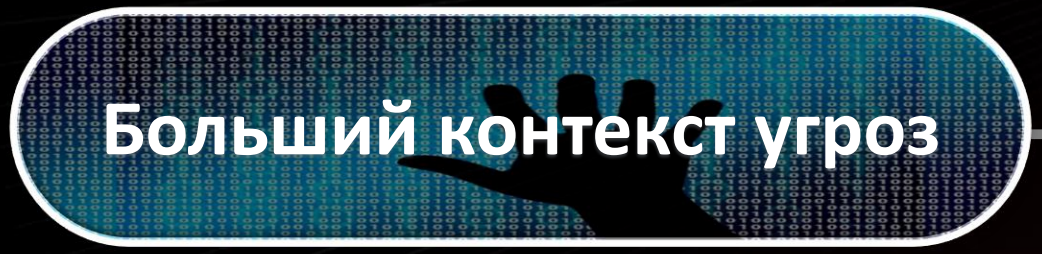
Поиск и выявление угроз

Обнаружение сложных направленных атак с помощью передовых техник и аналитической информации от экспертов по защите от угроз

Ускорение SOC. Идеальное сочетание: Взаимосвязь XDR и Управления рисками поверхности атаки (ASRM)

Ускорение обнаружения и реагирования





Extended Detection & Response (XDR)

Принятие решений с учетом рисков

Управление рисками поверхности атаки (ASRM)

Обнаружение поверхности атаки

Снижение рисков

Оценка рисков

Расширенная видимость

Больший контекст угроз

Быстрое реагирование

Extended Detection & Response (XDR)

Обнаружение

Реагирование

Расследование

Улучшение результатов и эффективности в обеспечении безопасности

Использование архитектуры Zero Trust

ASRM

Снижение рисков минимизирует число оповещений об угрозах

XDR

Подход Zero Trust динамически сокращает поверхность атаки

XDR и телеметрии идентичности обеспечивают больший контекст для контроля Zero Trust

Реализация модели Zero Trust

Использование архитектуры Zero Trust

ASRM

Данные об угрозах помогают оценить риск и вписать его в контекст

XDR

Непрерывная оценка служит основой для подхода Zero Trust

Автоматизированный контроль Zero Trust замедляет действия злоумышленников

Реализация модели Zero Trust

Улучшение результатов бизнеса

Усиление структуры безопасности

Платформенный подход обеспечивает обнаружение и видимость всех кибер-активов в цифровой среде

Повышение гибкости

Автоматизированное реагирование на угрозы и устранение рисков дает командам больше времени, чтобы сосредоточиться на создании ценностей

Повышение уровня кибербезопасности

Количественная оценка рисков помогает донести информацию и совместить практику управления киберрисками с операциями и целями бизнеса

Кто мы?

TREND MICRO

Trend Micro At a Glance

$1.93 Billion

2021 Gross Sales,
+9% YoY

94 Profitable Quarters

Every quarter since going public

385000+ SaaS Commercial Customers

500,000+ commercial customers, 150+ countries

52M

Protected Assets

#1 The Leader in Cloud Security

Based on global market share*

Leader in **XDR**

Based on offering strength and strategy*

#1 in Public Vulnerability Disclosure

+ Over 94 Billion threats blocked in 2021

65 Countries

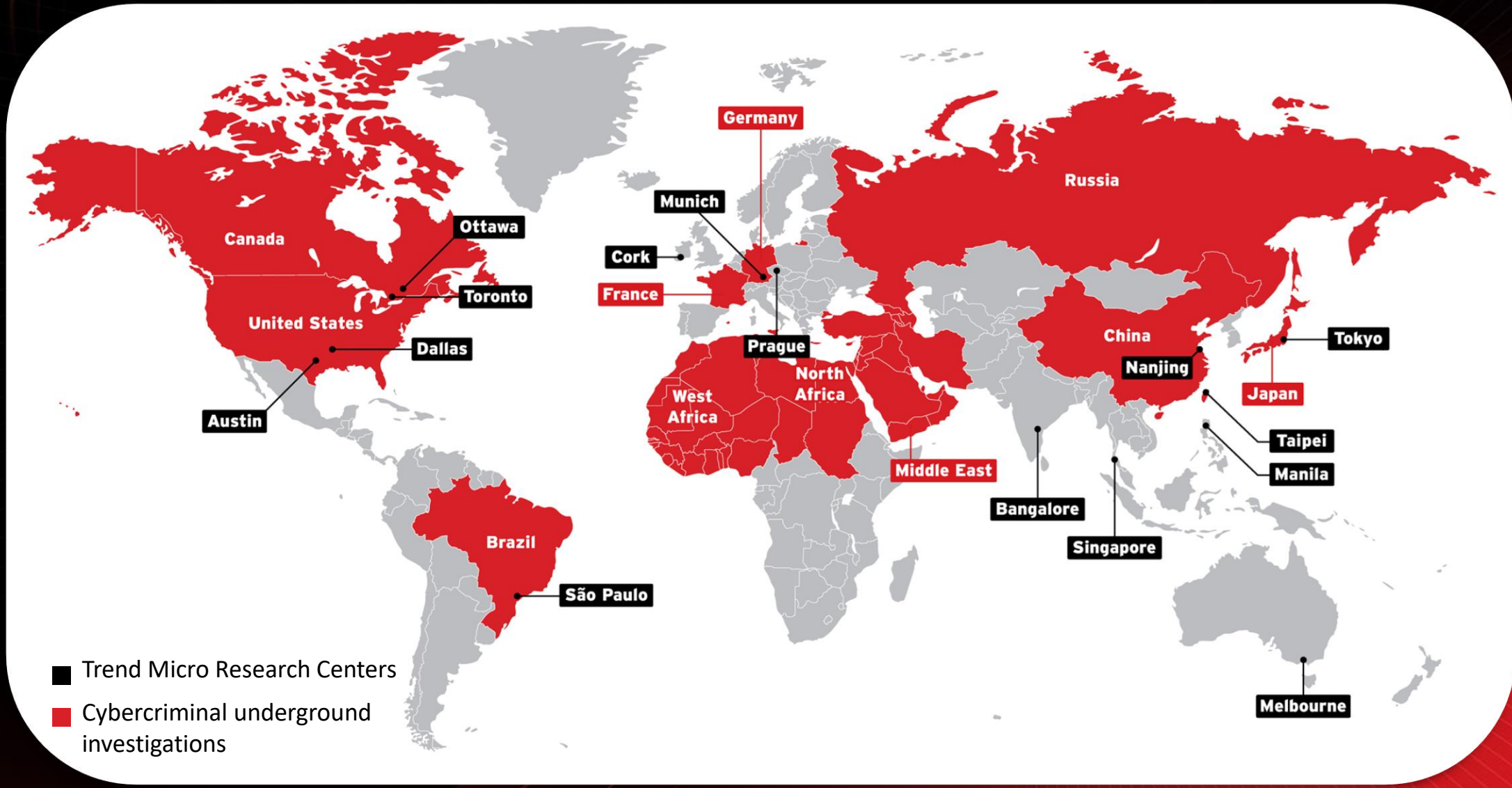
7000+

Employees

*IDC Cloud: www.trendmicro.com/en_us/business/products/hybrid-cloud.html?modal=r1a-btn-idc-learn-more-da0c46
*Forrester Wave, Extended Detection and Response (XDR):www.trendmicro.com/en_us/business/products/detection-response.html?modal=r1a-btn-forrester-xdr-see-why-ea3198

TREND MICRO

Powered by Trend Micro worldwide research



THE FORRESTER NEW WAVE™

Extended Detection And Response (XDR) Providers

Q4 2021

Trend Micro Лидер:

- **Наивысший общий** рейтинг по предложению в продукте.
- **"Отличалась"** от конкурентов в 7 из 10 индивидуальных категорий оценки.

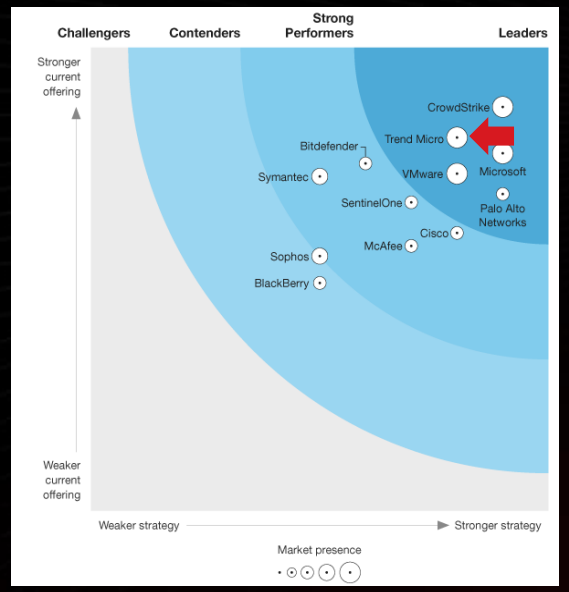
https://www.trendmicro.com/explore/forrester-wave-xdr

FORRESTER®
NEW WAVE LEADER 2021
Extended Detection And Response (XDR) Providers

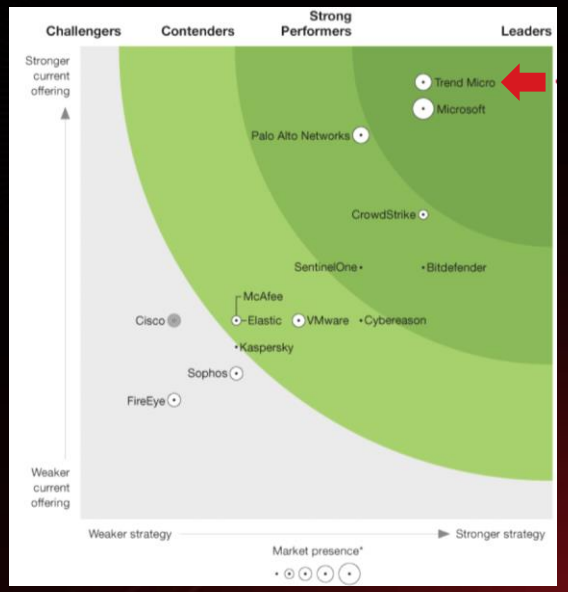
TREND MICRO

Лидер в обеспечении безопасности предприятия

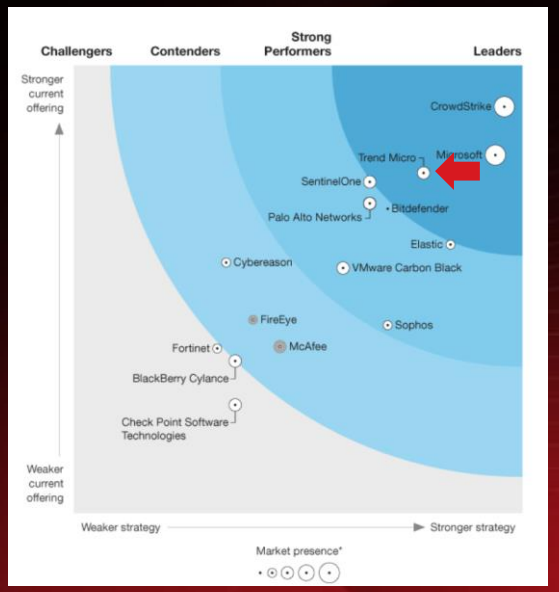
The Forrester Wave™: **Enterprise Email Security**, Q2 2021



The Forrester Wave™: **Endpoint Security Software as a Service**, Q2 2021



The Forrester New Wave™: **Extended Detection & Response (XDR)** Providers, Q4 2021



The Forrester Wave™: **Endpoint Detection and Response,** Q2 2022

Source: Forrester 2021

Лидер анализа и видимости сети

Компания Trend Micro - один из всего четырех поставщиков, получивших звание "Лидер". Мы получили 5 баллов из 5 в категории "Стратегия - инновации и видение", сохранив при этом ориентацию на удобство и простоту работы с клиентами.

Trend Micro предлагает NDR и NAV в составе нашей платформы кибербезопасности Trend Vision One™, обеспечивающей комплексное обнаружение угроз и реагирование на них в масштабах предприятия.

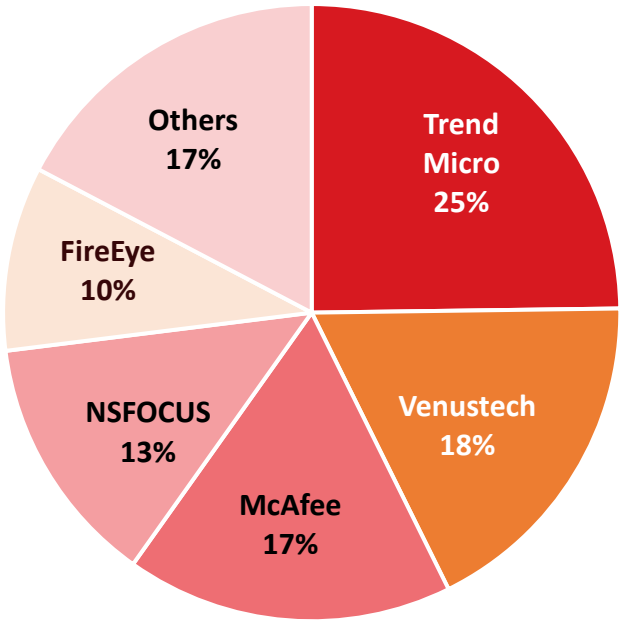
Source: Forrester 2023

Сила в Масштабах Предприятия

Gartner

Market Share Leader in IDPS

2021



Revenue in Million USD for 2020-21. Graphic prepared by Trend Micro based the Gartner report.
Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2021. March 2022

Magic Quadrant for Endpoint Protection Platforms (EPP)

Q2, 2021

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

2021 Market Guide for Cloud Workload Protection Platforms

Q2, 2021

8 of 8

Recommendations*

Trend Micro's assessment shows that we meet **ALL 8** of the Gartner recommendations for securing cloud workloads.*

*Based on Trend Micro's assessment of Gartner 2021 Market Guide for Cloud Workload Protection Platforms; Q2, 2021 | G00725997
Neil MacDonald, Tom Croll

TREND MICRO

Признано независимыми испытаниями

MITRE ENGENUITY™ | ATT&CK® Evaluations

- Высочайшее начальное обнаружение
- Низкий уровень шума

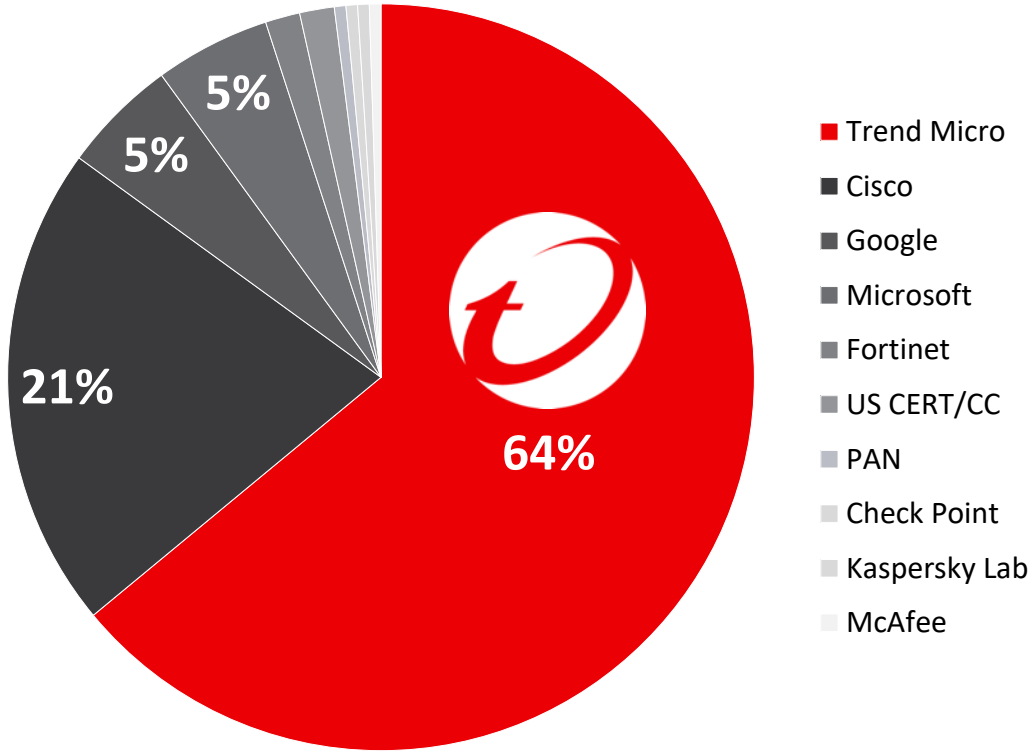
- Топ-3 по показателям видимости и телеметрии
- Обнаружено 100% атак на Linux

- 100% обнаружение всех этапов атаки
- Обнаружено и предотвращено 100% атак на Linux
- #1 для защиты

Лидер на рынке раскрытия информации об уязвимостях

ZERO DAY INITIATIVE

- **10 000+ независимых исследователей уязвимостей**
- **Лидер на рынке публичного раскрытия информации в течение последних 14 лет, обнаружи и сообщает о 64% уязвимостей в 2021 году**
- **Наиболее раскрываемые уязвимости с высоким уровнем воздействия (критические + высокой степени тяжести)**



Source: Quantifying the Public Vulnerability Market, Omdia, May 2022

Александр Джураев

+998 99 817 63 13

alexander_djuraev@trendmicro.com