ЗАЧЕМ ВНЕДРЯТЬ ЕДИНУЮ ЭКОСИСТЕМУ ЗАЩИТЫ

- Сокращение времени реакции на инциденты за счет автоматизации
- Устранение хаоса данных — единая картина угроз вместо разрозненных событий
- Закрытие слепых зон на конечных узлах и в сети
- Формирование единого контура сетевой безопасности
- Упрощение расследований инцидентов благодаря контекстной аналитике и визуализации цепочек атак
- Снижение операционных затрат на информационную безопасность

ПОЧЕМУ НАМ ДОВЕРЯЮТ

- Входим в рейтинг CNews100 и CNews Security: крупнейшие ИТ-компании России 2024
- Объединяем компетенции ИБ, ИТ, инженерно-технической охраны, ЦОД и сервисного центра
- Закрываем проекты под ключ — от аудита до внедрения и сопровождения
- Работаем с государственными организациями и бизнесом
- Предлагаем точечные, комплексные и поэтапные сценарии внедрения
- Проводим пилоты и демонстрации до старта проекта

СОТРУДНИЧАЕМ С ВЕДУЩИМИ РОССИЙСКИМИ ВЕНДОРАМИ

R-VISION | SECURITY VISION | Kaspersky | Positive Technologies | F6

sec.ussc.ru

t.me/UralSecurity

+7 (343) 379-98-34

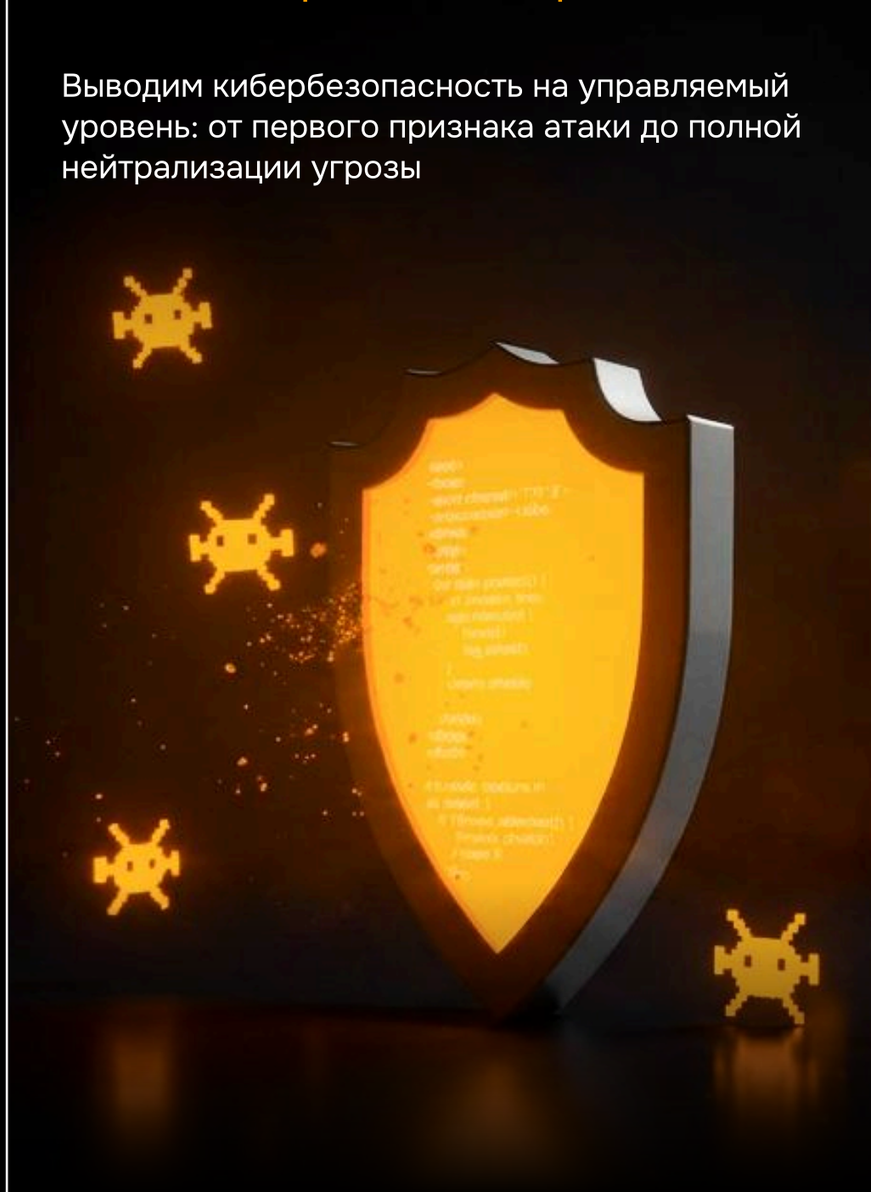
cybersec@ussc.ru

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

КОМПЛЕКСНЫЙ ПОДХОД К ОБНАРУЖЕНИЮ, АНАЛИЗУ И НЕЙТРАЛИЗАЦИИ УГРОЗ

5 ТЕХНОЛОГИЙ | 1 ЭКОСИСТЕМА | 0 СЛЕПЫХ ЗОН

Выводим кибербезопасность на управляемый уровень: от первого признака атаки до полной нейтрализации угрозы



РЕШЕНИЯ

5 ТЕХНОЛОГИЙ – 1 ЭКОСИСТЕМА

EDR

Endpoint Detection and Response (EDR) обеспечивает мониторинг и защиту конечных устройств в режиме реального времени, блокируя атаки на месте

- Непрерывный мониторинг активности на устройствах
- Выявление подозрительного поведения и атак
- Блокировка угроз на конечной точке
- Сбор и анализ телеметрии
- Расследование инцидентов на уровне хоста
- Изоляция зараженных устройств
- Поддержка реагирования и восстановления

NTA

Network Traffic Analysis (NTA) анализирует сетевой трафик для выявления аномалий, атак и скрытых угроз внутри инфраструктуры

- Анализ сетевого трафика в реальном времени
- Выявление аномалий и подозрительных паттернов
- Обнаружение атак и латерального перемещения
- Инвентаризация сетевых активов
- Построение карты сетевых взаимодействий
- Контроль теневой ИТ-инфраструктуры
- Поведенческая аналитика

SIEM

Security Information and Event Management (SIEM) объединяет события ИБ в единую систему, обеспечивая их анализ, корреляцию и контроль инцидентов

- Сбор и нормализация событий из разных источников
- Централизованное хранение данных
- Корреляция событий и выявление инцидентов
- Ретроспективный анализ и расследование
- Мониторинг и визуализация в единой консоли
- Формирование отчетности и соответствие требованиям
- Поддержка процессов реагирования

SOAR

Security Orchestration, Automation and Response (SOAR) автоматизирует процессы реагирования на инциденты ИБ, обеспечивает 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

Threat Intelligence Platform (TIP) обеспечивает 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

С ЧЕГО НАЧНЕМ

Этап 1	Аудит текущей инфраструктуры
Этап 2	Демонстрация решений
Этап 3	Пилот решений
Этап 4	Индивидуальный план внедрения
Этап 5	Внедрение под ключ

ВАРИАНТЫ РАБОТЫ

- Точечное внедрение
- Комплексное внедрение
- Поэтапное развитие
- Адаптация под отрасль