решение:
- сертифицировано ФСТЭК России по 4 уровню доверия
- включено в Единый реестр отечественного ПО

Минцифры России

г. Москва, ул. Садовническая 57, стр.2
+7(495) 803-36-60
www.securityvision.ru
sales@securityvision.ru

Описание функциональных модулей (продуктов) Security Vision

Security Orchestration Tools

Governance Risk Management and Compliance

Security Data Analysis

АО «ГОЗНАК» · ФГБУ НИИ «ИНТЕГРАЛ» · ФЕДЕРАЛЬНАЯ СЛУЖБА ОХРАНЫ РФ · ПРАВИТЕЛЬСТВО КРАСНОЯРСКОГО КРАЯ · ПРАВИТЕЛЬСТВО ТЮМЕНСКОЙ ОБЛАСТИ · ПРАВИТЕЛЬСТВО ЯРОСЛАВСКОЙ ОБЛАСТИ · СОВЕТ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОГО СОБРАНИЯ РФ · АО «ДОМ.РФ»

АО НПП «ИСТОК ИМ. ШОКИНА» · ПАО «СЕВЕРСТАЛЬ» · ООО «ЕВРАЗ» · АО КОНЦЕРН «РОСЭНЕРГОАТОМ» · АО ОХК «УРАЛХИМ» · ПАО ГМК «НОРИЛЬСКИЙ НИКЕЛЬ» · ПАО «ИНТЕР РАО» · ПАО «РУСГИДРО»

ПАО «СБЕРБАНК» · АО «АЛЬФА-БАНК» · ПАО «РОСБАНК» · АО «Т-БАНК» · АО «БАНК ГПБ» · ПАО БАНК «ФК ОТКРЫТИЕ» · АО «СМП БАНК» · ПАО «СДМ-БАНК»

ООО «X5 GROUP» · ПАО «МАГНИТ» · ГРУППА «ЧЕРКИЗОВО» · ООО ГК «РУСАГРО» · АО «ПЕРВЫЙ КАНАЛ» · АО «ПОЧТА РОССИИ» · ГОСКОРПОРАЦИЯ «РОСТЕХ» · ХОЛДИНГ «CAPITAL GROUP»

ПАО «МЕГАФОН» · ПАО «ВЫМПЕЛКОМ» · ООО «СОЛАР СЕКЬЮРИТИ» · ООО «АТ ГРУП» · ООО «ТТК-СВЯЗЬ» (ТРАНСТЕЛЕКОМ) · ООО «ИНФОСЕКЬЮРИТИ СЕРВИС» · КОММЕРЧЕСКИЙ SOC «РОСТЕХ»

Security Vision

Содержание

Описание функциональных модулей 2
SOAR 3
AM 5
VM 7
VS 8
SPC 9
ГосСОПКА 11
FinCERT 12
КИИ 13
CM 14
RM 16
ORM 18
BCM 19
TIP 21
UEBA 23

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ МОДУЛЕЙ

Продукты Security Vision развиваются в трёх направлениях согласно треугольнику: технологии + процессы + аналитика. Все они могут использоваться как самостоятельные решения или как модули в рамках единой инсталляции при решении комплексных задач. Основные задачи и возможности продуктов приведены в каталоге ниже.

Модули включают различное количество коннекторов по-умолчанию с возможностью расширения списка за счёт подключения дополнительных и перераспределением внутри имеющегося количества (конкурентные лицензии).

SOT (SECURITY ORCHESTRATION TOOLS)

Данное направление объединяет продукты для управления практической безопасностью и создания экосистемы разрозненных продуктов с последующей оркестрацией:

– **SOAR**, Security Orchestration, Automation and Response (см. стр.3)
включает модуль управления активами (AM) и 15 базовых коннекторов
– **AM**, Asset Management (см. стр.5)
включает 7 базовых коннекторов
– **VM**, Vulnerability Management (см. стр.7)
включает 4 базовых коннектора
– **VS**, Vulnerability Scanner (см. стр.8)
включает 20 базовых коннекторов
– **SPC**, Security Profile Compliance (см. стр.9)
включает 20 базовых коннекторов
– **ГОССОПКА**, Государственная Система Обнаружения, Предупреждения и ликвидации последствий Компьютерных Атак (см. стр.11)
включает 2 базовых коннектора
– **FINCERT**, Financial Computer Emergency Response Team (см. стр.12)
включает 2 базовых коннектора

GRC (GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE)

Данное направление объединяет продукты, предназначенные для решения задач стратегической («бумажной») безопасности и управления бизнес-процессами в компании:

– **КИИ**, Критическая Информационная Инфраструктура (см. стр.13)
– **CM**, Compliance Management (см. стр.14)
– **RM**, Risks Management (см. стр.16)
включает 2 базовых коннектора
– **ORM**, Operational Risks Management (см. стр.18)
– **BCM**, Business Continuity Management (см. стр.19)
включает 1 базовый коннектор

SDA (SECURITY DATA ANALYSIS)

Данное направление объединяет решения, которые автоматизируют выполнение аналитических задач, в том числе с применением технологий машинного обучения для обработки Bid Data:

– **TIP**, Threat Intelligence Platform (см. стр.21)
включает 20 базовых коннекторов
– **UEBA**, User and Entity Behavior Analysis (см. стр.23)
включает 20 базовых коннекторов

SOAR

Модуль управления инцидентами выстраивает гибкий процесс обработки инцидентов при помощи динамических сценариев реагирования и построением цепочки атаки (kill chain) по методологии NIST. Решение осуществляет регистрацию алертов и событий ИБ (в ручном или автоматическом режиме), сбор событий в окрестности инцидента (при необходимости) и автоматизацию действий (классификацию с использованием базы техник и тактик MITRE ATT&CK, обогащение данными из внешних ИТ- и ИБ-систем, управляющие воздействия) с целью нейтрализации инцидентов и их последствий.

Основной функционал:

– динамические плейбуки (сценарии реагирования, подстраивающиеся под инцидент, его тип и объекты, которые были обнаружены)
– классификация 200+ инцидентов с применением баз знаний (внутренних или внешних, например база 100+ техник и тактик MITRE ATT&CK)
– встроенные рекомендации по реагированию для аналитиков (в т.ч. неопытных) для 70+ техник и тактик
– объектно-ориентированное реагирование (активные действия, выполняющиеся автоматически и/или вручную из карточек и графов связей с возможностью отмены)
– работа не только с инцидентами, но и с цепочками атак (kill chain по методологии NIST) для управления сложными инцидентами
– сбор окрестности инцидента и событий с Windows/Linux хостов и серверов, а также встроенный механизм корреляции и обработки потока событий (sigma-правила)

Процессы управления инцидентами включают: назначение ответственных исполнителей, классификацию, категоризацию, выполнение различных команд на удалённых системах, эскалацию, сохранение истории изменения каждого поля, фиксацию основных метрик SLA, а также выполнение других действий согласно встроенной методологии:

1) подготовка описания сервисов, СЗИ, списков исключений, состава команд SOC и др. инструментов и процессов;
2) обогащение данными в окрестностях инцидента;
3) анализ и классификация, сбор цифровых свидетельств;
4) сдерживание и изоляция учётных записей, хостов, URL, email и доменов;
5) реагирование на основе ключевых объектов: 70+ преднастроенных действий для хостов, 20+ для УЗ, и др.;
6) восстановление скомпрометированных объектов из бэкапа, разблокировка;
7) пост-инцидент, недопущения повторения аналогичных инцидентов.

Выстраивание связей между инцидентами и объектами осуществляется при помощи графов, позволяющих выполнять действия (с использованием коннекторов) в интерактивном режиме. Граф связей и различные табличные представления объектов также включают отображение рекомендаций экспертов по различным этапам обработки инцидентов по результатам классификации.

Логика обработки карточек инцидентов строится в графическом конструкторе рабочих процессов, реализованном по принципу блок-схем. Простые блок-схемы помогают визуализировать и настроить любую последовательность задач, позволяющих предотвратить инцидент информационной безопасности. Рабочие процессы состоят из транзакций, которые могут быть ручными (для их совершения необходимы действия пользователя системы) и автоматическими (с учётом заданных условий).

На основании данных о сегментах сети и таблицах маршрутизации сетевых устройств модуль позволяет аналитику отобразить на карте сети, куда потенциально может распространиться инцидент (граф достижимости), исходя из данных о скомпрометированных узлах и их характеристиках. Система автоматически визуализирует маршрут распространения инцидента по инфраструктуре, с отображением времени компрометации узлов сети и используемых злоумышленником артефактов.

Для определения ложноположительных инцидентов применяется ML-модель, которая обучается на назначенных при закрытии инцидентов вердиктах, а при поступлении нового инцидента выдаёт рекомендацию о том, насколько (в процентах) он похож по совокупности своих атрибутов на ранее закрытые с вердиктом False Positive.

Для уведомления по различным значимым событиям всех участников процесса обработки инцидентов предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации по результатам обработки карточек инцидентов в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Гибкие low-code механизмы платформы позволяют пользователям непосредственно в интерфейсе портала создавать произвольные коннекторы к любым внешним системам без применения языков программирования и участия представителей разработчика.

Источником инцидентов чаще всего выступают системы класса SIEM. В модуле предустановлены и поддерживаются в актуальном состоянии коннекторы к популярным российским и зарубежным решениям, например: PT MaxPatrol SIEM, RuSIEM, Kaspersky SIEM (KUMA), Pangeo Radar, MF ArcSight ESM, IBM Qradar SIEM, Splunk Enterprise, Fortinet FortiSIEM, McAfee ESM.

Предусмотрены возможности сбора информации по событиям ИБ, обогащения, нейтрализации и координации действий при помощи преднастроенных коннекторов для различных систем, например: ElasticSearch, InfoWatch Traffic Monitor, Kaspersky Security Center, Kaspersky IPS, Symantec IPS, Symantec EPP, FireEye CMS IPS, Cisco IronPort ESA, Kaspersky Security Center, Atlassian JIRA, OTRS , HP Service Manager, Naumen Service Desk, VirusTotal, WhoIsXMLAPI, URLScan, IPInfo.io, IPGeolocation.io, AbuseIPDB, LOLBAS, Kali tools, Shodan, ChatGPT, TrendMicro DDA (Sandbox), Microsoft Exchange, Symantec Endpoint Protection, Check Point SandBlast, Microsoft Active Directory, SSH, PowerShell, Atlassian JIRA, Naumen Service Desk, Solar JSOC, электронный почтовый ящик (IMAP, POP3 и SMTP) и др.

Примечание: в описании представлены наиболее популярные системы. Для получения полного списка преднастроенных в модуле коннекторов обратитесь к представителю Security Vision.

AM

Модуль управления активами и инвентаризацией осуществляет поиск (как с использованием встроенных механизмов, так и с применением внешних систем) и оцифровку информационных активов компании для описания ИТ-ландшафта и автоматизацию работы с ними. Решение позволяет управлять процессами идентификации типов активов, их категорирования, инвентаризации и управления жизненным циклом оборудования и ПО на АРМ и серверах. В качестве активов могут выступать: пользователь, информация, информационные системы, технические сервисы, программное или аппаратное обеспечение.

Основной функционал:

– сетевой поиск новых активов по расписанию + безагентская инвентаризация (используются скрипты для ОС Windows и Linux)
– возможность управления ПО, оборудованием, УЗ и др. типами активов (например, запуск обновления ПО или выключение хоста удалённо по кнопке в интерфейсе)
– возможность разработки коннекторов к самописным и экзотическим системам помимо доступных «в коробке»
– табличные, древовидные представления и карточки АС, ИС, ПО, УЗ, СЗИ и др., с возможностью связать любые объекты друг с другом и сформировать собственные
– единая ресурсно-сервисная модель для ИТ, практической (инциденты, уязвимости) и «бумажной» (КИИ, риски, моделирование угроз) безопасности

Для обеспечения информационной безопасности компании важно отслеживать состояние активов с точки зрения уровня защищённости, понимать взаимосвязь активов и потоки передачи данных между ними. Процесс управления активами в рамках Security Vision состоит из нескольких ступеней:

– поиск активов в подсетях;
– инвентаризация активов (в ручном и автоматическом режиме);
– классификация активов;
– определение взаимосвязей между активами;
– определение владельцев и ответственных за обслуживание активов;
– мониторинг основных параметров обеспечения информационной безопасности.

Выполнение данной цепочки действий является основой для формирования эффективной стратегии защиты активов компании и представляет собой непрерывный и повторяющийся во времени (благодаря расписаниям) процесс.

В качестве источника информации об активах могут выступать:

– встроенный модуль безагентского сканирования;
– службы каталогов (Active Directory);
– сканеры уязвимостей (PT MaxPatrol 8/VM, Tenable Nessus, Qualys, RedCheck);
– SIEM (PT MaxPatrol SIEM, IBM QRadar, ArcSight ESM, Splunk Enterprise и др.);
– системы управления антивирусным ПО (Kaspersky, Symantec, TrendMicro и др.);
– системы управления конфигурациями (MS SCCM);
– базы данных, содержащие информацию об активах (в том числе и CMDB);
– ручное создание активов через пользовательский интерфейс или импорт CSV/Excel файла.

В дополнение к любым возможным интеграциям с внешними системами и сервисами модуль включает 5 коннекторов (NMap локальное исполнение, NMap XML, SSH, WMI и PowerShell), которые не нуждаются в лицензировании.

Безагентское сканирование происходит в несколько этапов, комбинируя различные техники сбора информации и автоматически подстраиваясь под доступные данные и ландшафт инфраструктуры.

Встроенный модуль сканирования сочетает неаутентифицированный и аутентифицированный методы сбора информации об активах в сети и содержит ряд механизмов, позволяющих определить принадлежность оборудования к тому или иному типу, выявив доступные сервисы и их версии даже без наличия авторизационных данных.

Процесс сбора информации может быть кастомизирован для соответствия требованиям заказчика и особенностям инфраструктуры. Все этапы сканирования доступны для редактирования из интерфейса платформы.

Присутствует возможность создания специальных политик сканирования для сетей, хостов и типов активов. В политике можно указать временные окна, регулярность и интенсивность сканирования и/или ограничения запрашиваемых в процессе сканирования сервисов.

Карточка актива содержит детальную информацию о его свойствах, таких как:

- технические параметры актива;
- ответственные за актив сотрудники и бизнес-подразделения;
- данные о статусе его жизненного цикла;
- бизнес-назначения актива;
- параметры критичности;
- требования к доступности и данные о резервном копировании;
- проведённые тестирования функционала;
- связанные активы;
- документы;
- история изменений, произведённых как операторами, так и самой системой, включая источники изменяемых данных.

Для предотвращения создания лишних копий сущностей и консолидации информации из всех источников в единой карточке активов применяются механизмы дедупликации и обогащения. Информация об источнике и времени получения конкретных данных доступна в карточке актива.

Для получения информации из сегментированной сети присутствует возможность создания распределённой системы инвентаризации посредством иерархической структуры сервисов коннекторов. Коннекторы позволяют автоматически обогащать данные информацией об инвентаризируемом сегменте и его расположении, что даёт возможность проводить инвентаризацию сетей, в том числе с одинаковой адресацией.

Для уведомления по различным значимым событиям всех участников процесса управления активами и инвентаризацией предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

В модуле имеется ряд предустановленных отчётов и дашбордов для анализа состояний активов, а также встроенный редактор, позволяющий пользователю формировать интересующие его отчёты и представления на основе данных, содержащихся в системе, с выгрузкой в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Примечание: в описании представлены наиболее популярные системы. Для получения полного списка преднастроенных в модуле коннекторов обратитесь к представителю Security Vision.

VM

Модуль управления уязвимостями позволяет консолидировать информацию с имеющихся сканеров анализа защищённости, платформ управления обновлениями и других продуктов сбора и анализа данных для выстраивания процессов обнаружения, приоритизации и устранения технических уязвимостей. Для координации действий модуль содержит встроенную систему управления заявками с контролем статусов исполнения и автоматическим назначением SLA, а также поддерживает двусторонние интеграции со сторонними SD/ITSM решениями.

Основной функционал:

– интеграция «из коробки» со сканерами Security Vision. MaxPatrol, Nessus, Qualys, RedCheck, Tenable и любых других для совместного применения
– возможность обогащения данных об уязвимостях дополнительной информацией из внешних источников (VulDB, Vulners, AttackersKB, OpenCVE и др.)
– статичные/обновляемые базы знаний, встроенные справочники БДУ ФСТЭК и CVE база NVD от NIST
– интеграции по API (сбор/отправка в виде HTTP-запросов) или другим способом (например, парсинг XML-файлов) с произвольными внешними системами
– управление политиками и степенью грандляции при постановке задач (например, по CVSS и параметрам активов или с применением дерева решениий)
– поддержка рабочих календарей, расчёт SLA в рабочих и/или календарных днях) и во встроенная и/или сторонная система тикетинга ITSM/SD (OTRS, JIRA, Naumen SD и др.)
– встроенные рекомендации по устранению, отображающие консолидированную информацию для приоритизации работы специалистов

Выстроенные рабочие процессы обеспечивают выполнение различных задач для организации полного цикла обработки технических уязвимостей, например:

– идентификация уязвимостей на объектах инфраструктуры организации;
– классификация выявленных уязвимостей;
– предоставление детального описания выявленных уязвимостей;
– приоритизация выявленных уязвимостей;
– предоставление вариантов устранения уязвимостей;
– назначение ответственных и сроков устранения выявленных уязвимостей;
– осуществление контроля устранения уязвимостей;
– подготовка отчётности о динамике обнаружения уязвимостей как на отдельных узлах, так и по всей организации.

Для уведомления по различным значимым событиям всех участников процесса управления уязвимостями предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации по результатам обработки технических уязвимостей в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Информация по уязвимостям предоставляет специалистам ИБ наиболее полный контекст, как с точки зрения текущего уровня защищённости корпоративных узлов (аудит, моделирование угроз, оценка рисков), так и в процессе реагирования на инциденты и управления ИТ-активами.

Примечание: в описании представлены наиболее популярные системы. Для получения полного списка преднастроенных в модуле коннекторов обратитесь к представителю Security Vision.

VS

Сканирование уязвимостей позволяет проводить поиск и анализ защищённости веб-приложений, контейнеров и других активов (пакетах, ПО и ОС) с возможностью применения отчуждаемого сканера, режимов белого и чёрного ящиков и ретро-скан. Поддерживает возможность ограничивать область проверки, управлять глубиной сканирования папок с учётом масок файлов и обеспечивать перебор паролей и подбор алгоритмов шифрования. Найденные при помощи модуля уязвимости связываются с активами компании в общей ресурсно-сервисной модели.

Основной функционал:

– встроенный сканер для поиска уязвимостей на активах (хостах, серверах, ПО, контейнерах и др.)
– обновляемая из облака база уязвимостей аналитиков Security Vision с возможностью подключения других источников
– возможность обогащения данных информацией из внешних аналитических сервисов (VulDB, Vulners, AttackersKB, OpenCVE и др.), БДУ ФСТЭК и CVE от NIST
– сканирование в режимах белого (пакеты, приложения и обновления без ограничения количества) и черного (пентест, с возможностью добавления собственных процессов) ящиков
– ретро-скан, разработанный для быстрого поиска выбранных уязвимостей по уже собранным данным по всем активам
– сканирование веб-приложений и контейнеров с возможностью отдельного поиска уязвимостей в образах, запущенных и/или остановленных Docker-контейнерах
– отчуждаемый сканер для сбора уязвимостей из закрытых сегментов сети и дальнейшей агрегацией из создаваемого файла

Сканер изучает уязвимости в репозиториях более высокого уровня (например, для ОС, основанных на других сборках) и поддерживает обогащение как из обновляемой аналитиками Security Vision базой в облаке, так и из внешних аналитических сервисов и баз данных угроз. Поддерживаются поиск уязвимостей в приложениях внутри контейнеров и загруженных через Windows Store.

Для уведомления по различным значимым событиям всех участников процесса управления уязвимостями предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации по результатам обработки технических уязвимостей в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Информация по уязвимостям предоставляет специалистам ИБ наиболее полный контекст, как с точки зрения текущего уровня защищённости корпоративных узлов (аудит, моделирование угроз, оценка рисков), так и в процессе реагирования на инциденты и управления ИТ-активами.

Примечание: в описании представлены наиболее популярные системы. Для получения полного списка преднастроенных в модуле коннекторов обратитесь к представителю Security Vision.

SPC

Модуль контроля параметров безопасности осуществляет поиск и оцифровку информационных активов организации, а также оценку их конфигураций и предназначен для отслеживания состояние активов с точки зрения уровня защищённости и описания взаимосвязей активов и потоков передачи данных между ними. Построение модели активов состоит из поиска и инвентаризации, классификации и определения взаимосвязей, владельцев и ответственного персонала, а также мониторинга основных параметров ИБ.

Основной функционал:

- сетевой поиск новых активов по расписанию + безагентская инвентаризация (используются скрипты для ОС Windows и Linux)
- возможность управления ПО, оборудованием, УЗ и др. типами активов (например, запуск обновления ПО или выключение хоста удалённо по кнопке в интерфейсе)
- единая ресурсно-сервисная модель активов организации
- ведение профилей технологических платформ (например, операционных систем, СУБД, прикладного ПО), содержащих перечень релевантных для конкретных технологических платформ проверок и относящимся к технологическим платформам активов
- сетевое сканирование активов, относящимся к технологическим платформам (вручную, автоматически по расписанию, оффлайн), для определения степени соответствия параметров безопасности эталонным значениям
- возможность конфигурирования активов технологической платформы для приведения значения параметров к эталонным значениям

Для обеспечения информационной безопасности компании важно отслеживать состояние активов с точки зрения уровня защищённости, понимать взаимосвязь активов и потоки передачи данных между ними. Построение модели активов в рамках Security Vision состоит из нескольких ступеней:

- поиск активов в подсетях;
- инвентаризация активов (в ручном и автоматическом режиме);
- классификация активов;
- определение взаимосвязей между активами;
- определение владельцев и ответственных за обслуживание активов;
- мониторинг основных параметров обеспечения информационной безопасности.

После формирования модели активов производится построение взаимосвязей информационных активов организация с профилями технологических платформ для дальнейшего формирования заданий на сканирование конфигураций активов.

Перечень технологических платформ для оценки конфигураций:

1) Прикладное ПО:
   - Nginx;
   - Apache tomcat;
   - MS Exchange;
   - MS IIS;
   - Postfix;
   - Docker;
   - OpenShift;
   - Kuberbetes;
   - zVirt.
2) Операционные системы:

- MS Windows Server 2012 и старше;
- MS Windows 10 и старше;
- RHEL 7 и старше;
- REDOS;
- AstraLinux;
- AltLinux;
- CentOS;
- Debian;
- Oracle Solaris;
- VmWare vCenter;
- VmWare ESXi;
- Cisco iOS;
- Cisco ASA;
- S-terra CSP VPN Gate;
- CheckPoint (Gaia).

3) Системы управления базами данных:

- PostgreSQL/PostgreSQL PRO 12 и старше;
- MS SQL Server 2017 и старше
- MySQL.

В случае выявления несоответствия конфигураций активов эталонным значениям есть возможность приведения их к эталону при помощи механизма коннекторов платформы.

Для уведомления по различным значимым событиям всех участников процесса контроля параметров безопасности предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации по результатам оценки параметров безопасности активов организации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

ГОССОПКА

Модуль взаимодействия с регулятором НКЦКИ (Национальным координационным центром по компьютерным инцидентам) позволяет осуществлять оперативный двусторонний обмен информацией: уведомление об инцидентах информационной безопасности, получение сообщений о подозрениях на инцидент с участием подконтрольных ресурсов организации и получение оперативных бюллетеней об угрозах и уязвимостях от регулятора. Модуль взаимодействия разработан с учётом регламентов НКЦКИ и интегрирован с системой управления инцидентами (SOAR).

Основной функционал:

– интеграция с SOAR и другими решениями в периметре заказчика (например, ITSM/SD или SIEM) для двустороннего обмена с ГосСОПКА НКЦКИ
– приём информационных сообщений и бюллетеней от регулятора (актуальная ситуация по отрасли/стране)
– отправка инцидентов по форме регулятора для выполнения требований законодательства (автоматически и/или по «кнопке»)
– единая база данных при использовании других модулей (SOAR, VM, RM и др.) для возможности связывания любых объектов между собой
– использование основного и резервного канала связи (API, корпоративная почта) при коммуникации с центрами реагирования для обеспечения отказоустойчивости.

Отправка электронных сообщений в центры ГосСОПКА может осуществляться как в автоматическом, так и в полуавтоматическом режимах (полуавтоматический режим предполагает добавление отдельной функциональной кнопки в карточке инцидента, которая позволяет инициировать отправку сведений оператором).

Основной способ передачи данных осуществляется через интеграцию с личным кабинетом субъекта ГосСОПКА посредством Application Programming Interface (API). В случаях отказа основного канала отправки сведений в модуле предусмотрено автоматизированное переключение на резервный канал (с использованием корпоративной электронной почты).

В дополнение к любым возможным интеграциям с внешними системами и сервисами модуль включает 2 встроенных коннектора (API, email), которые не нуждаются в лицензировании.

Интеграция с системой управления инцидентами позволяет на основании полученной информации автоматически сформировать новую сущность в виде задачи, заявки или инцидента – в зависимости от выстроенных внутренних процессов заказчика. Формирование новой сущности осуществляется путём разбора и анализа поступающих JSON-файлов, а дополнительные файлы других расширений (например, «бюллетень.pdf») прикрепляются к карточке в виде вложения.

Для уведомления по различным значимым событиям всех участников процесса предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Автоматизированный обмен информацией с центрами ГосСОПКА в рамках единой платформы управления информационной безопасности позволяет разгрузить персонал от рутинных операций, высвобождая ресурсы для выполнения интеллектуальных задач.

FINCERT

Модуль взаимодействия с регулятором ЦБ (Центральным Банком) позволяет осуществлять оперативный двусторонний обмен информацией: передачи информации об инцидентах и получение оперативных уведомлений/бюллетеней от регулятора. Модуль разработан с учётом стандарта Банка России СТО БР БФБО-1.5-2023 (может быть адаптирован под соответствующие требования других стран) и интегрирован с системой управления инцидентами SV SOAR, а при помощи коннекторов к источникам данных (АСОИ «ФинЦЕРТ») позволяет проводить их дальнейшую их обработку, с возможностью экспорта во внешние системы (ресурсы).

Основной функционал:

– интеграция с SOAR и другими решениями в периметре заказчика (например, ITSM/SD или SIEM) для двустороннего обмена с АСОИ ФинЦЕРТ ЦБ
– приём информационных сообщений и бюллетеней от регулятора (актуальная ситуация по отрасли/стране)
– отправка инцидентов по форме регулятора для выполнения требований законодательства (автоматически и/или по «кнопке»)
– единая база данных при использовании других модулей (SOAR, VM, RM и др.) для возможности связывания любых объектов между собой
– использование основного и резервного канала связи (API, корпоративная почта) при коммуникации с центрами реагирования для обеспечения отказоустойчивости

Отправка электронных сообщений в FinCERT может осуществляться как в автоматическом, так и в полуавтоматическом режимах (полуавтоматический режим предполагает добавление отдельной функциональной кнопки в карточке инцидента, которая позволяет инициировать отправку сведений оператором).

Реализация данных режимов осуществляется через интеграцию с личным кабинетом участника информационного обмена посредством Application Programming Interface (API).

Модуль включает 3 встроенных коннектора (API, email и файл), которые не нуждаются в лицензировании.

Для уведомления по различным значимым событиям всех участников процесса предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Специализированный коннектор позволяет в необходимом формате успешно передавать информацию по компьютерным атакам (КА), компьютерным инцидентам (КИ), операциям перевода денежных средств без согласия клиентов, а также получать запросы и бюллетени от АСОИ ФинЦЕРТ ЦБ.

КИИ

Модуль управления соответствием ФЗ-187 автоматизирует ряд процедур, которые способствуют исполнению требований категорирования объектов КИИ согласно Постановлению Правительства РФ № 127, а также проведение оценки соответствия объектов КИИ требованиям подзаконных актов ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации».

Основной функционал:

– формирование справочников (создание перечня ОКИИ, мер защиты и др.) для аудита соответствия требованиям приказов ФСТЭК №239, 235 и 236 для ОКИИ
– категорирование объектов с формированием опросных листов и автоматизацией сбора данных/расчёта интегральных показателей
– аудит соответствия требованиям для ОКИИ по каждой нереализованной или реализованной частично мере защиты с созданием задач по устранению замечаний
– встроенная система управления заявками и задачами регулятора (например, предоставление данных об эксплуатируемой АС)

Возможности платформы позволяют осуществлять:

– формирование перечня критических процессов;
– определение критичности процессов;
– формирование перечня объектов;
– анализ возможных источников угроз и действий предполагаемых нарушителей;
– анализ возможных угроз ИБ и сценариев компьютерных атак;
– оценку масштаба последствий и соотнесение со значением показателей категорий;
– определение категории значимости объекта КИИ;
– контроль реализации состава мер по обеспечению безопасности для значимого объекта.

Для уведомления по различным значимым событиям всех участников процесса управления соответствием КИИ предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений. Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Методология базируется также на следующих нормативных документах:

– Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»
– Приказ ФСТЭК России № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;
– Приказ ФСТЭК России № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
– Приказ ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

СМ

Модуль управления соответствием НМД (Нормативно-Методическим Документам) для проверки на соответствие требованиям стандартов с выбором методики оценки на основе стандартов из пакета экспертизы (в «коробке») или реализация собственной методики оценки организации в целом и отдельных её элементов (информационные системы, бизнес-процессы, помещения, бизнес-активы и др.). Автоматизация процессов снижает количество рутинных операций, позволяя более эффективно собирать и обрабатывать информацию в едином окне, управлять напоминаниями и оповещениями с регулярным контролем.

Основной функционал:

– комплаенс согласно выбранным мерам и требованиям (Приказы ФСТЭК № 17, 21, 31, ГОСТ 57580, ISO 27001, NIST и др.) с базой знаний мер защиты (БДУ ФСТЭК)
– загрузка стандартов из файлов, автоматический сбор и анализ опросных листов и автоматизация оценки соответствия
– создание рабочих процессов, карточек и ОЛ, направляемых всем участникам аудита (с привлечением экспертной группы или без) для оценки на соответствие
– управление расписанием оценок с включёнными процессами архивации, согласований, напоминаний и оповещений участников аудита
– возможность формирования плана мероприятий по устранению нарушений и замечаний с постановкой и отслеживанием задач
– гибкие редакторы отчётов и дашбордов для формирования отчётности и сквозной аналитики в реальном времени

Пользователь может сформировать корпоративные стандарты, добавляя собственные требования либо переиспользуя требования из существующих стандартов. Внедрена группировка требований по доменам для облегчения анализа, при этом есть возможность кастомизировать общий вид документа как визуально, так и функционально. Стандарт обладает статусной моделью, обеспечивающей процедуру актуализации и перевода в архив устаревших документов.

Пользователь не ограничен по лимиту и функционал в части заведения в систему новых стандартов любой конфигурации, при этом база знаний коробочных стандартов постоянно поддерживается и дополняется в рамках регулярного обновления. Преднастроенные шкала оценки и варианты ответов, с возможностью добавлять варианты ответы и их «веса» для каждого конкретного требования.

Модуль позволяет загрузить ресурсно-сервисную модель предприятия (продукты, бизнес-процессы, информационные системы и технические элементы, например, сервера, помещения и оборудование). Загружаемые активы можно связать с мерами защиты, что позволит автоматически получить верхнеуровневую оценку соответствия по всей компании.

В продукте поставляется база знаний мер защиты (БДУ ФСТЭК), а также возможность создавать пользовательские меры. Меры обладают статусной моделью, которая позволяет оценить текущее и плановое соответствие требованиям конкретных активов. Реализован функционал заявок на внедрение пользовательских мер с отслеживанием хода их выполнения.

Для уведомления по различным значимым событиям всех участников процесса управления соответствием НМД предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Один из основных механизмов уточнения и сбора информации в процессе оценки – автоматизированная генерация опросных листов с делегированием на подразделения и исполнителей (в зависимости от объекта оценки). Реализован контроль статусов и прогресса заполнения с встроенным жизненным циклом, предусматривающим проверку его заполнения аудитором и отправкой на доработку при необходимости. Предусмотрен автоматический механизм валидации и консолидации данных в единую интегральную оценку соответствия объекта требованиям. В результате работы модуль агрегирует все полученные данные в единой карточке процесса оценки и подготовит шаблон плана мероприятий по приведению объекта оценки в соответствие требованиям стандарта.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

Процесс оценки соответствия позволяет автоматически определить невыполненные требования (которые применимы к анализируемому объекту), выделить их в отдельный документ и сформировать план мероприятий по их реализации. Система позволяет сформировать задачи на внедрение мер защиты и мониторить их исполнение во внешних системах.

Задачи (с возможностью кастомизации жизненного цикла) на внедрение мер защиты предоставляют возможность отслеживать сроки взятия в работу и др. SLA, исполнение требований, назначение/переназначение ответственных, приём/отправку задач на доработку и др. статусы.

Реализована двусторонняя интеграция со сторонними системами ITSM/SD:

- JIRA;
- NAUMEN;
- OTRS.

Это позволяет синхронизировать задачи внутри SV CM и во внешней системе. Есть возможность создания интеграции с любой необходимой внешней системой.

При выполнении задач на внедрение мер защиты все изменения автоматически отражаются на активах ресурсно-сервисной модели и в последующем учитываются при проведении регулярной оценки.

RM

Модуль управления рисками кибербезопасности базируется на собственной методологии расчёта и предназначен для автоматизации процесса управления рисками информационной безопасности, в том числе с учётом общепринятых методик (ГОСТ Р ИСО 31000-2019). Модуль реализует и автоматизирует циклический процесс формирования реестра рисков, моделирования угроз, расчёта вероятности и ущерба сценариев реализации рисков, выработку и внедрение мер защиты для повышения киберустойчивости организации.

Основной функционал:

– учет, классификация и управление кибер-рисками по методологиям ФСТЭК, качественной и количественной (FAIR) оценок
– моделирование по методологии Монте-Карло с перебором множества сценариев и применением случайных величин
– поддержка кастомной методологии заказчика/партнёра, реализуемой в ходе проекта внедрения системы/модуля
– подключение любых сторонних систем для сбора данных и обогащения, а также создание коннекторов к самописным и экзотическим системам
– непрерывный и повторяющийся процесс оценки вероятности реализации угроз, эффективности мер защиты в команде с привлечением экспертов и владельцев АС
– единая ресурсно-сервисная модель, применяемая для ИТ- (активы) и ИБ- (инциденты, уязвимости, угрозы) подразделений

Единая ресурсно-сервисная модель предоставляет возможность вести реестр рисков (подробное описание уязвимостей, вероятность реализации угрозы и др.), а также учитывать активы, подвергающиеся опасности.

Процесс состоит из идентификации рисков, качественной оценки их уровня, управления заявками и других задач, включая:

– ведение справочника результатов моделирования угроз (объекты воздействия, потенциал нарушителя, меры защиты, способы реализации угроз ИБ, угрозы ИБ);
– определение области оценки риска (выбор актива типа «Информационная система») с автоматическим учётом его характеристик для дальнейшего расчёта оценки величины киберриска;
– формирование списка угроз ИБ из справочника для последующей оценки рисков;
– формирование экспертной группы для автоматической рассылки;
– автоматическая агрегация результатов оценок от экспертов в карточки рисков;
– автоматический расчёт согласно предустановленной формуле и выставление величины киберриска по отношению к каждой угрозе;
– формирование и выгрузка локального экспресс-отчёта по итогам оценки рисков кибербезопасности;
– формирование и отслеживание задач по обработке рисков, назначаемых на исполнителей.

Проведение оценки может как полностью проходить в онлайн формате, так и быть частично вынесено в офлайн за счёт функционала импорта и экспорта данных в файл (составление опросных листов, методик оценки, формирование стандартов, этап сбора информации), что полезно для работы с удалёнными локациями. Все качественные оценки переводятся в балльную систему, в рамках которой результаты оценки могут быть рассчитаны с учётом принятых в конкретной организации практик (среднее, медиана, максимум и др.). За счёт этого качественная и количественная оценка рассчитываются по единым формулам.

Функционал моделирования рисков методом Монте-Карло позволяет проводить множество итераций сценариев, используя случайные величины для учёта возможных изменений и вариаций в данных. В результате пользователь сможет оценить потенциальную величину потерь и подверженность риску, а с помощью параметров распределения частоты и ущерба отследить минимум/среднее/максимум значений для дальнейшего.

После того как все данные собраны и показатели риска рассчитаны, в системе применяется функционал обработки, в рамках моделируется эффект от внедрения тех или иных мер защиты и процесс сопоставления их стоимости со степенью снижения риска при их внедрении. Таким образом, в интерфейсе системы можно подобрать наиболее адекватный набор мер по соотношению «Цена и эффективность».

Для уведомления по различным значимым событиям всех участников процесса управления рисками кибербезопасности предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

ORM

Модуль управления операционными рисками позволяет выстроить полноценную автоматизированную информационную систему для учёта и фиксации событий операционных рисков, мониторинг ключевых индикаторов рисков, проведения самооценки и контроля согласно Положению Банка России №716-П ЦБ РФ. Функционал модуля позволяет реализовать весь комплекс мероприятий с участием необходимых функциональных подразделений с применением процессного подхода к учёту, обработке и управлению рисками кредитной организации.

Основной функционал:

– учет, классификация и управление различными видами операционных рисков (правовые и модельные риски, потери средств клиентов/контрагентов, работников и др.)
– встроенная методология (количественная оценка рисков) согласно Положению Банка России № 716-П с мониторингом ключевых индикаторов риска (КИР)
– поддержка кастомной методологии заказчика/партнёра, реализуемой в ходе проекта внедрения системы/модуля
– подключение любых сторонних систем для сбора данных и обогащения, а также создание коннекторов к самописным и экзотическим системам
– непрерывный и повторяющийся процесс оценки вероятности реализации рисков, эффективности мер защиты в команде с привлечением экспертов и владельцев АС

Благодаря гибкому конструктору рабочих процессов реализуются основные процедуры:

– идентификация ОР;
– сбор и регистрация событий ОР;
– определение потерь и возмещений;
– проведение количественной оценки уровня ОР;
– проведение качественной оценки уровня ОР;
– выбор и применение способов реагирования на ОР;
– мониторинг ОР, в том числе ключевых индикаторов риска (КИР).

В модуле предусмотрены учет, классификация и управление различными видами риска, включая риск информационной безопасности, риск информационных систем, правовой риск, риск ошибок в управлении проектами, риск ошибок в управленческих процессах, риск ошибок в процессах осуществления внутреннего контроля, модельный риск, риск потерь средств клиентов, контрагентов, работников и третьих лиц, риск ошибок процесса управления персоналом, операционный риск платёжной системы.

Для уведомления по различным значимым событиям всех участников процесса управления операционными рисками предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

BCM

Модуль управления непрерывностью бизнеса выстраивает процессы обеспечения непрерывности деятельности в случае наступления чрезвычайных ситуаций и разработку планов восстановления деятельности (DRP, Disaster Recovery Plan). Поддерживается оценка ключевых показателей эффективности согласно российским и международным стандартам, проведение GAP-анализа. Автоматизация обработки результатов и актуализации данных объектов позволяет эффективнее устранять замечания и отслеживать статусы задач.

Основной функционал:

– организация процессов с учётом следующих НМД: ISO 22301, ГОСТ 22301, Положение ЦБ 787-П, Указание ЦБ 4148-У, ПП РФ N 730
– оценка критичности бизнес-процессов и объектов, планирования требований в случае нештатных ситуаций с автоматизированной обработкой результатов и GAP-анализ
– создание рабочих процессов, карточек и опросных листов, направляемых всем участникам аудита (с привлечением экспертной группы или без) для оценки
– автоматическая актуализация взаимосвязей объектов (бизнес-процессы, информационные системы и др.) и их показателей (RTO, RPO, MTPD)
– разработка планов обеспечения непрерывности и проведение их тестирования с оценкой ключевых показателей эффективности и возможностью формирование плана мероприятий по устранению нарушений
– постановка и отслеживание задач по устранению замечаний для подключения исполнителей, а также гибкие редакторы отчётов и дашбордов в реальном времени

Единая ресурсно-сервисная модель предоставляет возможность вести учёт бизнес-процессов и связанных элементов/ресурсов/активов, а также учитывать активы, подвергающиеся опасности.

Модуль автоматизирует следующие два ключевых процесса:

– BIA (Business Impact Analysis), оценка критичности бизнес-процессов компании и связанных с ними объектов;
– BCP (Business Continuity Plan), ведение и поддержка планов обеспечения непрерывности бизнеса в случае возникновения нештатных ситуаций.

Модуль позволяет проводить оценку потенциальных последствий, включая связи бизнес-процессов и любых других объектов, фиксируя их значимость и выявляя зависимости. Разработка планов восстановления после ЧП (инцидентов) происходит заранее и консолидировано на регулярной основе, что позволяет обеспечить восстановление функционирования бизнес-процессов компании.

Для уведомления по различным значимым событиям всех участников процесса управления непрерывностью бизнеса предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений. Встроенные оповещения позволяют отслеживать изменения различных статусов (с возможностью добавить произвольные):

– создание/отклонение/отзыв/просрочка опросного листа;
– изменение ответственного;
– оповещение о возврате в работу;
– согласование опросного листа;
– появление нового актуального плана непрерывности;
– активация плана восстановления.

Содержание планов обеспечения непрерывности:

- шаги устранения сбоев;
- условия активации;
- роли и их обязанности;
- контакты и методы коммуникаций.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt. Встроенные отчёты позволяют анализировать различные показатели и срезы данных, например:

- активные задачи на корректировку;
- бизнес-процессы без плана непрерывности;
- критичные бизнес-процессы;
- все завершённые опросные листы;
- готовые к анализу процессы оценки;
- информационные системы (их зависимости и метрики);
- общая оценка состояния процессов компании;
- объекты, связанные с критичными бизнес-процессами (с учётом RTO).

Оценка последствий прерывания деятельности происходит в финансовом выражении и позволяет выявить расхождения в показателях RTO (Recovery Time Objective), RPO (Recovery Point Objective), MTPD (Maximum Tolerable Period of Disruption) взаимосвязанных активов.

TIP

Модуль анализа угроз кибербезопасности и проведения киберразведки обеспечивает автоматический сбор индикаторов (компрометации, атаки, угрозы и др. типы) из внешних источников (поставщиков фидов и аналитических сервисов). После обработки и нормализации данных происходит обогащение для выстраивания взаимосвязей и ландшафта атаки, что даёт аналитику более подробную картину происходящего. Модуль в режиме реального времени осуществляет обнаружение индикаторов в трафике (в т.ч. с помощью машинного обучения), после чего предлагает ручное или автоматическое реагирование.

Основной функционал:

– интеграция «из коробки» с коммерческими (Kaspersky, FAACT ex. Group IB, BI.Zone, RST Cloud) и open-source (Alien Vault, Feodo Tracker, DigitalSide) фидами
– все уровни индикаторов: технический (хэш, IP, URL, домен, email), тактический (процесс, JARM, ключ реестра), операционный (уязвимости, ВПО) и стратегический
– 50+ конфигураций коннекторов «из коробки» для получения потока событий из решений различных классов (SIEM, NGFW, Proxy/Email-сервера и др.)
– поддержка кастомных коннекторов и универсальных форматов (Syslog, CEF, LEEF, EMBLEM, Event log)
– возможность обогащения из внешних источников (VirusTotal, Shodan, LOLBAS, KasperskyOpenTIP, IPGeolocation.io и др.) и встроенных БДУ ФСТЭК и MITRE ATT&CK
– продвинутые механики обнаружения индикаторов в потоке событий: DGA-механизмы с использованием машинного обучения, match и retro-поиск по всем собранным данным
– встроенное реагирование без обязательного применения SOAR для автоматизации, в т.ч. запуск действий из аналитического графа связей

Решение выявляет потенциальные угрозы информационной безопасности на ранней стадии. Модуль обеспечивает автоматический сбор индикаторов компрометации (Indicator of Compromise, IoC) из внешних источников, нормализацию полученных данных, обогащение дополнительной информацией. Помимо классических IoC агрегируются индикаторы атак (Indicator of Attack, IoA), данные об угрозах, злоумышленниках и применяемого ими вредоносного программного обеспечения (ВПО), позволяя получить срезы данных на всех уровнях Threat Intelligence (TI).

Получение и обработка данных осуществляется посредством интеграции с сервисами-поставщиками с использованием механизмов универсальных коннекторов, позволяя:

– получать информацию об индикаторах;
– производить обработку и нормализацию полученной информации;
– осуществлять фильтрацию;
– обеспечивать дедупликацию данных;
– создавать новую запись базе или обновлять информацию в существующем индикаторе на основании настраиваемых признаков.

Модуль поддерживает форматы описания индикаторов компрометации MISP и STIX2, интеграцию для автоматической загрузки данных из матрицы MITRE ATT&CK, а также интеграции с различными решениями для сбора инфраструктурных событий и дальнейшего автоматического поиска в режиме реального времени.

Рабочий процесс обработки индикатора компрометации может осуществляться как автоматически, так и инициируемыми пользователем действиями в соответствии с утверждёнными в организации регламентами и процессами, включая:

– обогащение дополнительными данными на основании внешних сервисов и информационных систем заказчика;
– выявление угроз в инфраструктуре заказчика как на основании ретроспективного анализа, так и в режиме реального времени;
– обновление конфигурации средств защиты информации с целью блокирования активностей, связанных с возможной атакой;

В дополнение к любым возможным интеграциям с внешними системами и сервисами модуль включает встроенные коннекторы, которые не нуждаются в лицензировании:

– SIEM (MicroFocus ArcSight (QueryViewer, Logger API Query, Syslog), KUMA (Syslog), MaxPatrol SIEM (API), IBM Qradar (Ariel Query, Reference Sets, Syslog);
– Почтовые сервера (Microsoft Exchange);
– Сетевые устройства с форматами отправки данных (CEF, LEEF, EMBLEM);
– Прокси сервера (Squid, Blue Coat);
– Источники данных об уязвимостях (CVE NIST, БДУ ФСТЭК, НКЦКИ);
– Песочницы (TrendMicro DDA, Kaspersky TIP, Kaspersky KATA, Virus Total);
– Системы отправки данных об инциденте (Security Vision SOAR, R-Vision SOAR, MaxPatrol SIEM. Kaspersky KUMA, ArcSight SIEM, IBM Qradar);
– NGFW для отправки IP-адресов на блокировку (CheckPoint NGFW, Cisco ASA, Cisco Firepower, Cisco Switch, Juniper);
– Шлюзы безопасности электронной почты (Cisco IronPort ESA, FireEye, TrendMicro IMSVA).

Поддерживается обогащение индикаторов из внешних песочниц и аналитических сервисов, в случае их нахождения в инфраструктуре (IPGeolocation.io, KasperskyOpenTip, IPInfo.io, IpGeolocation.io (Whoisxmlapi), Shodan, VirusTotal, MaxMind Geo-IP, HaveiBeenPwned, URLScan.io).

Для уведомления по различным значимым событиям всех участников процесса предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности и визуализации статистической информации в модуле предусмотрены интерактивные дашборды (включая географическую карту и другие способы визуализации), а также экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.

UEBA

Модуль поведенческого анализа позволяет автоматически выстраивать типовые модели поведения объектов инфраструктуры (пользователей, устройств, процессов и др.), анализируя сырые потоки данных (сетевой трафик, логи Windows/Linux серверов и рабочих станций, прокси-серверов, почтовых серверов, и др.) и выявлять отклонения посредством применения различных правил и моделей машинного обучения. Решение адаптируется под ландшафт данных и обучается на реальном потоке событий. Также решение предоставляет гибкие инструменты по анализу, расследованию и реагированию.

Основной функционал:

– анализ сырых потоков данных от различных внешних систем и узлов организации, с автоматическим формированием моделей поведения объектов ИТ-инфраструктуры
– автоматическое выявление отклонений и аномалий в поведении объектов ИТ-инфраструктуры организации (формирование инцидентов ИБ) с применением разных моделей и методик машинного обучения, с последующим оповещением специалистов службы ИБ
– поддержка белых списков (для исключений) и списков критичных систем (для автоматического создания инцидентов без учёта событий и их веса)
– методы математической статистики (~50 встроенных правил) и применение машинного обучения (~9 ML-моделей)
– обнаружение изменений в активности учётных записей, устройств и процессов ~30 уникальных правил корреляции и sigma-rules с возможностью адаптации
– автоматизация базовых действий по реагированию на выявленные инциденты ИБ (обогащение информации по объектам, отправка инцидентов в системы класса SOAR/SIEM, управляющее воздействия путём блокировки объектов для сдерживания)

Возможности выявления аномалий в корпоративной инфраструктуре обеспечены применением большое количество разных моделей и методик машинного обучения с объединением результатов отдельных моделей в инциденты для дальнейшего расследования.

Система автоматически обучается на основании сырых событий по каждому объекту инфраструктуры. Учитываются как характеристики объектов и их взаимодействия, так и количественные показатели: объем трафика, количество соединений, время входа и др. По результатам обучения модуль детектирует отклонения и сохраняет их в виде событий с заданным весом, уникальным для каждого правила выявления отклонений.

После накопления событий система запускает стандартное правило корреляции, которое находит объекты и события по ним, и создаёт инцидент по каждому объекту инфраструктуры. Все выявленные ранее события группируются по объектам. минимизируя количество ложноположительных срабатываний (инциденты создаются только при накоплении определённого количества событий по каждому отдельному объекту с суммарным весом, превышающих пороговое значение).

Предустановлены различные ML-модели и специализированные правила выявления аномалий (с возможностью коррекции и расширения параметров через UI-конструкторы).

Для уведомления по различным значимым событиям всех участников процесса предусмотрены следующие каналы оповещения: e-mail, Telegram, внутриплатформенная система оповещений.

Для формирования отчётности в модуле предусмотрен экспорт в виде файлов различных форматов pdf, docx, xlsx, csv, ods, odt, txt.