SOC ФОРУМ

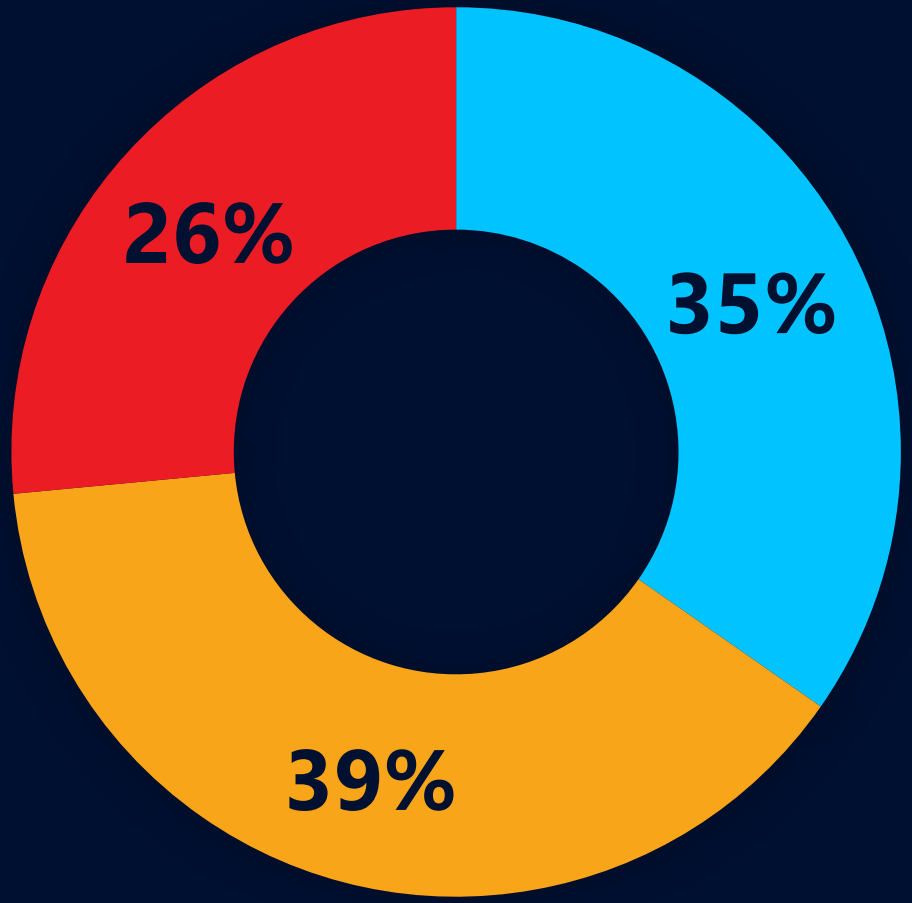
ЧТО ОБЩЕГО МЕЖДУ SOC И КИБЕРПОЛИГОНАМИ?

Ольга Елисеева,
руководитель департамента проектирования и внедрения

Инфосистемы Джет

РЕЗУЛЬТАТЫ ОПРОСА

ПРОВОДИТЕ ЛИ ВЫ В СВОЕЙ КОМПАНИИ КИБЕРУЧЕНИЯ?



- Да
- Нет, но задумываюсь, чтобы провести в ближайшее время
- Нет

СЕЙЧАС ИДЕТ СТАНОВЛЕНИЕ ИНДУСТРИИ

SOC ФОРУМ

JET CYBER CAMP

SOC

2015 г. — Что такое SOC?

2016 г. — Зачем нужен SOC?

2017 г. — ....

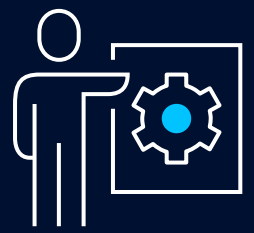
Понятия «киберучения» и «киберполигон» на данный момент не имеют чётких границ

ДВА ЭЛЕМЕНТА КИБЕРПОЛИГОНА

SOC ФОРУМ

JET CYBER CAMP

ТЕХНИЧЕСКИЙ



МНОГОСЛОЙНАЯ ИНФРАСТРУКТУРА

- Учебный ИТ-ландшафт
- Уязвимости
- Средства защиты

КОНТЕНТНЫЙ

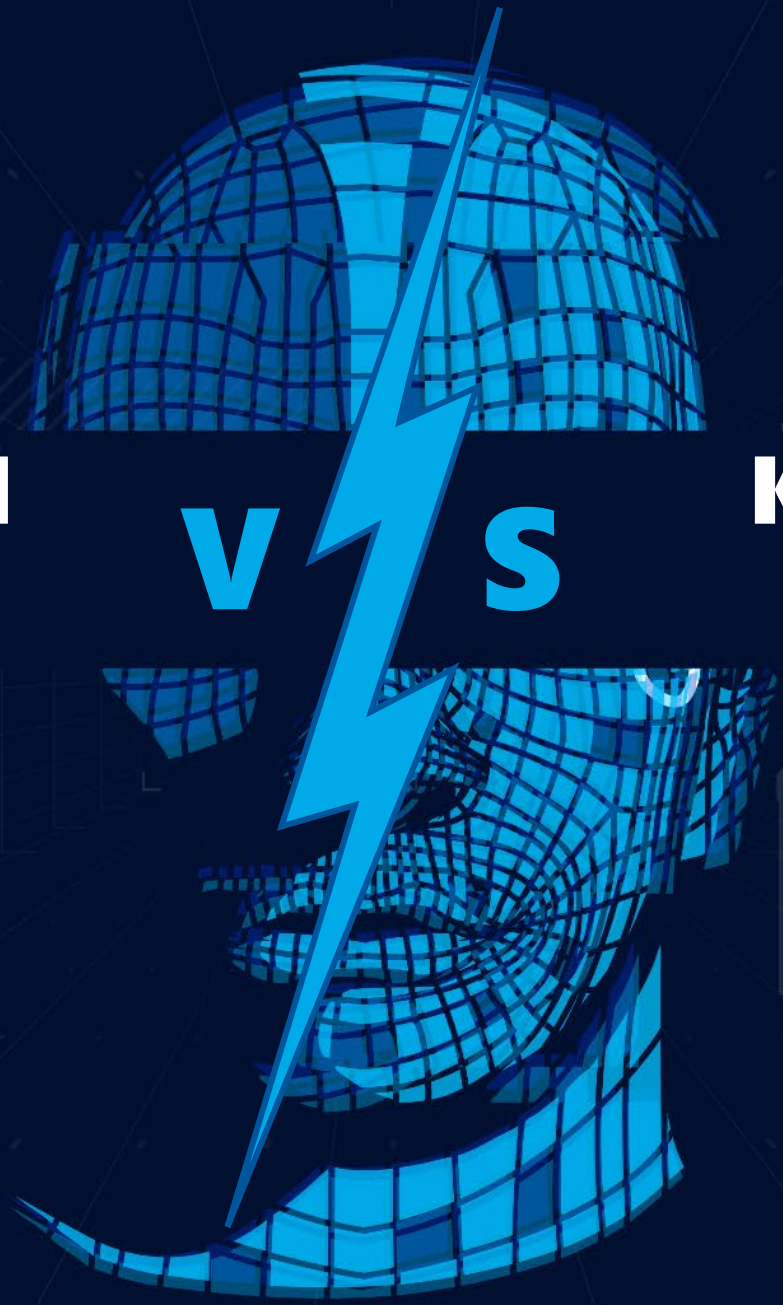
МЕТОДОЛОГИЧЕСКАЯ БАЗА

- Сценарии учений, сценарии атак
- Обучающие материалы, лабораторные работы, тесты
- Метрики, KPI, периодичность

SOC ФОРУМ

JET CYBER CAMP

КИБЕРПОЛИГОН ON-PREMISE



КИБЕРПОЛИГОН КАК ПРОДУКТ

РЕШАЕМЫЕ ЗАДАЧИ

SOC ФОРУМ

JET CYBER CAMP

1

КИБЕРЛАБОРАТОРИЯ

2

КИБЕРУЧЕНИЯ

3

ВИЗУАЛИЗАЦИЯ, SCORING

РЕАЛИЗАЦИЯ ТЕХНИЧЕСКОГО ЭЛЕМЕНТА

SOC ФОРУМ

JET CYBER CAMP

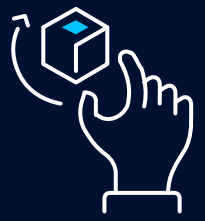
УЧЕБНЫЙ КЛАСС

ИТ-ЛАНДШАФТ

УЯЗВИМОСТИ

СРЕДСТВА ЗАЩИТЫ

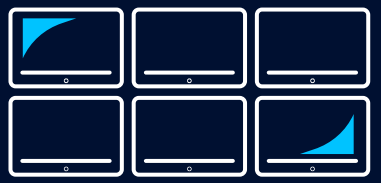
СЕРВЕРЫ



ВИРТУАЛИЗАЦИЯ

СЕТЬ

МЕДИА



ВИДЕОСТЕНА

SOC ФОРУМ

JET CYBER CAMP

ТРИ ГЛАВНЫХ ВЫВОДА

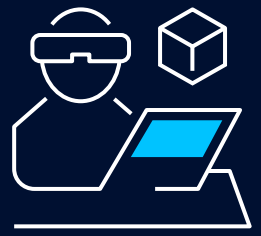
SOC ФОРУМ

JET CYBER CAMP

1

ЭКСПЛУАТАЦИЯ ИНФРАСТРУКТУРЫ

2



НОВЫЙ ОБУЧАЮЩИЙ КОНТЕНТ

3

БИЗНЕС-ПРОЦЕСС ВОКРУГ ТРЕНИРОВОК

SOC ФОРУМ

JET CYBER CAMP

КИБЕРПОЛИГОН ON-PREMISE

V S

КИБЕРПОЛИГОН КАК ПРОДУКТ

РЕШАЕМЫЕ ЗАДАЧИ

SOC ФОРУМ

JET CYBER CAMP

1

ОБМЕН ОПЫТОМ

2

ПОДГОТОВКА КОМАНДЫ

3

СИСТЕМНОСТЬ ОБУЧЕНИЯ

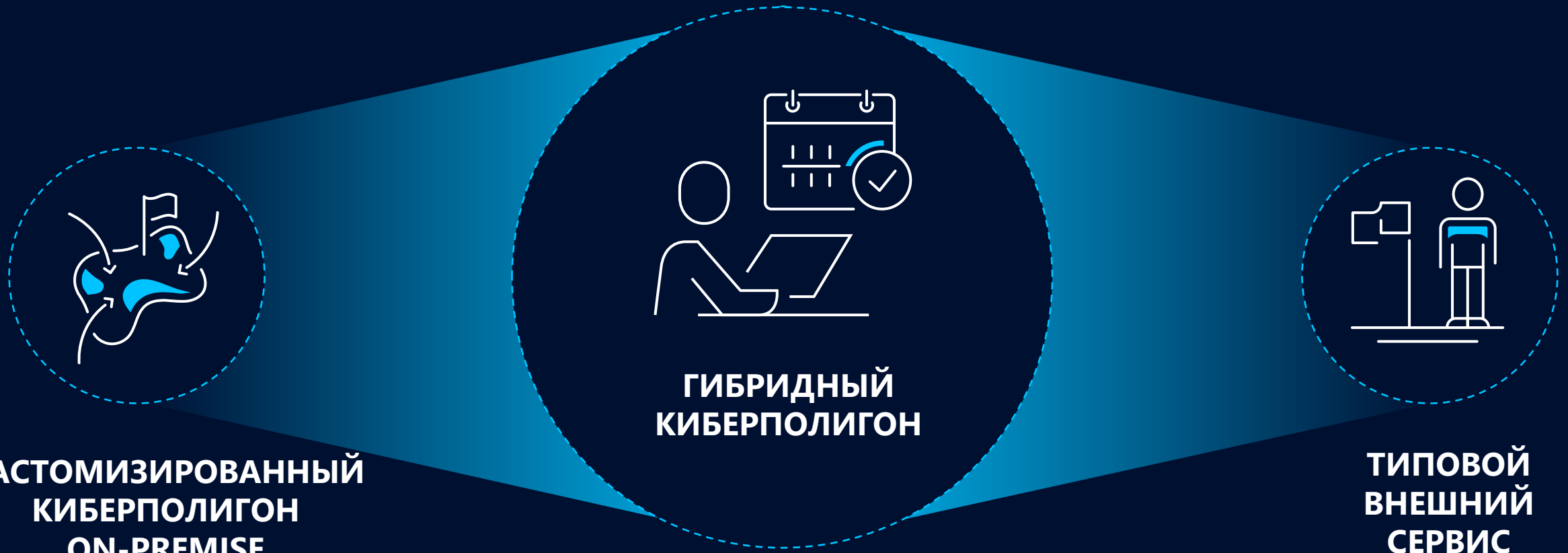
ЭВОЛЮЦИЯ ИНДУСТРИИ SOC

ИНДУСТРИЯ SOC СЕЙЧАС

КАК МЫ ВИДИМ РАЗВИТИЕ ИНДУСТРИИ КИБЕРУЧЕНИЙ

SOC ФОРУМ

JET CYBER CAMP



БАРЬЕРЫ НА ПУТИ К ПРОДУКТУ

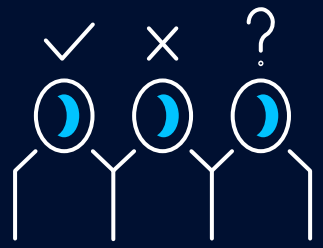
SOC ФОРУМ

JET CYBER CAMP

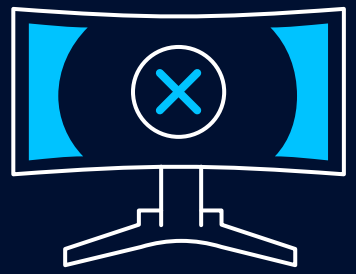
СМЕШАННАЯ АРХИТЕКТУРА

СЛОЖНОСТЬ РЕАЛИЗАЦИИ РЕЗЕРВНОГО КОПИРОВАНИЯ

ОТСУТСТВИЕ АВТОМАТИЗАЦИИ



SIEM С ВЫСОКИМ ПОРОГОМ ВХОДА ДЛЯ УЧАСТНИКОВ

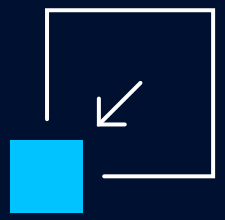


ОТСУТСТВИЕ ЦЕНТРАЛИЗОВАННОГО ИНТЕРФЕЙСА

РЕЗУЛЬТАТ

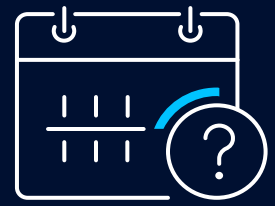
SOC ФОРУМ

JET CYBER CAMP



НЕВОЗМОЖНОСТЬ
МАСШТАБИРОВАТЬ

ВЫСОКИЕ НАКЛАДНЫЕ РАСХОДЫ
НА ОБСЛУЖИВАНИЕ
И РАЗВИТИЕ



СЛОЖНОСТИ С УПРАВЛЕНИЕМ
СРОКАМИ

НОВАЯ АРХИТЕКТУРА ОТ ЦЕЛИ

SOC ФОРУМ

JET CYBER CAMP

ЦЕЛЬ

Гибкая инфраструктура, которая работает устойчиво, легко добавляются компоненты инфраструктуры

РЕШЕНИЕ

- Логические уровни: ядро и модули
- Каждый сценарий – это изолированная инфраструктура
- Единая точка терминации трафика и управления подключениями
- Ansible
- Docker
- Zabbix

НОВАЯ АРХИТЕКТУРА ОТ ЦЕЛИ

SOC ФОРУМ

JET CYBER CAMP

ЦЕЛЬ

Гибкая инфраструктура, которая работает устойчиво, легко добавляются компоненты инфраструктуры

Быстрая адаптация инфраструктуры под запрос клиента

РЕШЕНИЕ

- Скопировать сеть клиента легко, т.к у нас все в разных VLAN
- Логическое воспроизведение сетевой топологии клиента (OPNsense)
- SIEM с шиной для гибкой замены на другой SIEM
- Тиражирование с помощью Docker, Ansible

НОВАЯ АРХИТЕКТУРА ОТ ЦЕЛИ

SOC ФОРУМ

JET CYBER CAMP

ЦЕЛЬ

Гибкая инфраструктура, которая работает устойчиво, легко добавляются компоненты инфраструктуры

Быстрая адаптация инфраструктуры под запрос клиента

Контент от подготовки атаки со стороны хакеров до ее блокировки от реальных практиков

РЕШЕНИЕ

- LMS – как единый портал
- Платформа доступна с любого устройства, поддерживающего веб-браузеры
- Тренер может подключиться к сессии участника
- Разные типы заданий: теория и практика, тесты
- Работа в командах
- Возможность пробовать себя в разных ролях

НЕДОСТАТОЧНО ТЕСТИРОВАНИЯ В МОДЕЛИ ЗАЩИТЫ

SOC ФОРУМ

JET CYBER CAMP

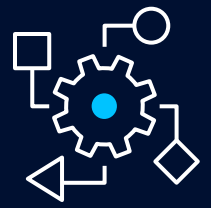
Уровень 1
Затруднение продвижения

Уровень 2
Обнаружение и реагирование

Уровень 3
Тестирование

Киберучения и RedTeam

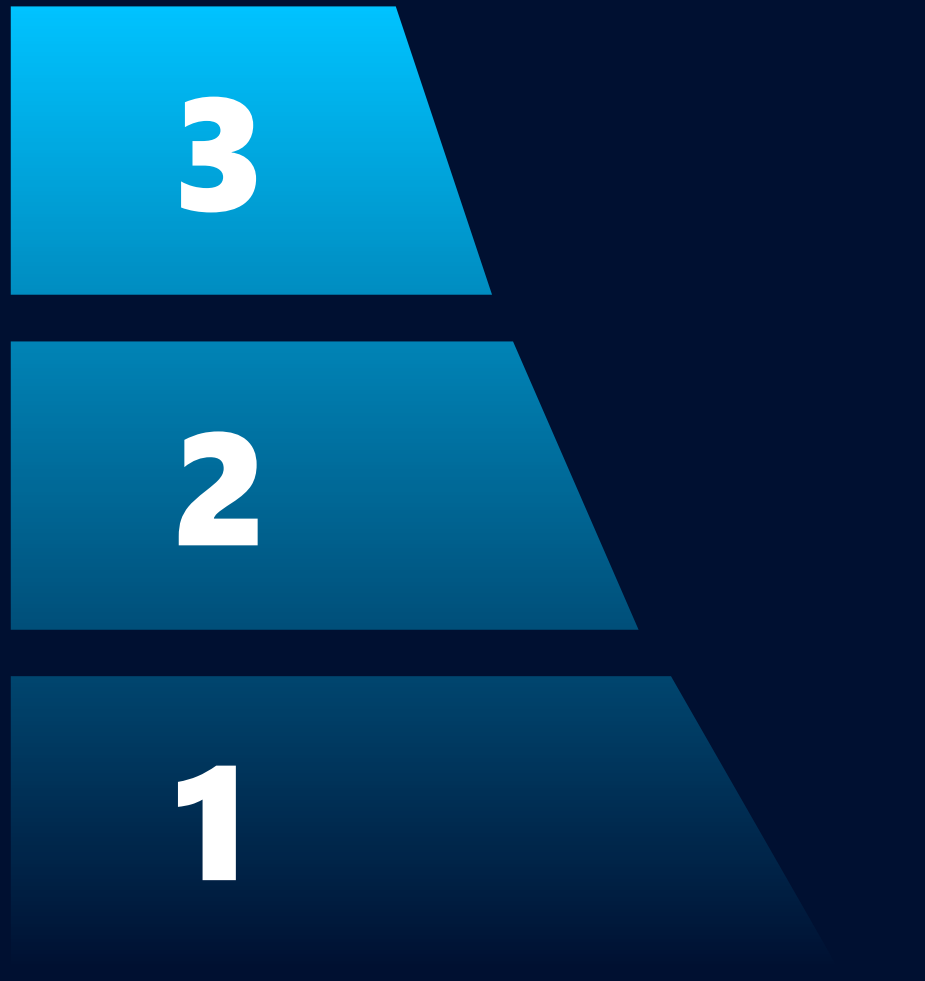
Мониторинг



Изменения БП

Изменения ИТ

СЗИ



SOC ФОРУМ

СТРОИМ ИНДУСТРИЮ ВМЕСТЕ!

Ольга Елисеева,
руководитель департамента
проектирования и внедрения

Инфосистемы Джет