Больше материалов: Boosty | Sponsr | TG

Аннотация – В этом документе представлен анализ Continuous Threat Exposure Management (CTEM) – стратегического подхода к кибербезопасности, в котором особое внимание уделяется непрерывному мониторингу, выявлению, оценке киберугроз и уязвимостей и управлению ими.

В ходе анализа будут рассмотрены различные аспекты CTEM, включая его определение, этапы внедрения и преимущества для специалистов по кибербезопасности и организаций в различных отраслях.

Выводы, представленные в этом анализе, представляют ценность для специалистов по безопасности в различных отраслях для совершенствования мер кибербезопасности и снижения вероятности рисков.

I. Введение

Непрерывное управление выявлением угроз (CTEM) – это стратегия кибербезопасности, которая фокусируется на выявлении, оценке и снижении рисков в цифровой среде организации посредством непрерывного мониторинга и повышения уровня безопасности. CTEM – это не отдельный инструмент или технология, а набор процессов и возможностей, выраженных в программе/структуре, которая включает в себя определение сферы охвата, обнаружение, расстановку приоритетов, валидацию и практическую реализацию.

CTEM – это упреждающий и непрерывный подход, который отличается от традиционного управления уязвимостями (реактивного похода), фокусируется на широком спектре угроз, включает существующие меры безопасности и использует передовые инструменты моделирования для проверки.

A. Инструменты и технологии

CTEM использует множество инструментов и технологий для поддержки своего внедрения и совершенствования. Эти инструменты помогают на этапах обнаружения, оценки, расстановки приоритетов, валидации и практической реализации цикла управления угрозами. Ключевые инструменты и технологии включают CAASM (Cyber Asset Attack Surface Management), EASM (External Attack Surface Management), EM (Exposure Management), RSAS (Red Team Automation Systems).

Эти инструменты обеспечивают наглядное представление о сегментах сети, средствах контроля безопасности, типах угроз и тактиках / приёмах и имеют решающее значение для выявления и анализа векторов атаки организации, которая включает внешнюю, внутреннюю и облачную среду

B. Методология

Программа CTEM состоит из пяти этапов:

- **Определение области действия**: Определение начальной области воздействия, учёт критически важной для бизнеса активов, вместо сосредоточения на известных уязвимостях.
- **Обнаружение**: Активный поиск и идентификация потенциальных уязвимостей с использованием таких инструментов, как автоматические сканеры, ручное тестирование и тестирование на проникновение.
- **Определение приоритетов**: сосредоточение внимания на наиболее значительных угрозах, которые могут повлиять на бизнес, и соответствующее определение приоритетности усилий по устранению последствий.
- **Валидация**: Оценка эффективности операций по исправлению и обеспечение надлежащего устранения уязвимостей.
- **Практическая реализация**: введение в действие результатов CTEM и определение стандартов коммуникации и документированных рабочих процессов между командами

C. «Лучшие практики»

Лучшие практики определения приоритетности угроз при внедрении CTEM включают:

- **Взаимодействие с заинтересованными сторонами**: такими как ИТ, юридические подразделения, комплаенс и бизнес-подразделения, для понимания их конкретных требований и проблем.
- **Регулярные обновления**: установка регулярного графика обновлений и исправлений для защиты сети от текущих известных угроз и превентивного устранения потенциальных угроз в будущем.
- **План реагирования на инциденты**: разработка эффективного (и регулярно обновляемого в соответствии с возникающими угрозами) плана реагирования на инциденты для оперативного реагирования на угрозы.

УГРОЗЫ БЕЗОПАСНОСТИ

Больше материалов: Boosty | Sponsr | TG

- **Оптимизированные процессы снижения рисков**: все существующие процессы снижения рисков должны быть оптимизированы и масштабируемы. Это поможет управлять возросшим спросом на передачу данных между системами после внедрения программы CTEM
- **Использование искусственного интеллекта**: использование подхода, основанного на искусственном интеллекте, для определения приоритетов угроз. Это может помочь справиться с динамичным характером угроз и обеспечить направление ресурсов туда, где они имеют наибольшее значение.
- **Непрерывное совершенствование**: CTEM — это непрерывный процесс, и организациям следует регулярно пересматривать и корректировать свои стратегии приоритизации угроз по мере появления новых угроз и эволюции бизнес-целей

II. Возможности и ограничения внедрения CTEM

A. Возможности

- **Упреждающее управление рисками**: CTEM позволяет организациям последовательно отслеживать, оценивать и снижать риски безопасности с помощью планов стратегических улучшений
- **Определение приоритетов угроз**: CTEM обеспечивает системный подход для эффективной расстановки приоритетов потенциальных угроз
- **Повышенная устойчивость к киберугрозам**: CTEM повышает способность организации противостоять кибер-угрозам и восстанавливаться после них
- **Аналитические данные для принятия мер**: CTEM генерирует информацию о кибер-угрозах на основе данных
- **Соответствие бизнес-целям**: CTEM гарантирует, что усилия по обеспечению безопасности и планы управления рисками соответствуют целям компании
- **Адаптивность**: Гибкий и масштабируемый характер CTEM гарантирует, что его можно адаптировать к конкретным потребностям любой организации
- **Экономия средств**: CTEM может значительно снизить затраты, связанные с нарушениями безопасности, за счёт упреждающего выявления и смягчения угроз

B. Ограничения

Несмотря на его преимущества, существует ряд ограничений и проблем, связанных с внедрением CTEM:

- **Пробелы в интеграции**: CTEM требует комплексного подхода в рамках программы обеспечения безопасности, что означает, что она должна быть построена с использованием комбинации существующих технических решений. При неправильном управлении это может привести к возникновению пробелов в интеграции, поскольку различные решения могут не работать слаженно вместе
- **Зависимость от несопоставимых решений**: Неспособность внедрить CTEM приводит зависимости от несопоставимых решений. Это может привести к неэффективности и несогласованности в управлении угрозами
- **Ограниченная поддержка в условиях ограничений реального времени**: CTEM работает в пределах определённого временного горизонта, следуя «мандатам» по управлению, рискам и соблюдению требований, и информирует об изменениях в долгосрочных стратегиях. Это может не полностью учитывать ограничения в режиме реального времени, налагаемые действиями по обнаружению угроз и реагированию на них.
- **Ресурсоёмкость**: Реализация CTEM может быть ресурсоёмкой, требующей значительного времени и усилий для постоянного мониторинга и оценки состояния безопасности организации
- **Необходимость непрерывной проверки**: CTEM уделяет значительное внимание проверке, используя такие инструменты, как моделирование взломов и атак (BAS) и проверка средств контроля безопасности, для проверки защиты организации от имитируемых угроз. Это требует постоянных усилий и ресурсов для обеспечения эффективности внедрённых средств контроля
- **Проблемы при определении приоритетов угроз**: хотя CTEM стремится определять приоритеты угроз на основе их потенциального воздействия, это может быть непросто из-за динамичного характера угроз и необходимости согласовывать эти усилия с целями бизнеса

III. Сложности внедрения CTEM

Согласование действий специалистов, не связанных с безопасностью: ИТ-инфраструктура, DevOps и службы безопасности часто имеют пробелы в коммуникации, что может представлять проблему при внедрении CTEM

- **Взгляд на картину в целом (преодоление диагностической перегрузки)**: Комплексная программа CTEM охватывает множество областей, каждая из которых имеет свой набор инструментов; при этом следует иметь в виду, что объединение всей информации для понимания приоритетов и обязанностей может быть сложной задачей
- **Принятие подхода, ориентированного на учёт рисков**: Традиционные меры кибербезопасности часто направлены на достижение соответствия требованиям. CTEM уделяет особое внимание пониманию рисков, специфичных для уникального контекста организации, и управлению ими, что требует тонкого понимания ландшафта бизнеса
- **Интеграция инструментов и технологий непрерывного мониторинга**: поскольку организации внедряют инновации, такие как Интернет вещей (IoT) и облачные вычисления, они должны адаптировать свои платформы CTEM для решения уникальных задач, связанных с этими технологиями

ИРОНИЯ БЕЗОПАСНОСТИ

Больше материалов: Boosty | Sponsr | TG

IV. Ключевые шаги по внедрению CTEM

Внедрение CTEM включает систематический пятиэтапный процесс, который помогает организациям активно управлять рисками кибербезопасности и снижать их. Внедрение CTEM — это непрерывный цикл, поскольку ландшафт угроз постоянно меняется следует регулярно пересматривать каждый шаг, чтобы адаптироваться к новым угрозам и изменениям в цифровой среде:

- Определение области применения (Scoping)
- Обнаружение (Discovery)
- Определение приоритетов (Prioritization)
- Проверка (Validation)
- Практическая реализация (Mobilization)

A. Определение области применения (Scoping)

На этом этапе группам безопасности необходимо понять, какие системы, активы и сегменты инфраструктуры имеют решающее значение для бизнеса и могут стать потенциальными целями для киберугроз и будут включены в область применения и определение заинтересованных сторон, которые будут вовлечены. Это включает в себя определение ключевых векторов атаки, на которых можно управлять уязвимостями.

Процесс определения области обеспечивает точную идентификацию критических и уязвимых систем, что делает его основополагающим шагом в разработке мер безопасности. Этап определения объёма работ составляет основу программы CTEM и имеет важное значение для её общего успеха, поскольку он устанавливает рамки для последующих этапов. Важно включить все соответствующие области в сферу действия CTEM, такие как внешние атаки и облачные среды, чтобы не оставлять незащищёнными любые потенциальные точки взлома.

B. Обнаружение (Discovery)

Организация активно ищет и выявляет уязвимости и слабые места в оцениваемых активах с применением инструментов и технологий для поиска и анализа потенциальных проблем безопасности на внешнем контуре атак, которая охватывает внешнюю, внутреннюю и облачную среды. Этот этап включает в себя идентификацию и каталогизацию всех уязвимых ресурсов организации, таких как оборудование, программное обеспечение, базы данных и сетевая инфраструктура. На этапе обнаружения предприятия используют широкий спектр инструментов и методов обнаружения ИТ для аудита всех своих ИТ-ресурсов. Часто это включает проведение оценок уязвимостей, тестирования на проникновение и других аудитов безопасности. Цель состоит в активном поиске и выявлении потенциальных уязвимостей в системах и активах организации.

На этапе обнаружения важно привлечь разнообразную команду экспертов, включая ИТ-персонал, сотрудников службы безопасности и других сотрудников, которые могут иметь уникальный взгляд на потенциальные уязвимости. Это гарантирует выявление и оценку всех потенциальных угроз. Этап обнаружения служит связующим звеном между этапами определения объёма и определения приоритетов в процессе CTEM. После этапа анализа, на котором определяются ключевые вектора атаки и заинтересованные стороны, этап обнаружения фокусируется на детальной идентификации всех активов и уязвимостей.

C. Определение приоритетов (Prioritization)

Этот этап имеет решающее значение, поскольку помогает организациям определить, каким ценным активам необходимо уделить приоритетное внимание на основе их потенциального воздействия на бизнес, так как не все можно защитить сразу.

На этапе определения приоритетов организации оценивают уровень риска. Это включает в себя компенсирующие средства контроля безопасности и потенциальные уязвимости, выявленные на этапе обнаружения, исходя из того, насколько вероятно, что они будут использованы.

Основная цель расстановки приоритетов – составить список задач для эффективного снижения рисков. Это позволяет организациям оптимально распределять свои ресурсы, обеспечивая эффективное использование. А также определить, какие активы являются наиболее важными и нуждаются в наивысшем уровне защиты.

Текущий этап – это непрерывный процесс, который включает в себя постоянную переоценку, ранжирование и выбор активов, требующих немедленного внимания. Этот этап динамичен и должен адаптироваться для эффективного противодействия возникающим угрозам.

D. Проверка (Validation)

Этот этап обеспечивает точную оценку уязвимости организации к угрозам и эффективности операций по исправлению. На этапе проверки организации оценивают, как они справились бы с реальной атакой, и оценивают свою способность защититься от неё. Это включает в себя использование таких практик, как моделирование взломов и атак (BAS) и тренинги Red Team для имитации атак и проверки защиты на месте.

Этап проверки гарантирует, что планы по устранению уязвимостей и угроз, выявленных на этапе определения приоритетов, эффективны. Это может включать добавление дополнительных мер предосторожности, обновление программного обеспечения или изменение настроек безопасности.

Также важно привлечь к этапу проверки широкий круг заинтересованных сторон, включая ИТ-персонал, сотрудников службы безопасности и другие соответствующие команды. Это гарантирует, что процесс валидации будет всеобъемлющим и что меры по исправлению будут эффективными во всей организации

*E. **Практическая реализация (Mobilization)***

Этот этап заключается в практической реализации результатов процесса CTEM и осуществлении

УРОКИ БЕЗОПАСНОСТИ

необходимых действий для устранения выявленных рисков.

На этапе практической реализации организации приводят в действие планы по устранению уязвимостей и угроз, выявленных на этапе определения приоритетов и подтверждённых на этапе валидации. Это может включать добавление дополнительных мер предосторожности, обновление программного обеспечения или изменение параметров безопасности.

Этот этап также включает в себя обеспечение того, чтобы все команды в организации были проинформированы и согласованы с усилиями по обеспечению безопасности. Это может включать автоматизацию мер по смягчению последствий за счёт интеграции с платформами управления информацией о безопасности и событиями (SIEM) и управления безопасностью, автоматизации и реагирования (SOAR), а также установление стандартов связи и документированных межкомандных рабочих процессов.

На данном этапе становится понятно, что восстановление не может быть полностью автоматизировано и требует вмешательства человека и подчёркивается необходимость того, чтобы руководители служб безопасности мобилизовали ответные меры и устранили риски из окружающей среды.

V. Другие аспекты реализации

A. *Определение приоритетов угроз*

Этап определения приоритетов — это третий этап в CTEM. На этом этапе организации оценивают потенциальные уязвимости, выявленные на этапе обнаружения, исходя из того, насколько вероятно, что они будут использованы, и потенциального воздействия, которое это окажет на организацию. Ключевые шаги, связанные с определением приоритетов угроз:

- **Оценка критичности и вероятности**: Компании часто используют методологию оценки рисков для анализа критичности и вероятности каждой уязвимости. Это включает в себя оценку потенциального ущерба, который мог бы быть причинён в случае использования уязвимости.
- **Учёт влияния на бизнес**: программы CTEM помогают организациям определять приоритеты угроз на основе их потенциального воздействия на бизнес. Это включает в себя рассмотрение таких факторов, как критичность затронутой системы или данных, потенциальные финансовые последствия и потенциальный ущерб репутации.
- **Наличие компенсирующих средств контроля**: Наличие компенсирующих средств контроля, которые являются альтернативными мерами, способными снизить риск использования уязвимости, также является фактором при определении приоритетов.
- **Толерантность к остаточному риску**: Толерантность организации к остаточному риску, который остаётся после применения всех средств контроля, является ещё одним фактором, который может влиять на расстановку приоритетов.
- **Распределение ресурсов**: на основе расстановки приоритетов организации могут эффективно распределять ресурсы для устранения наиболее значительных рисков. Такой стратегический подход к управлению угрозами приводит к более эффективному использованию ресурсов и более быстрому реагированию на наиболее потенциально опасные угрозы

B. *Методы приоритизации*

Распространённые методы и рекомендации по приоритизации угроз при внедрении CTEM включают:

- **Определение приоритетов с учётом потребностей бизнеса**: CTEM устанавливает приоритеты в соответствии с бизнес-целями, уделяя особое внимание наиболее критичным угрозам и уязвимостям, которые могут повлиять на наиболее ценные активы организации. Такой подход гарантирует, что ресурсы распределяются там, где они имеют наибольшее значение, согласовывая усилия организации с постоянно меняющимся ландшафтом угроз
- **Анализ воздействия**: Определение приоритетов должно включать анализ потенциального воздействия каждой угрозы. Оценивая критичность и потенциальный ущерб от каждой угрозы, организации могут эффективно распределять ресурсы для устранения наиболее значительных рисков
- **Динамическая расстановка приоритетов**: Ландшафт угроз динамичен, и новые уязвимости появляются регулярно. Следовательно, стратегии расстановки приоритетов должны быть адаптируемыми для эффективного противодействия возникающим угрозам.
- **Распределение ресурсов**: Человеческие ресурсы ограничены, и группы безопасности должны расставлять приоритеты в своих усилиях. Ключевым моментом является выделение ресурсов для устранения критичных уязвимостей, которые могут оказать существенное влияние на организацию

Чтобы обеспечить соответствие приоритизации угроз бизнес-целям, организациям следует включить стратегические бизнес-цели в свою программу CTEM. Такой подход позволяет организациям оценивать критичность и потенциальный ущерб от каждой угрозы, а затем соответствующим образом распределять ресурсы, гарантируя, что меры безопасности будут сосредоточены на защите наиболее важных бизнес-активов

VI. Эффективность программы CTEM

Для измерения эффективности программы непрерывного управления выявлением угроз (CTEM) организации могут использовать несколько ключевых показателей эффективности. Используя эти показатели и постоянно отслеживая их, организации могут получить представление об эффективности своей программы CTEM и принимать обоснованные решения по повышению своей кибербезопасности. Важно отметить, что эффективность

ИРОНИЯ БЕЗОПАСНОСТИ

программы CTEM не является статичной и должна регулярно оцениваться для адаптации к меняющемуся ландшафту угроз и потребностям бизнеса.

- **Снижение рисков**: оценка снижения рисков безопасности, отслеживая количество выявленных и устранённых уязвимостей с течением времени. Успешная программа CTEM должна демонстрировать тенденцию к снижению количества и серьёзности рисков для безопасности
- **Улучшенное обнаружение угроз**: оценка эффективности возможностей обнаружения угроз, отслеживая время, необходимое для обнаружения новых уязвимостей или угроз. Более низкое среднее время обнаружения (MTTD) указывает на более эффективную программу CTEM
- **Время для исправления**: оценка скорости устранения выявленных угроз и уязвимостей. Успешная программа CTEM должна помочь сократить время между обнаружением и устранением неполадок, известное как среднее время реагирования (MTTR)
- **Эффективность контроля безопасности**: Использование таких инструментов, как проверка контроля безопасности и моделирование взломов и атак, чтобы протестировать защиту организации от имитируемых угроз. Полученные результаты могут подтвердить эффективность внедрённых средств контроля и действующих на месте мер безопасности
- **Показатели соответствия**: для отраслей с нормативными требованиями достижение и поддержание соответствия является ключевым показателем успеха. Отслеживание нарушения или проблем, связанных с соблюдением требований, чтобы оценить эффективность программы CTEM в поддержании нормативных стандартов
- **Соответствие требованиям и приоритетам**: это можно измерить качественно, оценив, направлены ли усилия по восстановлению на защиту наиболее важных бизнес-активов и соответствуют ли они ключевым целям бизнеса
- **Обратная связь с заинтересованными сторонами**: Сбор и анализ обратной связи от заинтересованных сторон, вовлечённых в процесс CTEM. Положительные отзывы могут указывать на то, что программа достигает своих целей и хорошо воспринимается теми, кого она затрагивает

VII. Плотность уязвимостей и время на устранение

Плотность уязвимостей и время на устранение — это два ключевых показателя, которые можно использовать для измерения эффективности программы непрерывного управления выявлением угроз (CTEM).

Плотность уязвимостей — это показатель количества уязвимостей на единицу кода или систему. Он даёт представление об общем состоянии безопасности систем организации. Более низкая плотность уязвимостей указывает на более безопасную систему, в то время как более высокая плотность уязвимостей предполагает больший потенциал для использования. Для эффективного использования этого показателя организациям следует отслеживать изменения плотности уязвимостей с течением времени. Тенденция к снижению указывает на то, что программа CTEM эффективно выявляет и устраняет уязвимости, тем самым улучшая уровень безопасности организации. Показатель рассчитывается путём деления общего количества уязвимостей на общее количество систем или приложений. Этот показатель может быть использован для оценки количества остаточных уязвимостей во вновь выпущенной программной системе с учётом её размера. Высокая плотность уязвимостей указывает на то, что существует больше уязвимостей, требующих устранения, что может привести к более высокому риску эксплуатации. Организации должны стремиться поддерживать низкую плотность уязвимости, чтобы снизить риск эксплуатации

Время до устранения (также известное как Среднее время реагирования или MTTR) — это показатель среднего времени, необходимого для реагирования и устранения выявленных уязвимостей или угроз. Более низкий MTTR указывает на эффективную реакцию и разрешение, что предполагает более эффективную программу CTEM. Этот показатель имеет решающее значение, поскольку чем дольше уязвимость остаётся без внимания, тем выше вероятность того, что ею могут воспользоваться злоумышленники. Следовательно, успешная программа CTEM должна помочь сократить время между обнаружением и исправлением. Оно рассчитывается путём вычитания даты обнаружения из даты исправления. Проще говоря, MTTR — это количество дней, необходимое для устранения уязвимости в системе безопасности после её обнаружения. MTTR также может рассчитываться в каждом конкретном случае или на макроуровне. **Уравнение для MTTR выглядит следующим образом: MTTR = (Общая сумма обнаружений и времени исправления) / (Общее количество инцидентов)**. Меньшее время на исправление указывает на то, что уязвимости устраняются быстро, и снижает риск эксплуатации. Организациям следует стремиться к сокращению времени на исправление, чтобы снизить риск

Оба показателя дают ценную информацию об эффективности программы CTEM. Постоянно отслеживая эти показатели, организации могут определить области, требующие улучшения, и принять меры по повышению уровня своей безопасности.

VIII. Альтернативы

Существуют альтернативы CTEM, которые могут лучше подходить для определённых организаций или сценариев:

- **Open-source Cloud Security Posture Management (CSPM)**: Инструменты с открытым исходным кодом являются экономически эффективными и гибкими решениями для обеспечения облачной безопасности. Они предлагают преимущества поддержки сообщества и возможности настройки. Однако их внедрение может быть ресурсоёмким и может поставить организацию в зависимость от сообщества в плане обновлений и улучшений

ИРОНИЯ ВЗЛОМА ЛОСТИ

- **Vanta**: платформа для развития молодёжного киберспорта, которая предоставляет экспертный коучинг и наставничество. Он получил аккредитацию от STEM.org, что свидетельствует о его приверженности развитию необходимых навыков, таких как инновации, командная работа.
- **Defense Surface Management (DSM)**: DSM предоставляет более эффективный способ подключения данных анализа угроз (TID) и CTEM. Это помогает организациям расставить приоритеты и оптимизировать свою защиту путём выявления сильных и слабых сторон и сравнения возможностей с тактиками, методами и процедурами противодействия (TTP)
- **CloudBees Jenkins Enterprise and Operations Center**: Эти инструменты предоставляют больше возможностей для визуализации конвейеров доставки программного обеспечения и восстановления после сбоев. Они обеспечивают большую наглядность операций Jenkins и позволяют централизованно управлять кластерами Jenkins masters, разработками и аналитикой производительности.
- **Unifying Remediation** : Этот подход использует автоматизацию для оптимизации реагирования на проблемы безопасности, сокращая ручное вмешательство и время реагирования. Это также включает рассмотрение контекста проблем безопасности, что помогает выявить наиболее важные проблемы, понять их первопричины и определить эффективные стратегии устранения
- **Pen Testing**: В то время как CTEM ориентирована на выявление и предотвращение как можно большего количества уязвимостей, тестирование с помощью пера — это управляемый человеком наступательный тест, который пытается достичь определённой цели. Использование обеих методологий значительно повышает прозрачность и обеспечивает более комплексный подход к обеспечению безопасности
- **Automation in Tax Preparation**: Автоматизация может помочь устранить риск человеческой ошибки, которая может возникнуть при ручном вводе данных, что приведёт к более точной финансовой отчётности. Это также может упростить процессы аудита, позволяя налоговым специалистам выявлять и расставлять приоритеты в областях с высоким уровнем риска.

ИРОНИЯ БЕЗОПАСНОСТИ