SOLAR

Solar Образование

ПОВЫШЕНИЕ КОМПЕТЕНЦИЙ И ОТРАБОТКА
ПРАКТИЧЕСКИХ НАВЫКОВ ПО КИБЕРБЕЗОПАСНОСТИ

2024

Безопасность = навыки

SOLAR

2000–2010

ТЕХНОЛОГИИ

Эпоха насыщения технологиями
Покупка SIEM и других средств защиты информации

2010–2020

ПРОЦЕССЫ

Эпоха выстраивания процессов
Построение собственных SOC или выбор надежного провайдера

2020–2030

ПЕРСОНАЛ

Эпоха практических компетенций
Необходимо уметь отражать атаки и ликвидировать их последствия

Несоответствие подготовки команд защиты актуальным вызовам кибербезопасности

SOLAR

в **5** раз

за год выросло число атак хактивистов

76 %

кейсов связано с проникновением хакеров в инфраструктуру через известные уязвимости

7 дней

в среднем требовалось хакерам для достижения конечной цели атаки

НЕХВАТКА КВАЛИФИЦИРОВАННЫХ КАДРОВ И ОТСУТСТВИЕ ОРИЕНТАЦИИ НА ПРАКТИКУ

- Недостаточный уровень квалификации
- Отсутствие слаженности команд
- Низкая скорость принятия решений
- Отсутствие развития сотрудников ИБ
- Нехватка практических навыков отражения кибератак
- Киберучения и тренировки носят эпизодический характер

Источник: ГК «Солар»

КИБЕРУЧЕНИЯ

Практические киберучения
с готовыми сценариями
на платформе Solar CyberMir

Командно-штабные тренировки
для организационной отработки
сценариев реагирования

Киберчемпионаты
с вариативностью СЗИ,
инфраструктуры и сценариев

ОБРАЗОВАНИЕ

Программы развития навыков
киберзащиты для Blue Team,
практическая отработка
на киберполигоне

Модульный образовательный
киберинтенсив для получения
ключевых знаний и навыков ИБ

ПОСТРОЕНИЕ КИБЕРПОЛИГОНОВ

Построение киберполигонов
на базе инфраструктуры заказчика
с использованием платформы
Solar CyberMir

КИБЕРУЧЕНИЯ

Цели проведения киберучений

SOLAR

ОЦЕНКА

Проверка навыков сотрудников службы ИБ по выявлению и предотвращению последствий кибератак

ТРЕНИРОВКА

Повышение компетенций специалистов служб ИБ за счет практического применения навыков на киберполигоне

РАЗВИТИЕ

Подготовка рекомендаций и разработка программ развития сотрудников службы ИБ

ГЛАВНЫЙ РЕЗУЛЬТАТ КИБЕРУЧЕНИЙ

Слаженная работа службы ИБ, где каждый сотрудник понимает свои задачи и знает о необходимых действия в случае наступления инцидента информационной безопасности

Киберучения сегодня – это базовый инструмент для проверки уровня навыков службы ИБ и тренировки противодействия атакам злоумышленников

52%

компаний уже имеют опыт проведения киберучений*

75%

компаний планируют проведение киберучений в будущем*

87%

компаний считают, что киберучения нужно проводить минимум каждые полгода*

* По данным исследования ГК «Солар», октябрь 2023, выборка более 100 компаний

Типы киберучений

SOLAR

ПРАКТИЧЕСКИЕ КИБЕРУЧЕНИЯ

Это стандартные киберучения
на типовой учебной инфраструктуре
с готовыми сценариями.

ONE-DAY SOC

Проверка навыков по обнаружению и расследованию кибератак и рекомендации по развитию компетенций сотрудников

ONE-DAY RESPONSE

Проверка уровня подготовки команды к расследованию и противодействию кибератакам и рекомендации по развитию компетенций сотрудников

КАСТОМНЫЕ КИБЕРУЧЕНИЯ

Киберучения с возможностью изменения СЗИ, инфраструктуры и сценариев по требованиям заказчика.
От одной команды участников до 40 команд.
Разные форматы тренировки, соревнования и т.д.

КОМАНДНО-ШТАБНЫЕ ТРЕНИРОВКИ

Проверка процессов реагирования на инциденты ИБ выстроенным у Заказчика на примере кейсов

Участвуют сотрудники ИБ-, ИТ- и смежных подразделений согласно существующим регламентам реагирования Заказчика

КИБЕРУЧЕНИЯ И ОБУЧЕНИЕ

Интеграция киберучений в программы развития специалистов, например:

+ Киберучения ONE-DAY SOC – оценка исходного уровня компетенций

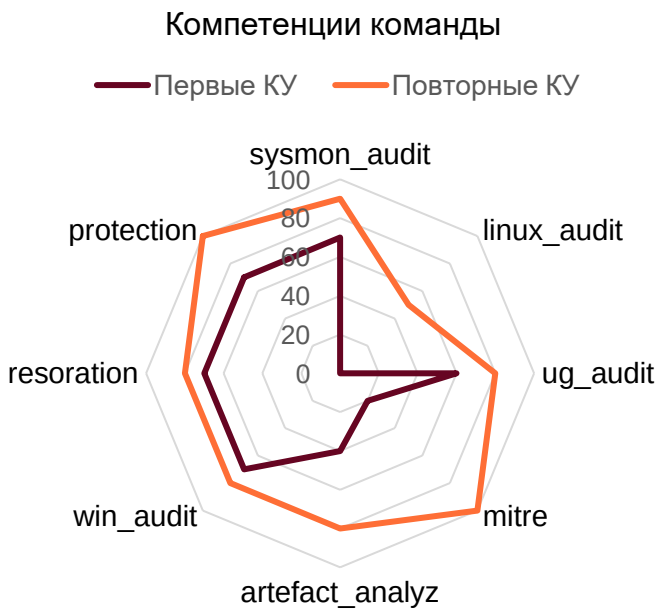
+ киберинтенсив – развитие теоретических знаний и практических навыков

+ Киберучения ONE-DAY SOC – оценка прогресса

Кейс 1: рост навыков команд после КУ

SOLAR

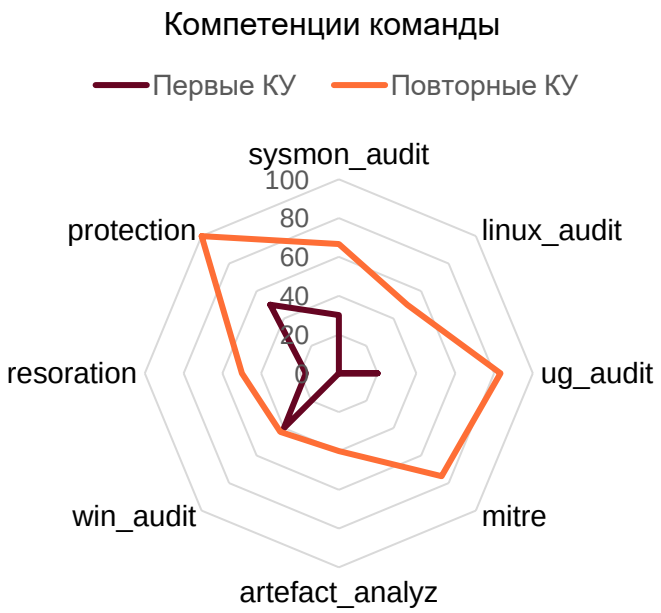
1я команда: первые и повторные* киберучения



+32,5%

средний результат команды на повторных КУ

2я команда: первые и повторные* киберучения



+44%

средний результат команды на повторных КУ

*В повторных киберучениях использовались другие вектора атак

Результаты проекта:

74% участников отметили, что получили новые знания

76% NPS

Образование

Команда киберзащиты: роли и навыки для отражения кибератак

SOLAR

КОМАНДА КИБЕРЗАЩИТЫ обеспечивает обработку инцидента в моменте:

- Обнаружение
- Реагирование
  - Анализ
  - Сдерживание
  - Уничтожение
  - Восстановление

(подготовка и работа после инцидента – отдельно)

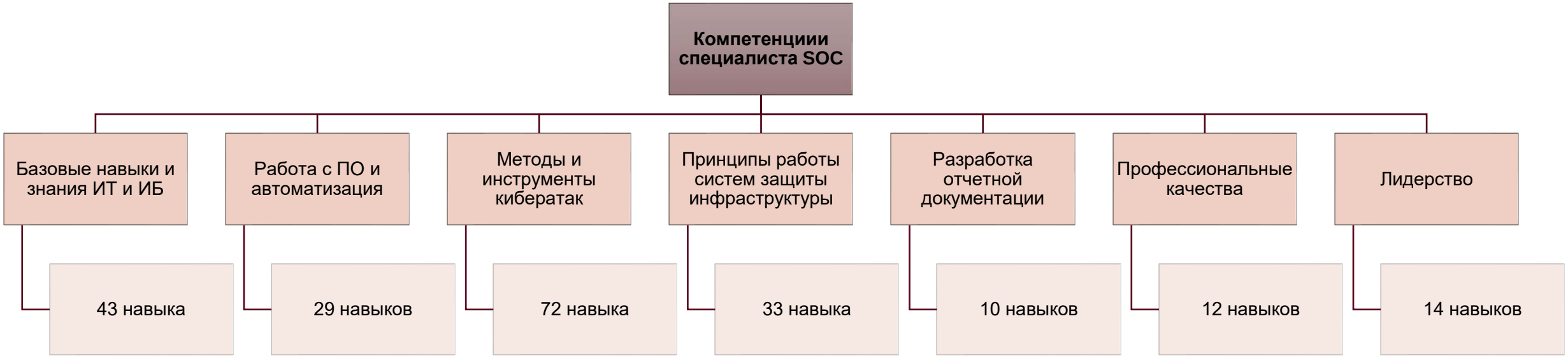
РОЛИ ДЛЯ ВЫПОЛНЕНИЯ

- Инженеры мониторинга инцидентов
- Эксперты по анализу артефактов и вредоносов
- Администраторы СЗИ
- Доменные администраторы
- Сетевые администраторы
- Инженеры систем резервного копирования

НАВЫКИ

- Экспертиза в SIEM
  - настройка
  - операционная работа
- Анализ инцидентов (артефактов) по MITRE ATT&CK
- Администрирование СЗИ
  - NGFW, IPS, WAF, EDR…
- Администрирование безопасности OS и сети
  - Windows / Linux
  - сетевая безопасность
- Аудит и анализ
  - сетевого траффика
  - Windows / Linux
  - анализ кода
- Восстановление
  - работа с Back-up системами
  - Windows / Linux
  - приложений
- Коммуникации в команде

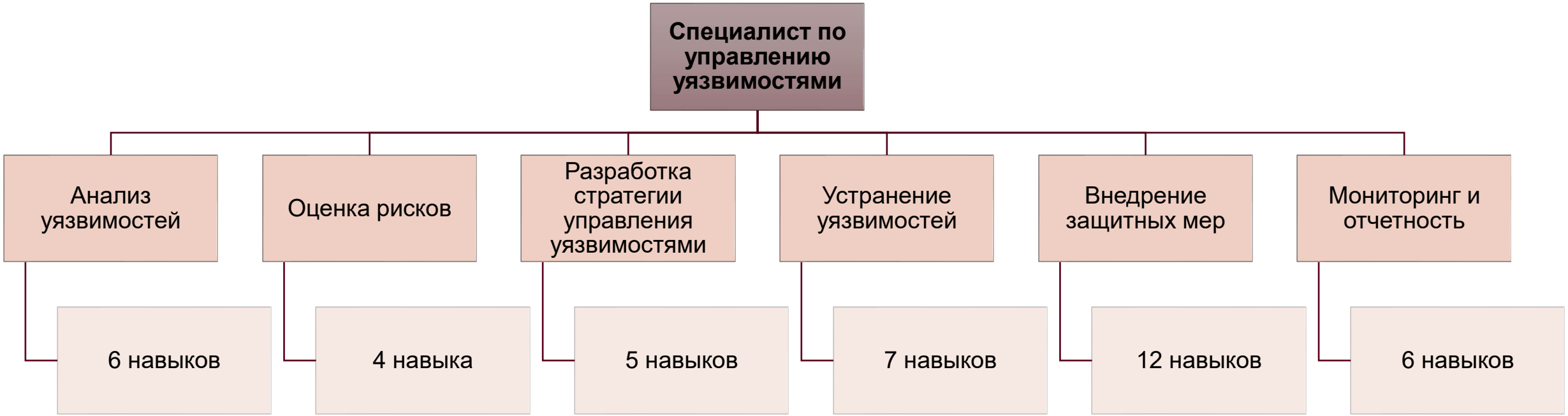
Матрица компетенций



Джун L1
Джун L2
Джун L3
Мидл
Сениор
Руководитель

Матрица компетенций

SOLAR



Для команды киберзащиты - Киберинтенсив

SOLAR

Модули (160 часов):

- Основы информационной безопасности
- Безопасность ОС Linux & Windows
- Сетевая безопасность
- Управление угрозами информационной безопасности
- Управление инцидентами информационной безопасности
- Межсетевые экраны нового поколения
- Системы расширенного обнаружения и устранения угроз
- Работа с Honeypot
- Расследование артефактов
- OWASP Top 10
- Системы предотвращения утечек
- Социальная инженерия
- Разведка по открытым источникам
- Построение безопасности IT-архитектуры
- Безопасность Active Directory
- Администрирование и безопасность протокола LDAP

Для команд исследователей уязвимостей

SOLAR

Этичный хакинг – продвинутый (200 часов)

- Модуль 1. Введение в этичный хакинг
- Модуль 2. Сбор информации
- Модуль 3. Сканирование сети
- Модуль 4. Анализ уязвимостей
- Модуль 5. Хакинг системы
- Модуль 6. Трояны и другое вредоносное программное обеспечение
- Модуль 7. Снифферы
- Модуль 8. Социальная инженерия
- Модуль 9. Отказ в обслуживании
- Модуль 10. Перехват сеанса
- Модуль 11. Криптография и стеганография
- Модуль 12. Обход систем обнаружения вторжений, фаерволлов и систем-ловушек
- Модуль 13. Хакинг веб-серверов
- Модуль 14. Хакинг веб-приложений
- Модуль 15. SQL инъекции
- Модуль 16. Киберучения
- [extra] Модуль 17. Хакинг беспроводных сетей
- [extra] Модуль 18. Хакинг мобильных платформ
- [extra] Модуль 19. Хакинг интернета вещей
- [extra] Модуль 20. Облачные вычисления

Для анализа артефактов и проведения криминалистики

SOLAR

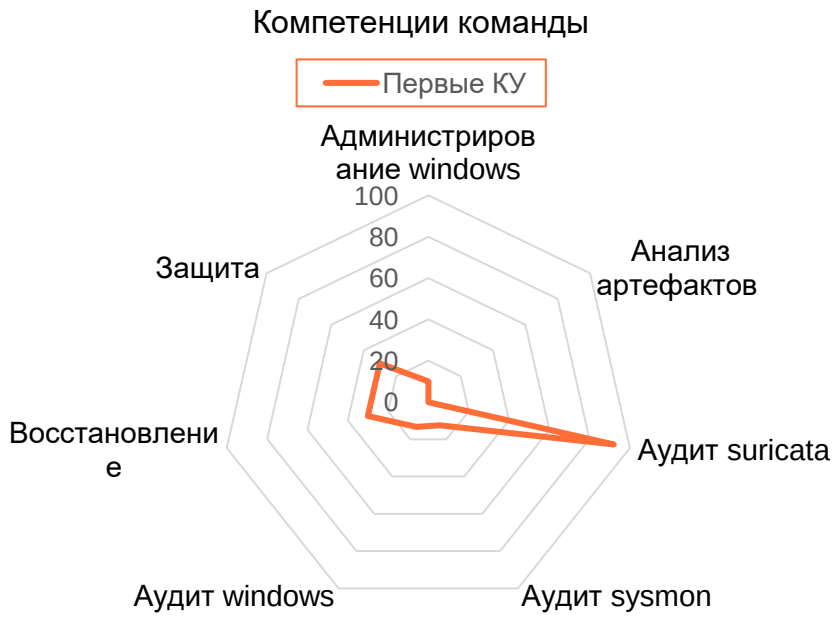
Форензика (120 часов)

- Модуль 1. Введение в криминалистику
- Модуль 2. Свойства физических носителей
- Модуль 3. Архитектура OS Linux
- Модуль 4. Архитектура OS Windows
- Модуль 5. Физическая и сетевая криминалистика
- Модуль 6. Криминалистика в OS Linux
- Модуль 7. Криминалистика в OS Windows

Кейс 2: рост навыков команд после КУ и киберинтенсива

SOLAR

Средний результат команды на первых киберучениях **26,4%**



Средний результат команды на повторных киберучениях **59,6%**

*В повторных киберучениях использовались другие вектора атак

НА 33,2% УВЕЛИЧИЛСЯ СРЕДНИЙ РЕЗУЛЬТАТ КОМАНДЫ НА ПОВТОРНЫХ КИБЕРУЧЕНИЯХ

SOLAR

+7 (499) 755-07-70
cybermir@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1