Ростелеком
Солар

Solar CyberBoost

Безопасность = навыки

Ростелеком Солар

Актуальные вызовы и тренды кибербезопасности

Изменение ландшафта киберугроз

- Переход от простых массовых атак к сложным точечным ударам
- Рост сложности и количества угроз
- Появление новых продуктов на рынке
- Использование учетных данных, утекших в 2022

Тренды кибератак: эксплуатация уязвимостей, атаки через подрядчиков, ВПО, утечки реальные или не очень (за счет ранее скомпрометированных УЗ)

Кибербразведка – тренд ближайших нескольких лет: злоумышленники хотят действовать наверняка, а не вслепую

Атаки будут усложняться: киберпреступники будут использовать нетипичные методы и техники

Источник: «Ростелеком-Солар»

Ростелеком Солар

Несоответствие подготовки команд защиты актуальным вызовам кибербезопасности

в 5 раз

за год выросло число атак хактивистов

72 %

кейсов связано с проникновением хакеров в инфраструктуру через известные уязвимости

7 дней

в среднем требовалось хакерам для достижения конечной цели атаки

Источник: «Ростелеком-Солар»

Нехватка квалифицированных кадров и отсутствие ориентации на практику

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

Ростелеком Солар

Продукты киберполигона «Ростелеком-Солар»

Построение киберполигонов

Построение киберполигонов
на базе инфраструктуры заказчика
с использованием платформы
«Солар Кибермир»

Создание цифровых двойников
сегментов ИТ-инфраструктуры
заказчика на базе мощностей
киберполигона «Ростелеком-Солар»

Киберучения

Практические киберучения
на платформе «Солар Кибермир»

- Стандартные сценарии
- Кастомные сценарии

Командно-штабные тренировки для
организационной отработки
сценариев реагирования

Командные соревнования
в формате CTF

Солар КиберБуст

Модульный образовательный
киберинтенсив для получения
ключевых знаний и навыков ИБ

Комплексная образовательная
программа развития навыков
киберзащиты для Blue Team,
практическая отработка
на киберполигоне

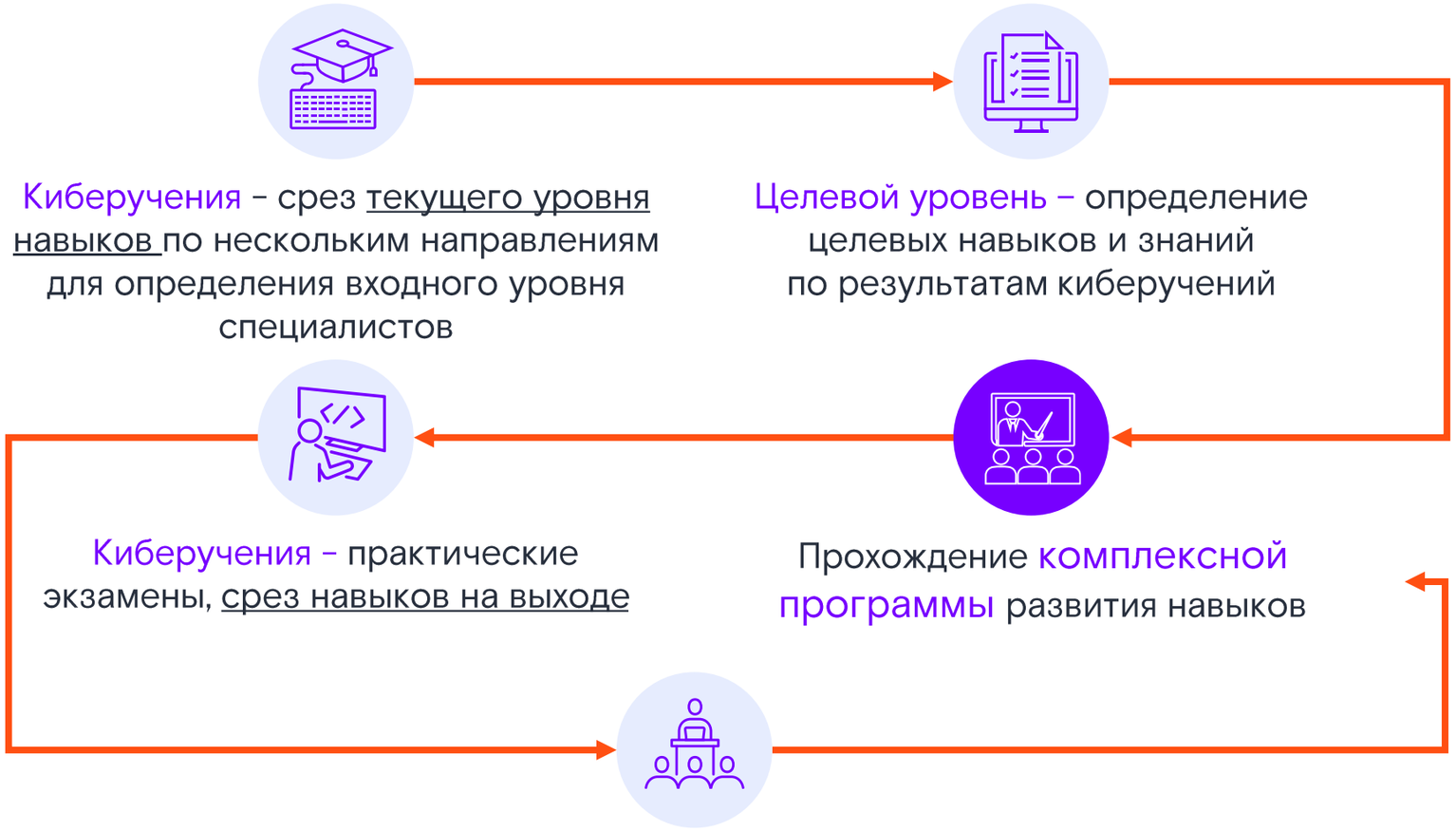
Платформа «Солар Кибермир» лежит в основе всех продуктов киберполигона «Ростелеком-Солар» для организации киберучений, построения киберполигонов и развития навыков кибербезопасности

Ростелеком
Солар

Этапы комплексной программы развития навыков кибербезопасности

Ростелеком
Солар

Полный цикл повышения навыков кибербезопасности



Киберучения – срез текущего уровня навыков по нескольким направлениям для определения входного уровня специалистов

Целевой уровень – определение целевых навыков и знаний по результатам киберучений

Прохождение комплексной программы развития навыков

Киберучения – практические экзамены, срез навыков на выходе

Корректировка целей, рекомендации для достижения более продвинутого уровня

- Составление программы развития навыков с учетом входного и целевого уровней навыков, её проведение
- Повышение готовности к отражению кибератак
- Апробация процессов реагирования на практике
- Согласованность действий и эффективная коммуникация в команде

Ростелеком Солар

Построение программы с учетом входного среза навыков

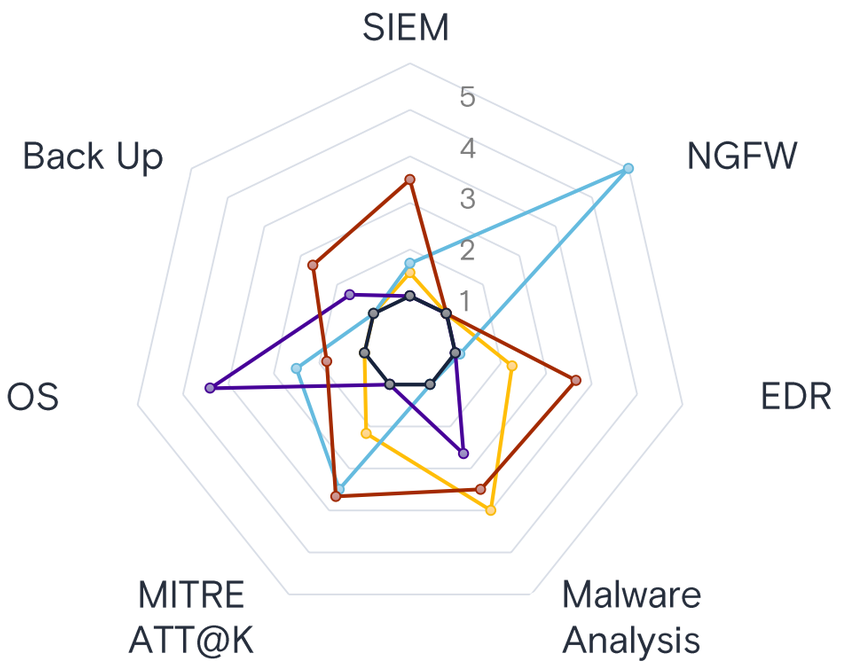
Матрица компетенций

В начале программы составляем матрицу компетенций по 7-9 направлениям для каждого сотрудника в зависимости от специализации.

Тестирование и оценка навыков

Практические навыки и согласованность действий команды тестируются в рамках киберучений, с которых начинается программа, формируется срез навыков.

Матрица компетенций на основании тестирования в формате киберучений



Ростелеком Солар

Целевой уровень

В зависимости от специфики и задач организации формируется целевой уровень навыков и знаний, который должен быть достигнут в результате программы.
Есть два основных подхода:
«Level Up» и «Customized Level»

Определение целевого уровня: варианты

Level Up – развитие навыков каждого специалиста на 1 уровень выше

Улучшение навыков всех специалистов по каждому направлению на 1 уровень выше.

Customized Level– развитие навыков всей команды под общий целевой уровень

Улучшение навыков всех специалистов по всем направлениям до целевого уровня.

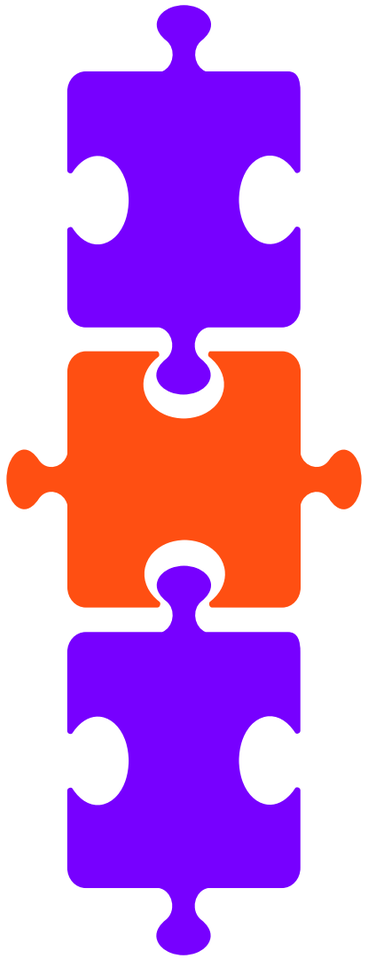
Чем выше критичность инфраструктуры, тем выше целевой уровень.

Ростелеком
Солар

Программа развития навыков
Solar CyberBoost

Развитие навыков

Учебный план составляется из модулей, необходимых каждому специалисту. Обучение сопровождается большим количеством практических заданий различных типов.



Ключевые знания по кибербезопасности

Получение ключевых знаний и навыков по информационной безопасности

Навыки обработки инцидентов

Практико-ориентированное обучение специалистов для результативной обработки инцидентов и предотвращения потерь от кибератак

Пользование ИБ-продуктами

Обучение по ИБ-продуктам с возможностью проверить работу СЗИ на киберполигоне

Ростелеком
Солар

Практические киберучения

Итоговые киберучения, срез навыков

По окончании обучения все специалисты проходят киберучения для закрепления полученных навыков и составления итогового среза компетенций.

Фиксируем прогресс в развитии навыков команды на практике

Цели проведения

- Увеличение скорости реакции группы реагирования для минимизации ущерба от киберинцидентов
- Проверка и развитие компетенций специалистов для предотвращения киберинцидентов
- Демонстрация и апробация тактик и техник злоумышленников на киберполигоне

Результаты

- Оценка практических навыков специалистов
- Рекомендации по развитию компетенций для команды участников или для конкретного специалиста

Ростелеком Солар

Удостоверение о повышении квалификации

Удостоверение

Всем успешно освоившим программу и прошедшим тестирование специалистам выдаются Удостоверение о повышении квалификации.

Корректировка целей

Кроме того, мы даем рекомендации для дальнейшего развития компетенций и получения более продвинутого уровня навыков.

После успешного освоения программы развития навыков специалисты получат Удостоверение о повышении квалификации установленного образца с внесением данных в ФИС ФРДО.


РОССИЙСКАЯ ФЕДЕРАЦИЯ

УДОСТОВЕРЕНИЕ

О ПОВЫШЕНИИ КВАЛИФИКАЦИИ

000000000000

Документ о квалификации

Регистрационный номер

Город

Дата выдачи

Настоящее удостоверение свидетельствует о том, что

прошел(а) повышение квалификации в (на)

по дополнительной профессиональной программе

в объёме

Итоговая работа на тему:

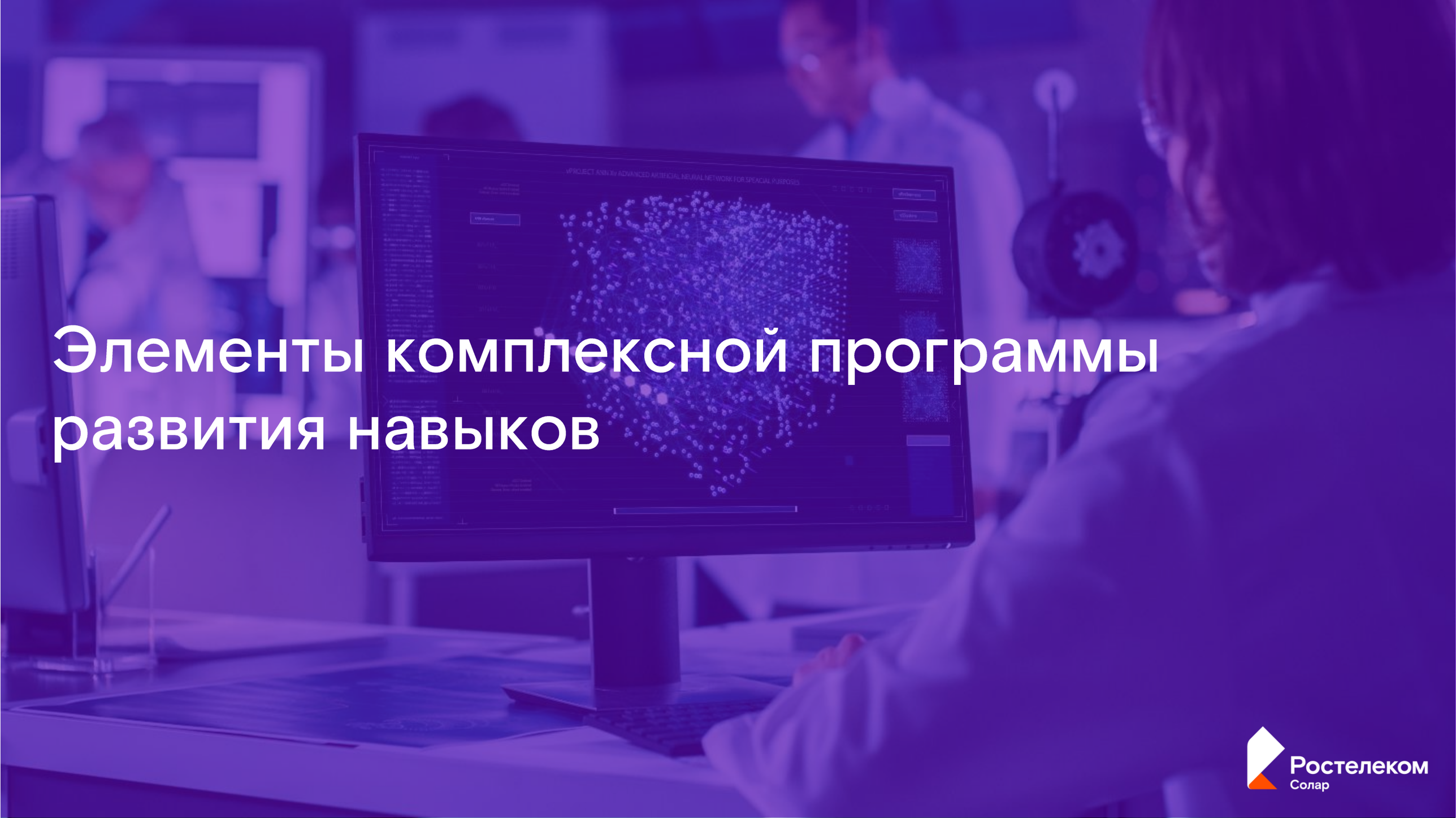
М.П. *Руководитель*

Ростелеком Солар

Пример программы развития навыков

Успешное прохождение блока в каждой ячейке обеспечивает переход на следующий уровень

	SIEM	Восстановление	Администрирование безопасности OS	Анализ инцидентов MITRE ATT&CK	Анализ зловредного кода	EDR	NGFW, IPS
Уровень 5 (81-100 баллов)	▪ Оптимизация производительности SIEM ▪ Стратегическое планирование безопасности с SIEM	▪ Разработка планов BCP ▪ Обучение команд Blue Team	▪ Интеграция с IDM системами ▪ Интеграция с SIEM системами	▪ Обучение команд Blue Team ▪ Разработка стратегии эшелонированной защиты	▪ Создание собственных инструментов ▪ Анализ алгоритмов шифрования и дешифровки	▪ Разработка стратегии безопасности конечных точек ▪ Обучение команд Blue Team	▪ Интеграция NGFW в сочетании с другими инструментами
Уровень 4 (61-80 баллов)	▪ Разработка процедур и сценариев реагирования ▪ Настройка коннекторов	▪ Разработка планов DRP ▪ Координация Blue Team	▪ Усиление безопасности Windows ▪ Усиление безопасности Linux	▪ Разработка политик защиты ▪ Глубокий анализ и исследование атак	▪ Глубокий анализ артефактов и методов атак ▪ Разработка сценариев обнаружения	▪ Разработка сценариев обнаружения аномалий ▪ Глубокий анализ угроз	▪ Настройка зашиты от DDOS атак ▪ Анализ SSL трафика ▪ Разработка сигнатур IDS
Уровень 3 (41-60 баллов)	▪ Создание комплексных запросов и фильтров ▪ Глубокий анализ логов для выявления угроз ▪ Создание правил корреляции	▪ Углубленное восстановление данных ▪ Планирование непрерывности бизнеса ▪ Координация команды восстановления	▪ Администрирование LDAP ▪ Тонкая настройка Active directory	▪ Обнаружение скрытых атак ▪ Разработка сценариев реагирования	▪ Reverse-engineering ▪ Применение SandBox	▪ Создание и настройка правил и политик EDR ▪ Интеграция с другими системами безопасности	▪ Мониторинг и анализ событий NGFW ▪ Основы и сервисы NGFW/IPS/IDS ▪ Оркестрация NGFW
Уровень 2 (21-40 баллов)	▪ Поиск и анализ событий ▪ Создание базовых запросов ▪ Настройка правил алертинга	▪ Составление плана восстановления ▪ Резервное копирование и восстановление данных	▪ Мониторинг безопасности ▪ Управление учетными записями ОС	▪ Выявление тактик и техник ▪ Умение отличать атаки (Реальные/ False positive)	▪ Работа с отладчиками ▪ Разработка регламентов установки ПО	▪ Мониторинг алертов и событий ▪ Основы реагирования на инциденты	▪ Анализ сетевого трафика ▪ Базовые правила фильтрации трафика ▪ Настройка правил IDS/IPS
Уровень 1 (0-20 баллов)	▪ Log management ▪ Анализ логов Windows/lLinux ▪ Основы SIEM	▪ Идентификация/классификация инцидента ИБ ▪ Изоляция систем ▪ Документирование инцидента	▪ Администрирование ОС Windows/Linux ▪ Установка и настройка обновлений ОС	▪ Понимание MITRE ATT&CK ▪ Определение инцидентов по MITRE ATT&CK	▪ Основные типы вредоносного ПО ▪ Антивирусное ПО	▪ Установка EDR-агента н конечных устройствах ▪ Изоляция устройств и удаление угроз	▪ Основы (IDS/IPS) ▪ Модель OSI



Элементы комплексной программы развития навыков

Ростелеком
Солар

Комплексная программа развития навыков киберзащиты

Развитие навыков специалистов любого уровня подготовки для практической готовности к отражению кибератак

Кибербуст для Blue Team

Ключевые знания по кибербезопасности

Получение ключевых знаний и навыков по информационной безопасности

- Базовые навыки администрирования
- КиберИнтенсив

Навыки обработки инцидентов

Практико-ориентированное обучение для результативной обработки инцидентов и предотвращения потерь от кибератак

- Курс «Мониторинг и выявление инцидентов»
- Курс «Реагирование на инциденты»
- Курс «Исследователь уязвимостей»

Пользование ИБ-продуктами

Обучение по ИБ-продуктам с возможностью проверить работу СЗИ на киберполигоне

- Продукты российских вендоров

Ростелеком Солар

Ключевые знания по кибербезопасности

Построение программы с учетом уровня подготовки специалистов и конечной цели обучения, измерение итогового результата на практике

Интенсив

- Программа состоит из 14 основных теоретическо-практических модулей
- Киберучения для закрепления навыков
- Возможность выбора необходимых модулей в зависимости от потребностей организации
- Соотношение лекционного материала к практическим занятиям – 30:70

Курсы по базовым навыкам администрирования

- Ввод в профессию для начинающих специалистов без опыта и специальной подготовки
- Получение базовых знаний по операционным системам, освоение особенностей установки, настройки и администрирования ОС
- Отличия операционных систем
- Соотношение лекционного материала к практическим занятиям – 30:70

Ростелеком Солар

Развитие навыков обработки инцидентов

Программы составлены на базе 8-летнего опыта Solar JSOC по непрерывной защите 850+ крупных коммерческих и государственных организаций от киберугроз любой сложности.

- Изучение инструментов, методов и процедур, необходимых для эффективного обнаружения и локализации действий противника и устранения последствий инцидентов
- Полное понимание известных уязвимостей и методов их эксплуатации
- Каждый курс сопровождается отработкой полученных навыков на приближенной к реальности инфраструктуре киберполигона
- Возможность выбора необходимых модулей в зависимости от потребностей организации

Курсы:

Мониторинг и анализ сети

Реагирование на инциденты

Исследователь уязвимостей

Отработка практических навыков на базе киберполигона

Ростелеком Солар

Пользование ИБ-продуктами

Политика мультивендорности - ориентируемся на те средства защиты, которые используются в организации

- В инфраструктуре киберполигона используются продукты различных отечественных поставщиков решений
- Возможность протестировать взаимодействие СЗИ с другими продуктами на инфраструктуре киберполигона

Ключевые классы СЗИ:

FW/NGFW	IDS/IPS
DLP	EPP
PAM	NTA
VM	EDR/XDR
Криптошлюзы (ГОСТ)	И не только...

Ростелеком Солар

Уникальность комплексной программы

1 **Практика на киберполигоне**

платформа с готовыми сценариями киберучений, доступом к виртуальной инфраструктуре и визуализацией прохождения кибератак

2 **Замер навыков в формате киберучений**

по окончании киберучений для составления и корректировки индивидуального вектора развития каждой организации и специалиста

3 **Мультивендорность**

продукты и решения различных отечественных вендоров на инфраструктуре киберполигона

4 **Экспертиза в кибербезопасности**

опыт Solar JSOC по защите ключевых информационных систем России

5 **Кастомизация программы**

построение программы с учетом уровня подготовки и конечной цели обучения, измерение итогового результата на практике

6 **Полный спектр знаний**

в рамках единой комплексной программы – получение ключевых знаний, практическое развитие навыков, вендорские курсы по ИБ-продуктам

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

cybermir@rt-solar.ru