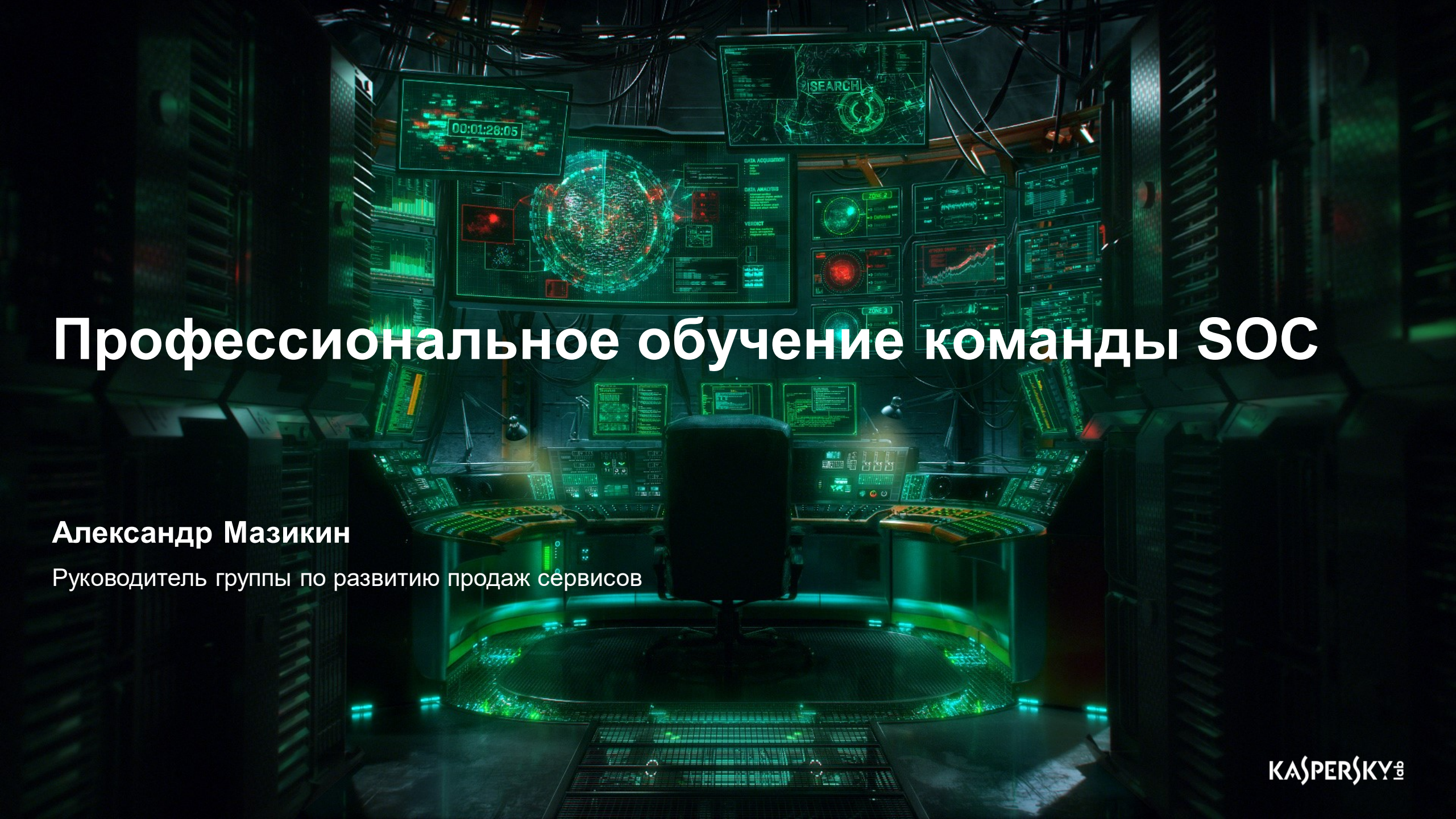


Профессиональное обучение команды SOC

Александр Мазикин

Руководитель группы по развитию продаж сервисов

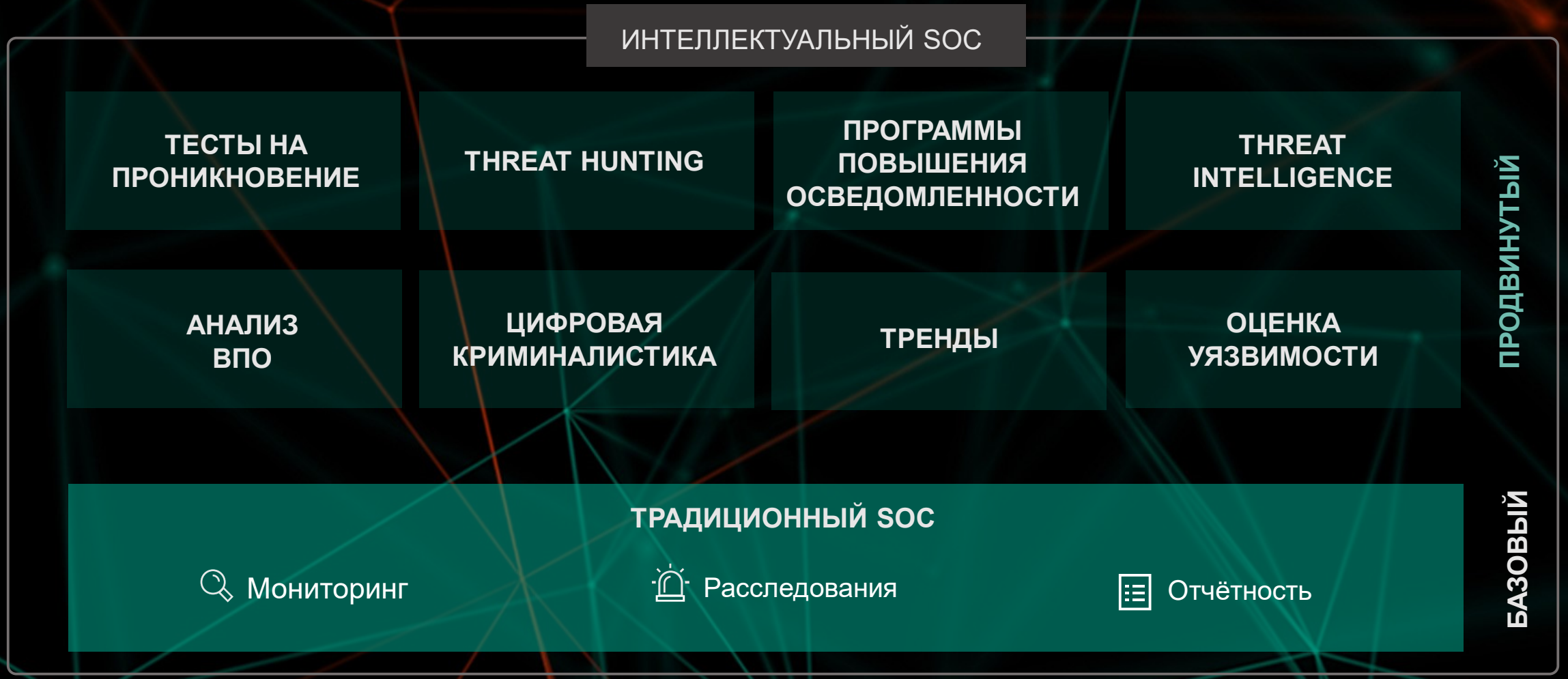
KASPERSKY lab

Основа основ

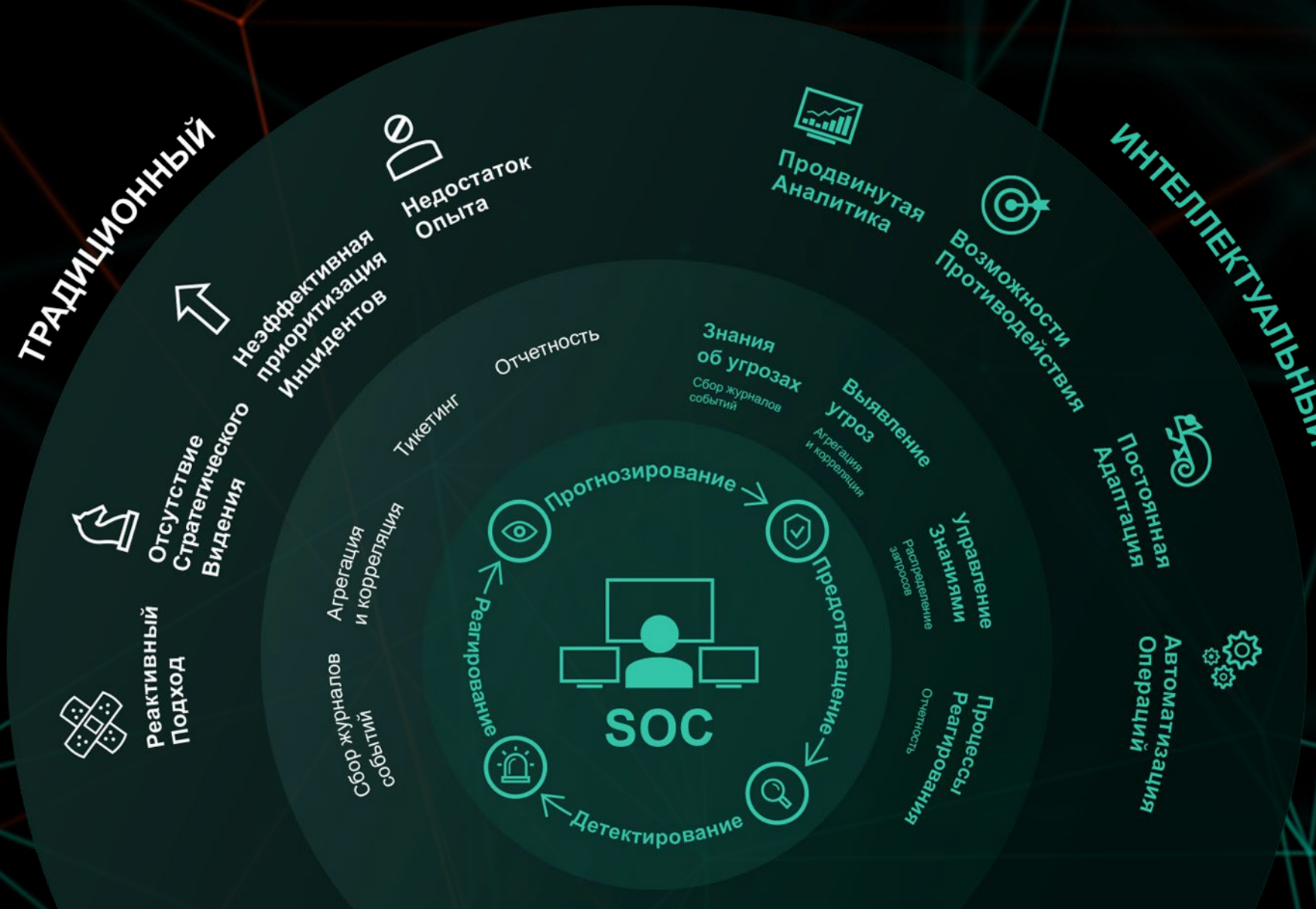
SOC (Security Operation Center) является централизованным подразделением, которое занимается вопросами безопасности на организационном и техническом уровне[1]

[1] https://en.wikipedia.org/wiki/Security_operations_center

SOC Сервисы

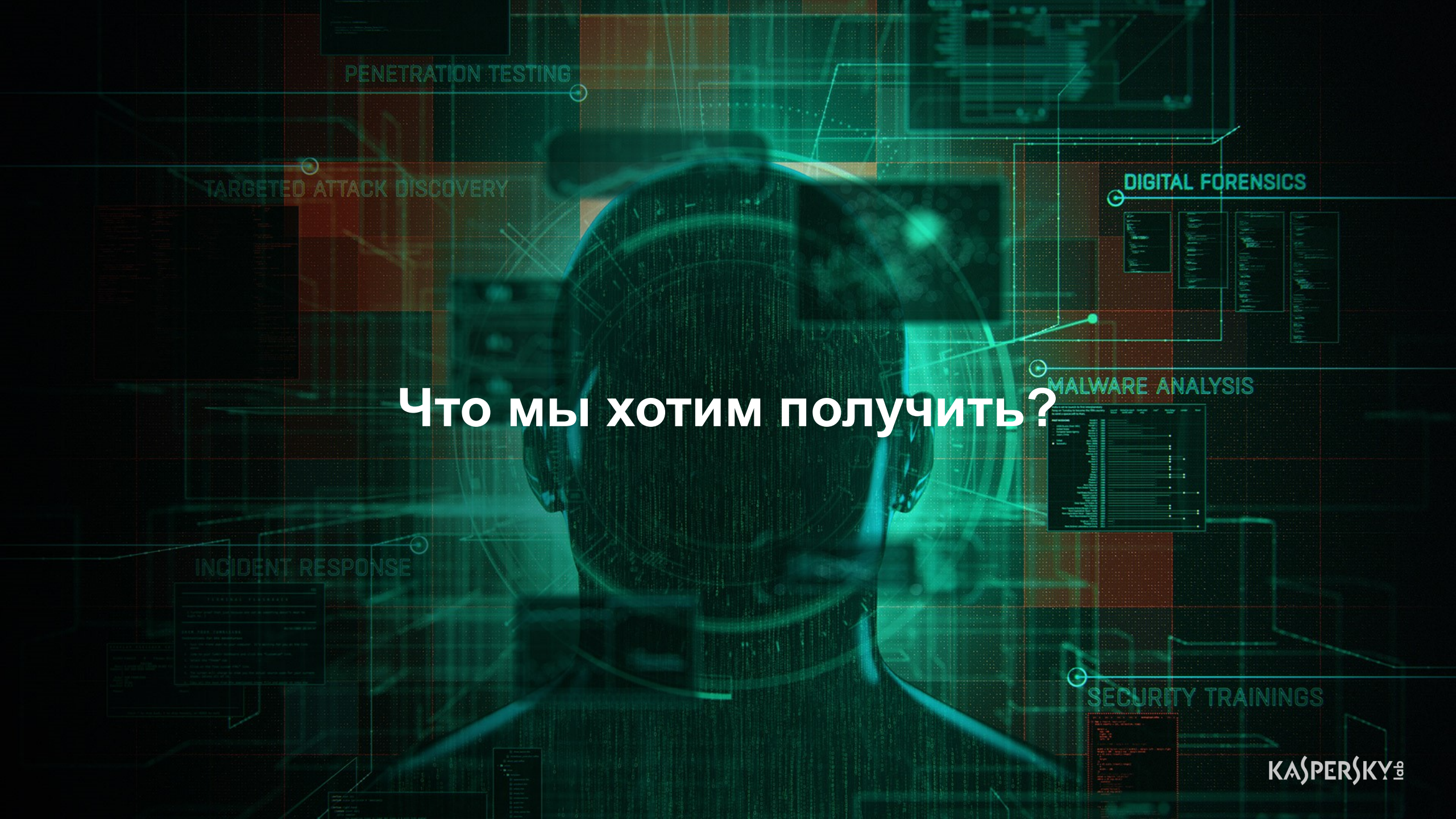

ИНТЕЛЛЕКТУАЛЬНЫЙ SOC
ТЕСТЫ НА ПРОНИКНОВЕНИЕ
THREAT HUNTING
ПРОГРАММЫ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ
THREAT INTELLIGENCE
АНАЛИЗ ВПО
ЦИФРОВАЯ КРИМИНАЛИСТИКА
ТРЕНДЫ
ОЦЕНКА УЯЗВИМОСТИ
ПРОДВИНУТЫЙ
ТРАДИЦИОННЫЙ SOC
Мониторинг
Расследования
Отчётность
БАЗОВЫЙ

SOC Сервисы


ТРАДИЦИОННЫЙ
Недостаток Опыта
Неэффективная приоритизация Инцидентов
Отсутствие Стратегического Видения
Реактивный Подход
ИНТЕЛЛЕКТУАЛЬНЫЙ
Продвинутая Аналитика
Возможности Противодействия
Постоянная Адаптация
Автоматизация Операций
Отчетность
Тикетинг
Знания об угрозах
Сбор журналов событий
Выявление угроз
Агрегация и корреляция
Управление Знаниями
Распределение запросов
Процессы Реагирования
Отчетность
Агрегация и корреляция
Сбор журналов событий
Прогнозирование
Предотвращение
Детектирование
Реагирование
SOC

SOC Роли – Базовый

Роль	Описание	Задачи
Tier-1 Аналитик	Сбор событий	• Мониоринг и определение инцидентов • Первоначальный анализ и эскалация • Сканирование на наличие уязвимостей • Управление инструментами мониторинга
Tier-2 Аналитик	Реагирование на инциденты	• Анилиз инцидентов полученных от первой линии • Проведение расследований • Локализация и устранение инцидентов • Обновление правил, индикаторов и пр.
SOC Менеджер	Управление и стратегия	• Управление командой, подбор персонала, обучение и пр. • Разработка стратегии • Метрики



Что мы хотим получить?

SOC Роли – Продвинутый

Роль	Описание	Задачи
Tier-3	Threat Intelligence и Threat Hunting	• Threat Hunting • SIEM Use-case разработка • Исследование закрытых ресурсов (darkweb) • Проведение тестов на проникновение • Модель угроз
Эксперт в области цифровой криминалистики	Что, как, когда и где произошло?	• Анализ цифровых улик • Участие в расследование инцидентов
Аналитик ВПО	Функционал атаки	• Анализ и обратная разработка ВПО • Участие в расследование инцидентов
Threat Intelligence Аналитик	Использование Threat Intelligence	• Открытые источники TI • Аналитическе отчеты • TTPs и индикаторы • Фиды: приоритезация и использование • Анализ данных от вендоров
Эксперт в области тестов на проникновение	Оценка защищенности	• Оценка и поиск уязвимостей • Тесты на проникновение

Реагирование на инциденты

Темы	Навыки
• Общие сведения о реагировании на инциденты • Обнаружение и первичный анализ • Цифровой анализ • Создание правил обнаружения (YARA, Snort, Bro)	• Отличие APT от других типов угроз • Понимание различных методов атаки и анатомии целевых атак • Применение специальных методов мониторинга и обнаружения • Выполнение процедуры реагирования на инциденты • Восстановление хронологической картины и логики инцидента • Создание правил обнаружения и подготовка отчетов

Цифровая криминалистика

Темы	Навыки
• Оперативное реагирование и сбор цифровых улик • Внутренняя структура реестра Windows • Анализ артефактов в Windows • Криминалистический анализ браузера • Анализ электронной почты	• Организация лаборатории цифровой криминалистики • Сбор цифровых улик и порядок обращения с ними • Воссоздание хронологической картины инцидента с помощью временных меток • Выявление следов вторжения посредством анализа артефактов в ОС Windows • Анализ истории браузера и электронной почты • Эффективное применение средств и методов цифровой аналитики

Цифровая криминалистика (экспертный уровень)

Темы	Навыки
• Экспертная криминалистика в ОС Windows • Восстановление данных • Сетевая и облачная криминалистика • Криминалистический анализ дампов памяти • Хронологический анализ • Практическая криминалистика реальных целевых атак	• Глубокий анализ файловой системы • Восстановление удаленных файлов • Анализ сетевого трафика • Обнаружение вредоносной активности по дампам памяти • Восстановление хронологии Инцидента

Анализ и обратная разработка вредоносного ПО

Темы	Навыки
• Цели и методы анализа и обратной разработки вредоносного ПО • Внутреннее устройство ОС Windows, исполняемые файлы, ассемблер x86 • Базовые методы статического анализа • Базовые методы динамического анализа • Анализ файлов .NET, Visual Basic, Win64 • Методы анализа скриптов и программ, отличных от исполняемых файлов	• Построение безопасной среды для анализа вредоносных программ: развертывание «песочницы» и всехнеобходимых инструментов • Понимание принципов исполнения программ в ОС Windows • Распаковка, отладка и анализ вредоносного объекта, определение его функций • Обнаружение вредоносных сайтов путем анализа вредоносных скриптов • Проведение экспресс-анализа вредоносных программ

Анализ и обратная разработка вредоносного ПО (экспертный уровень)

Темы	Навыки
• Методы расширенного статического анализа • Методы расширенного динамического анализа • Обратная разработка APT-угроз (полная проработка сценария APT-атаки, начиная с фишингового сообщения электронной почты и заканчивая как можно более глубоким анализом) • Анализ протоколов (анализ зашифрованных коммуникаций по протоколу C2, методы расшифровки трафика) • Анализ руткитов и буткитов	• Использование передовых методов обратной разработки и распознавание методов защиты от обратной разработки (обфускация, защита от отладки) • Расширенный анализ руткитов и буткитов • Анализ шелл-кода эксплойтов, внедренного в различные виды файлов, а также вредоносных программ для сред, отличных от Windows

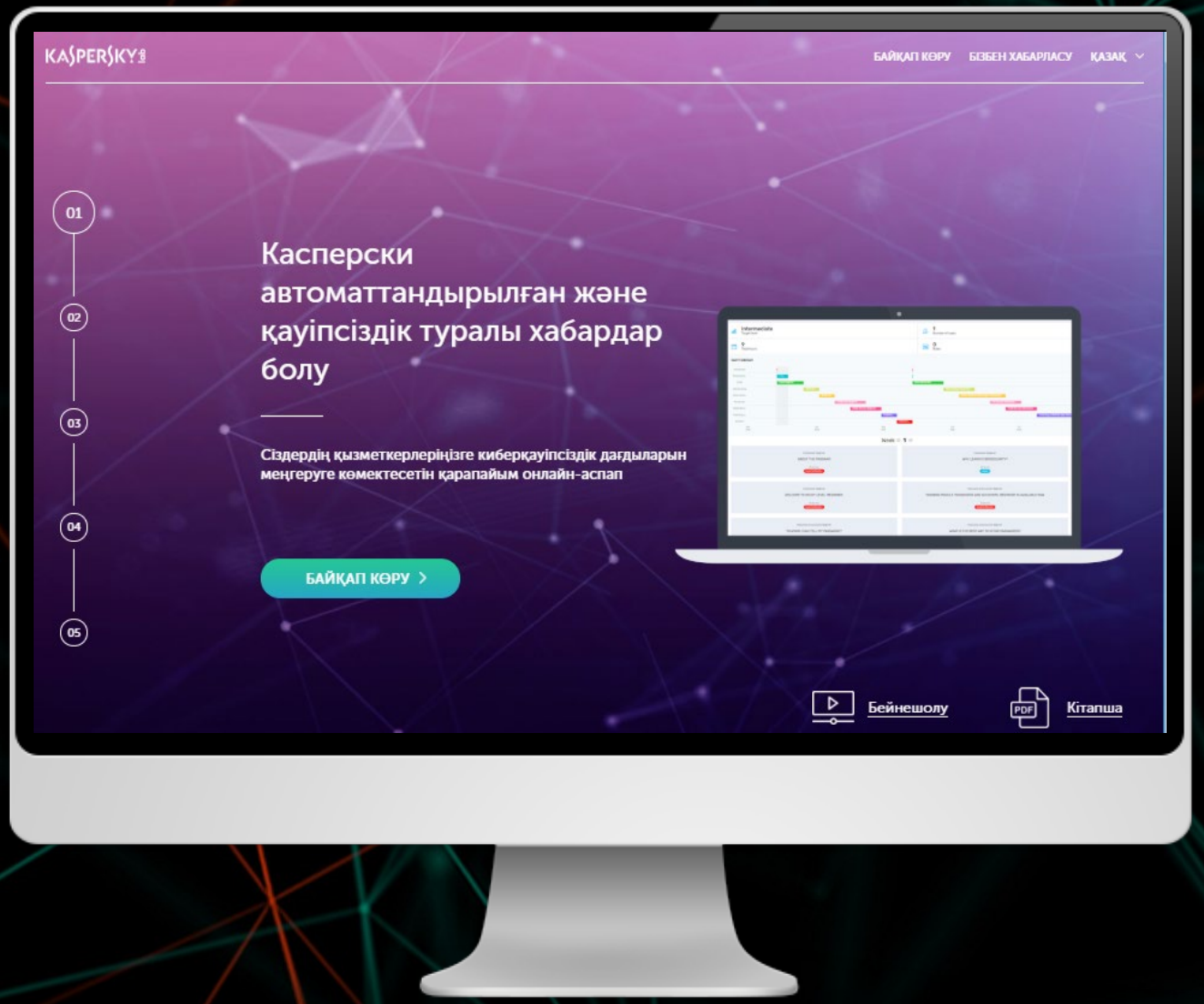
YARA

Темы	Навыки
• Введение в синтаксис правил YARA • Способы быстрого и эффективного создания правил • YARA-генераторы • Тестирование правил YARA на ложные срабатывания • Поиск новых необнаруженных образцов с помощью VirusTotal • Использование внешних модулей в YARA для эффективного поиска угроз • Поиск аномалий • Набор упражнений для совершенствования навыков работы с YARA	• Создание эффективных правил YARA • Тестирование правил YARA • Дальнейшее совершенствование правил для эффективного обнаружения угроз

Экспертные тренинги для команды SOC

Тренинг	Количество дней
Реагирование на инциденты	5
Цифовая криминалистика	5
Цифровая криминалистика (экспертный)	5
Анализ и обратная разработка вредоносного ПО	5
Анализ и обратная разработка вредоносного ПО (экспертный)	5
Yara	2

Программа повышения осведомленности



www.k-asap.kz

KASPERSKY lab

Что еще вендор может дать команде SOC?

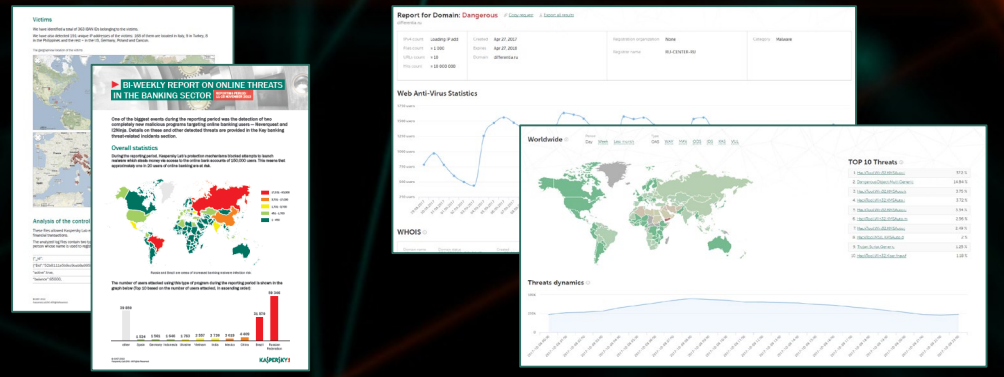
Threat Intelligence

Аналитические отчёты + индикаторы (IOC's) и Yara правила

Информация об угрозах, актуальных для организации

Инструменты: Threat Lookup, Sandbox

Потоки данных



Сервисы

Threat Hunting

Реагирование на инциденты

Цифровая криминалистика

Анализ вредоносного ПО

Анализ защищенности и тесты на проникновение

KASPERSKY lab

LET'S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab