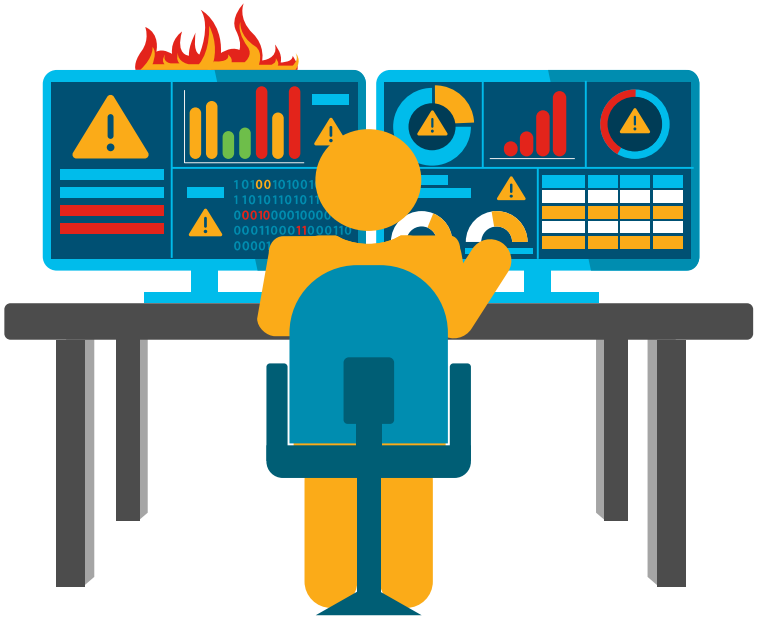
Почему L1 SOC бесполезны?

Из опыта построения SOC у десятков заказчиков и аутсорсинга SOC у сотни заказчиков

Алексей Лукацкий
Бизнес-консультант по кибербезопасности
28 ноября 2018

Аналитики L1 в SOC не нужны!



Роли традиционной команды SOC

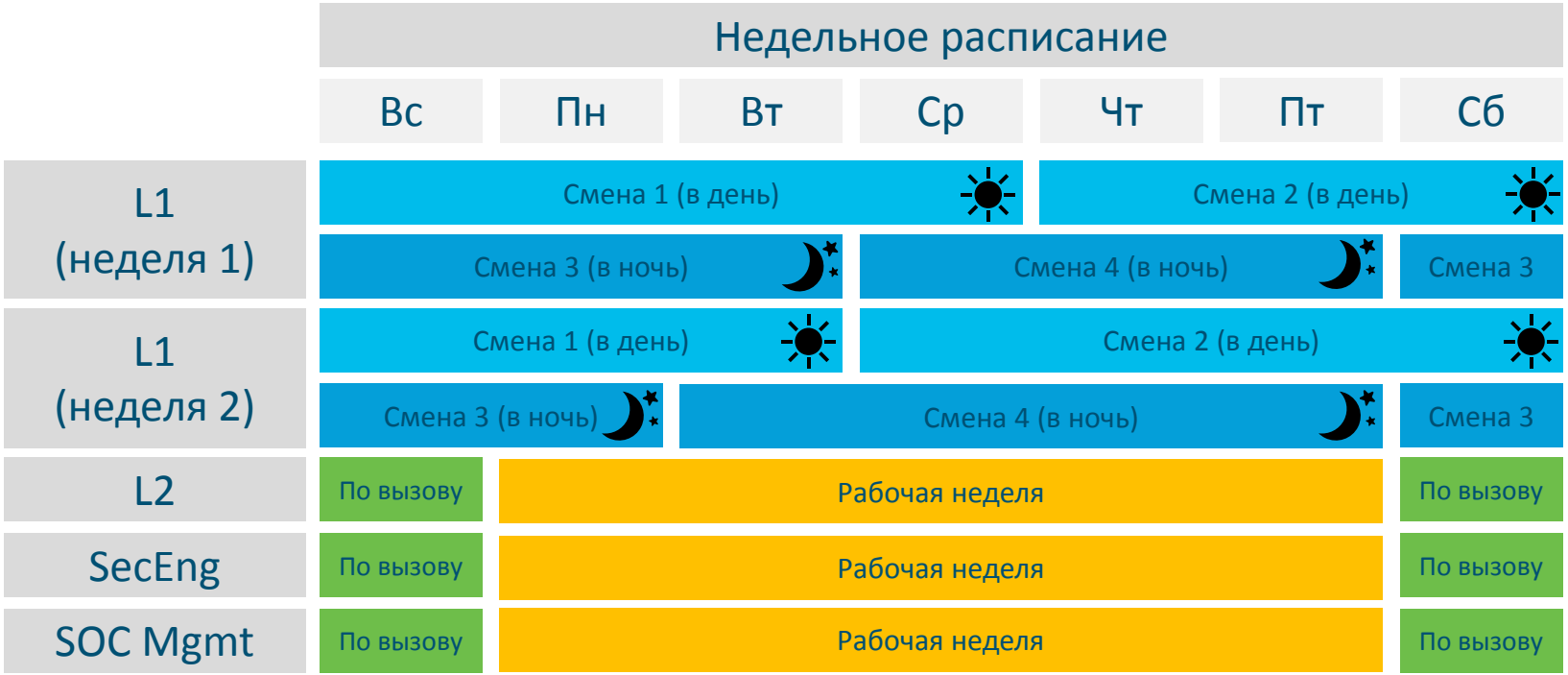
Начнем с фактов

Разные модели работы SOC в режиме 24 x 7

	Кейс 1	Кейс 2	Кейс 3
Минимальное число команд / людей	5 / 5	6 / 6	6 / 6
Часов в смену	10	10	12
Среднее число часов в неделю	42 + 2 часа сверхурочных	40	42
Плюсы	Ротация рабочих и нерабочих дней на выходные	40-часовая неделя с 3-мя выходными Работа в те же дни каждую неделю	Никто не работает больше трех дней подряд 3-хдневные каникулы каждые выходные
Минусы	Отсутствие постоянных рабочих дней	3 команды каждые выходные не работают, а 3 – работают каждые выходные	Длинная смена Работа до 62 часов в неделю 2 часа сверхурочных на сотрудника
Цикл повторения	20 дней	21 день	28 дней

12-тичасовые смены в день

Недельный график



Режим работы SOC и длительность смена

- Типичные режимы работы аналитиков SOC - 8 x 5, 12 x 5, 18 x 7, 24 x 7
- Минимум – 7 человек для режима 7 x 24 с часовым перекрытием в смене и одним «плавающим» сотрудником для закрытия отпусков и болезней
- 10 аналитиков - для режима 24 x 7 x 365
- + 2 наиболее опытных аналитика (L2) работают в режиме 8 x 5 и доступны для покрытия смен для запланированных и непланируемых отсутствий

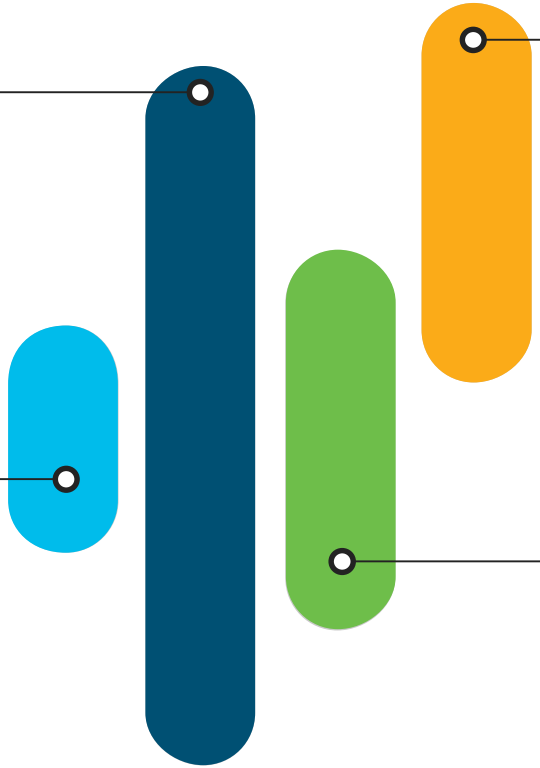
Зарплата аналитиков

На кадровых ресурсах большое число вакансий для специалистов SOC

Разброс зарплат (не везде опубликованы) – 25-150 тысяч рублей (зависит от региона)

Нередко в описании вакансии аналитика **аутсорсингого** SOC пишется «можно без опыта»

Что влияет на стоимость аналитика SOC?



Налоги и взносы

НДФЛ – 13% (для резидентов)

ПФР, ФСС, ФОМС – 30% или 10% (при превышении лимита ФОТ)

Разное

Аренда, мебель, ПО, железо и т.п.

Зарплата

Москва – 100 тысяч рублей

СПб – 80 тысяч рублей

Регионы – 25 тысяч рублей

Внеурочная работа / выходные

Обучение

Первичное обучение, повышение квалификации и OTJ

План обучения

Обучение для аналитиков L1

База при наличии SIEM

	SANS	Россия	Вендор
Основы обнаружения атак	$6610	$250	
Основы TCP/IP		$150	
Безопасность Linux / Windows		по $500	
Безопасность приложений		по $250	
Анализ с помощью SIEM	$6610	$1000	
Cisco Cyber Ops			$3595
CompTIA CySa+ (Cybersecurity Analyst)			$340
ArcSight Certified Security Analyst			$4000
IBM Certified Associate Administrator – Security QRadar SIEM		$1000	$2500

Без стоимости сертификации и поездки на обучение

Что такое аналитик SOC?

Навыки

- Выполнение задач, действий и процедур, необходимых для использования используемого оборудования
- Технические навыки
- Принятие решений
- Коммуникационные навыки
- Межличностные навыки

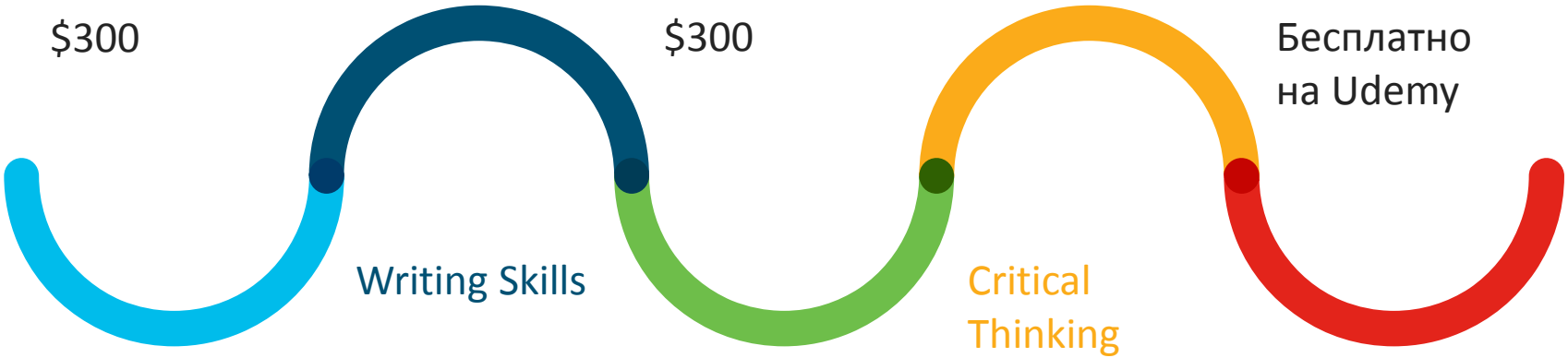
Знания

- Процедуры и процесс
- Требуемые задачи
- Оборудование и способы его работы
- Опасности, сбои и риски
- Рабочие правила и ограничения
- Окружение

Человек

- Психология
- Физиология
- Мотивация

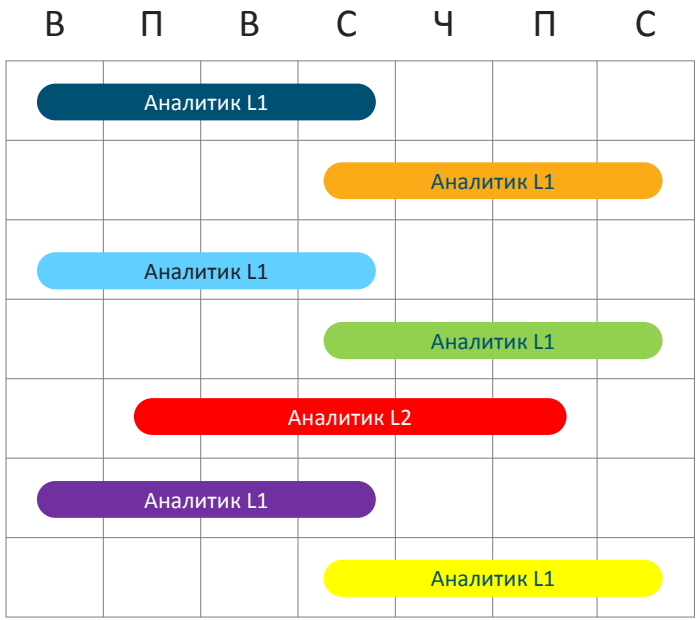
Что еще надо уметь и знать?

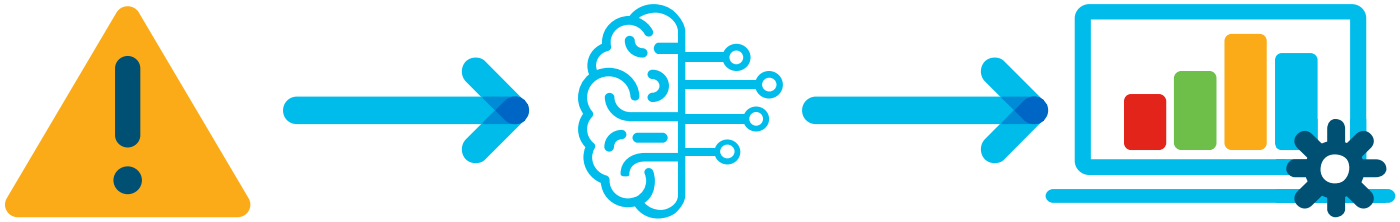


Можно попробовать сократить число аналитиков за счет выбора режима работы, длительности смены и использования аутсорсинга

Расписание работы аналитиков

- От правильного расписания зависит эффективность работы
- Аналитики тоже люди и хотят иметь личную жизнь
- 12-ти часовые смены минимизируют число аналитиков, но снижают продуктивность и качество



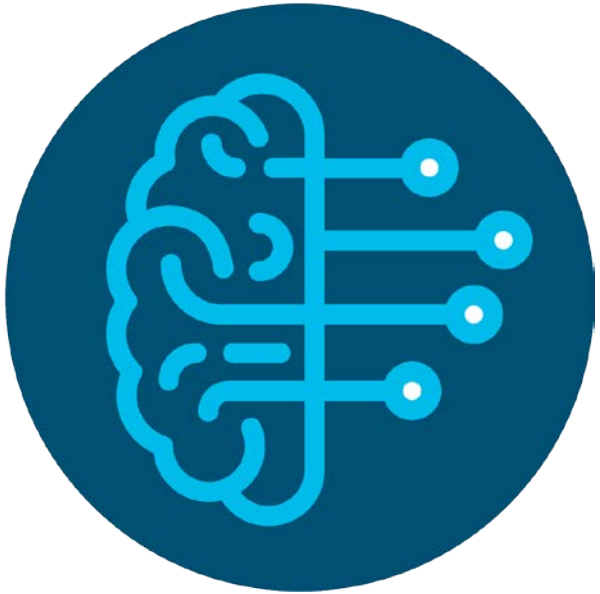


1,2 триллиона событий ИБ

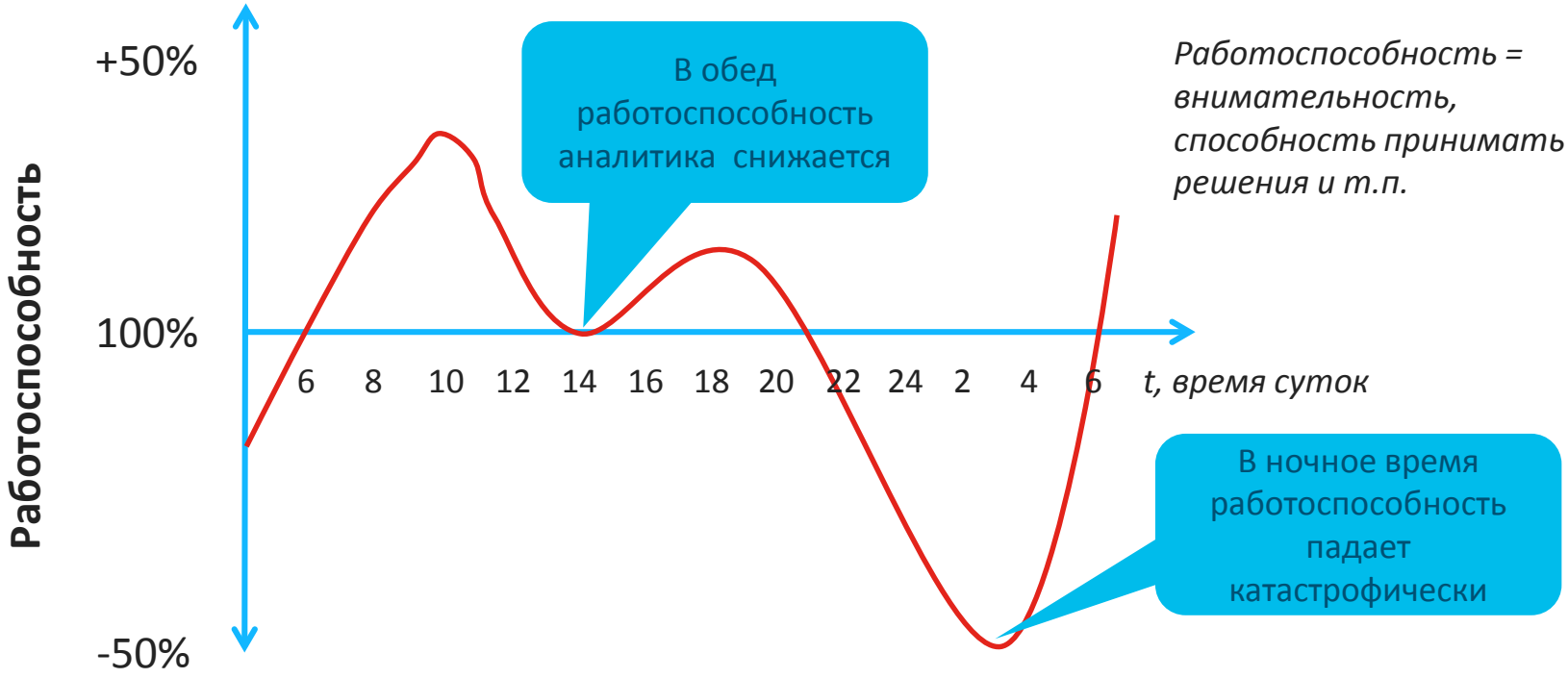
22 инцидента ИБ

Источник: служба ИБ Cisco

Психология и физиология SOC или почему не нужны аналитики L1?

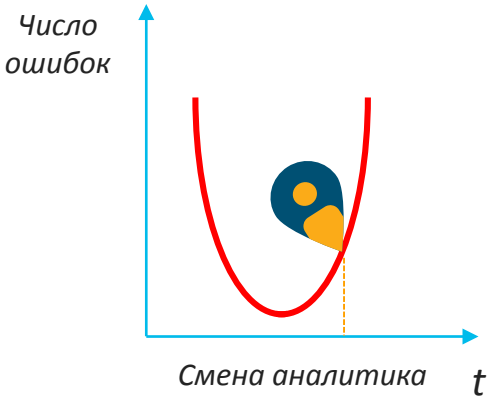


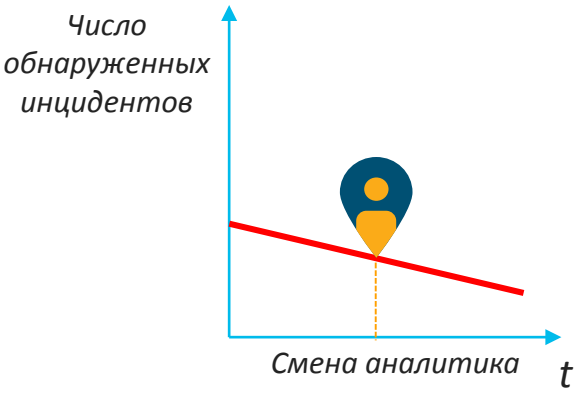
Естественный дневной ритм человека

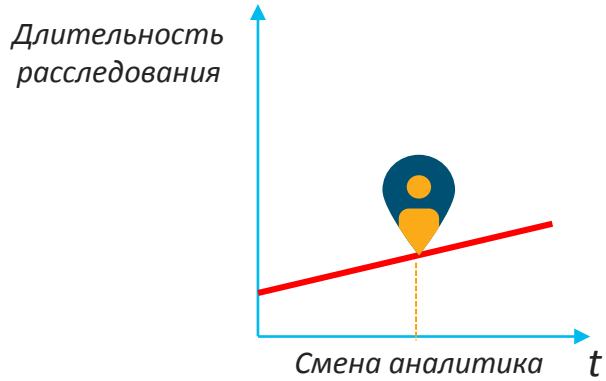


У «жаворонков» и «сов» графики будут чуть сдвинуты относительно друг друга

Наблюдения за работой аналитиков SOC







Указанные показатели работы аналитиков SOC также являются измеряемыми метриками SOC и с помощью ML их можно даже предсказывать, эффективно выстраивая работу персонала

Особенности ночной смены
А это половина времени работы SOC

- Сон и биологические часы никогда не перестраиваются даже если работать все время в ночную смену
- Стресс и напряжение после дневного сна приводят к снижение внимательности, росту времени реакции, ухудшению памяти
- Социальные изменения, в частности выпадение из социума и проблемы в семье (при ее наличии)
- Последствия для здоровья – кардиология, потеря аппетита и проблемы с пищеварением

Нельзя не учитывать физиологию работы аналитика

После 12-ти минут непрерывного мониторинга аналитик пропускает 45% активности на мониторе. После 22-х – 95%

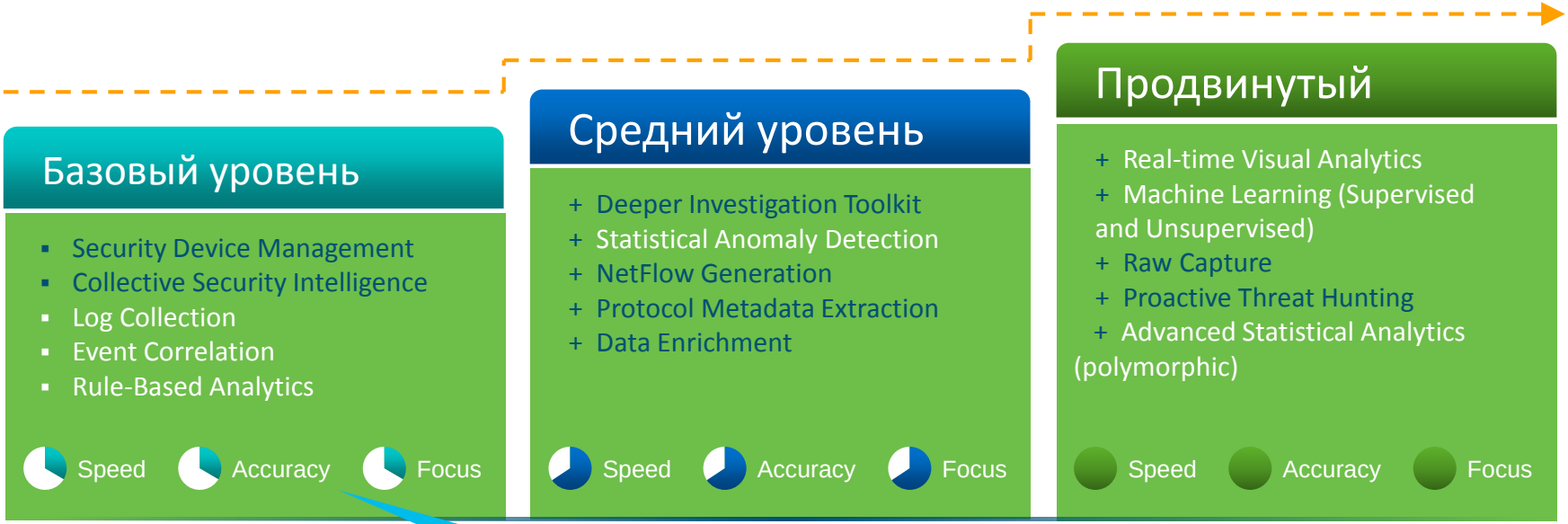
После 20-40 минут активного мониторинга у аналитика наступает психологическая слепота

Почему первая линия SOC не нужна?

- Аналитики L1 занимаются мониторингом событий и обнаружением простых инцидентов
- Автоматизация поможет исключить аналитиков L1, которые и так видят около 10% всего того, что должны
- Оставшиеся 90% - это игра и в нее надо быть вовлеченным

Уровень ротации аналитиков L1 – около 90%

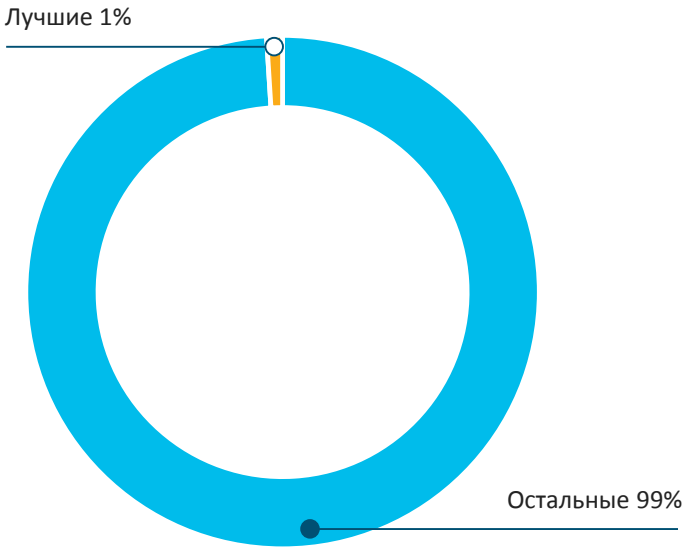
Что ищут аналитики L1 – известное или неизвестное?



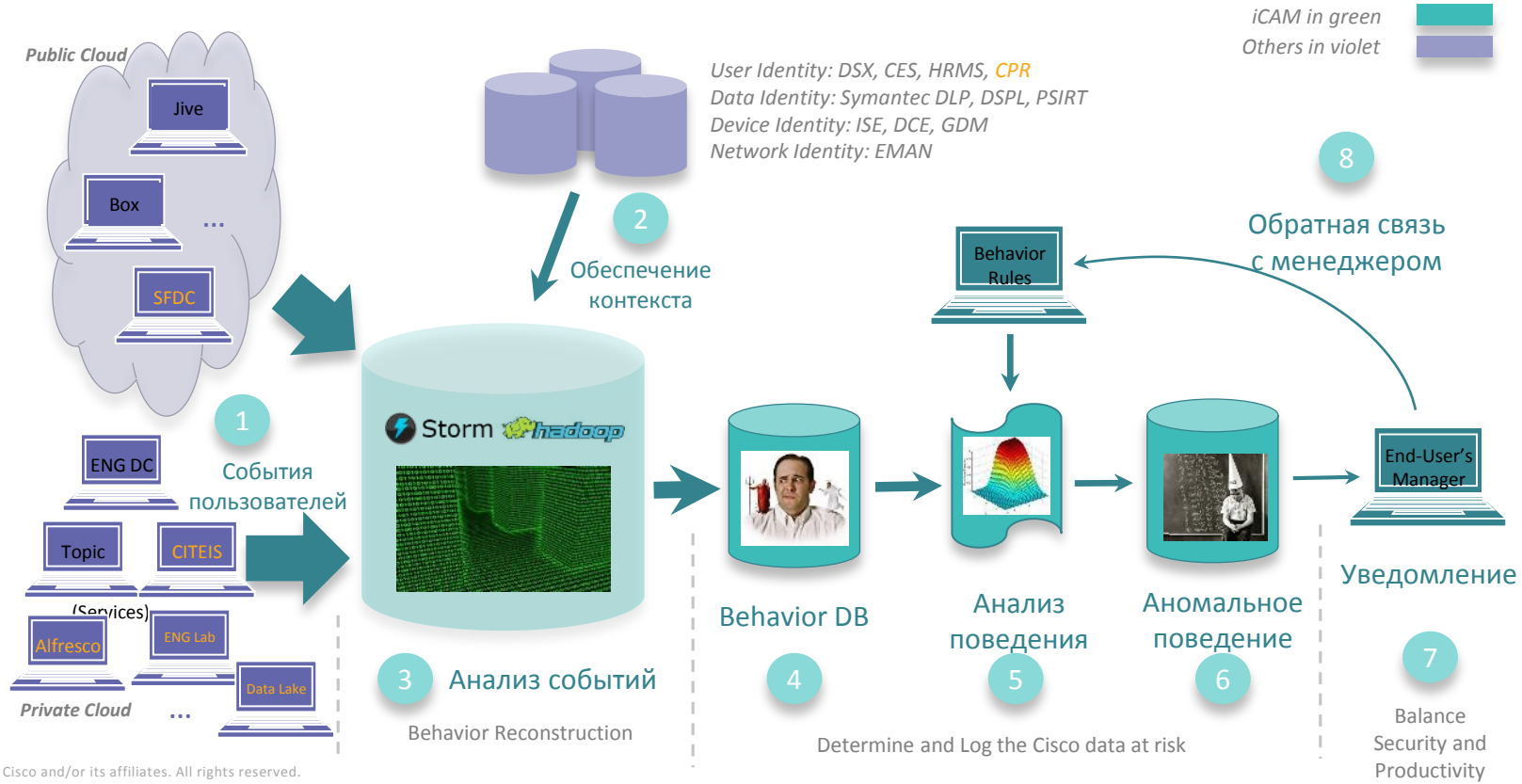
L1 – это для этого уровня зрелости аналитических технологий SOC

Покупать или создавать инструментарий?

- 99% SOCов используют готовые, приобретенные решения по ИБ
- 1% SOCов разрабатывают свой инструментарий или дорабатывают open source решения



iCAM: внутренняя разработка Cisco



Эффект от iCAM в Cisco

Ценность для бизнеса	• **40+ миллиардов** файлов Cisco были защищены • **16,000+** серверов мониторится
Скорость	• **10** секунд на детектирование риска • **24** часа на устранение риска
Объемы	• **4+ миллиардов** событий ежедневно • **±2000** инцидентов в квартал
Качество операций	• User-To-Ops: **100,000 : 1** • **90%** сигналов тревоги управляются автоматически • Только **1%** инцидентов требует ручной поддержки от Ops

15,2 миллиона долларов ежегодной экономии / сохранности

Рекомендации

Конкретные рекомендации

Планирование нагрузки в зависимости от длительности и времени смены

Менять смены либо часто (каждые 2-3 дня), либо редко (3-4 недели)

Ограничение ночной смены максимум 12-тью часами (включая сверхурочную работу)

Ограничение ночной смены максимум **8-мью часами**, если работа монотонная, критичная требующая концентрации

Возможно стоит сделать смену с переменной длительностью или с гибким временем начала и конца смены

Конкретные рекомендации (продолжение)

Поощряйте регулярные перерывы

Ограничьте рабочие дни 5-7 днями и сделайте отдых между сменами адекватной

Установите предел в 2-3 подряд смены, если смены более 8 часов и приходятся на ночь или раннее утро

Разрешите аналитикам 2 ночи полноценного сна при переключении между ночной и дневной сменами (и наоборот)

Предусмотрите в графике свободные выходные (сб., вс.)

ДЕЛАТЬ

Конкретные рекомендации (продолжение)

Обеспечьте для ночной смены те же преимущества, что и для дневной (комната отдыха, столовая и т.п.)

Убедитесь, что руководитель SOC понимает особенности сменной работы и умеет распознавать проблемы, связанные со сменой

Для аналитиков по вызову / в режиме ожидания обеспечьте режим отдыха

Убедитесь, что аналитики и их семьи знакомы с рисками, связанными со сменной работой

Освободите персонал на время обучения и развития

ДЕЛАТЬ

Конкретные рекомендации (продолжение)

Избегайте монотонной, требующей концентрации внимания или критически важной работы в ночные, ранние утренние часы, в конце длинной смены и в другие периоды низкий активности

Не включайте аналитиков в постоянные ночные смены

Не используйте недельную или двухнедельную ротацию

Не позволяйте аналитикам отказываться от перерывов с целью сокращения времени своей смены

Не разрывайте смены

НЕ ДЕЛАТЬ

Конкретные рекомендации (окончание)

Планируйте завершение задач в рамках одной смены

Предложите аналитикам выбор между постоянными и сменяемыми сменами

Не начинайте рабочую смену ранее 7 утра

Позвольте аналитикам самостоятельности выбирать перерывы в работе

Используйте ротацию смен по часовой стрелке (1-я – утро, 2-я – вечерняя, 3-я – ночная), а не против

Вопросы?