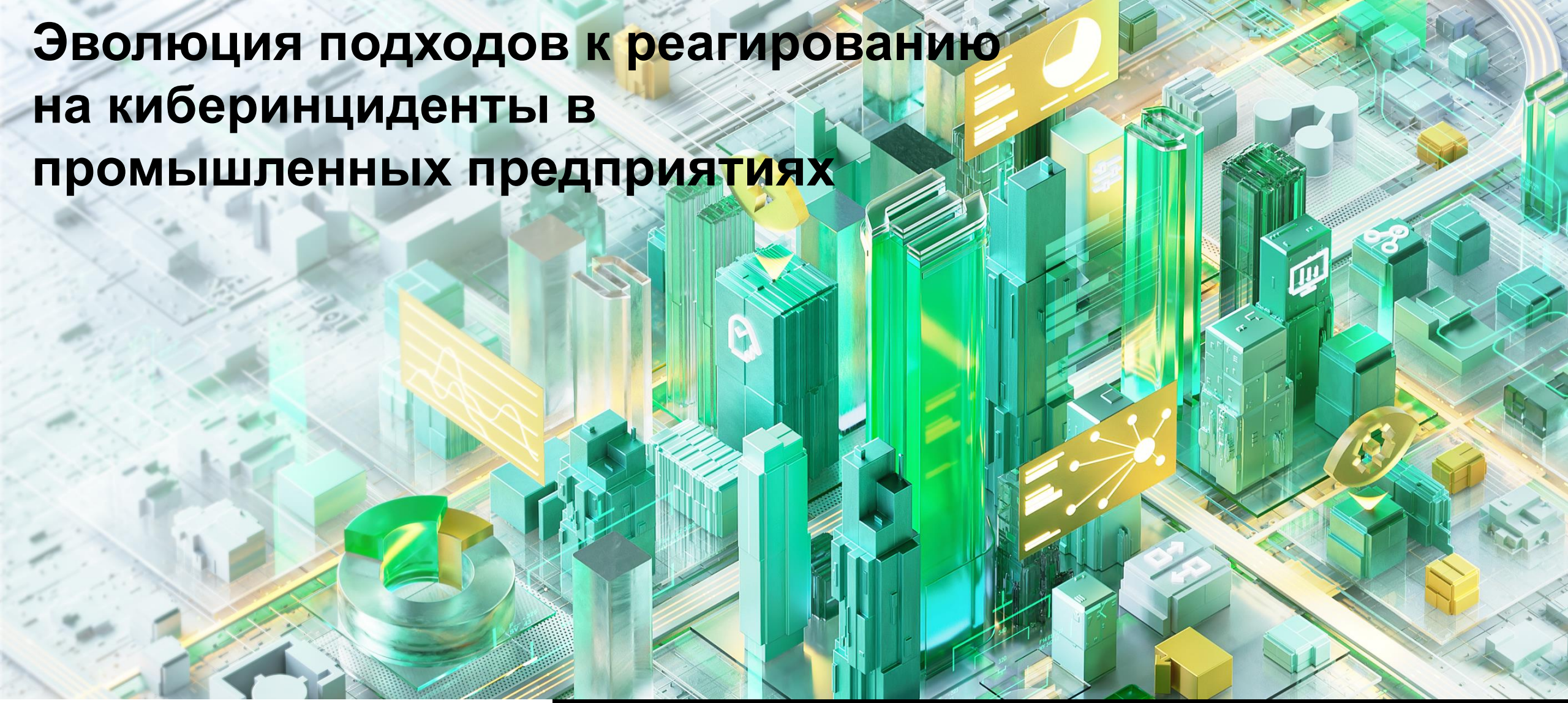
Эволюция подходов к реагированию на киберинциденты в промышленных предприятиях



Security Vision

Николай Гончаров
Директор департамента мониторинга кибербезопасности

Сегодня обсудим:

- Актуальность и проблематика кибербезопасности в промышленных предприятиях
- Изменения, произошедшие в защите промышленных систем
- Изменения, произошедшие в подходах мониторинга и реагирования
- Роль центров мониторинга кибербезопасности

Актуальность и проблематика

Рост киберугроз в промышленных системах

- Индустриальные объекты привлекают всё больше внимания хакеров из-за высокой критичности производственных процессов

Изменение подходов к организации инфраструктуры

- Промышленные сети исторически были физически изолированы, но с развитием цифровизации барьеры стираются, открывая новые векторы атак

Возросшие риски

- Не только утечка данных, но и возможная остановка производства, выход из строя оборудования, угрозы техногенных аварий

Новые требования к безопасности

- Стандартные методы, ориентированные только на IT-среду, недостаточны для защиты технологической (OT) инфраструктуры

Повышенное внимание регуляторов

- Ужесточение норм и стандартов области критической инфраструктуры

Ландшафт угроз для промышленных систем

	Ранняя стадия	Начало цифровой трансформации	Современный этап
Цели атак	• Редкие атаки на промышленность, основной фокус – IT-инфраструктура	• Рост атак на промышленные объекты, появление целевых атак	• Целенаправленные атаки на промышленные системы, критическую инфраструктуру
Мотивация атакующих	• Случайные эксперименты • Низкая экономическая заинтересованность	• Осознание потенциальной выгоды (промышленный шпионаж, саботаж)	• Финансовая (выкуп, кража/шпионаж) • Геополитическая, террористическая, идеологическая мотивация
Типичные векторы атак	• **Случайные вирусы** Физический перенос вредоносного ПО через внешние носители (дискеты, CD, USB)	• Использование уязвимостей в организации сетевого взаимодействия • Удалённый доступ через корпоративную сеть • Появление специализированного вредоносного ПО • Вредоносные внешние носители • Социальная инженерия (фишинг)	• Целенаправленные атаки через уязвимости в корпоративном сегменте (Эксплуатация уязвимостей в протоколах и ПО) • Атаки через подрядчиков • Использование программ вымогателей и шифровальщиков • Атаки через уязвимости в IOT • Атаки через цепочку поставок • Социальная инженерия и фишинг
Последствия атак	• Ограниченный ущерб, в основном простои отдельных систем	• Вывод систем из строя, первые серьезные перебои в работе промышленности	• Полная остановка производств, разрушение оборудования, утечка данных

Изменения произошедшие в защите промышленных систем

Security Vision

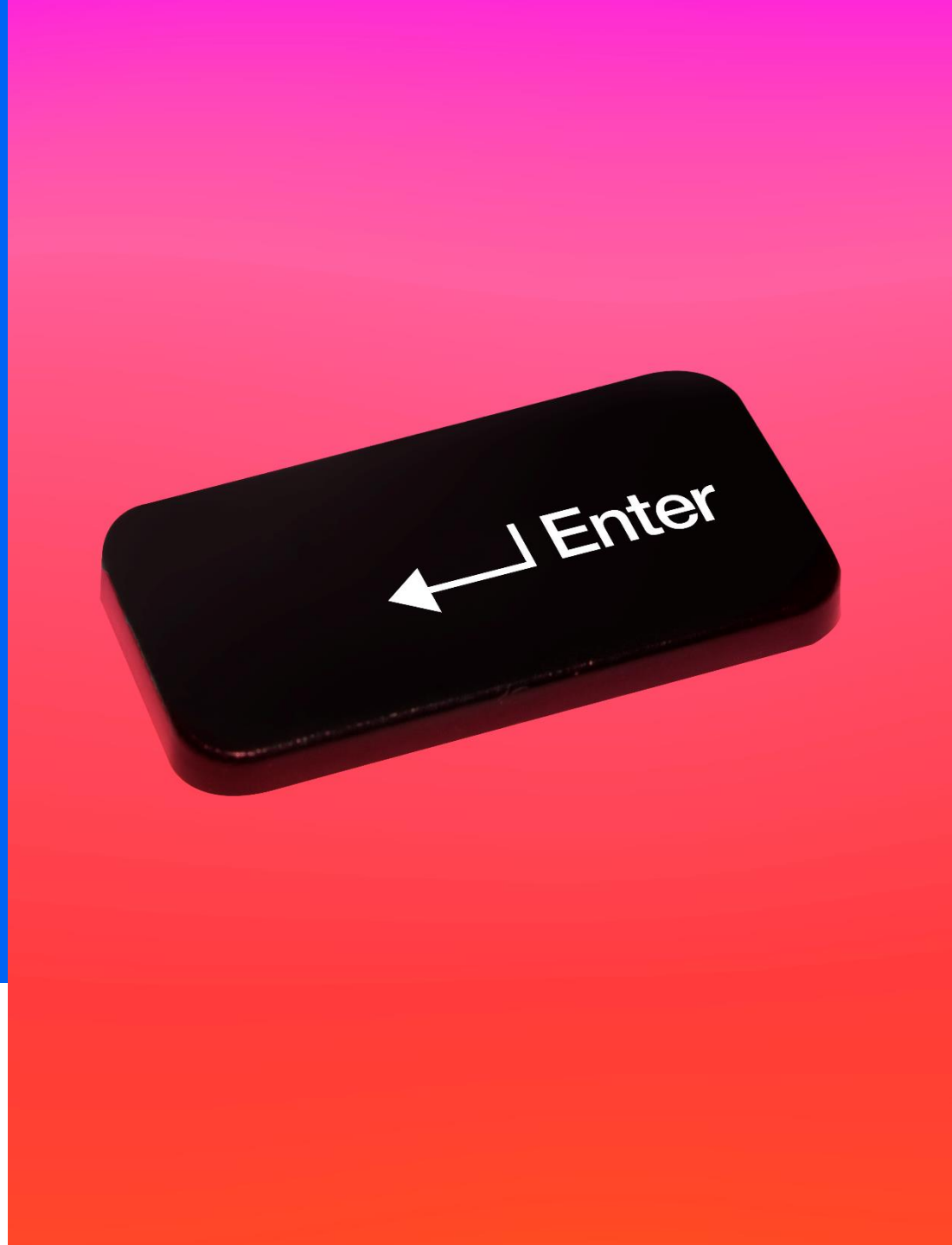
Ключевые изменения в организации защиты

	Ранняя стадия	Начало цифровой трансформации	Современный этап
Общий подход к защите	• Основной упор на физическую изоляцию OT-сетей • Основной фокус на физическую безопасность • Минимальная координация между подразделениям (ИБ, IT и OT)	• Постепенное сближение подразделений (ИБ, IT и OT). • Внедрение базовых мер для защиты промышленных систем • Начало формирования целостного взгляда на защиту технологического контура.	• Многоуровневый подход, учитывающий гибридные IT/OT-сети • Комплексная архитектура безопасности (контроль доступа, сегментация, мониторинг и т.д.) • Совместная стратегия обеспечения IT- и OT-безопасности под единым управлением и мониторингом
Технологии безопасности	• Использование базовых СЗИ в корпоративном сегменте • Локальный сбор логов без глубокой аналитики • Методы обнаружения – сигнатурные • Управление доступом на уровне статистических паролей и ограничение политик	• Внедрение SIEM в корпоративной среде, создание SOC, но ограниченное применение в OT • Начало использования специализированных СЗИ для технологических сетей • Начальные эксперименты с системами аналитики, Big Data, ML. • Внедрение многофакторной аутентификации	• Современные СЗИ(EDR, NTA, NGFW) • Комплексные платформы мониторинга и реагирования (SIEM + SOAR) для IT/OT, UBA/ML/AI для обнаружения аномалий • Активное использование профильных СЗИ, детальный анализ сетевых протоколов и команд управления • Применение технологий Honeypot/Deception • Использование TI/TH

Ключевые изменения в организации защиты

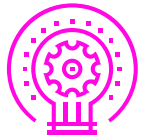
	Ранняя стадия	Начало цифровой трансформации	Современный этап
Расследование инцидентов и планы восстановления	• Мониторинг инцидентов практически отсутствует • Отсутствуют планы по реагированию на инциденты • Случаи атак редко документируются • Нет чёткого распределения ролей и обязанностей • Реакция «по факту»: устранение последствий, когда инцидент уже произошёл • Отсутствие системного анализа причин или механизмов атаки	• Начало разработки первых планов реагирования и регламентов • Начало Обучения специалистов по кибербезопасности в OT-сфере • Начало интеграции с SOC • Расследования киберинцидентов без проактивного поиска угроз • Редкое проведение киберучений	• Готовые планы по реагированию с учётом специфики OT • Глубокая интеграция с SOC • Автоматизация реагирования и чёткое распределение ответственности между подразделениями • Глубокие расследования с применением TI/TH • Проведение тестов на проникновение и эксплуатацию уязвимостей • Проведение регулярных киберучений
Нормативные требования и стандарты	• Практически отсутствуют чёткие регуляторные нормы для промышленных систем • Защита внедряется в основном по желанию компании	• Появление первых отраслевых требований • Осознание необходимости соответствовать стандартам	• Ужесточение требований, особенно к критическим инфраструктурам • Регулярные аудиты и отчётность • Рост штрафов за несоблюдение норм • Включение безопасности промышленного сектора как обязательный элемент Compliance
Человеческий фактор	• Обучение персонала ограничено • Операторы/инженеры OT не рассматриваются как ключевое звено кибербезопасности • Низкая осведомлённость о возможных кибератаках и методах социальной инженерии	• Появляются точечные тренинги для операторов/инженеров по основам информационной безопасности • Повышенное внимание к случайным ошибкам персонала и использованию внешних устройств	• Регулярные тренинги и сертификации для разных уровней сотрудников (от операторов до менеджмента) • Активные киберучения • Культура безопасности - часть корпоративной политики

Изменения, произошедшие в подходах мониторинга и реагирования



Security Vision

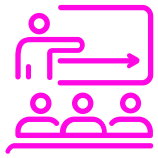
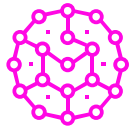
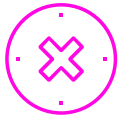
Изменения, произошедшие в подходах мониторинга и реагирования

	Начало цифровой трансформации	Современный этап
 **Мониторинг инфраструктуры**	— Обеспечение видимости всех ключевых компонентов инфраструктуры (APM, сервера, сетевые устройства, базы данных) через сбор логов и событий • **Технологии:** — SIEM – сбор и мониторинг логов с сетевых устройств, серверов и конечных точек. Мониторинг осуществляется в основном на основе статических правил • **Ограничения:** — Ограниченная видимость и слабая способность обнаруживать аномалии в поведении пользователей или новых атак, которые не попадали под предопределённые сигнатуры и правила корреляции	— Полный мониторинг всей IT-экосистемы, включая облачные и гибридные среды, с акцентом на проактивное выявление аномалий и угроз **Технологии:** — SIEM, SOAR, AI, ML, UEBA на базе одной платформы (Next Generation) — TI/TH — EDR, NTA, NGFW • **Преимущества:** — Глубокая аналитика поведения пользователей и автоматическое выявление аномалий на основе данных машинного обучения, что позволяет выявлять атаки до их реализации
 **Обнаружение и корреляция инцидентов**	— Обнаружение инцидентов на основе корреляции событий и предопределённых правил, настроенных в SIEM • **Технологии:** — SIEM с корреляцией событий на основе статических правил — Различные СЗИ (IDS/IPS, AV, FW и .тд) — Логи инфраструктуры (AD/DC, DNS, Proxy, BD и т.д) — Сетевые устройства • **Ограничения:** • Высокий уровень ложных срабатываний и ограниченная возможность для выявления сложных угроз, таких как APT, из-за зависимости от статических правил	— Обнаружение инцидентов в реальном времени на основе продвинутых аналитических моделей и данных о поведении пользователей и устройств • **Технологии :** — Дополнительно к уже имеющимся: — SIEM, SOAR, AI, ML, UEBA на базе одной платформы (Next Generation) — TI/TH — EDR, NTA, NGFW • **Преимущества:** — Использование динамических моделей поведения позволяет обнаруживать неизвестные угрозы и предугадывать их развитие, что снижает количество ложных срабатываний

Изменения, произошедшие в подходах мониторинга и реагирования

	Начало цифровой трансформации	Современный этап
 **Реагирование на инциденты**	— Реагирование на инциденты после их выявления вручную или полуавтоматическими средствами, блокировка атак через FW и другие защитные механизмы • **Технологии:** — SIEM — Различные СЗИ (IDS/IPS, AV, FW и .тд) — Администрирование инфраструктуры (AD/DC, DNS, Proxy, BD и т.д) — Сетевые устройства • **Ограничения:** — Задержка в реакции из-за зависимости от человеческого фактора и отсутствия автоматизации процессов. Это увеличивало время устранения угроз и повышало риск ущерба	— Автоматизация реагирования на инциденты с минимальным участием человека. Реакция происходит в режиме реального времени с минимальными задержками • **Технологии:** — SIEM, SOAR, AI, ML, UEBA на базе одной платформы (Next Generation) — TI/TH — EDR, NTA, NGFW • Преимущества: — Снижение времени на реакцию благодаря автоматизации процесса, что позволяет мгновенно реагировать на инциденты и минимизировать ущерб
 **Управление инцидентами и отчётность**	— Ведение отчётности и управление инцидентами вручную, обеспечение соответствия требованиям стандартов и нормативов • **Технологии:** • SIEM для генерации отчётов и хранения логов • Таблицы Excel • Ручное документирование • **Ограничения:** • Большое количество времени, затрачиваемого на отчётность, ручное управление процессами и сложности с выполнением требований нормативов	— Автоматизация управления инцидентами и отчётности, интеграция с регуляторными требованиями • **Технологии:** — SOAR — GRC • **Преимущества:** — Быстрая и точная отчётность с минимальными затратами времени, автоматическое соответствие требованиям стандартов и регуляторов

Изменения, произошедшие в подходах мониторинга и реагирования

	Начало цифровой трансформации	Современный этап
 **Анализ угроз и предотвращение атак**	— Реакция на инциденты после их выявления, предотвращение угроз через обновление сигнатур и корреляционных правил • **Технологии:** — SIEM — Различные СЗИ (IDS/IPS, AV, FW и .тд) — Администрирование инфраструктуры (AD/DC, DNS, Proxy, BD и т.д) — Сетевые устройства • **Ограничения:** — Ограниченная способность к проактивной защите, так как большинство угроз предотвращались только после их появления	— Проактивное предотвращение атак до их реализации с использованием предиктивной аналитики, AI и данных TI/TH • **Технологии:** — SIEM, SOAR, AI, ML, UEBA на базе одной платформы (Next Generation) — TI/TH — EDR, NTA, NGFW • **Преимущества:** — Способность предотвратить атаки до их реализации, быстрое реагирование на новые угрозы, усиление охраны от целевых атак (APT)
 **Обработка большого объёма данных**	— Увеличение объёма логов из различных источников, но данные поступали в основном из внутренних серверов, сетевых устройств и систем безопасности	— Экспоненциальный рост данных, кратно возросло количество систем, подключённых к мониторингу(Включая внешние периметры), кратно увеличилось количество передаваемых данных
 **Ложные срабатывания**	— Большое количество ложных срабатываний на фоне полезных данных. — Высокий уровень ложных срабатываний из-за использования статических правил и ограниченной аналитики. Каждое срабатывание требовало ручной проверки	— Несмотря на автоматизацию, использование современных средств и распределение задач анализа между современными СЗИ, использование AI и ML, проблема ложных срабатываний сохраняется — Системы ещё не совершенны, и часто требуется ручная верификация сложных инцидентов

Изменения, произошедшие в подходах мониторинга и реагирования

- Современный SOC становится более ориентирован на предсказание угроз и проактивное выявление инцидентов

Технологии стали гораздо более проактивными и автоматизированными

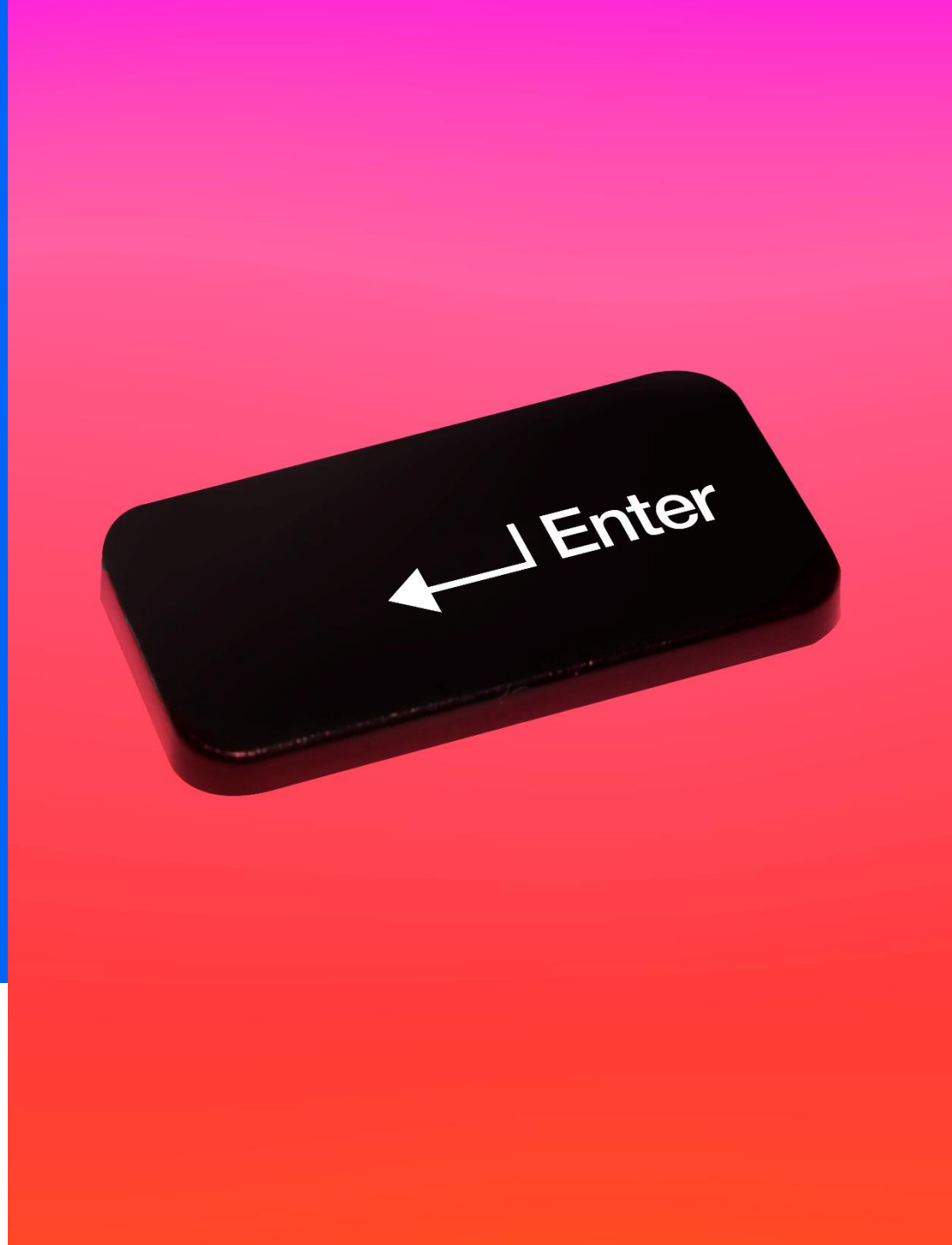
Интеграция с бизнесом и другими подразделениями

- Стала ключевым фактором. SOC теперь глубоко интегрирован в бизнес-процессы компании

- Играют всё более важную роль, особенно с учётом санкций и необходимости независимости от западных поставщиков

Российские решения для SOC

Роль центров мониторинга кибербезопасности



Security Vision

Современный центр мониторинга кибербезопасности

- **Основная задача** – предотвращения инцидентов до их возникновения и быстрое реагирование на инциденты в режиме реального времени
- Тесная коллаборация с бизнес целями и задачами

Люди

- **Аналитики/эксперты L1, L2, L3**
- **Архитекторы и инженеры**
- **Администраторы**

BI дашборды

SLA и комплексный подход

- Время реагирования
- Полнота информирования
- Доступность 24/7/365
- Масштабируемость

Технологии

Российские решения

- Основные системы – Next generation платформы, объединяющие технологии (SIEM, SOAR, AI, ML, UEBA, AM, VM)
- Различные СЗИ (IDS/IPS, AV, FW и .тд)
- TI/TH
- EDR, NTA, NGFW
- Deception

Инфраструктура

- АРМ + Сервера
- СХД
- (AD/DC, DNS, Proxy, BD и т.д)
- Сетевые устройства

Процессы

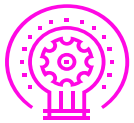
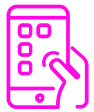
- Автоматизация процессов работы SOC
- Мониторинг и обнаружение угроз
- Управление инцидентами безопасности
- Реагирование на выявленные угрозы
- Корреляция событий и управление логами
- Проведение расследований
- Анализ новых **угроз – проведение киберразведки**
- Управление уязвимостями
- Управление активами
- Киберучения

- Строительство учитывает бизнес-задачи и процессы компании и интегрировано во всю инфраструктуру, включая ИТ и ОТ

Функции SOC (MITRE - стратегий SOC-центра мирового уровня)

Обработка данных в реальном времени	Единый координирующий центр (Колл-центр)	Мониторинг, анализ и разбор данных в режиме реального времени	Приоритизация событий	Оперативное информирование		
Работа с внешними источника информации	Сбор и анализ внешних данных	Сбор и анализ бюллетени безопасности	Подготовка собственных материалов для публикации	Обогащение правил SOC на основе внешних данных	Стратегическое планирование	Оценка угроз
Стратегическое планирование и развитие	Исследование и Оценка угроз	Анализ и внедрение новых решений для развития SOC	RnD	Стратегическое планирование	Разработка новых правил корреляции и сигнатур	
Анализ и реагирование на инциденты	Анализ инцидентов	Фиксация действий нарушителя	Координация реагирования на инциденты	Выполнение контрмер	Работы по реагированию на месте	Удалённое реагирование
Проведение криминалистической экспертизы	Снятие цифровых образов и их анализ	восстановление цепочки действия злоумышленника	Сбор цифровых доказательств	Реверс инжиниринг вредоносного ПО	Анализ прочих файлов и образов	
Техническое обеспечение работоспособностиSOC	Поддержание работы инфраструктуры	Поддержание работы СЗИ	Поддержание работы средств по получению и анализа данных	Поддержание работоспособности основных систем SOC		
Аудит и работа с внутренними угрозами	Сбор и хранение данных аудита	Управление и обработка данными аудита	Поддержка при работе с внутренними угрозами	Расследование случаев внутренних нарушений		
Проведение оценки защищённости	Сканирование и актуализация топологии сети	Оценка защищённости	Сканирование сети на наличие уязвимостей	Проведение тестирования на проникновение		
Прочее	Оценка средств защиты	Повышение осведомлённости	Консультирование по вопросам информационной безопасности	Взаимодействие с общественностью и СМИ	Взаимодействие с общественностью и СМИ	

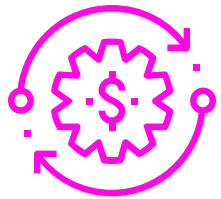
Роль центров мониторинга кибербезопасности

	Начало цифровой трансформации	Современный этап
 **Подход**	• **Реактивный подход** • SOC реагируют на инциденты после их обнаружения и фокусировались на минимизации ущерба, восстановлении систем и анализе последствий атаки	• **Проактивный и предиктивный** • Используются технологии для предотвращения инцидентов до их возникновения, таких как прогнозирование атак с помощью искусственного интеллекта и машинного обучения. Фокус сместился на предотвращение угроз до их реализации и на быстрое реагирование на инциденты в режиме реального времени
 **Технологии обнаружения и реагирования**	• Большинство решений по безопасности полагаются на сигнатурные методы обнаружения угроз (например, антивирусы, IDS), которые могли идентифицировать только известные угрозы • Правила корреляция в SIEM нацеленные на известные атаки • Базовые СЗИ (IDS/IPS, AV, FW и .тд)	• Активно внедряется и используется поведенческая аналитика, машинное обучение + AI для выявления аномалий и новых угроз. • Поведенческий анализ позволяет выявлять подозрительные активности (для которых нет сигнатур) в сети и реагировать на новые типы атак • Базовые СЗИ + Развитие технологий: TI/TH ,EDR, NTA, NGFW, Deception
 **Автоматизация**	• Большинство процессов – **ручные** • Операторы SOC вручную обрабатывали инциденты, что требовало больших ресурсов и времени	• Большинство процессов – **автоматизированы** • Современные SOC используют платформы SOAR для автоматизации процессов реагирования на инциденты
 **Инфраструктура**	• **Локальная**	• **Распределённая**
 **Мобильность и гибкость персонала**	• **Фиксированные рабочие места**	• **Гибридные и дистанционные рабочие места**

Роль центров мониторинга кибербезопасности

	Начало цифровой трансформации	Современный этап
Персонал	• **Аналитики/эксперты** • **Архитекторы и инженеры**	• Роли стали более интегрированными и мультифункциональными • Аналитики/эксперты L1, L2, L3 (TI/TH, инженер по автоматизации процессов безопасности, AI/ML инженер) – распределение по • Архитекторы и инженеры • Администраторы
Процессы	• Мониторинг и обнаружение угроз • Управление инцидентами безопасности • Корреляция событий и управление логами	• Автоматизация процессов работы SOC • Мониторинг и обнаружение угроз • Управление инцидентами безопасности • Реагирование на выявленные угрозы • Корреляция событий и управление логами • Проведение расследований • Анализ новых угроз – проведение кибервразведки • Управление уязвимостями • Управление активами • Киберучения
SLA	• SLA на базовое реагирование	• SLA и комплексный подход
Отчётность	• Ручная + Excel	• Автоматизированная • BI дашборды
Вендора решений	• Иностранные	• Российские

Роль центров мониторинга кибербезопасности



участие в бизнес-процессах

Начало цифровой трансформации	Современный этап
Изолированность SOC от бизнеса: SOC функционирует как отдельное техническое подразделение, не интегрированное с бизнес-процессами компании. Это приводило к недооценке влияния киберугроз на бизнес	**Стратегическая роль SOC:** SOC активно взаимодействуют с бизнес-подразделениями, помогая оценивать бизнес-риски и влиять на стратегические решения. SOC стал важным элементом в общей бизнес-стратегии компании
Фокус на технические задачи: SOC занимается только вопросами кибербезопасности и управляет только техническими рисками в IT-инфраструктуре, но не принимая участия OT и в управлении бизнес-рисками и их оценке	**Фокус на управление бизнес-рисками:** SOC интегрирован в процессы управления рисками на уровне компании и оказывает непосредственное влияние на принятие бизнес-решений, включая оценку влияния киберугроз на репутацию, финансы и стратегические цели компании

Историческая перспектива и предпосылки в защите промышленных систем

Ранняя стадия	Начало цифровой трансформации	Современный этап
• Отсутствие взаимосвязей между сегментами OT и IT • Фокус на физическую изоляцию сегментов и защиту внешнего периметра • Редкие случаи кибератак на промешенные системы • Применение минимального набора мер по обеспечению кибербезопасности • Отсутствие полноценного мониторинга событий	• Рост взаимосвязей между сегментам IT и OT • Появление удаленного доступа для обслуживания промышленных систем • Появление первых целенаправленных кибератак • Смещение фокуса защиты в сторону обеспечения кибербезопасности • Развитие технологии обеспечения защиты и мониторинга кибербезопасности • Формирование политик по обеспечению кибербезопасности, первых отраслевых стандартов	• Активная цифровизация производства, внедрение IoT-систем • Ужесточение регуляторных норм и стандартов • Массовые целенаправленные кибератаки • Широкое внедрение комплексных систем управления кибербезопасностью • Переход к преактивной, интегрированной защите с использованием машинного обучения и систем автоматизации

Спасибо за внимание

Telegram

Блог

Хабр

Security Vision

Николай Гончаров

Директор департамента мониторинга кибербезопасности

Интеллектуальная платформа информационной безопасности

securityvision.ru