

# КИБЕРГРАМОТНОСТЬ СОТРУДНИКОВ И ФОРМИРОВАНИЕ КИБЕРКУЛЬТУРЫ



О ЧЁМ ЗАБЫВАЕТ СОВРЕМЕННАЯ  
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**СОТРУДНИК –  
САМОЕ  
СЛАБОЕ  
ЗВЕНО**

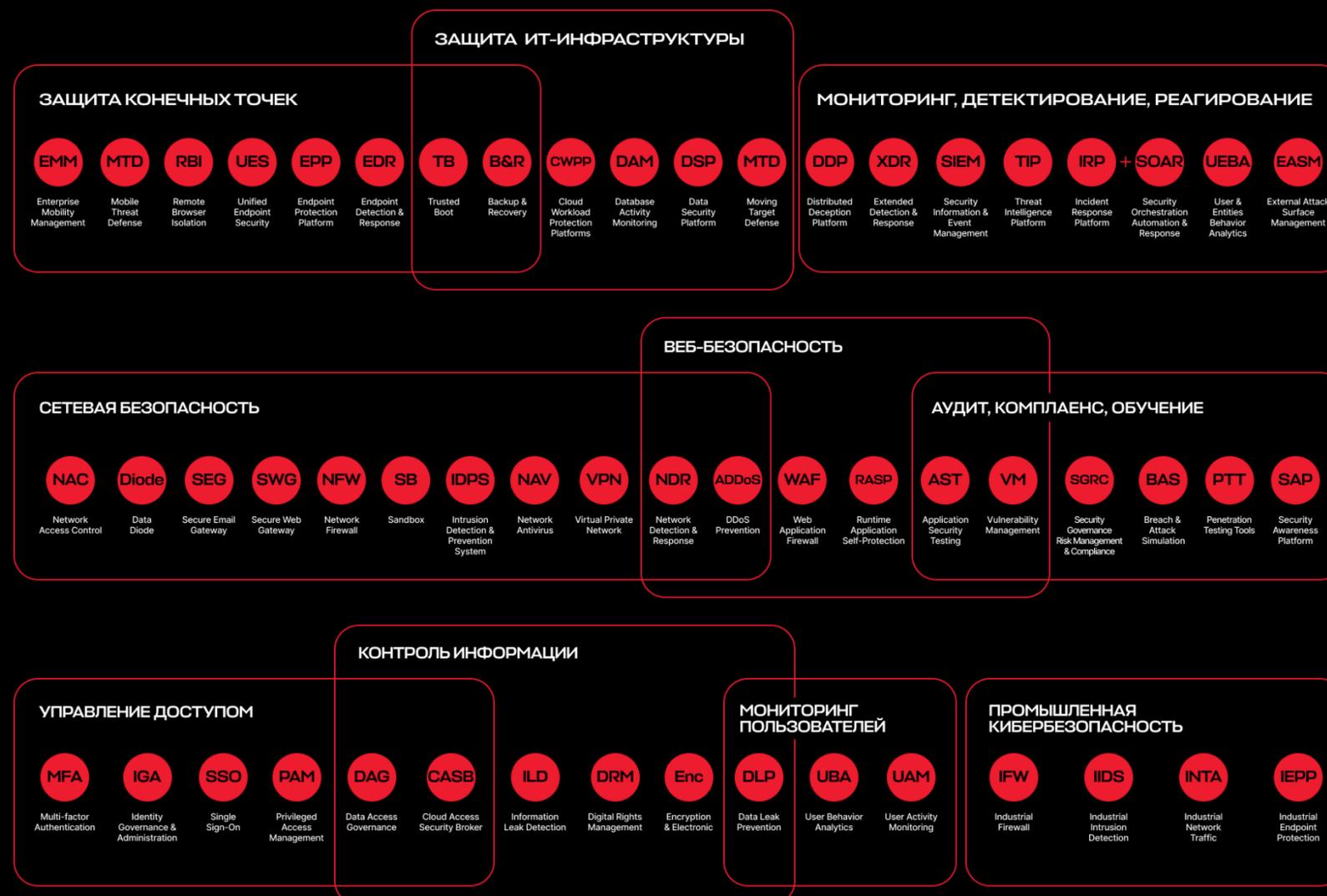


# ПОЧЕМУ ВЗЛАМЫВАЮТ СИСТЕМЫ?

- ⚡ Социальная инженерия обходит любую защиту
- ⚡ Игнорирование правил безопасности
- ⚡ Человеческий фактор – слабое звено в системе безопасности

**Покупка систем безопасности не гарантирует защиты от социальной инженерии!**

## ЛЕЧИМ ПРИЧИНУ, А НЕ СИМПТОМЫ



# КАК РЕШИТЬ ПРОБЛЕМУ?



КАК НАМЕКНУТЬ СОТРУДНИКУ,  
ЧТО НУЖНО БЫТЬ ВНИМАТЕЛЬНЕЕ  
И НЕ СОВЕРШАТЬ ОШИБОК



HARD  
VERSION

# КАК ВЫГЛЯДИТ СПЕЦИАЛИСТ ИБ



В ГЛАЗАХ  
СОТРУДНИКА

# КОМПАНИИ ВАЖНО ЗНАТЬ, ЧТО ПРОИЗОШЛО



Чем раньше об атаке  
станет известно, тем  
меньше ущерба она  
принесёт компании.

Молчание – золото, но  
в этом случае – золото  
по затратам.



# PEOPLE-CENTRIC SECURITY



# КОМПЛЕКСНЫЙ ПОДХОД К БЕЗОПАСНОСТИ

Средства  
кибербезопасности

Процессы обеспечения  
кибербезопасности

Работа с персоналом = **MUSTHAVE**  
Продукт класса **Security Awareness**



# phishman

- решение класса **Security Awareness** для анализа поведения сотрудников и определения уровня их компетенций с помощью встроенного фишингового модуля и интеграций с внешними системами безопасности

# ПРИНЦИП РАБОТЫ, ЕСЛИ ПРОСТО

ТЕСТИРОВАНИЕ  
КОМПАНИИ

ФОРМИРОВАНИЕ  
НАВЫКОВ

КОНТРОЛЬ  
ПРОГРЕССА

АВТОМАТИЗАЦИЯ  
ПРОЦЕССА



Фишинговый модуль  
+ Интеграция с «ИС»\*

Собственная СДО +  
Возможность интегра-  
ции с собственной СДО

Тестирование

Конструктор  
сценариев

\*ИС – информационные системы.

# КУРСЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Противодействие социальной инженерии

События и инциденты ИБ: как обнаружить и сообщить

Примеры инцидентов ИБ

Основы информационной безопасности

Ответственность за несоблюдение требований законодательства

Проверка знаний по информационной безопасности

Создание надежных паролей

Кто виноват и что делать: ответственность за правонарушения в сфере информации и информационных технологий

Концепция Phishman

Защита мобильных устройств

Правила безопасной удаленной работы

Информационная безопасность для ИТ-шников

Защита конфиденциальной информации

Антивирусная защита

Для чего в компании отдел ИБ: курс для топ-менеджмента

Как защититься от атаки в Telegram

# СПЕЦИАЛИЗИРОВАННЫЕ КУРСЫ

Защита персональных данных

Защита информационной безопасности объектов критической информационной инфраструктуры

■ (КИИ)

■ (для руководителей подразделений ОККИИ)

Обеспечение информационной безопасности объектов критической инфраструктуры

Безопасная разработка

Задачи работников службы эксплуатации в обеспечении безопасности ОККИИ

Задачи службы функционального сопровождения в обеспечении безопасности ОККИИ

Задачи службы информационной безопасности в обеспечении безопасности объектов критической инфраструктуры (для работников подразделения информационной безопасности)

Обеспечение информационной безопасности объектов критической информационной инфраструктуры

■ в нефтегазовой отрасли

■ в сфере энергетики

■ в металлургической промышленности

■ в транспортной отрасли

# РЕЗУЛЬТАТ

Обученные сотрудники видят подозрительное там, где другие не замечают.

Укрепляется безопасность компании. Формируется культура безопасности, где каждый отвечает за защиту информации.

НА **70%**

СОКРАЩЕНИЕ ЧИСЛА СОБЫТИЙ ИБ  
В ПЕРВЫЙ МЕСЯЦ  
ИСПОЛЬЗОВАНИЯ

Системное обучение помогает распознавать и предотвращать угрозы.

Сотрудники становятся «сенсорами», выявляя подозрительные письма, ссылки и запросы, оперативно сообщая об инцидентах

\*На основании результатов пилотных проектов ООО «ФИШМАН»

phishman.ru

# УЖЕ РАБОТАЮТ С PHISHMAN:





**БЕЗОПАСНОСТЬ,  
КОТОРУЮ НЕ ОТНЯТЬ**



# НАСКОЛЬКО ВАШИ СОТРУДНИКИ УСТОЙЧИВЫ К ФИШИНГУ?

**РОМАН ПАВЛЕНКО**

Руководитель отдела продаж

Тел. Моб: +7 (964) 569-98-17

[Roman.Pavlenko@phishman.ru](mailto:Roman.Pavlenko@phishman.ru)



Мои контакты в QR коде