Краткий справочник по кибербезопасности Cisco за 2016 год

Почему важна безопасность?

- Повсеместная безопасность
- Безопасность: важная тема для обсуждения на уровне руководства компании

Почему именно Cisco?

- Лидер в сфере кибербезопасности
- Группа Talos: анализ и исследование угроз безопасности

Стратегия безопасности Cisco

- Проблемы
- Стратегия безопасности Cisco

Портфель продуктов Cisco для обеспечения безопасности

- Безопасность сети и ЦОД
- Защита от сложного вредоносного ПО
- Безопасность облачных вычислений
- Безопасность электронной почты и веб-трафика
- Безопасность промышленных сетей

Почему важна безопасность?

Повсеместная безопасность

Цифровая экономика и Всеобъемлющий Интернет (IoE) открывают массу возможностей для компаний и потребителей — ожидается, что в следующие 10 лет потенциальная ценность для организаций превысит 19 триллионов долларов США. Вместе с тем значительно увеличивается и опасность со стороны хакеров и киберпреступников. В условиях Всеобъемлющего Интернета поверхность атаки значительно расширяется, соответственно, и киберпреступники рассчитывают увеличить объем своей экономики с 450 миллиардов долл. США до более чем 1 триллиона долл. США.

Наиболее эффективный способ противостоять динамическому ландшафту угроз – сделать безопасность такой же повсеместной и всеобъемлющей как сам Всеобъемлющий Интернет: безопасность должна обеспечиваться всегда и везде — где бы ни находились сотрудники и данные.

Благодаря интеграции функций обеспечения безопасности по всей распределенной сети, безопасность становится тем регулятором, который позволяет бизнесу пользоваться всеми преимуществами и возможностями, предлагаемыми новыми цифровыми бизнес-моделями и Интернетом вещей (IoT) и при этом оставаться надежно защищенным на всем протяжении атаки — до, во время и после.

Безопасность: важная тема для обсуждения на уровне руководства компании

Вопросы информационной безопасности и риска потери интеллектуальной собственности, компрометации данных заказчиков и подрыва доверия с их стороны, и как следствие, снижение прибыли, все чаще обсуждаются на уровне руководства компании и совета директоров.

- Задача директоров по информационной безопасности (CISO) - убедить свое руководство в необходимости дополнительных инвестиций в безопасность
- Это очень важные вопросы, так как организации становятся все более гибкими и стараются развивать свои бизнес-модели в соответствии с новыми тенденциями в сфере мобильных технологий, облачных вычислений и усовершенствованных целенаправленных атак

Почему именно Cisco?

Cisco – лидер в сфере кибербезопасности

Компания Cisco высоко ценится в отрасли и предлагает ряд лучших в своем классе решений (см. рис. 1). Cisco была названа лучшей компанией в сфере информационной безопасности за 2016 год по версии журнала 2016 SC Magazine. Решение Cisco Identity Services Engine (ISE) также стало лучшим решением по управлению сетевым доступом (NAC).

Рисунок 1 Решения Cisco по обеспечению безопасности заслужили признание рынка

Портфель решений Cisco по информационной безопасности был позитивно оценен в рейтинге поставщиков агентства Gartner за 2015 год и занял позицию лидера в Магическом квадранте Gartner по следующим продуктам:

- Системы предотвращения вторжений (ноябрь, 2015 г.)
- Защищенные шлюзы электронной почты (июль, 2015 г.)

Компания Cisco постоянно занимает лидирующие позиции на графиках Security Value Maps (SVM) компании NSS Labs и имела самый высокий бал по эффективности защиты на следующих графиках SVM:

- Системы обнаружения брешей — 99,2 % (сентябрь, 2015 г.)
- IPS нового поколения — 99,5 % (апрель, 2015 г.)
- Межсетевые экраны нового поколения — 99,2% (ноябрь, 2014 г.)

Независимое тестирование решений для обеспечения информационной безопасности подтверждает данные производителя об эффективности и производительности продукта. Помимо собственных результатов тестирования важное значение имеют тесты, проводящиеся сторонними компаниями, и в этом случае Cisco также год за годом продолжает оставаться лидером.

Рисунок 2 Неизменное лидерство в вопросе эффективности систем безопасности

Группа Talos по аналитике и исследованиям безопасности: признанный опыт в сфере анализа угроз от лидеров в сфере кибербезопасности

Группа Cisco Talos по аналитике и исследованию безопасности состоит из самых лучших экспертов в области безопасности, чья система анализа угроз позволяет обнаруживать, анализировать угрозы и обеспечивать защиту как от уже известных, так и от только появляющихся угроз благодаря агрегации и анализу не имеющих себе равных данных телеметрии Cisco:

- 19,7 млрд отраженных угроз в день
- 1,5 млн образцов вредоносного ПО в день
- 1,1 млрд заблокированных веб-запросов в день
- 1 млрд репутационных запросов к SenderBase в день
- 2 557 767 заблокированных угроз в секунду

Talos также поддерживает наборы официальных правил для Snort, ClamAV, SenderBase и SpamCop.

Специалисты по исследованию угроз группы TALOS также тесно работают со специалистами по обработке и анализу данных и инженерами по инфраструктуре команды OpenDNS Security Labs. OpenDNS создает системы больших данных, 3D визуализации и статистические модели для автоматического определения того, где была организована инфраструктура киберпреступников до того, как атаки попадут в Интернет. OpenDNS также поддерживает программы PhishTank, DNScrypt и OpenGraffiti.

Исследования Cisco в области безопасности: www.cisco.com/go/talos
Отчеты Cisco по информационной безопасности: www.cisco.com/go/securityreports
Блог OpenDNS Security Labs: labs.opendns.com/blog

Проблемы обеспечения безопасности

Три основные тенденции, появившиеся одновременно, делают задачу защиты сети как никогда более трудной, при этом, помогая хакерам находить новые способы прорыва обороны (см. рис. 3).

Рисунок 3 Проблемы обеспечения безопасности

Меняющиеся бизнес-модели: Всеобъемлющий Интернет (IoE) ускоряет изменения, создавая новые векторы атаки и усложняя для организаций задачи защиты сетей. В то же время, при условии надежной защиты, IoE открывает огромные перспективы для бизнеса.

Динамический ландшафт угроз: злоумышленники стали действовать все более изощрено и получать все больше финансирования, атаки из статических превратились в динамические, из открытых – в скрытые. В случае отсутствия в организации возможностей для обнаружения угроз в реальном времени, это грозит ей огромными рисками.

Сложность и фрагментарность: большинство организаций имеют десятки самых разных технологий обеспечения безопасности, которые зачастую несовместимы между собой, кроме того ситуация усугубляется отсутствием на рынке достаточного числа опытных специалистов в этой области.

Стратегия безопасности Cisco

Подход к безопасности, ориентированный на защиту от угроз и оперативность, позволяет организация снизить сложность и фрагментарность, обеспечивая непревзойденную видимость, постоянный контроль и защиту от сложных угроз во всей распределенной сети и на всем продолжении атаки (см. рис. 5).

Рисунок 4 Модель комплексной безопасности

Обеспечение мониторинга: возможность получения информации об угрозах в глобальном масштабе и учет контекста для дальнейшего более подробного анализа и лучшего принятия решений.

Ориентация на защиту от угроз: обнаружение, понимание и блокирование угроз в течение всего жизненного цикла атаки.

На основе платформы: снижение фрагментарности за счет унификации платформ для защиты сети, устройств и облака.

Только Cisco предоставляет решения, которые интегрируются между собой в единую систему безопасности.

Рисунок 5 Продукты для обеспечения безопасности на всем продолжении атаки

Безопасность с учетом контекста: использование преимуществ физических и виртуальных хостов, операционных систем, приложений, сервисов, протоколов, пользователей и анализа контента и поведения сети.

Непрерывное обеспечение безопасности: агрегация и корреляция данных по всей распределенной сети, возможность отличать активные атаки и разведывательные действия от фоновых помех.

Ретроспективная защита: непрерывный анализ поведения файловой активности с течением времени с целью обнаружения вредоносного ПО, которое может менять свое поведение для предотвращения своего обнаружения, понимание всей глубины заражения, установление его причин и устранение причин и последствий атак.

Портфель продуктов Cisco для обеспечения безопасности

Безопасность сети и ЦОД нового поколения

Возможность защиты наиболее важных данных с использованием функций защиты от угроз, виртуализации системы безопасности, сегментации и управления политиками.

Межсетевой экран нового поколения Cisco Firepower Next Generation Firewall (NGFW)

Межсетевой экран Cisco Firepower NGFW - это первый в отрасли полностью интегрированный межсетевой экран нового поколения, ориентированный на защиту от угроз с возможностью обеспечения высочайшей безопасности заказчиков, быстрого устранения сложных угроз и лучшей оптимизации процессов. Это позволяет заказчикам блокировать большее число угроз, получать максимум от их ресурсов и позиционировать безопасность как фактор роста для использования новых бизнес-возможностей.

Cisco Firepower серии 4100

- Платформа безопасности с ориентацией на защиту от угроз, позволяющая учесть широкий спектр потребностей – от Интернет-периметра до центра обработки данных (ЦОД)
- Оптимизация производительности и плотности - варианты интерфейсов 10Ge и 40Ge и скорость более 60 Гбит/с в форм-факторе 1 RU
- Унифицированный мониторинг и управление политиками МСЭ, контроль приложений, IPS нового поколения, защита от сложного вредоносного ПО, фильтрация URL, сканирование сети и др.

Cisco Firepower серии 9300

- Масштабируемая платформа операторского класса, предназначенная для операторов связи и других компаний, которым необходимо малое время задержки и исключительная пропускная способность
- Динамическое использование сервисов проверки безопасности в сетевой фабрике наряду с предоставлением интеллектуальных сервисов безопасности Cisco и ее партнеров (например, WAF, DDoS и т.п.)
- Модульная архитектура безопасности обеспечивает гибкую конфигурацию и масштабирование производительности

Cisco Firepower Management Center

- Полностью интегрированное управление устройствами сетевой безопасности Cisco, ориентированными на защиту от угроз (NGFW, NGIPS, AMP, фильтрация URL), с одной консоли

- Централизованное управление правилами и конфигурацией МСЭ, глубокий контроль более 4000 приложений, политики предотвращения вторжений и анализ сложного вредоносного ПО
- Автоматическая корреляция индикаторов компрометации по всей сети с сенсорам оконечных устройств с автоматическим ранжированием рисков, что позволяет вашим специалистам по безопасности правильно распределять свои приоритеты
- Сканирование всей вашей сети в поисках уязвимостей на оконечных устройствах без необходимости установки агентов
- Интеграция с внешними средствами защиты партнеров Cisco – сканеры безопасности, системы расследования инцидентов, системы захвата сетевого трафика, SIEM-решения и т.п.

Cisco ASA 5500-X с сервисами FirePOWER (NGFW)

- Первый в отрасли NGFW с ориентацией на защиту от угроз
- Сочетание МСЭ ASA с системой Cisco IPS (NGIPS) нового поколения, системой защиты от сложного вредоносного ПО (AMP) и системой фильтрации URL
- Серия платформ разного размера и с разными форм-факторами

Cisco ASA 5585-X с сервисами FirePOWER (NGFW)

- Физическое устройство обеспечения безопасности специально для ЦОД
- Обеспечивает высочайшую производительность, надежность и масштабируемость за счет самой лучшей в индустрии кластеризации
- Сочетает межсетевой экран ASA с решениями Cisco Firepower NGIPS и Cisco AMP

Cisco FirePOWER Next-Generation IPS (NGIPS)

- Лучшая в отрасли защита от сложных угроз
- Обеспечивает лучшую в отрасли пропускную способность, эффективность обнаружение угроз и низкую стоимость владения (TCO)
- Серия платформ разного размера и с разными форм-факторами
- Снижение сложности при одновременном обеспечении постоянного контроля, надежного мониторинга и защиты от сложных угроз на всем протяжении атаки

Виртуальное многофункциональное устройство обеспечения безопасности Cisco (ASAv)

- Поддерживает архитектуру традиционных сетей SDN, сетей SDN нового поколения и архитектуру Cisco, ориентированную на приложения (ACI)
- Обеспечивает все возможности межсетевого экрана ASA и VPN, поддерживая множество сред гипервизора, сокращая административные накладные расходы и увеличивая операционную эффективность
- Ускорение и упрощение предоставления сервисов безопасности благодаря предварительно заданным конфигурациям и обеспечение динамически масштабируемой безопасности
- Обеспечение поддержки виртуального коммутатора vSwitch для ЦОД Cisco, гибридных ЦОД и ЦОД сторонних поставщиков

Виртуальная система Cisco IPS нового поколения для VMware

- Предлагает виртуализированное решение Cisco FirePOWER NGIPS
- Восстанавливает возможности мониторинга, утраченные во время виртуализации
- Обеспечивает выполнение требований индустрии платежных карт (PCI) в виртуальных средах

Решение для защиты от целенаправленных угроз

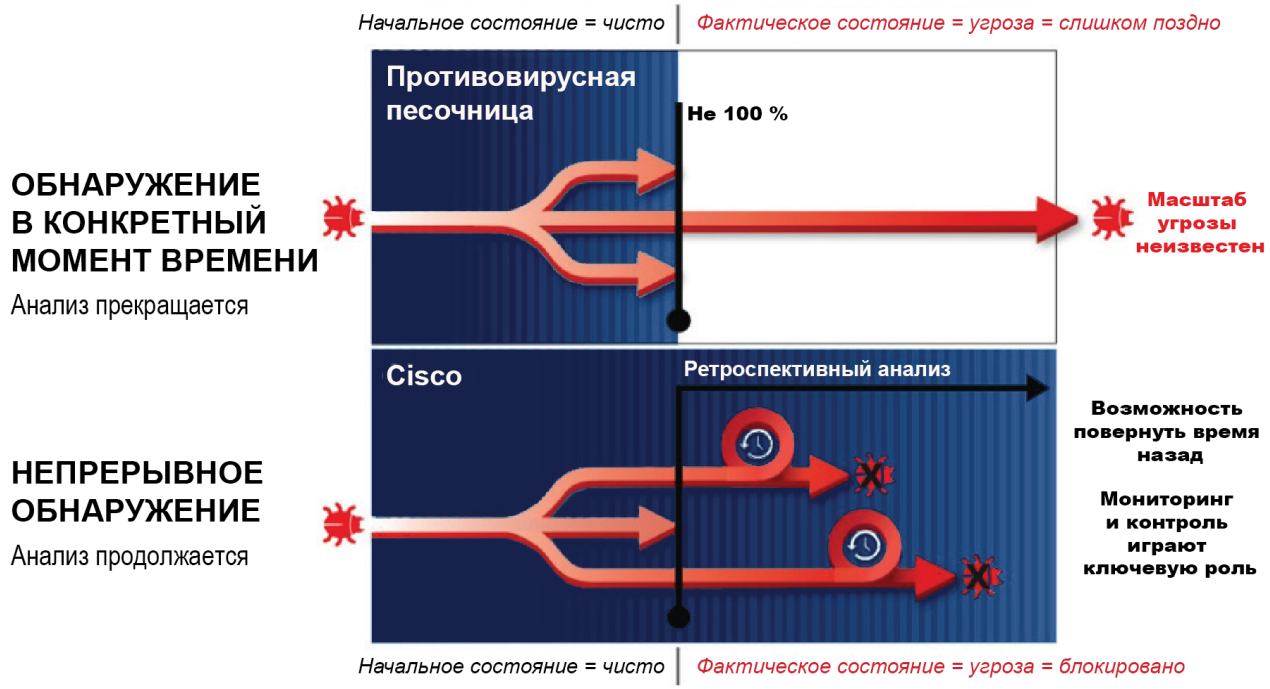
Защита от сложного вредоносного ПО

Решение Cisco Advanced Malware Protection (AMP) предоставляет необходимые специалистам по безопасности возможности мониторинга и контроля, позволяющие не только предотвращать нарушения безопасности, но также быстро обнаруживать, сдерживать и устранять вредоносное ПО до нанесения им ущерба. AMP непрерывно анализирует и записывает всю активность файлов в системе (см. рис. 6) на разных участках сети – периметр, внутренняя сеть, ПК, облака, почтовые шлюзы и т.п. Если файл начинает вести себя подозрительно, AMP ретроспективно предупреждает специалистов по безопасности и предоставляет подробную историю поведения вредоносного ПО во времени. Затем для изоляции или устранения атаки достаточно всего несколько раз щелкнуть мышью.

Решение AMP обеспечивает это благодаря следующим особенностям.

- Лучший анализ угроз и вредоносного ПО с помощью 7 различных алгоритмов
- Защита в любой момент времени с использованием сигнатур файлов, их репутации, «песочницы», анализа сетевого взаимодействия и метаданных для изоляции известных и новых видов угроз
- Непрерывный анализ и ретроспективная безопасность для определения вредоносного ПО, которое не было обнаружено в ходе первоначальной проверки

Рисунок 6 Обнаружение в конкретный момент времени и непрерывное обнаружение



Решение AMP Everywhere

Cisco предлагает самый широкий в отрасли портфель интегрированных решений для защиты от сложного вредоносного ПО, обеспечивающих надежную защиту по всем многочисленным векторам атаки — в сети, на оконечных устройствах, мобильных устройствах, в виртуальных средах, для электронной почты и веб-трафика.

- Cisco AMP для оконечных устройств (Windows, Linux, Android, CentOS, MacOS и т.д.)
- Cisco AMP для сетей
- Cisco AMP — виртуальное устройство в частном облаке
- Cisco AMP на базе межсетевых экранов ASA с сервисами FirePOWER.
- Cisco AMP для устройств защиты электронной почты Cisco ESA
- Cisco AMP для устройств защиты веб-трафика Cisco WSA
- Cisco AMP для облачного устройства защиты веб-трафика Cisco CWS
- Cisco AMP для маршрутизатора с интегрированными сервисами Cisco ISR

Cisco AMP Threat Grid

- Объединяет возможности статического и динамического анализа вредоносного ПО с интеллектуальным анализом угроз в одном унифицированном решении – в виде локального изолированного от Интернет устройства или в виде облачного портала
- Интегрирует функции анализа поведения в режиме реального времени и актуальные данные об угрозах в уже существующую инфраструктуру безопасности
- Предоставляет интегрированный функционал «песочницы» для решений Cisco – Cisco ASA с сервисами FirePOWER, ESA, WSA, AMP для сетей и AMP для оконечных устройств для защиты от известных и неизвестных атак на всем их протяжении.

Система StealthWatch

Система StealthWatch® позволяет значительно улучшить мониторинг сети, повысить безопасность и оперативно реагировать на аномалии и инциденты во всей сети, включая облачные среды и мобильные устройства. StealthWatch позволяет в реальном времени с учетом ситуации получать необходимую информацию обо всех пользователях, устройствах и трафике в сети, ЦОД, в облаке и на мобильных устройствах, предоставляя специалистам по безопасности возможность быстро и эффективно обнаруживать угрозы и реагировать на них за счет обеспечения непрерывного мониторинга в реальном времени и полной картины всего сетевого трафика.

Система StealthWatch обеспечивает это благодаря следующим особенностям.

- Поведенческий анализ берет за основу нормальное поведение сети и легко вычисляет любые аномальные отклонения от этой модели
- Возможности расследования высочайшего уровня со сложными функциями анализа безопасности
- Cisco NetFlow, Identity Services Engine (ISE) и TrustSec, а также портфель решений Cisco для сетевых технологий используют сети как сенсор и регулятор безопасности

Безопасность сети и анализ угроз на уровне DNS

OpenDNS имеет самый большой сервис DNS, интегрированный для обеспечения безопасности. Глобальная сеть OpenDNS непрерывно обрабатывает более 80 миллиардов Интернет-запросов ежедневно от 65 миллионов пользователей. Затем специалисты OpenDNS Security Labs обрабатывают эти данные с использованием статистических моделей для определения, предсказания и предотвращения уже известных и только появляющихся угроз. Каждый день блокируется более 80 миллионов вредоносных запросов, а прогнозный анализ позволяет получить данные более чем с 17 миллионов новых доменных имен. Но лучше всего то, что для этого решения не нужно ни устанавливать оборудование, ни внедрять отдельное программное обеспечение.

OpenDNS Umbrella

Облачная служба сетевой безопасности защищает любое устройство, в любом месте, даже вне вашей сети.

- Новый уровень защиты от нарушений: блокирование вредоносного ПО, фишинговых атак и предотвращение утечек и компрометации систем через любой порт или протокол до того, как атака сможет прорвать оборону вашей системы
- Мониторинг вашей сети при работе в Интернет и локально: вся интернет-активность в реальном времени записывается и разносится по соответствующим типам: угрозы безопасности, веб-контент или облачный сервис
- Автоматическое переключение (роуминг) между стационарным и мобильным, между беспроводным и мобильным подключением
- Интеграция на основе API-интерфейса с вашими решениями по безопасности: все вредоносные действия, направленные на ваши домены и обнаруженные вашими существующими системами, блокируются в считанные секунды

OpenDNS Investigate

Обеспечивает анализ угроз по доменам и IP-адресам в Интернете.

- График глобальной интернет-активности в реальном времени и в ретроспективе: наиболее полное представление о взаимосвязях и эволюции интернет-доменов, IP-адресов и ASN
- Проникновение в инфраструктуру злоумышленников: использование динамической поисковой системы или API-интерфейса RESTful для получения разнообразных наборов данных и статистических моделей
- Увеличение данных SIEM и ускорение рабочих процессов: использование глобального контекста и прогнозного анализа для приоритизации реагирования на инциденты и предсказания атак

Безопасность веб-трафика и электронной почты

Портфель решений Cisco для защиты контента позволяет защитить организации от растущего числа угроз для веб-трафика и электронной почты. Безопасность веб-трафика и электронной почты – это критически важные компоненты целостной стратегии безопасности.

Физическое и облачное устройства защиты электронной почты Cisco Email Security Appliance (ESA) и Cisco Cloud Email Security (CES)

- Защита от спама, вирусов, фишинга, утечек и смешанных угроз для организаций любого размера
- Обеспечение соответствия нормативным требованиям и защиты репутации и бренда
- Обеспечение аутентификации входящей и исходящей почты для защиты от ее подмены
- Доступно в виде облачного и гибридного (устройство в физической среде заказчика плюс облако) решения

Физическое и облачное устройства защиты веб-трафика Cisco Web Security Appliance (WSA) и Cisco Cloud Web Security (CWS)

- Защита веб-трафика в сети и за пределами сети, а также возможности для подробного анализа использования сети, включая функцию мониторинга и контроля приложений
- Защита от сложных угроз с помощью решений Advanced Malware Protection (AMP) и Cognitive Threat Analytics (CTA)
- Гибкое развертывание, включая локальные и облачные модели, использование существующей инфраструктуры и масштабирование в соответствии с этой инфраструктурой
- Настраиваемые отчеты позволяют получить аналитические данные для принятия обоснованных решений

Cisco Cognitive Threat Analytics (CTA)

Обеспечивает анализ Web-логов с целью обнаружения в них признаком компрометации и заражения.

- Облачный анализ Web-логов от Cisco Web Security Appliance, Cisco Cloud Web Security, а также прокси-решений третьих фирм в поиске признаков заражения внутренней сети предприятия
- Обнаружения инкапсуляции трафика вредоносного ПО, шифрования трафика, DGA-доменов и т.п.
- Интеграция с решениями Cisco (ISE, AMP и другими) для автоматизации процесса блокирования обнаруженных угроз

Безопасный доступ и мобильность

Расширение возможностей мониторинга и контроля сети и мобильных пользователей благодаря решениям высоконадежного доступа на основе идентификации

Cisco Identity Services Engine (ISE)

- Централизованное и открытое решение, обеспечивающее автоматизацию безопасного доступа к сетевым ресурсам в традиционных сетях Cisco, сетях с технологией TrustSec и сетях других поставщиков
- Включает BYOD, гостевой доступ и приложения безопасного доступа IoT, а также управление политиками и устройствами обеспечения безопасности (TACACS+)
- Обеспечивает соответствие оконечных устройств нормативным требованиям безопасности и позволяет обмениваться открытыми данными телеметрических систем разных производителей и быстро сдерживать

угрозы для автоматического прекращения работы небезопасных оконечных устройств

Технология Cisco TrustSec®

- Упрощает сегментацию сети за счет автоматизации правил межсетевого экрана и управления списками контроля доступа, используя политики безопасности, заданные простым языком, и определяя группы безопасности на основе бизнес-ролей сотрудников и узлов, а не IP-адресов
- Быстро изолирует и сдерживает угрозы для ограничения влияния нарушения
- Встроена в инфраструктуру Cisco. Поддерживается более чем в 40 семействах продуктов Cisco, включая коммутаторы Cisco Catalyst® и Cisco Nexus, маршрутизаторы Cisco ISR и межсетевые экраны Cisco ASA
- Технология создана на основе открытых протоколов, поэтому может использоваться в сетях других поставщиков

Решение Cisco AnyConnect® Secure Mobility

- Обеспечивает высокобезопасный, простой и надежный доступ в любое время, из любого места, с любого устройства под управлением Windows, Linux, MacOS, iOS, Android, BlackBerry и др.
- Обеспечивает соответствие узлов требованиям политик ИТ и ИБ
- Обеспечивает мониторинг поведения пользователей и оконечных устройств как внутри сети организации, так и вне ее пределов, с помощью модуля мониторинга сети
- Интегрируется с другими решениями безопасности Cisco, такими как Cisco ISE, AMP для оконечных устройств и Cisco CWS для защиты от рисков в масштабе всего предприятия

Другие решения по кибербезопасности Cisco

Компания Cisco предлагает и ряд дополнительных решений по кибербезопасности.

Cisco Industrial Security Appliance 3000 (ISA)

- Промышленный межсетевой экран, построенный на базе платформы Cisco ASA с сервисами FirePOWER, но предназначенный для работы в агрессивных средах промышленных сетей и поддерживающий широкий спектр промышленных протоколов

Wireless IPS

- Обнаружение и предотвращение атак, осуществляемых в беспроводных сетях
- Локализация посторонних беспроводных устройств и их подавление с целью снижения риска нарушения работы беспроводной сети

Defense Orchestrator

- Централизованное облачное управление политиками безопасности для тысяч устройств на платформах Cisco ASA и Cisco Firepower

Cisco Cloud Access Security

- Контроль и разграничение доступа к облачным платформам (например, Amazon, Google, Dropbox, Offise 365, Salesforce и др.)
- Обнаружение утечек данных из облачных хранилищ и контроль аномального поведения пользователей

Услуги по кибербезопасности

Эффективное и защищенное функционирование решений по кибербезопасности невозможно без правильной архитектуры с последующим внедрением и настройкой средств защиты в зависимости от задач заказчика. Кроме того, в процессе эксплуатации решений по кибербезопасности может возникнуть необходимость централизованного и круглосуточного управления приобретенными решениями, а также реагирования на инциденты информационной безопасности. С этой целью компания Cisco предлагает широкий спектр различных услуг в области кибербезопасности.

Планирование

- Сервис оценки защищенности ИБ позволяет определить слабые места корпоративной сети на различных уровнях. В состав данного сервиса могут входить услуги тестов на проникновение и Red Team.
- Сервис Threat Awareness позволяет оценить текущее заражение сети или атаки, направленные на сеть, без установки каких-либо средств защиты и без реконфигурации существующих устройств и программного обеспечения.
- Сервис архитектуры и дизайна ИБ позволяет оценить, насколько существующая инфраструктура соответствует потребностям организации и перестроить ее в случае несоответствия.
- Сервис разработки стратегии ИБ позволяет разработать средне- и долгосрочную стратегию ИБ предприятия в зависимости от бизнес-целей предприятия, модели угроз и требований законодательства.

Внедрение

- Внедрение и настройка средств защиты в зависимости от потребностей организации.
- Миграция позволяет перейти с устаревших или конкурирующих решений на актуальные и более подходящие целям компании решения по кибербезопасности.
- Оптимизация позволит настроить существующие средства защиты под нужды организации и текущее состояние защищенности.

Управление

- Услуги Managed Security позволяют передать на аутсорсинг круглосуточные управление и мониторинг всех средств защиты предприятия с гарантированным качеством обслуживания (SLA).
- Услуги Hosted Security позволяет операторам связи и хостинг провайдерам реализовать и предложить своим заказчикам широкий спектр услуг по кибербезопасности.
- Для поддержки поставляемых средств защиты и системного программного обеспечения компания Cisco предлагает услуги SMARTnet (удаленные и с выездом сервисного инженера на место), включающие оперативное (до 4 часов) обновление программного и аппаратного обеспечения.

Финансирование

- Подразделение Cisco Capital предлагает простые и гибкие схемы финансирования для приобретения, аренды и лизинга устройств безопасности и сетевого оборудования Cisco.

Обучение

- Компания Cisco Systems предлагает множество авторизованных программ обучения по информационной безопасности. Курсы позволяют подготовиться к сдаче экзаменов на получение различных уровней сертификации по безопасности Cisco Specialist или Cisco Certified Security Professional (CCSP).

Соответствие требованиям

Существует множество российских и международных стандартов и требований по информационной безопасности – PCI DSS, Sarbanes Oxley Act, ISO 17799, GLBA (Gramm-Leach- Bliley Act), HIPAA, Базель II, приказы ФСТЭК России (№17, 21 и 31), стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации", Положение Банка России 382-П, ГОСТ Р ИСО/МЭК 15408 и др. Решения Cisco по информационной безопасности соответствуют основным требованиям этих стандартов и рекомендаций. Во многих случаях это подтверждается соответствующими сертификатами.

В России компания Cisco сертифицировала свои защитные устройства Cisco ASA, маршрутизаторы с Cisco ISR, ASR, GSR, CGR, коммутаторы Cisco Catalyst, Nexus и CGS, системы обнаружения атак Cisco IPS и NGIPS, а также различные системы управления на соответствие техническим условиям, руководящим документам и заданиям по безопасности по различным схемам сертификации – преимущественно серия и партия. Всего сертифицировано свыше 125 наименований продуктов Cisco, из которых 30+ по схеме «серийное производство».

Общее число выданных Федеральной службой по техническому и экспортному контролю компании Cisco сертификатов превысило 650, что существенно больше числа сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности.

Также компания Cisco совместно с российской компанией С-Терра СиЭсПи разработала, производит в России и сертифицировала по требованиям ФСБ специальный VPN-модуль для маршрутизаторов Cisco ISR. Аналогичный модуль на базе программного обеспечения Инфотекс, Фактор-ТС и TSS в настоящий момент находятся на сертификации в ФСБ.

- Более подробную информацию и отчеты по безопасности см. по ссылке **www.cisco.com/go/security**.

Дополнительная информация

Cisco Security
cisco.com/go/security

Сообщество по информационной безопасности
communities.cisco.com/community/technology/security

Блог Cisco по информационной безопасности
blogs.cisco.com/security

Поддержка партнеров
www.cisco.com/web/partners/support

Cisco Security Intelligence Operations
tools.Cisco.com/security/center/home.x

Партнерский портал OpenDNS
https://communities.cisco.com/docs/DOC-64565

Любые вопросы по информационной безопасности Cisco можно задать по адресу:
security-request@cisco.com (на русском языке)

C45-1 23456-00 01/15