ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1645 (09/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

Безопасность облачных вычислений – Передовой опыт и руководящие указания в области облачных вычислений

Требования к платформе ситуационной осведомленности о сетевой безопасности для облачных вычислений

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

Сети передачи данных, взаимосвязь открытых систем и безопасность

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	X.1000–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200–X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300–X.1499
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600–X.1699
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	**X.1640–X.1659**
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750–X.1799
БЕЗОПАСНОСТЬ IMT-2020	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1645

Требования к платформе ситуационной осведомленности о сетевой безопасности для облачных вычислений

Резюме

Ситуационная осведомленность о сетевой безопасности (NSSA) строится на основе ситуационной осведомленности. Обычно она включает четыре процесса – сбор данных, анализ ситуации в области безопасности, оценку ситуации в области безопасности и прогнозирование тенденций ситуации в области безопасности – и, как правило, имеет следующие возможности: 1) обнаружение и постоянный мониторинг угроз различных атак, аномального поведения и степени их влияния; 2) интеллектуальный анализ данных, анализ угроз и отслеживание аномального поведения; 3) прогнозирование в области безопасности и раннее предупреждение; 4) визуализация ситуации в области безопасности.

Для поставщиков услуг облачных вычислений платформа NSSA играет важную роль в совершенствовании защиты безопасности облачных вычислений, возможности обнаружения нарушений безопасности или аномального поведения, принятия решений в области безопасности и возможности реагирования на чрезвычайные ситуации, и даже может содействовать улучшению механизма раннего предупреждения для облачных вычислений.

В Рекомендации МСЭ-Т X.1645 вводится концепция NSSA, освещается развитие и анализируются преимущества NSSA в решении проблем безопасности облачных вычислений, а также излагаются требования к платформе NSSA для облачных вычислений.

Хронологическая справка[*]

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1645	08.09.2023 г.	17-я	11.1002/1000/15527

Ключевые слова

Анализ больших данных, облачные вычисления, ситуационная осведомленность о сетевой безопасности, ситуационная осведомленность.

[*] Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
	3.1 Термины, определенные в других документах	1
	3.2 Термины, определенные в настоящей Рекомендации	1
4	Сокращения и акронимы	2
5	Соглашения	2
6	Введение в ситуационную осведомленность о сетевой безопасности	3
7	Анализ	4
8	Требования к платформе ситуационной осведомленности о безопасности для облачных вычислений	5
	8.1 Требования к сбору данных	5
	8.2 Требования к хранению данных	7
	8.3 Требования к ситуационным вычислениям и анализу	10
	8.4 Требования к ситуационной оценке	13
	8.5 Требования к ситуационной визуализации	16
Библиография		18

Рекомендация МСЭ-Т X.1645

Требования к платформе ситуационной осведомленности о сетевой безопасности для облачных вычислений

1 Сфера применения

В настоящей Рекомендации представлены концепция ситуационной осведомленности о сетевой безопасности (NSSA) и требования к платформе NSSA для облачных вычислений. Данная Рекомендация предназначена для поставщиков услуг облачных вычислений.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 облачные вычисления (cloud computing) [b-ITU-T Y.3500]: Парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу.

3.1.2 облачная услуга (cloud service) [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, которые активируются с помощью заявленного интерфейса.

3.1.3 потребитель облачной услуги (cloud service customer) [b-ITU-T Y.3500]: Сторона, которая состоит в деловых отношениях в целях использования облачной услуги.

3.1.4 поставщик облачной услуги (cloud service provider) [b-ITU-T Y.3500]: Сторона, которая предоставляет облачные услуги.

3.1.5 уязвимость (vulnerability) [b-NIST-SP-800-30]: Слабое место в информационной системе, процедурах обеспечения безопасности системы, внутренних средствах управления или реализации, которое может быть использовано источником угрозы.

3.1.6 оперативная информация об угрозах (threat intelligence) [b-ITU-T X.1217]: Совокупность систематизированной, проанализированной и уточненной информации о потенциальных и текущих атаках, которые могут угрожать организации.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 ситуационная осведомленность (situational awareness): Возможность оценить текущее состояние элементов в данной среде, а также их соотношение по нескольким измерениям, включая время и пространство.

ПРИМЕЧАНИЕ. – Это достигается путем сбора данных из различных источников, объединения этих данных и их последующего анализа. Целью ситуационной осведомленности является интеграция и анализ информации из разных источников для получения всестороннего понимания ее значения.

3.2.2 ситуационная осведомленность о сетевой безопасности (network security situational awareness (NSSA)): Возможность выявлять и оценивать ключевые элементы сетевой безопасности, а также классифицировать их в соответствии с правилами, используя временные и пространственные измерения.

ПРИМЕЧАНИЕ. – Данная информация позволяет оценивать общую ситуацию в области безопасности сети и прогнозировать новые тенденции в области сетевой безопасности с помощью таких методов, как статистический анализ, интеллектуальный анализ данных и искусственный интеллект. Полученные результаты могут быть представлены либо в удобочитаемом для человека формате, либо в качестве входных данных для автоматизации обеспечения сетевой безопасности.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AI	Artificial Intelligence	ИИ	Искусственный интеллект
C&C	Command and Control		Управление и контроль
CRUD	Create, Read, Update and Delete		Создание, чтение, обновление и удаление
CSC	Cloud Service Customer		Потребитель облачной услуги
CSP	Cloud Service Provider		Поставщик облачной услуги
DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
DGA	Domain Generation Algorithm		Алгоритм создания домена
HBase	Hadoop Database		База данных Hadoop
IDS	Intrusion Detection System		Система обнаружения вторжений
IPS	Intrusion Prevention System		Система предотвращения вторжений
JDBC	Java Database Connectivity		Интерфейс взаимодействия Java и баз данных
MPP	Massively Parallel Processing		Массовая параллельная обработка
NoSQL	Not only Structured Query Language		Не только язык структурированных запросов
NSSA	Network Security Situational Awareness		Ситуационная осведомленность о сетевой безопасности
ODBC	Open Database Connectivity		Открытый интерфейс доступа к базам данных
SNMP	Simple Network Management Protocol		Простой протокол управления сетью
SQL	Structured Query Language		Язык структурированных запросов
VM	Virtual Machine	ВМ	Виртуальная машина
VPN	Virtual Private Network	ВЧС	Виртуальная частная сеть
WAF	Web Application Firewall		Брандмауэр веб-приложений

5 Соглашения

Ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Для заявления о соответствии это требование не является обязательным.

В тексте настоящей Рекомендации и приложений к ней встречаются слова "должен", "не должен", "следует" и "может", и в таком случае их следует понимать соответственно как "требуется", "запрещается", "рекомендуется" и "возможно". Такие фразы или ключевые слова, фигурирующие в дополнении или материалах, явно помеченных как информационные, должны толковаться как не несущие нормативного смысла.

6 Введение в ситуационную осведомленность о сетевой безопасности

Современные сетевые атаки разработаны для достижения четких целей, поскольку у злоумышленников обычно имеются точные планы, и, как правило, проникновение в сеть происходит на длительное время. Соответственно защита безопасности представляется типичным примером "временно́й конфронтации". В традиционной архитектуре безопасности различные компоненты или продукты для обеспечения безопасности устанавливаются только с собственными правилами защиты, политикой предупреждений, механизмами обработки и хранения журналов регистрации событий при отсутствии механизма координации действий между компонентами и продуктами. Это создает эффект изоляции, который ослабляет возможности защиты от более скрытных и профессиональных изощренных атак.

Ситуационная осведомленность о сетевой безопасности (NSSA) строится на основе ситуационной осведомленности и представляет собой особое приложение в системе сетевой безопасности. Обычно оно включает в себя четыре процесса – сбор данных, восприятие ситуации в области безопасности, оценку ситуации и прогнозирование ситуации в области безопасности – и, как правило, обеспечивает следующие возможности:

– обнаружение и постоянный мониторинг угроз различных атак, в том числе аномального поведения, и степени их влияния;

– интеллектуальный анализ данных, детализацию, анализ угроз и отслеживание аномального поведения;

– прогнозирование ситуации в области безопасности и раннее предупреждение;

– визуализацию ситуации в области безопасности.

В контексте сетевой безопасности информационная асимметрия – это сценарий, когда злоумышленник обладает более глубокими знаниями о системах, сети или процессах организации, чем сама эта организация. В такой ситуации злоумышленники находятся в выгодном положении в плане разработки стратегии и реализации атак. NSSA очень важна для устранения информационной асимметрии между атаками и защитой, а также для ускорения реагирования на инциденты и их отслеживания.

Тем временем успехи в области анализа больших данных, облачных вычислений и искусственного интеллекта (ИИ) открыли широкие возможности и предоставили ресурсы для развития NSSA. Например, платформы NSSA могут эффективно поддерживать массовое хранение журналов регистрации событий безопасности, используя и анализируя большие данные, чтобы обеспечить постоянный мониторинг масштабных ситуаций в области сетевой безопасности; развитие искусственного интеллекта может предоставить больше методов анализа и возможностей прогнозирования рисков для NSSA, что поможет эффективно повысить точность прогнозирования; а развитие облачных вычислений может обеспечить более гибкую и стабильную архитектуру инфраструктуры платформы NSSA.

Типичная структура платформы NSSA представлена на рисунке 6-1.

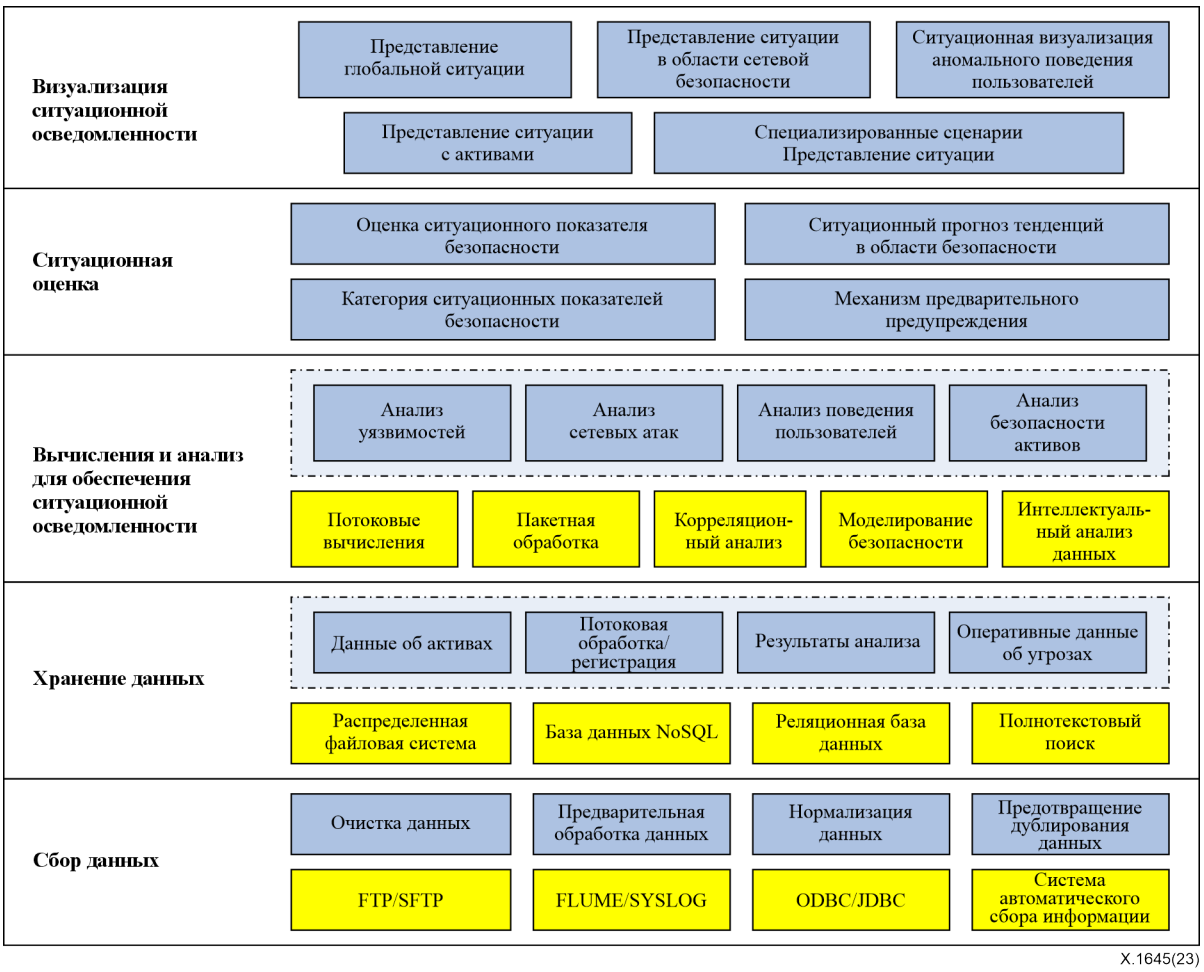

Рисунок 6-1 – Структура платформы ситуационной осведомленности о сетевой безопасности

7 Анализ

Благодаря быстрому развитию информационных технологий и зрелости их экосистемы облачные вычисления представляют собой критически важную информационную инфраструктуру нового поколения. Облачные вычисления принесли много преимуществ, но при этом оказались связаны с гораздо большим количеством проблем в области безопасности, особенно в плане эксплуатации и обслуживания, а именно.

1) При быстром увеличении масштаба разнообразные компоненты безопасности, развернутые в инфраструктуре облачных вычислений, накапливают массивные данные по безопасности и выдают повторяющиеся предупреждения. В этом сценарии инженерам по эксплуатации и техническому обслуживанию затруднительно будет решать задачи в ограниченные сроки.

2) Большинство компонентов системы безопасности изолированы друг от друга, что неизбежно приводит к эффекту секционирования. Это затрудняет создание скоординированного механизма защиты в среде облачных вычислений.

3) Среда облачных вычислений обычно отличается сложностью и может включать в себя общедоступное облако, частное облако и гибридное облако. Это затрудняет принятие оптимальных решений по безопасности из-за отсутствия макроскопической и полной картины для поставщиков услуг и даже пользователей облачных вычислений.

Для решения этих проблем подходит NSSA. Основываясь на технологии больших данных, NSSA может эффективно поддерживать хранение, использование и интеллектуальный анализ данных из массивов разнородных журналов регистрации событий безопасности. Кроме того, с помощью корреляционного анализа множества различных данных можно эффективно организовать работу различных компонентов системы безопасности, улучшить возможности обнаружения угроз и повысить эффективность работы инженеров по безопасности. NSSA также может обеспечить

возможность получить визуальное представление обо всей ситуации в плане безопасности облачных вычислений. В то же время в NSSA удобно использовать технологию ИИ, которая может улучшить возможности обнаружения, диагностики и прогнозирования ситуационной осведомленности о безопасности для облачных вычислений.

Таким образом, NSSA играет важную роль в совершенствовании защиты безопасности облачных вычислений, принятия решений по безопасности и возможности реагирования на чрезвычайные ситуации и, следовательно, может способствовать улучшению механизма раннего предупреждения для поставщиков услуг облачных вычислений.

В то же время платформа NSSA, развернутая в среде облачных вычислений, должна обеспечивать следующие возможности.

1) Сбор данных должен быть адаптирован к динамическим изменениям активов облачных вычислений, поскольку эти активы могут создаваться и удаляться более гибко и часто, чем при традиционной ИТ-архитектуре.
2) Платформа NSSA должна учитывать такую характеристику услуги облачных вычислений, как совместное использование ресурсов несколькими арендаторами и гибкое управление ресурсами, которые могут привести к быстрой смене источников данных. Быстрая смена арендаторов и способов их обслуживания соответственно приведет к изменениям в системе сбора данных платформы NSSA.
3) Платформа NSSA должна продолжать взаимодействие и кооперацию с платформой управления облачными вычислениями для получения доступа к различным видам данных, таким как текущее состояние и журналы регистрации событий безопасности, касающихся ресурсов облачных вычислений, для достижения глубокого понимания/осведомленности о ресурсах облачных вычислений. Например, NSSA не может не взаимодействовать с платформой управления облаком, чтобы наблюдать за сетевыми соединениями между виртуальными машинами в одной и той же сетевой области уровня 2 ВОС.
4) Платформа NSSA должна поддерживать возможность доступа к данным из нескольких облаков, чтобы предоставить пользователям единое представление об активах как в гибридном, так и в общедоступном облаке.

Применение и развертывание платформы NSSA обеспечивают возможность решения вышеуказанных технических проблем. Платформа NSSA позволяет всесторонне, точно и детально регистрировать различные события, относящиеся к безопасности, и аномальное поведение – как во временном, так и в пространственном измерениях, анализировать различные элементы безопасности, оценить ситуацию с безопасностью в целом и спрогнозировать тенденции, что поможет поставщику облачных вычислений повысить возможности по обеспечению безопасности, принятию решений по безопасности и реагированию на инциденты, а также усовершенствовать механизм раннего предупреждения об угрозах безопасности.

8 Требования к платформе ситуационной осведомленности о безопасности для облачных вычислений

8.1 Требования к сбору данных

8.1.1 Механизм сбора данных

Узлы сбора данных платформы NSSA должны активно или пассивно поддерживать сбор различных типов данных, таких как данные журналов сетевого трафика, системных журналов, журналов промежуточного программного обеспечения и журналов регистрации событий безопасности, касающихся инфраструктуры облачных вычислений. При активном подходе данные собираются путем периодического мониторинга или сканирования целевых источников, а при пассивном – главным образом путем получения или импортирования данных из различных источников.

1) Требуется, чтобы при сборе данных использовался активный подход, такой как сбор данных путем сканирования, обхода или с помощью простого протокола управления сетью (SNMP).
2) Требуется, чтобы при сборе данных использовался пассивный подход, например получение данных по протоколу syslog или каналу NetFlow, а также ручное импортирование данных.

Функции сбора данных должны быть адаптированы к средам облачных вычислений следующим образом.

1) Рекомендуется, чтобы при сборе данных обеспечивался сбор данных в облаках разного типа, таких как мультиоблака и гибридные облака.

2) Рекомендуется, чтобы при сборе данных учитывались динамические изменения ресурсов в среде облачных вычислений.

3) При сборе данных рекомендуется поддерживать сбор журналов регистрации сетевого трафика восток–запад платформ облачных вычислений.

Узлы сбора данных платформы NSSA должны обладать следующими возможностями.

1) Узлы сбора данных должны выполнять фильтрацию и проверять достоверность данных, например тип данных и диапазон значений, а также отфильтровывать недействительные данные в соответствии с предварительно установленными правилами.

2) Рекомендуется, чтобы в узлах сбора данных был внедрен механизм повторного сбора данных в случае сбоев.

8.1.2 Источник данных

Платформа NSSA должна поддерживать операции создания, чтения, обновления и удаления (CRUD) своих данных, а также сбора данных перечисленных ниже типов.

1) Следует поддерживать сбор данных об активах платформ облачных вычислений, таких как данные об активах пулов виртуальных ресурсов, сетевого оборудования, хост-систем, оборудования, систем, программного обеспечения безопасности и платформ управления облачными вычислениями.

2) Следует поддерживать сбор различных типов данных журналов регистрации событий, таких как журналы веб-доступа, журналы событий, относящихся к безопасности, журналы бизнес-операций и журналы входа в систему, из нескольких источников, таких как хост-системы, промежуточное ПО и платформы управления облачными вычислениями, а также поддерживать возможности получения результатов анализа журналов от других систем.

3) Следует поддерживать сбор данных об уязвимостях от множества устройств и компонентов платформ облачных вычислений, например об уязвимости переполнения буфера, уязвимости внедрения кода, уязвимости бизнес-логики, уязвимости дизайна, уязвимости конфигурации и т. д.

4) Следует поддерживать сбор данных о множестве событий сетевых атак, таких как DDoS-атаки, атаки с использованием уязвимостей и несанкционированный доступ.

5) Следует поддерживать сбор оперативных данных об угрозах, таких как оперативные данные об угрозах по IP-адресам/доменам/URL, образцы вредоносных программ, черный список управления и контроля (C&C) и уязвимости.

8.1.3 Предварительная обработка данных

Для удовлетворения требований, предъявляемых к качеству данных, платформа NSSA должна выполнять операции очистки и фильтрации, стандартизации, сопоставления и дополнения, объединения и недопущения дублирования собранных данных, а затем хранить стандартизированные данные.

1) Очистка данных. Платформа NSSA должна поддерживать очистку данных, если в собранных данных присутствуют ошибки, неполные данные, недействительные данные и другие проблемы, в том числе:

   - требуется поддерживать преобразование, обработку и фильтрацию данных в случае несогласованности форматов данных, наличия ошибок ввода данных и неполноты данных;
   - рекомендуется поддерживать фильтрацию и очистку данных на основе условных операций, сопоставления стандартных выражений и вычисления выражений;
   - рекомендуется обеспечивать недопущение дублирования данных.

2) Стандартизация данных. Платформа NSSA должна поддерживать единообразное форматирование разнородных данных различных типов и сохранение собранных исходных данных, в том числе:

- требуется поддерживать стандартизацию полей данных на основе правил для полей данных каждого типа;
- рекомендуется поддерживать единообразное форматирование необработанного контента с помощью стандартных выражений;
- рекомендуется поддерживать сохранение собранных исходных данных, чтобы обеспечить последующий анализ отслеживания и дальнейшее усовершенствование.

3) Сопоставление и дополнение данных. Платформа NSSA должна поддерживать сопоставление и дополнение стандартизированных данных, включая информацию о пользователях, активах, географическом местоположении и оперативные данные об угрозах, а также поддерживать выбор определенных данных и полей, которые необходимо дополнить.

4) Объединение данных. Платформа NSSA должна поддерживать объединение стандартизированных данных на основе установленных правил, а также поддерживать выбор определенных данных и полей для объединения.

8.1.4 Требования безопасности при сборе данных

1) Платформа NSSA должна поддерживать управление доступом к узлам сбора данных и мониторинг процесса сбора данных со своевременным оповещением о нештатных ситуациях.

2) В процессе сбора данных необходимо строго ограничить место временного хранения данных, которое не может быть изменено произвольно.

3) Платформа NSSA должна поддерживать иерархическую классификацию и идентификацию собранных данных и использовать средства защиты, такие как шифрование конфиденциальных данных, например данных об активах, оперативных данных и данных журналов регистрации событий.

4) Платформа NSSA должна поддерживать маскирование и десенсибилизацию конфиденциальных данных перед их предварительной обработкой и анализом, а также удовлетворять требованиям обеспечения безопасности собранных данных.

5) Платформа NSSA должна вести журнал собранных данных и операций для своевременного оповещения об аномальных событиях и контроля, включая следующее:

- требуется осуществлять контроль операций пользователей и администраторов, чтобы выявлять злонамеренное поведение, такое как неправомерное использование данных, предупреждать о нем и реагировать на него;
- во время сбора данных рекомендуется подавать предупредительные сигналы о прерываниях передачи;
- рекомендуется подавать предупредительные сигналы, если во время сбора и передачи данных объем сохраненных данных превысил установленный порог.

8.2 Требования к хранению данных

В хранилище данных платформы NSSA следует применять методы обработки больших данных для удовлетворения потребностей в хранении данных из множества источников, многомерных данных и непрерывно растущего объема данных, генерируемых средой облачных вычислений, таких как результаты анализа и оперативные данные о внешних угрозах. Платформа NSSA должна поддерживать механизмы хранения в соответствии с различными доменами и классификациями разных типов данных, а также удовлетворять требованиям разных методов анализа и изоляции данных. Кроме того, платформа NSSA должна обеспечивать доступность, целостность и конфиденциальность данных хранилища.

8.2.1 Категоризация хранения данных

Рекомендуется, чтобы платформа NSSA поддерживала хранение неструктурированных, структурированных и полуструктурированных данных в зависимости от их источника, а также несколько категорий хранилищ данных, включая реляционное хранилище, базу данных NoSQL (не только язык структурированных запросов), распределенное хранилище файлов и распределенный полнотекстовый поиск.

Рекомендуемые категории хранения данных платформы NSSA описаны в таблице 8-1.

Таблица 8-1 – Категоризация данных

Источник данных	Содержание данных	Объем данных	Категоризация хранилища данных (рекомендуемая)
Облачная хост-система/ контейнер/ОС	Журналы операций, журналы безопасности, данные о рабочем состоянии, файлы конфигурации и т. д.	Большой	Распределенное хранилище файлов/распределенный полнотекстовый поиск/база данных NoSQL
Платформа управления облаком	Журналы доступа, журналы операций, файлы конфигурации, данные рабочих процессов и т. д.	Средний	Распределенное хранилище файлов/распределенный полнотекстовый поиск/база данных NoSQL
Сетевое оборудование	Журналы регистрации событий маршрутизаторов, коммутаторов и сетевой платформы, таблицы маршрутизации, файлы конфигурации и т. д.	Большой	Распределенное хранилище файлов/распределенный полнотекстовый поиск/база данных NoSQL
Оборудование системы безопасности	Журналы регистрации событий брандмауэра, системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), виртуальной частной сети (VPN), брандмауэра веб-приложений (WAF), файлы конфигурации и т. д.	Большой	Распределенное хранилище файлов/распределенный полнотекстовый поиск/база данных NoSQL
Система приложений	Журналы базы данных, промежуточное ПО, системы приложений, файлы конфигурации и т. д.	Большой	Распределенное хранилище файлов/распределенный полнотекстовый поиск/база данных NoSQL
Основные данные	Данные об активах, данные учетных записей, словарь IP, данные об услугах и т. д.	Средний	Рациональная база данных/ распределенный полнотекстовый поиск/база данных NoSQL
Сетевой трафик	Данные DPI, данные о сетевых потоках и т. д.	Очень большой	Распределенное хранилище файлов
Оперативная информация об угрозах	Стратегический анализ, тактический анализ, информация о безопасности и т. д.	Средний	Распределенное хранилище файлов/распределенный полнотекстовый поиск/база данных NoSQL
Результаты анализа	События безопасности, данные о соответствии, индекс безопасности и т. д.	Средний	Рациональная база данных/ распределенный полнотекстовый поиск/база данных NoSQL

8.2.2 Технические требования к хранению данных

Следует разработать гибкую и масштабируемую архитектуру хранения данных платформы NSSA, чтобы удовлетворить требования, связанные с постоянным ростом объема данных, а также требования классификации и иерархического хранения данных. Кроме того, жизненный цикл хранения данных должен варьироваться в соответствии с необходимостью соблюдения правил, бизнес-требованиями и экономическими затратами.

1) Платформа NSSA должна поддерживать основные рациональные базы данных. Рациональная база данных должна поддерживать полный интерфейс доступа к реляционной модели, включая стандартный интерфейс SQL и стандартный интерфейс разработки приложений (JDBC, ODBC и т. д.).

2) Платформа NSSA должна поддерживать основные базы данных NoSQL.

3) Платформа NSSA должна поддерживать типичные компоненты больших данных, такие как Hive, HBase и MPP, в целях поддержки расширенных функций.

4) Платформа NSSA должна использовать компоненты полнотекстового поиска, поддерживающие поиск по ключевым словам, поиск по множеству ключевых слов, комбинированный полнотекстовый поиск и поиск по другим полям, а также сопоставление префиксов, нечеткое сопоставление и другие условия поиска.

5) На платформе NSSA рекомендуется применять компоненты распределенной шины передачи сообщений, такие как Kafka, RabbitMQ и т. д. Рекомендуется, чтобы компоненты распределенной шины передачи сообщений поддерживали такие функции, как сжатие данных, установление времени хранения данных и автоматическое удаление данных с истекшим сроком действия.

6) Платформа NSSA должна поддерживать онлайн-хранение и механизмы резервного копирования, гарантируя готовность данных.

7) Платформа NSSA должна поддерживать хранение метаданных, которые включают в основном:

   - технические метаданные и их использование для обслуживания данных, например способ хранения данных для обеспечения эффективного доступа к ним;
   - метаданные управления, такие как политика управления доступом к данным и результаты обработки данных.

8.2.3 Требования безопасности при хранении данных

1) Для предотвращения несанкционированного доступа к данным платформа NSSA должна включать механизмы управления доступом, такие как управление доступом к хранилищу данных на основе ролей.

2) Платформа NSSA должна поддерживать шифрование данных на запоминающем устройстве для особенно важных или конфиденциальных данных. Рекомендуется уточнить требования к шифрованию данных на запоминающих устройствах для различных типов данных на основе их классификации и иерархического определения, например требования к алгоритмам шифрования данных и управлению ключами шифрования.

3) На платформе NSSA требуется реализовать соответствующие методы и меры контроля для обеспечения эффективности сохранения целостности данных при их хранении и согласованности множества копий данных.

4) На платформе NSSA требуется реализовать соответствующие методы и меры контроля для обеспечения доступности хранилища данных. Рекомендуется, основываясь на принципах классификации данных, уточнить правила резервного копирования и восстановления различных данных, такие как режимы резервного копирования, требования к периоду хранения и времени восстановления.

5) Платформа NSSA должна периодически тестировать механизмы хранения данных, проверяя возможности выявления ошибок в данных и их восстановления из резервной копии.

6) Платформа NSSA должна генерировать все журналы операций хранения данных, обеспечивая отслеживаемость процессов хранения и предоставляя возможность предупреждения об аномальном поведении.

8.3 Требования к ситуационным вычислениям и анализу

Платформа NSSA выполняет ситуационные вычисления и анализ главным образом посредством вычислительно-аналитического механизма и функциональных модулей ситуационного анализа.

1) Вычислительно-аналитический механизм обеспечивает вычислительные возможности функциональных модулей ситуационного анализа для моделирования и анализа угроз. Вычислительно-аналитический механизм включает в себя средства моделирования состояния безопасности и структуры вычислений при обработке больших данных, такие как автономный вычислительный механизм и вычисления в режиме реального времени.

2) Функциональные модули ситуационного анализа в основном выполняют ситуационный анализ безопасности сети в среде облачных вычислений на основе интеллектуального анализа данных, детализации и анализа угроз на основе различных агрегированных данных об активах, таких как события безопасности, данные журналов регистрации событий и данные по сетевому трафику.

3) Чтобы повысить эффективность расчета и анализа, перед моделированием состояния безопасности необходимо создать унифицированное представление различных событий, относящихся к безопасности, и информации об активах, которое можно получить с помощью векторизации контекста. Метод векторизации отображает контекст на евклидовом пространстве и обычно служит предпосылкой для внедрения различных ИИ-алгоритмов расчета подобия и корреляции.

8.3.1 Требования к вычислительно-аналитическому механизму

8.3.1.1 Моделирование состояния безопасности

Моделирование состояния безопасности должно включать корреляционное моделирование, статистическое моделирование, корреляционное моделирование оперативной информации об угрозах и ИИ-моделирование, обеспечивая возможности углубленного анализа и интеллектуального анализа основных ситуационных данных.

1) **Корреляционное моделирование** – метод сопоставления на основе правил, используемый для выполнения анализа разнородных событий с помощью логических ассоциаций и сопоставления признаков.
   - Требуется поддержание логического корреляционного анализа, основанного на причинно-следственных связях между инцидентами безопасности.
   - Требуется поддержание корреляции разнородных данных из множества источников по множеству аспектов, таких как время и пространство.
   - Рекомендуется поддержание кластеризации предупредительной информации в соответствии с динамическими ситуациями сетевой безопасности, чтобы уменьшить количество предупреждений и повысить эффективность реагирования.

2) **Статистическое моделирование** – использование статистических методов для вычисления количественных характеристик различных событий, таких как частота и период возникновения, и для получения распределения данных о событии, основных характеристик, тенденций в виде временных последовательностей, информации о наличии аномальных значений и сводных результатов событий.
   - Рекомендуется поддержание выполнения статистического анализа событий безопасности, режимов безопасности, угроз безопасности и других характеристик, а также получение важных статистических характеристик угроз безопасности из различных источников данных.

3) **Объединение механизмов анализа угроз**. Рекомендуется поддержание интеграции функций анализа угроз, чтобы точно выявлять оперативные события на основе анализа угроз в среде облачных вычислений.

4) **ИИ-моделирование**. Рекомендуется поддержание различных встроенных алгоритмов искусственного интеллекта, включая алгоритмы синхронизации, классификации, кластеризации и другие прототипы алгоритмов, предоставляя пользователям возможности обучения и анализа произвольных данных, а также анализа угроз нового уровня и неизвестных угроз безопасности.

- Рекомендуется поддержание основных алгоритмов, таких как кластерный анализ, ассоциативный анализ, анализ дерева решений, регрессионный анализ и другие алгоритмы ИИ-анализа/машинного обучения.
- Платформа NSSA должна поддерживать централизованное управление моделированием состояния безопасности и политикой в области безопасности в целях содействия эффективной реализации и быстрому развертыванию системы.

8.3.1.2 Вычислительная платформа для больших данных

Для обеспечения пакетной обработки статических данных и анализа динамических (потоковых) данных в режиме реального времени требуется поддерживать платформы как автономных вычислений, так и вычислений в режиме реального времени.

1) **Платформа автономных вычислений**. Требуется поддержание возможности развертывания автономных алгоритмов, учебных моделей и сценариев машинного обучения. Аналитики могут использовать механизм автономного анализа для углубленного интеллектуального анализа данных, получая немедленную обратную связь о результатах работы алгоритма, что обеспечивает возможность обучения модели.

2) **Платформа потоковых вычислений в режиме реального времени**. Рекомендуется, чтобы платформа вычислений в режиме реального времени могла поддерживать распределенную архитектуру, а емкость хранилища данных можно было регулировать динамически. Высокий уровень доступности и разделение политик чтения и записи могут обеспечить раздельное чтение и запись данных при автономном анализе данных.

8.3.2 Требования к функциональным модулям ситуационного анализа

Опираясь на механизм вычислений и анализа, функциональные модули ситуационного анализа обеспечивают средства анализа на основе сценариев для различных данных об активах, событиях безопасности, журналов, данных о трафике и других данных, а также предоставляют сценарии анализа безопасности на основе множества данных для получения сигналов на основе сценариев оповещения и раннего предупреждения. Функциональные модули ситуационного анализа включают анализ сетевой безопасности, анализ безопасности активов и анализ связанного с высоким риском поведения пользователей в среде облачных вычислений.

8.3.2.1 Анализ сетевой безопасности

Модуль анализа сетевой безопасности должен обладать возможностью анализировать возникающие в среде облачных вычислений различные ситуации, связанные с атаками на сеть, такие как аномальный сетевой трафик, распространение вредоносной программы и доступ с помощью вредоносного доменного имени, а также возможностью отслеживать тенденции в отношении их изменения.

1) Рекомендуется поддерживать обнаружение и статистический анализ общей ситуации в отношении распространенных атак и анализировать тенденции изменения текущей ситуации с атаками.

- Рекомендуется поддерживать функции обнаружения и анализа сетевых атак на основе данных из множества источников, включая случаи проникновения в сеть, веб-атаки, вредоносное ПО, DDoS-атаки, зондирование сети, подозрительные действия и сетевые атаки других типов.
- Рекомендуется поддерживать статистический анализ сетевых атак разного типа и анализ изменения тенденций в различных типах атак.

2) Рекомендуется поддерживать обнаружение и статистический анализ общей ситуации с аномальным сетевым трафиком в среде облачных вычислений и анализировать изменение тенденций в текущем аномальном сетевом трафике.

- Рекомендуется поддерживать возможность обнаружения аномалий сетевого трафика, а также возможность обнаруживать и анализировать аномальный трафик протоколов на основе распространенных вирусных портов.
- Рекомендуется поддерживать статистический анализ аномального сетевого трафика и объединение и статистику аномального трафика протоколов, а также анализировать тенденции в аномальном трафике.

3) Рекомендуется поддерживать анализ общей ситуации с распространением в среде облачных вычислений вредоносных программ, таких как вирусы, черви и трояны, а также анализировать текущие тенденции в отношении распространения вредоносных программ.

4) Рекомендуется поддерживать обнаружение и статистический анализ узлов управления и контроля ботнетов и зомби-узлов, а также поддерживать анализ распространения и изменения тенденций в ситуации с ботнетами.

5) Рекомендуется поддерживать анализ статистики доступа и распространения вредоносных доменных имен, IP-адресов контроля и управления и доменных имен алгоритма создания домена (DGA).

6) Рекомендуется поддерживать модель цепочки атак для отслеживания источника событий, связанных с атаками, путем классификации сгенерированных событий безопасности в соответствии с процессом атаки, который включает в себя сбор информации, проникновение в сеть, управление и контроль (C&C), горизонтальное проникновение, достижение цели и уничтожение улик.

7) Рекомендуется поддерживать анализ информации о злоумышленниках на основе оперативной информации об угрозах.

8.3.2.2 Анализ безопасности активов

Необходимо поддерживать анализ состояния безопасности различных активов платформы облачных вычислений. Рекомендуется анализировать состояние безопасности инфраструктуры облачных вычислений, виртуальных машин, контейнеров и бизнес-систем с помощью журналов регистрации событий оборудования безопасности, системных журналов, результатов сканирования уязвимостей и других данных. Используется анализ двух типов – анализ атак на систему и анализ уязвимостей системы.

8.3.2.3 Анализ информации об активах

1) Требуется поддерживать статистический анализ активов, включая анализ, основанный на классификации, категоризации и приоритетах активов, а также возможность обновления состояния активов, например их добавления или удаления.

2) Требуется поддерживать анализ распределения активов, включая анализ на основе географической информации об активах, их принадлежности к подразделениям и важных веб-приложений.

3) Требуется поддерживать поиск и отображение информации об активах в соответствии с IP-адресами активов, категориями, приоритетами, географической информацией.

8.3.2.4 Анализ угроз активам

1) Требуется поддерживать анализ угроз атак на систему, включая обнаружение попыток уничтожения содержания журналов, повышения уровня системных привилегий, ошибочных записей в журналах и атак методом полного перебора. Анализ может быть проведен на основе корреляционного анализа данных активов, журналов устройств, журналов хост-систем, данных системы безопасности и информации об угрозах.

2) Требуется поддерживать статистический анализ и анализ тенденций в ситуации с угрозами активам.

8.3.2.5 Анализ уязвимости активов

1) Требуется поддерживать корреляционный анализ результатов сканирования уязвимостей активов и журналов обнаружения устройств, относящихся к безопасности, для выполнения анализа использования уязвимостей, включая анализ уязвимостей хост-компьютеров/ВМ/контейнеров и анализ уязвимостей приложений, а также статистический анализ активов, подверженных риску использования уязвимостей, в зависимости от времени, бизнес-системы, уровня уязвимости и других параметров.

8.3.2.6 Анализ соответствия конфигураций активов

1) Требуется поддерживать анализ результатов проверки соответствия конфигурации операционных систем, программного обеспечения виртуализации, баз данных, сетевого оборудования и промежуточного программного обеспечения в среде облачных вычислений.

2) Требуется поддерживать статистический анализ обнаруженных несоответствующих элементов и анализ рисков, связанных с использованием злоумышленниками несоответствующих элементов для атаки на активы.

8.3.2.7 Анализ поведения пользователей

Рекомендуется поддерживать обнаружение и анализ аномального поведения внутренних пользователей, имеющих доступ к платформе облачных вычислений, и аномального поведения активов и бизнес-систем, а также профилирующий анализ поведения пользователей.

1) Рекомендуется поддерживать анализ аномального операционного поведения пользователей, включая аномальные операции с конфиденциальными данными, вход в учетную запись с истекшим сроком действия, несанкционированное повышение полномочий, выполнение команд в отношении конфиденциальных данных, атаки методом полного перебора и вход в систему с аномального адреса.

2) Рекомендуется поддерживать профилирование на основе поведения внутренних пользователей, включая изучение индивидуальных поведенческих характеристик и характеристик групп пользователей.

3) Рекомендуется поддерживать настройку правил аномального поведения и моделей поведения.

4) Рекомендуется поддерживать анализ аномального поведения на основе профилей пользователей и сравнивать индивидуальное или групповое поведение за один день с предыдущими данными о поведении в целях анализа аномалий.

5) Рекомендуется поддерживать анализ аномального поведения различных ресурсов облачных вычислений и иметь возможность выявлять аномальное поведение, которое может иметь место в среде облачных вычислений, например аномальное поведение облачных хост-систем, аномальные инструменты вызывающей системы, аномальное поведение сети и незаконные исходящие вызовы.

8.4 Требования к ситуационной оценке

Ситуационная оценка платформы NSSA должна поддерживать динамическую ситуационную оценку общего состояния безопасности в среде облачных вычислений, прогнозирование ситуационных тенденций на основе анализа многомерных данных безопасности, результатов анализа безопасности платформы облачных вычислений и оценочного моделирования категории ситуационного показателя. Она поддерживает передачу заблаговременных предупреждений и взаимодействие с механизмами принятия решений по обеспечению безопасности и реагирования на чрезвычайные ситуации поставщика облачной услуги (CSP)/потребителя облачной услуги (CSC).

8.4.1 Ситуационная оценка

Сфера ситуационной оценки безопасности включает в себя всестороннюю оценку ситуации с облачной платформой, оценку ситуации, относящейся к безопасности облачных активов, оценку угроз, уязвимостей, сетевых атак, а также оценку состояния доступности облачной платформы и ее компонентов.

1) Требуется собирать информацию об активах в качестве источника данных для построения категории индекса ситуационной оценки безопасности. Информация об активах должна включать в себя конкретные версии операционных систем, промежуточного программного обеспечения, приложений и баз данных, топологию сети, стоимость активов и т. д., что поможет сформировать разумные оценочные показатели.

2) Требуется поддерживать категорию индекса ситуационной оценки безопасности платформы облачных вычислений путем разработки общих количественных показателей с единой шкалой для измерений ситуационной безопасности и количественной оценки различных элементов ситуации, связанной с безопасностью сети.

- Для ситуационной оценки сети рекомендуется разработать как качественные, так и количественные показатели. Качественные показатели – это субъективные оценки, основанные на мнении профессиональных экспертов по безопасности. Например, эксперты по безопасности могут присвоить уровни серьезности для данных уязвимостей или сетевых атак на основе собственного опыта. Количественные показатели являются результатом сбора и анализа необработанных данных.
- При работе с показателями угроз рекомендуется поддерживать расчет подобия и расчет корреляции, в том числе:
  - рекомендуется использовать расчет подобия контекста угроз для распознавания быстро нарастающих угроз, таких как сканирование, взлом методом перебора и DDoS-атаки, во избежание резких изменений конкретного показателя, вызванных большим количеством повторных тревожных сигналов;
  - рекомендуется использовать анализ корреляции между информацией об угрозах и активах для распознавания угроз методом слепой атаки и массированных попыток, что поможет сотрудникам службы безопасности быстро обнаружить индикаторы высокого риска, которые действительно требуют их реагирования;
  - для выполнения корреляционного анализа и анализа подобия рекомендуется внедрить унифицированную структуру алгоритмов, таких как алгоритм на основе косинуса угла; унифицированная структура алгоритмов поможет заметно снизить стоимость обслуживания при использовании алгоритмов.
- Для ситуационной оценки сетевой безопасности рекомендуется разработать общий показатель и детализированные показатели. Общий показатель отражает общие характеристики оценки безопасности платформы облачных вычислений; детализированные показатели могут быть определены для разных компонентов или систем и отражать различия между результатами ситуационной оценки разных компонентов/систем.
- Рекомендуется поддерживать разработку категорий индексов ситуационной безопасности, в том числе:
  - разработку операционных показателей для платформ облачных вычислений, таких как использование пулов облачных ресурсов и задержки доступа для предприятий;
  - разработку индикаторов угроз безопасности сети, включая различные инциденты, связанные с безопасностью сети, которые можно дополнительно просчитать и оценить с точки зрения их частоты и степени серьезности;
  - разработку показателей для оценки безопасности облачных активов, таких как степень угрозы активам и уязвимость активов, включая степень серьезности уязвимости и возможность устранение уязвимости;
  - разработку показателей для оценки безопасности поведения пользователей, такие как случаи аномального доступа пользователей, аномального входа в систему и загрузки вредоносных программ; также требуется внедрение методов защиты конфиденциальности пользователей, таких как десенсибилизация и обезличивание данных.

3) Рекомендуется поддерживать построение механизма всесторонней ситуационной оценки безопасности или моделирование на основе иерархических, многомерных категорий показателей.

- Требуется поддерживать стандартизацию детализированных показателей, включая как качественные, так и количественные показатели, во избежание необъективных результатов оценки из-за различий в единицах измерения и величинах. Рекомендуется применять методы преобразования качественных показателей в числовые значения для дальнейшего расчета или анализа.
- Рекомендуется поддерживать механизмы многомерной ситуационной оценки, включая оценку, ориентированную на риски, оценку, ориентированную на угрозы, или моделирование на основе данных в виде временных последовательностей.
- Рекомендуется поддерживать различные модели оценки, в том числе модели, основанные на теоретических математических моделях, или суждения, основанные на знаниях.
- Рекомендуется поддерживать иерархический метод оценки снизу вверх путем всесторонней обработки показателей ситуации нижних уровней с последующим вычислением результатов ситуационной оценки верхних уровней и постепенным вычислением общей ситуационной оценки безопасности.
- При использовании иерархических методов оценки рекомендуется поддерживать расчет подобия для обеспечения возможности интерпретации оценки конкретной ситуации на фоне предыдущих и ближайших значений. Для получения окончательной оценки может быть построен многомерный вектор путем выбора предыдущих результатов определенного уровня, и этот вектор можно использовать для вычисления подобия предыдущих ближайших значений по алгоритмам на основе косинуса угла, пространственного векторного расстояния и др. Вычисление подобия поможет персоналу службы безопасности быстрее выявлять аномалии и достичь более точной ситуационной осведомленности.

4) Рекомендуется поддерживать возможность эффективного отслеживания предыдущих оценок ситуации в области безопасности облачной платформы путем предварительной обработки журналов, индексации ключевых полей, полнотекстового поиска и нечетких запросов.

8.4.2 Перспективный прогноз ситуационных тенденций

Основываясь на определении и отслеживании состояния безопасности среды облачных вычислений, выявлении элементов безопасности и ключевых показателей, способных вызвать изменения ситуации в сети, платформа NSSA должна поддерживать прогнозирование общей тенденции в отношении безопасности, тенденции в отношении безопасности отдельных компонентов и потенциальных рисков для безопасности на основе ориентированных на облачную платформу моделей перспективной оценки ситуации в области безопасности.

1) Требуется поддерживать построение категории иерархических и многомерных показателей на основе собранных данных и результатов анализа, а также прогнозирование ситуационных тенденций с помощью соответствующих прогностических моделей.

2) Рекомендуется поддерживать основные прогностические модели, включая модели регрессионного прогнозирования на основе машинного обучения, модели глубокого обучения, модели прогнозирования на основе дифференциальных уравнений в профессиональных областях.

3) Рекомендуется поддерживать вычисленные результаты прогнозирования путем объединения различных моделей прогнозирования для повышения точности прогнозирования, в частности:
   - контролировать точность каждой модели, вычисляя значения функции потерь между прогнозом и результатами обработки данных;
   - объединять результаты каждой модели с применением весовых коэффициентов, вносить адаптивные корректировки весовых коэффициентов разных моделей; например, вес каждой модели можно адаптивно скорректировать на основе результата мониторинга функции потерь; для обновления модели и повышения точности также может автоматически запускаться процесс автономного обучения по последним данным.

8.4.3 Механизмы предварительного предупреждения

Платформа NSSA должна обеспечивать механизмы раннего предупреждения о потенциальных угрозах безопасности в среде облачных вычислений на основе результатов анализа безопасности, ситуационной оценки и ситуационного прогнозирования.

1) Рекомендуется обеспечивать ранние предупреждения об уязвимостях активов, сопоставляя уязвимости с оперативной информацией об угрозах, соответствующими данными о событиях, связанных с безопасностью, и т. д., а также анализируя уязвимости активов облачной платформы.

2) Рекомендуется поддерживать распространение ранних предупреждений о потенциальных сетевых атаках на основе прогнозируемых тенденций, включая вредоносное сканирование, веб-атаки, DDoS-атаки, атаки с подбором пароля и атаки с использованием уязвимостей систем.

3) Рекомендуется поддерживать распространение ранних предупреждений о потенциальных аномальных действиях пользователей на основе прогнозирования тенденций, включая аномальные операции с конфиденциальными данными, входы в учетную запись с истекшим сроком действия, выполнение команд с высоким риском и т. д. Перед распространением предупреждений необходимо использовать методы десенсибилизации и обезличивания данных для защиты конфиденциальности пользователей.

4) Рекомендуется поддерживать распространение ранних предупреждений о необнаруженных угрозах безопасности, связывая между собой выявленные аномальные действия, оперативную информацию об угрозах, исходные журналы регистрации событий и т. д.

5) Механизмы раннего предупреждения:

   - рекомендуется поддерживать распространение ранних предупреждений на основе установленных правил, которые можно настроить соответствующим образом;
   - рекомендуется поддерживать иерархическое управление ранними предупреждениями и категоризацию уровней предупреждений в соответствии с их степенью важности и серьезности;
   - рекомендуется поддерживать распространение предупреждений через API, с помощью которых сторонние системы могут получать предупреждения и реагировать соответствующим образом.

8.5 Требования к ситуационной визуализации

Платформа NSSA должна поддерживать отображение ситуации в области безопасности по нескольким сценариям, включая общую ситуацию в области безопасности, ситуацию в области безопасности сети, ситуацию в области безопасности активов, а также настройку ситуации в области безопасности. В то же время рекомендуется поддерживать использование нескольких типов представлений для отображения подробной информации о ситуации в области безопасности, таких как радарная диаграмма, корреляционная информационная карта и карта путей угроз, а также поддерживать детализацию информации в области безопасности.

8.5.1 Визуализация общей ситуации в области безопасности

1) Рекомендуется поддерживать представление общей оценки состояния в области безопасности платформы облачных вычислений с помощью баллов или уровней.

2) Рекомендуется поддерживать представление общей ситуации в области безопасности платформы облачных вычислений в графическом виде, включая ранжирование рисков, отображение тенденций в отношении сетевых атак, уязвимостей и рискованного поведения пользователей.

3) Рекомендуется поддерживать представление ситуации в области безопасности для разных арендаторов, разных бизнес-операций, разных активов и т. д. на платформе облачных вычислений и сравнение с данными прошлых лет для отображения тенденций.

4) Рекомендуется поддерживать представление в режиме реального времени агрегированных сигналов тревоги о событиях в области сетевой безопасности, аномальном поведении пользователей и состоянии в области безопасности активов на платформе облачных вычислений, а также поддерживать детализацию этих сигналов тревоги в графическом виде.

8.5.2 Визуализация ситуации в области безопасности сети

1) Рекомендуется поддерживать графическое представление рисков для безопасности сети платформы облачных вычислений в нескольких измерениях, включая результаты статистического анализа сетевых атак, типы сетевых атак, географическое распределение сетевых атак, аномальный сетевой трафик, исходные и целевые IP-адреса атак.

2) Рекомендуется поддерживать представление в режиме реального времени предупредительных сигналов безопасности платформы облачных вычислений, таких как атаки на сеть, аномальный сетевой трафик и вредоносные программы. Предупредительная информация включает метку времени, тип безопасности, степень серьезности, а также исходные и целевые IP-адреса атак.

3) Рекомендуется поддерживать получение детализированной информации о ситуации в области сетевой безопасности.

8.5.3 Визуализация ситуации в области безопасности активов

1) Рекомендуется поддерживать графическое представление информации об активах платформы облачных вычислений, включая размеры активов, типы активов, принадлежность активов, распределение активов.

2) Рекомендуется поддерживать графическое представление результатов статистического анализа платформы облачных вычислений, включая анализ уязвимостей активов, сетевых атак, ошибок конфигурации.

3) Рекомендуется поддерживать проведение в режиме реального времени анализа рисков для безопасности различных активов платформы облачных вычислений по нескольким измерениям, включая наименование актива, IP-адрес актива, типы атак, типы уязвимостей, количество уязвимостей, ошибки конфигурации.

4) Рекомендуется поддерживать детализацию информации о ситуации в области безопасности активов.

8.5.4 Визуализация ситуации в области аномального поведения пользователей

1) Рекомендуется поддерживать представление аномального поведения пользователей платформы облачных вычислений в нескольких измерениях, включая типы аномального поведения, тенденции в области аномального поведения и типы аномальных пользователей (учетных записей или IP-адресов).

2) Рекомендуется поддерживать распространение в режиме реального времени предупреждений об аномальном поведении пользователей платформы облачных вычислений, включая время распространения предупреждения, типы предупредительных сигналов, степень серьезности, типы аномальных пользователей (учетных записей).

3) Рекомендуется поддерживать детализацию информации об аномальном поведении пользователей.

8.5.5 Настраиваемая визуализация ситуации в области безопасности

Рекомендуется поддерживать возможность настройки представления ситуации для конкретных бизнес-сценариев и возможность импорта конфигураций в графическом виде или с помощью сценариев в соответствии с бизнес-требованиями, ролями администраторов и другими индивидуальными требованиями платформы облачных вычислений.

Библиография

[b-ITU-T X.1217] Рекомендация МСЭ-Т X.1217 (2021 г.), *Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи.*

[b-ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 г.), *Основы безопасности облачных вычислений.*

[b-ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 г.) | ISO/IEC 17788:2014, *Информационные технологии – Облачные вычисления – Обзор и терминология.*

[b-NIST-SP-800-30] NIST Special Publication 1800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2024 г.