Защита от цифровых рисков,

основанная на использовании разведывательной информации

Cyberint

ЗАЩИТА ОТ ЦИФРОВЫХ РИСКОВ, ОСНОВАННАЯ НА ИСПОЛЬЗОВАНИИ РАЗВЕДЫВАТЕЛЬНОЙ ИНФОРМАЦИИ

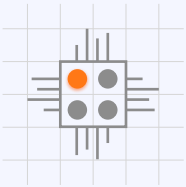
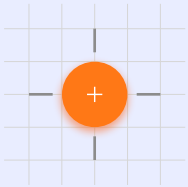
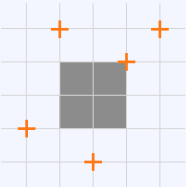
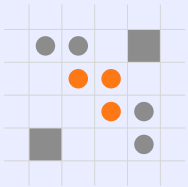
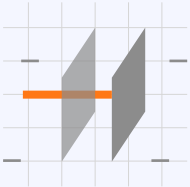
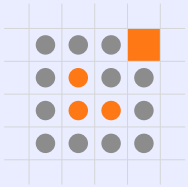
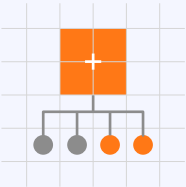
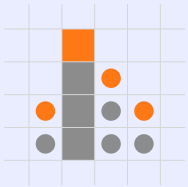
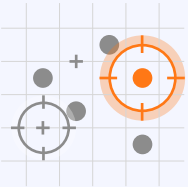
Используя уникальное сочетание Argos™ — собственной платформы аналитики угроз и высококвалифицированных аналитиков по анализу угроз, Cyberint предлагает новый подход к защите от цифровых рисков (DRP), предлагая решения, направленные на решение следующих задач:

- **Определение, какие релевантные угрозы** следует учитывать для разработки эффективной программы по обеспечению кибербезопасности
- **Иллюстрация** совету директоров и руководству **актуального статуса по киберриску** с четким планом действий
- **Сбор предиктивных сведений** для выявления намерений, методов и инструментов, направленных на минимизацию целевых угроз до их материализации
- **Постоянный мониторинг подверженности цифровому риску,** которым могут воспользоваться киберпреступники
- **Обнаружение нарушений по мере их распространения** за пределы периметра организации
- **Получение информации об атаках,** направленных на ваш бренд и клиентов, которые постоянно возникают за пределами вашей сети

БИЗНЕС – ЗАДАЧИ, КОТОРЫМИ ЗАНИМАЕТСЯ CYBERINT:

- **ЗАЩИТА БРЕНДА**
- **КИБЕР-РИСК ТРЕТЬЕЙ СТОРОНЫ**
- **ЦИФРОВОЙ МОНИТОРИНГ ПОВЕРХНОСТИ РИСКОВ**
- **МОШЕННИЧЕСТВО**
- **УТЕЧКА ДАННЫХ**
- **ОБНАРУЖЕНИЕ АТАКУЮЩЕГО ПО**
- **ОБНАРУЖЕНИЕ ТЕНЕВОГО ИНТЕРНЕТА**
- **РАЗВЕДКА УГРОЗ БЕЗОПАСНОСТИ**

ПРЕДЛОЖЕНИЕ CYBERINT

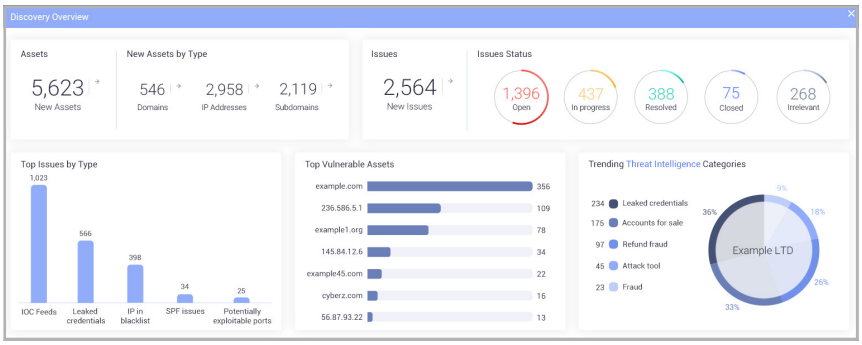
ТЕХНОЛОГИЯ ARGOS™	УПРАВЛЯЕМОЕ ОБСЛУЖИВАНИЕ
 РАЗВЕДКА УГРОЗ БЕЗОПАСНОСТИ	 ЦЕЛЕВОЙ МОНИТОРИНГ
 МОНИТОРИНГ ТЕНЕВОГО ИНТЕРНЕТА	 ВИРТУАЛЬНАЯ АГЕНТУРНАЯ РАЗВЕДОВАТЕЛЬНАЯ ИНФОРМАЦИЯ
 ПОВЕРХНОСТНОЕ КАРТИРОВАНИЕ РИСКА	 ГЛУБОКИЕ РАССЛЕДОВАНИЯ
 ЭКСПЕРТНЫЙ ХОЛСТ	 АНАЛИЗ КАРТИНЫ УГРОЗ
 ОБНАРУЖЕНИЕ ФИШИНГА И ОСВОБОЖДЕНИЕ	

ОСНОВАННАЯ НА ИСПОЛЬЗОВАНИИ РАЗВЕДЫВАТЕЛЬНОЙ ИНФОРМАЦИИ ПЛАТФОРМА ARGOS™ ДЛЯ ЗАЩИТЫ ОТ ЦИФРОВЫХ РИСКОВ

Argos™ — это мультипользовательская платформа SaaS (программа как услуга) с несколькими модулями:

ПОВЕРХНОСТНОЕ КАРТИРОВАНИЕ ПОВЕРХНОСТИ АТАКИ

Картирование поверхности атаки Argos™ выявляет цифровой след организации и на постоянной основе отслеживает активы за пределами периметра, обеспечивая обзор указанных активов с установлением приоритетов на основе серьезности проблем, которые необходимо решить, выделяя соответствующие угрозы, уязвимости и слабые места.

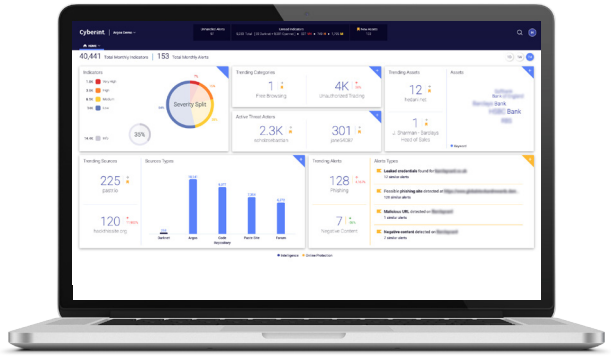


Платформа Argos™ для защиты от цифровых рисков, Поверхностный мониторинг атак

СБОР И АНАЛИЗ РАЗВЕДДАННЫХ ОБ УГРОЗАХ

Cyberin — это мониторинг тысяч источников угроз в открытом, глубоком и теневом Интернете в режиме реального времени, который позволяет собирать миллионы разведывательных данных в день в озеро внутренних данных Argos™.

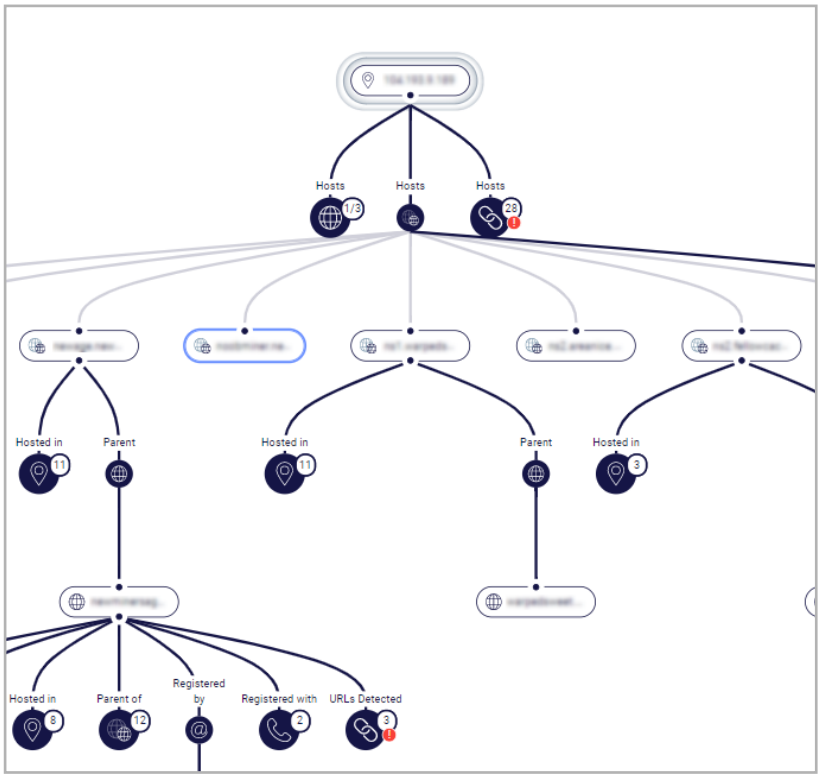
Необработанные элементы разведданных автоматически сопоставляются с активами организации (IP-адресами, доменами, брендами, управленцами и т. д.) и классифицируются в соответствии с конкретным вариантом использования: фишинг, вредоносные кампании, вставка учетных данных, мошенничество по утечке данных и другие. Используя защищенный алгоритм машинного обучения Cyberint, эти необработанные разведданные распределяются по приоритетам в соответствии с потенциальным риском и воздействием, что позволяет проводить автоматизированный и малозатратный анализ.



Платформа Argos™ для защиты от цифровых рисков

Механизмы автоматического и полуавтоматического анализа генерируют предупреждения интеллектуальной системы, которые затем распространяются среди групп безопасности с подробным анализом, расширенным контекстом, профилированием субъектов угроз и многим другим, что позволяет организации принимать эффективные меры.

ЭКСПЕРТНЫЙ ХОЛСТ



Платформа Argos™ для защиты от цифровых рисков, Экспертный холст

Модуль Экспертного холста от Cyberint позволяет идентифицировать и профилировать субъектов угроз, а также проводить глубокое исследование используемых ими инструментов, тактик и процедур (TTP).

Экспертный холст используется для обогащения контекста конкретных или нескольких систем управления вводом-выводом, интеграции нескольких сервисов в единую платформу расследования для поддержки различных типов соединений, включая разведданные об угрозах Argos™, сервисы WHOIS (база данных о пользователях), пассивную систему имён доменов, социальное обнаружение, выявление вредоносного кода и т. д.

ПРОАКТИВНАЯ ТЕХНОЛОГИЯ ОБНАРУЖЕНИЯ ФИШИНГА И ОСВОБОЖДЕНИЕ

Фишинг остается серьезным риском для цифровых организаций, который приводит к захвату аккаунтов, оттоку клиентов и негативному влиянию на репутацию бренда. Решаю эту проблему, Cyberint разработала Phishing Beacon (Сигнал фишинга) – защищенный модуль, позволяющий в режиме реального времени видеть вновь созданные фишинговые сайты, клонированные из содержимого веб-сайтов организации, — эффективная технология, используемая злоумышленниками. Быстрое обнаружение Cyberint позволяет нам блокировать фишинговые сайты от имени организации для быстрого устранения риска.

ЧТО ЭТО ЗНАЧИТ ДЛЯ ВАС

- **УМЕНЬШИТЬ ТЕНЕВЫЕ ИТ РИСК БЕЗОПАСНОСТИ**
- **ПОЛУЧИТЬ ОБЗОР ПОВЕРХНОСТИ АТАКИ**
- **СОКРАТИТЬ ВРЕМЯ ЗАДЕРЖКИ УГРОЗЫ**
- **РАСШИРИТЬ ВОЗМОЖНОСТИ КОМАНДЫ**
- **СНИЗИТЬ TCO КИБЕРБЕЗОПАСНОСТИ**

УПРАВЛЯЕМЫЙ СЕРВИС

Индивидуальные услуги киберразведки, соответствующие вашим потребностям

УВЕЛИЧЕНИЕ КОМАНДЫ РАЗВЕДКИ ОБ УГРОЗАХ

Cyberint предлагает управляемую программу защиты от цифровых рисков, обеспечивающую доступ к нашей платформе Argos™ и команду аналитиков киберугроз, повышающих качество и производительность любой программы CTI.

Партнерство с командой аналитиков Cyberint включает повседневное взаимодействие с преданным аналитиком, который становится членом вашей внутренней команды. Аналитики назначаются на основе их знания отраслей и глубокого понимания потребностей бизнеса. Все необработанные разведданные, выявленные Argos™, тщательно проверяются, увязываются с контекстом и соотносятся с реальными рисками, используя огромные объемы данных, собранных из открытого, глубокого и теневого интернета.

Наша команда аналитиков многоязычна, что позволяет понимать участников угроз на их родном языке. Кроме того, владение аналитиком «жаргоном» и культурой киберпреступников позволяет выявлять, проверять и смягчать те угрозы, которые, скорее всего, будут реализованы в виде атак. Cyberint предоставляет ценный человеческий фактор, когда дело касается исследований, расследований и операций по разведке угроз. Возможности виртуальной агентурной разведки (HUMINT), то есть живое взаимодействие со злоумышленниками, обеспечивают более глубокую контекстуализацию, необходимую для эффективного решения проблемы.

ИССЛЕДОВАНИЯ CYBERINT

Группа кибер расследователей Cyberint изучает границы ландшафта киберугроз, чтобы поддерживать стратегическую видимость актуальных угроз. Команда кибер расследований анализирует огромные объемы данных, чтобы создавать стратегические отчеты об угрозах, позволяя лицам, принимающим решения, выявлять значимые тенденции и получать более широкое и глубокое представление о цифровых рисках, нацеленных на их организацию. Отчет включает периодический анализ текущих отраслевых рисков, заметных участников угроз, анализ TTP и многое другое.

ПОСЛЕДНИЕ ОТЧЕТЫ CYBERINT

Финансовый сектор Филлипин
Разведывательный отчет об угрозах

ЗАГРУЗИТЬ

REvil - Кража, шифрование и аукцион
Исследовательский отчет

ЗАГРУЗИТЬ

Целевые атаки программ-вымогателей в Тайван
Исследовательский отчет

ЗАГРУЗИТЬ

ПРЕИМУЩЕСТВА ПАРТНЕРСТВА С УПРАВЛЯЕМЫМИ УСЛУГАМИ РАЗВЕДКА УГРОЗ БЕЗОПАСНОСТИ ПОД РУКОВОДСТВОМ CYBERINT

ОБНАРУЖЕНИЕ УГРОЗЫ

Обнаружение угроз с помощью прогнозирующего интеллекта

ОПРЕДЕЛЕНИЕ СЕРЬЕЗНОСТИ

Определите серьезность угроз и поймите «ситуацию в целом»

ВИРТУАЛЬНЫЕ ВОЗМОЖНОСТИ АГЕНТУРНОЙ РАЗВЕДКИ

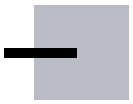
напрямую общаться со злоумышленниками, выявлять связь их деятельность с конкретными кампаниями и получать больше контекста и разведывательной информации

ИДЕНТИФИКАЦИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

Выявление и предоставление ценной разведывательной информации о том, как реагировать и смягчать последствия

ОБНАРУЖЕНИЕ ФИШИНГА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Операции по обнаружению и удалению фишинговых веб-сайтов в режиме реального времени



РАССЛЕДОВАНИЕ VIP УГРОЗ

Отслеживайте действия своего управленческого персонала в сети, чтобы предотвратить получение злоумышленниками личной информации с целью злонамеренного использования

КАРТИРОВАНИЕ И МОНИТОРИНГ

Отображение и мониторинг цифрового присутствия организации, включая утечки учетных данных, цифровые уязвимые места и утечку конфиденциальных документов

Gartner peerinsights™ 4.8 ★★★★★

ОТ НАШИХ КЛИЕНТОВ

«Это управляемая услуга, которая обеспечивает реальную ценность, преобразовывая результаты в релевантную информацию и предупреждения, адаптированные к нашему бизнесу».

Крупная розничная торговая фирма в США

«Пока вы не используете Cyberint, у вас действительно нет верного представления о том, кто пытается атаковать вашу организацию».

Крупная розничная торговая фирма по электронной коммерции в США

СВЯЖИТЕСЬ С НАМИ

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

США
214 W 29th St.
New York, 10001
Tel: +1-646-568-7813

ИЗРАИЛЬ
17 Ха-Мефалсим
Ст.4951447 Петах-Тиква
Тел.: +972-3-7286-777

UNITED KINGDOM
14 Грейс Инн Роуд, Холборн
WC1X 8HN, Лондон
Тел.: +44-203-514-1515

СИНГАПУР
135 Сесиль Ст. #10-01 MYP
ПЛАЗА 069536
Тел.: +65-3163-5760

ЛАТАМ
Панама-Сити
Тел.: +1-929-399-8495