Тренды построения SOC для холдинговой структуры

РГ «Кибербезопасность» НТИ «Энерджинет»

Гуревич Алексей

Атаки на энергетический сектор

За первый квартал 2025 года рост атак в среднем увеличился на 40% и превышает аналогичный показатель за первое полугодие 2024 года и на 60% — показатели четвёртого квартала 2024 года.

Особенности кибератак в 2025 году

Смещение мотивации

В 2024 году большинство атак (60%) было направлено на получение доступа к финансовым данным, то в 2025 году лишь четверть инцидентов связана с попытками похитить деньги. Количество атак с шпионскими целями выросло до 41%.

Увеличение количества случаев фишинга в ТЭК

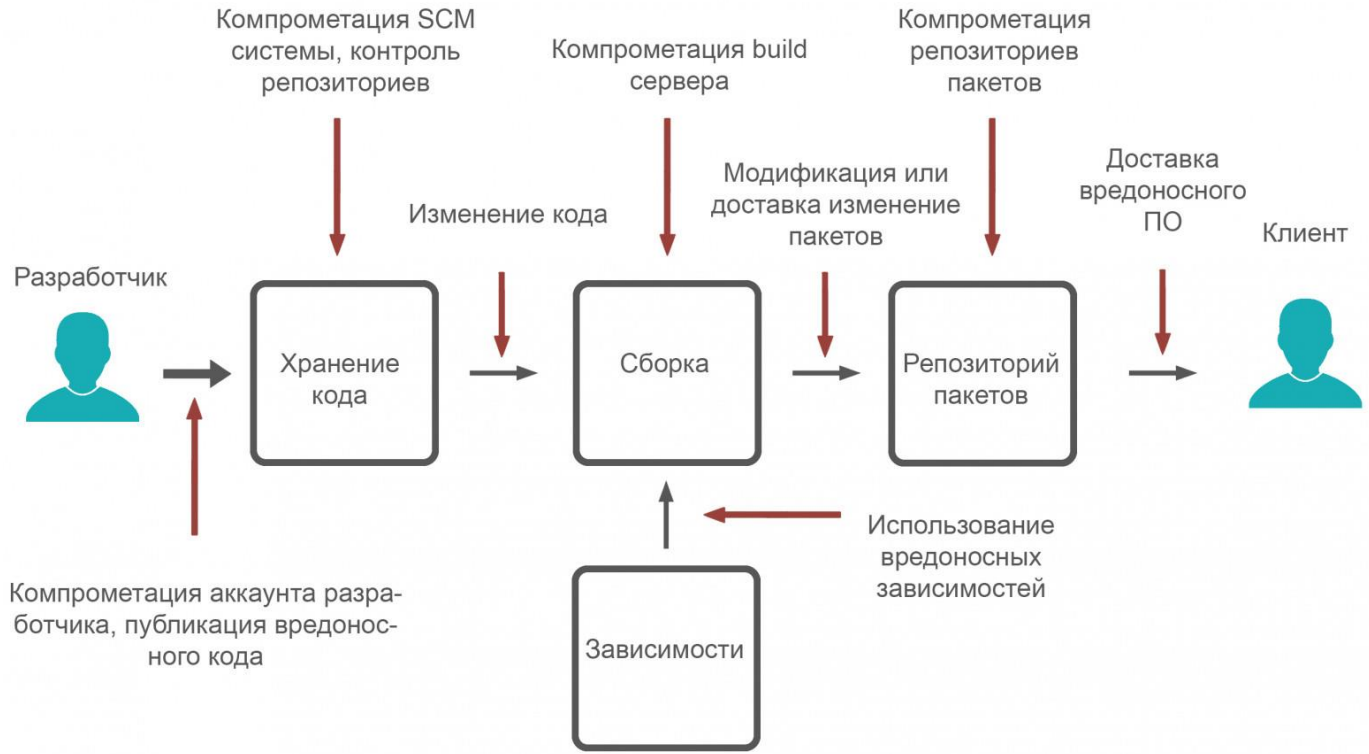
Рассылаются фальшивые предложения об инвестиционных продуктах или выплатах дивидендов.

Рост атак на SCADA

Может привести к остановке производственных линий или полного прекращения работы предприятия, что создаёт не только экономические и репутационные риски, но и угрозу для жизни людей.

В результате нефтегазовая отрасль вошла в топ-5 наиболее атакуемых секторов экономики, I квартал стал особенно тяжёлым месяцем по количеству DDoS-атак.

Атаки на «цепочки поставок» программного обеспечения



- Все еще отсутствие обязательных требований для подрядчиков промышленных предприятий и в первую очередь субъектов КИИ о защите своей информационной инфраструктуры;
- Не хватает финансового и кадрового обеспечения для выстраивания ИБ процессов проектирования и пуско-наладочных работ.

Требования: Мониторинг инцидентов ИБ

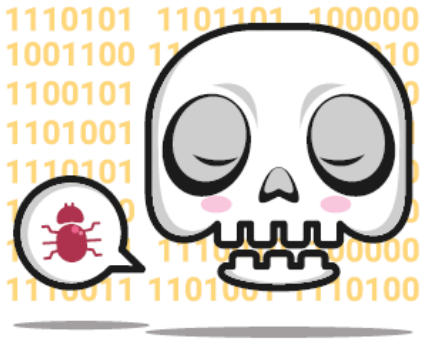
Наличие процессов мониторинга ИБ в РФ является не рекомендацией, а прямым законодательным требованием для компаний:

- Всех операторов ПДн.
- Субъектов критической информационной инфраструктуры (особенно для значимых объектов КИИ, где мониторинг должен быть непрерывным).
- Операторов ГИС.
- Организаций в регулируемых отраслях (ТЭК, связь, транспорт, финансы и др.).

Мониторинг ИБ компании – модель MSSP

По модели MSSP (Managed Security Service Provider) – на базе внешнего ИТ-интегратора или инсорсера

1. Мультитенантность: Обслуживание множества дочерних организаций на единой платформе.
2. Стандартизация: Услуги на основе типового сервиса с фиксированным SLA, минимум кастомизации (доработка правил нормализации и корреляции).
3. Масштабируемость: адаптирование под новых клиентов и рост инфраструктуры.
4. Экономия на CAPEX: снижение затрат на инфраструктуру, ПО и найм «с нуля».
5. Доступ к экспертизе 24/7.
6. Фокус на массовых угрозах: Оптимизация под распространенные атаки (малвар, сканирование).
7. Управляемый стек технологий: MSSP выбирает, внедряет и поддерживает инструменты (SIEM, SOAR, TIP, EDR и др.).
8. Отчетность по SLA: время реакции, количество инцидентов.



Мониторинг ИБ компании – модель in house

По модели собственного SOC

1. Полный контроль и кастомизация: Адаптация процессов, инструментов и отчетности *идеально* под нужды бизнеса.
2. Глубокий контекст: Аналитики знают среду компании изнутри, повышая точность и снижая ложные срабатывания.
3. Прямая интеграция и скорость: Прямое взаимодействие с внутренними системами (ITSM, CMDB) и командами; потенциально высокая скорость реакции.
4. Фокус на уникальных/целевых угрозах: Возможность концентрироваться на APT, отраслевых и специфических атаках.
5. Полная прозрачность и владение данными: Прямой доступ ко всем данным, настройкам и логике работы инструментов.
6. Развитие внутренней экспертизы: Построение и удержание собственной команды экспертов.
7. Прямая ответственность: Четкое разграничение зон ответственности внутри компании.
8. Оптимизация под Compliance: Тонкая настройка под строгие регуляторные требования компании.

Ограничения моделей

MSSP

1. Ограниченная кастомизация и контекст.
2. "Обезличенность" и сложности эскалации.
3. Проблемы интеграции и "черный ящик".
4. Зависимость от MSSP и сложность смены.
5. Размытость ответственности.

in house

1. Очень высокие затраты (CapEx & OpEx).
2. Сложность найма и удержания кадров.
3. Долгий срок выхода на эффективность.
4. Сложность поддержания и развития.
5. Управление производительностью и зрелостью.

РГ «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности

EnergyNetCS@ya.ru