Центр кибербезопасности УЦСБ

— ваш партнер по внедрению передовых практик и технологий для защиты критически важных систем от цифровых атак.

Компетенции команды и глубокое погружение в архитектуру систем автоматизации позволяют точно переложить ваши бизнес-задачи и процессы на логику работы платформ, настроить качественную автоматизацию. Партнерские отношения с разработчиками решений дают возможность нам обеспечить кастомную настройку и расширение базового функционала при необходимости.

Мы профессионально подберем эффективную архитектуру системы и внедрим автоматизацию задач вашего бизнеса.

udv|group Start X R-Vision

Контакты

sec.ussc.ru

t.me/UralSecurity

+7 (343) 379-98-34
cybersec@ussc.ru

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Автоматизация ИБ

Внедрение инструментов автоматизации для комплаенс-контроля, эффективного сдерживания, устранения и расследования кибератак

Автоматизируйте процессы ИБ, чтобы

01 Выполнить требования внутренних стандартов и отраслевого законодательства

02 Действовать на опережение: сократить среднее время детектирования и реагирования на инциденты

03 Снизить риск кибератаки, минимизировать возможный финансовый и репутационный ущерб для компании

04 Минимизировать степень влияния человеческого фактора

05 Снизить нагрузку на команду за счет уменьшения повторяющихся и рутинных задач

06 Организовать учет активов, типизацию инцидентов и формирование сквозной аналитики

SGRC

Системы класса Security Governance, Risk Management and Compliance (Security GRC) автоматизируют управление информационной безопасностью, рисками и соответствием требованиям законодательства

- Категорирование объектов КИИ
- Классификация объектов защиты
- Моделирование угроз
- Контроль соответствия требованиям ИБ
- Управление инцидентами, рисками и мероприятиями
- Работа с документами по направлению

SOAR/ IRP

Системы класса Security Orchestration, Automation and Response (SOAR) автоматизируют процессы реагирования на инциденты ИБ, обеспечивают оркестрацию средств защиты информации и обогащение данных о событиях безопасности

- Управление ИТ-активами
- Регистрация, обработка и учет всех событий и инцидентов
- Обогащение данных об инцидентах
- Ранжирование событий по степени риска
- Автоматическое выполнение рутинных задач аналитика
- Запуск сценариев реагирования на инциденты ИБ (плейбуки)
- Координация средств защиты информации (оркестрация)
- Взаимодействие с ГосСОПКА

TIP

Системы класса Threat Intelligence Platform (TIP) обеспечивают обогащение систем управления ИБ данными киберразведки на основе открытых источников и баз данных ведущих игроков рынка

- Автоматический сбор, нормализация и обогащение индикаторов компрометации
- Передача обработанных данных напрямую на внутренние средства защиты
- Поиск и обнаружение индикаторов во внутренней инфраструктуре организации с помощью сенсоров

SECURITY AWARENESS

Решения класса Security Awareness автоматизируют процесс повышения осведомленности персонала в области обеспечения ИБ

- Назначение и контроль прохождения тренингов и курсов
- Оценка знаний, включая тестирование и имитацию фишинговых атак
- Сводная аналитика по подготовке