08/12/2021

КИБЕРКРИМИНАЛИСТИКА: РАЗВИВАЕМ ВОЗМОЖНОСТИ SOC

Дмитрий Лифанов

Ведущий Аналитик Центра мониторинга
и реагирования на инциденты ИБ Jet CSIRT
csirt@jet.su

SOC ФОРУМ

В ЧЕМ ПРОБЛЕМА?

PREVENTION

DETECTION

RESPONSE

В ЧЕМ ПРОБЛЕМА?

PREVENTION DETECTION RESPONSE

ВНУТРЕННИЕ РЕШЕНИЯ

ВНЕШНИЕ РЕШЕНИЯ И СЕРВИСЫ

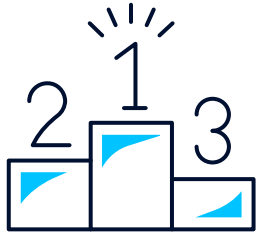
В ЧЕМ ПРОБЛЕМА?

ВНУТРЕННИЕ РЕШЕНИЯ

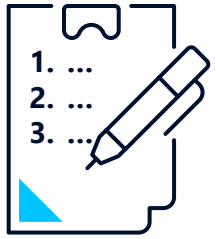
JET CSIRT RESPONSE

В ЧЕМ ПРОБЛЕМА?

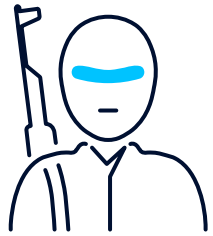
БОЛЬШИНСТВО SOC НЕ ОЖИДАЕТ ИНЦИДЕНТА



КОНКУРЕНЦИЯ МЕЖДУ SOC И IR КОМАНДАМИ



ОТСУТСТВИЕ ПЛАНА НА СЛУЧАЙ ИНЦИДЕНТА



ГЛАВНАЯ ЦЕЛЬ: ПОИСК ВИНОВНОГО

КАК РЕШИТЬ?

СТАРТОВАЯ ПОДГОТОВКА ДО ИНЦИДЕНТА

- Начальное интервьюирование
- Выделение ответственных
- Проработка плана базового реагирования

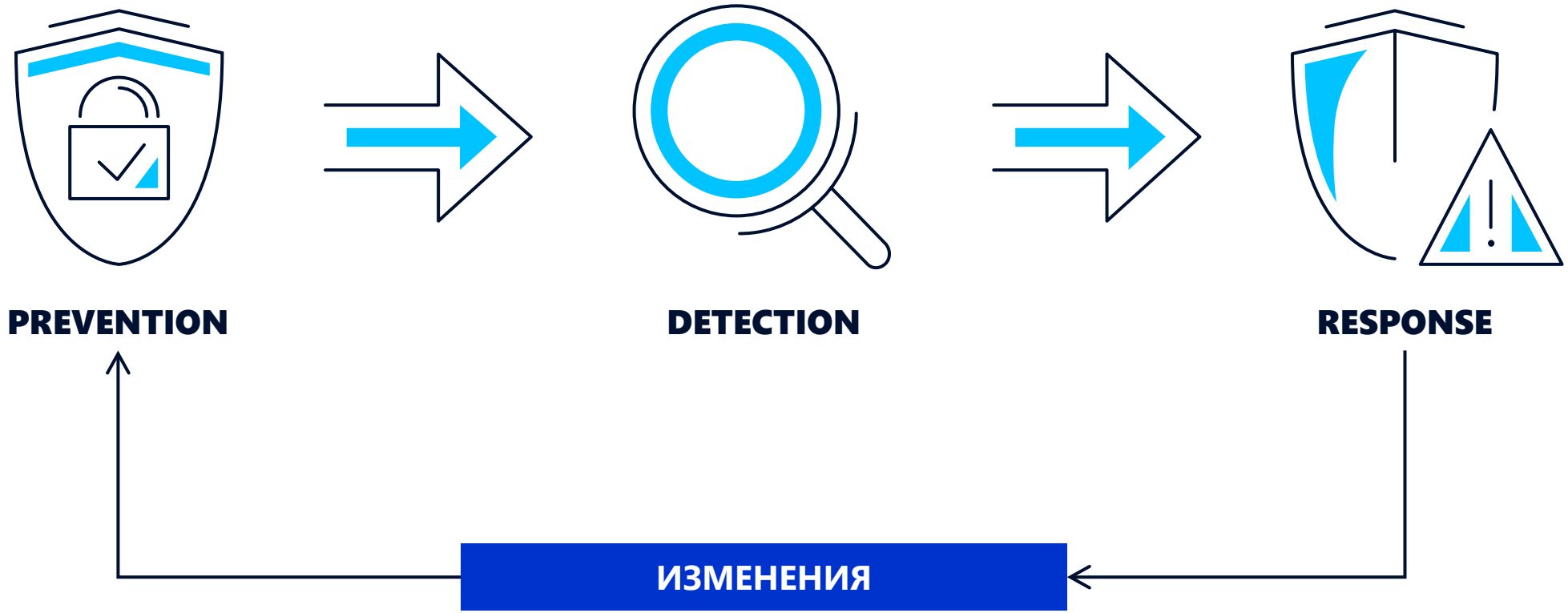
ТЕХНИЧЕСКОЕ УСИЛЕНИЕ

- MDR-инструменты
- Threat Hunting
- Purple Team

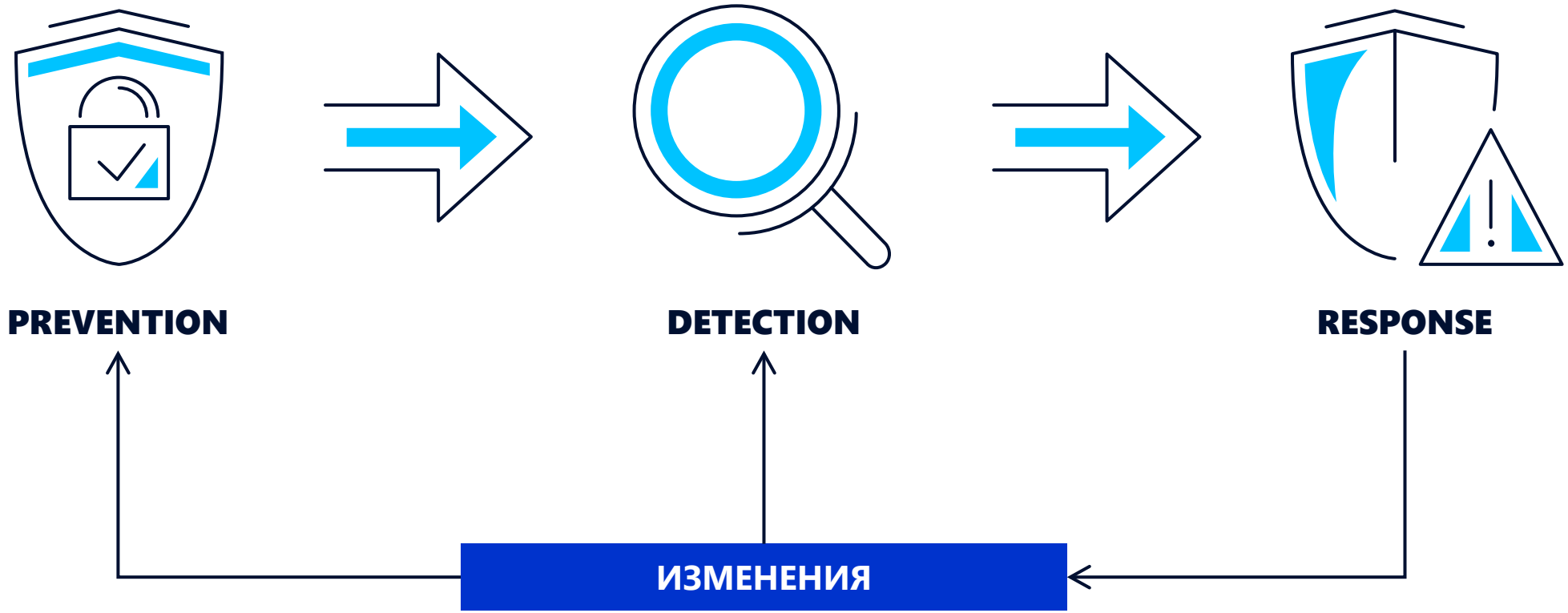
ПРИВЛЕЧЕНИЕ В РАМКАХ IR АКТИВНОСТЕЙ

- Знание инфраструктуры
- Погруженность в текущие процессы
- Новый опыт

ЧТО ДАЛЬШЕ?



ЧТО ДАЛЬШЕ?

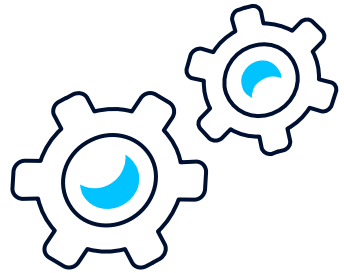


ЧТО ДАЛЬШЕ?

СБОР ДАННЫХ

АНАЛИЗ TTP И ИНСТРУМЕНТОВ

РАСПРЕДЕЛЕНИЕ ПО НАПРАВЛЕНИЯМ



РАЗРАБОТКА КОНТЕНТА

ОТ ИНЦИДЕНТА К THREAT HUNTING ГИПОТЕЗЕ

ОТ ИНЦИДЕНТА К THREAT HUNTING ГИПОТЕЗЕ

3 НАЙДЕННЫХ БЭКДОРА НА УСТРОЙСТВАХ

- Закрепление через .conf файлы продукта
- LD_PRELOAD бэкдор
- Web-shell для приложения управления

7 ГИПОТЕЗ INITIAL ACCESS, EXECUTION И PERSISTENCE

- Boot or Logon Autostart Execution
- Hijack Execution Flow
- Scheduled Task/Job
- Command and Scripting Interpreter
- Server Software Component

ОХВАТ ПРОДУКТОВОЙ СЕРИИ ВЕНДОРА

- Вся продуктовая линейка вне зависимости от функционального назначения

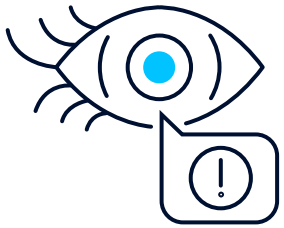
РАЗВИТИЕ ПРАВИЛА ДЕТЕКТИРОВАНИЯ

РАЗВИТИЕ ПРАВИЛ МОНИТОРИНГА

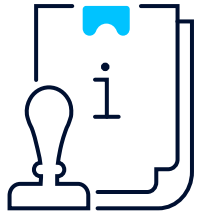
НА ПРИМЕРЕ АТАК НА GITLAB

RANSOMWARE-АТАКА НА ВНЕШНЮЮ КОМАНДУ РАЗРАБОТКИ

ТАРГЕТИРОВАННЫЕ ПРАВИЛА

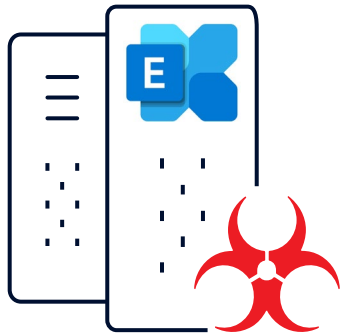


ШАБЛОНЫ УВЕДОМЛЕНИЙ



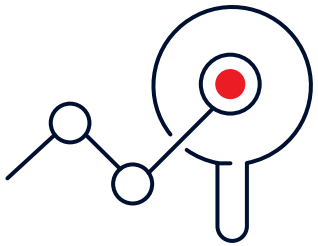
ИНСТРУКЦИИ ПО РЕАГИРОВАНИЮ

РАЗВИТИЕ ПРАВИЛ МОНИТОРИНГА
НА ПРИМЕРЕ АТАК НА EXCHANGE



АТАКИ
НА EXCHANGE-СЕРВЕРА

БЫСТРЫЕ ХАНТЫ
НА ПЕРВЫХ АТАКАХ



ПЕРЕРАБОТКА ХАНТОВ
ПОД МОНИТОРИНГ

08/12/2021

СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Лифанов

Ведущий Аналитик Центра мониторинга и реагирования на инциденты ИБ Jet CSIRT

csirt@jet.su

ОСТАЛИСЬ ВОПРОСЫ? ПИШИТЕ НА CSIRT@JET.SU