Как правильно построить процессы ИБ с ограниченным бюджетом

Саетгараиев Наиль

Ведущий технический эксперт направления Kaspersky

kaspersky

Современные реалии ИБ

Расширяется и/или изменяется IT-инфраструктура, которая требует защиты

Усложняется ландшафт угроз и расширяется поверхность атаки, добавляется целевая киберагрессия

Усиливаются требования регуляторов, особенно в отношении обеспечения защиты КИИ

Средние потери в результате одного киберинцидента

~$1 млн*

Процесс работы с инцидентами становится более сложным и ресурсозатратным

Присутствует глобальный дефицит ИБ-экспертов на рынке труда и неоптимальное использование их времени и таланта

kaspersky

3 СЛОЖНЫЕ АТАКИ

Kaspersky Expert Security

Служба ИБ или SOC

- Повышение экспертизы: Kaspersky Cybersecurity Training
- Аналитика угроз: Kaspersky Threat Intelligence
- Расширенное обнаружение и реагирование: Kaspersky EDR Expert; Kaspersky Unified Monitoring and Analysis Platform; Kaspersky Anti Targeted Attack
- Реагирование на угрозы: Kaspersky Incident Response
- Анализ защищенности: Kaspersky Security Assessment

2 СКРЫТЫЕ УГРОЗЫ

Kaspersky Optimum Security

Команда ИБ

- Базовое обнаружение и реагирование: Kaspersky EDR для бизнеса Оптимальный
- Песочница: Kaspersky Sandbox
- Обогащение данными: Kaspersky Threat Intelligence Portal
- Киберграмотность: Kaspersky Security Awareness
- Защита контейнеров: Kaspersky Container Security
- Умная защита для среднего бизнеса: Kaspersky Smart

Kaspersky Managed Detection and Response

1 ОБЫЧНЫЕ УГРОЗЫ

Kaspersky Security Foundations

ИТ

- Конечные устройства: Kaspersky Security для бизнеса; Kaspersky Embedded System Security; Kaspersky Security для виртуальных и облачных сред; Kaspersky Secure Mobility Management
- Сеть: Kaspersky Security для почтовых серверов; Kaspersky Security for Internet Gateway
- Данные: Kaspersky Security для систем хранения данных
- Поддержка: MSA и профессиональные сервисы

Цифровая Трансформация. Успешная. Эффективная.

softline SOFL

Базовый EDR: Kaspersky EDR для бизнеса Оптимальный

kaspersky

Продвинутая защита конечных точек

- Защита от новейших угроз, в том числе от бесфайловых вирусов
- Адаптивный контроль аномалий
- Автоматическое устранение угроз
- Развертывание в облаке или локально

Прозрачность

- Визуализация пути атаки
- Сканирование индикаторов компрометации
- Единая карточка обнаружения

Расследование

- Анализ первопричин
- Детали по инциденту
- Обогащение данными Threat Intelligence

Реагирование

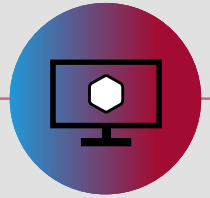
- Рекомендации по реагированию
- Реагирование «в одно нажатие» и автоматическое реагирование
- Сетевая изоляция, запрет запуска, карантин

kaspersky

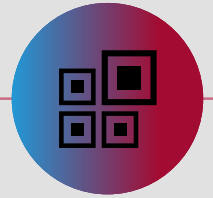
Функциональное сравнение уровней Kaspersky Smart

Kaspersky Smart	Smart I	**Smart II**
Технологии	SIEM	SIEM + EDR
Комплексный мониторинг и корреляция событий ИБ в рамках всей инфраструктуры	●	●
Базовые действия по реагированию (при установленном у заказчика KES, KWTS, KSMG)	●	●
Готовая интеграция с самыми распространёнными источниками данных, ИТ- и ИБ-системами	●	●
Помощь в соответствии требованиям регуляторов, включая возможность предоставления данных о случившихся инцидентах	●	●
Фокус на самую популярную точку (хосты) входа злоумышленников: контроль и визуализация происходящего		●
Передовое обнаружение и расследование сложных угроз на уровне конечных точек		●
Расширенные действия по реагированию, в том числе в масштабе всей инфраструктуры		●

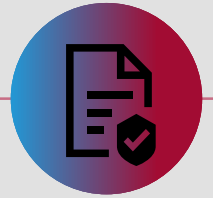
kaspersky



Единая поставка самой актуальной киберзащиты для среднего размера инфраструктур



Не только мониторинг и обнаружение, но и реагирование



Помощь в соблюдении требований регуляторов

Решение для комплексной защиты среднего размера организаций с минимальными требованиями к аппаратным мощностям и возможностью установки на виртуальные машины*

*KVM – 250, 500, 750 узлов, VMware – 1000 узлов

softline®

Цифровая Трансформация.
Успешная. Эффективная.