Тема 7

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

ТЗИСК

Социальная инженерия

метод получения необходимого доступа к информации, основанный на особенностях психологии людей

Что такое социальная инженерия?

Социальная инженерия (СИ) / Social engineering (SE)

Определение: совокупность приёмов, методов и технологий формирования условий и обстоятельств, которые максимально эффективно приводят к необходимому результату с использованием социологии и психологии.

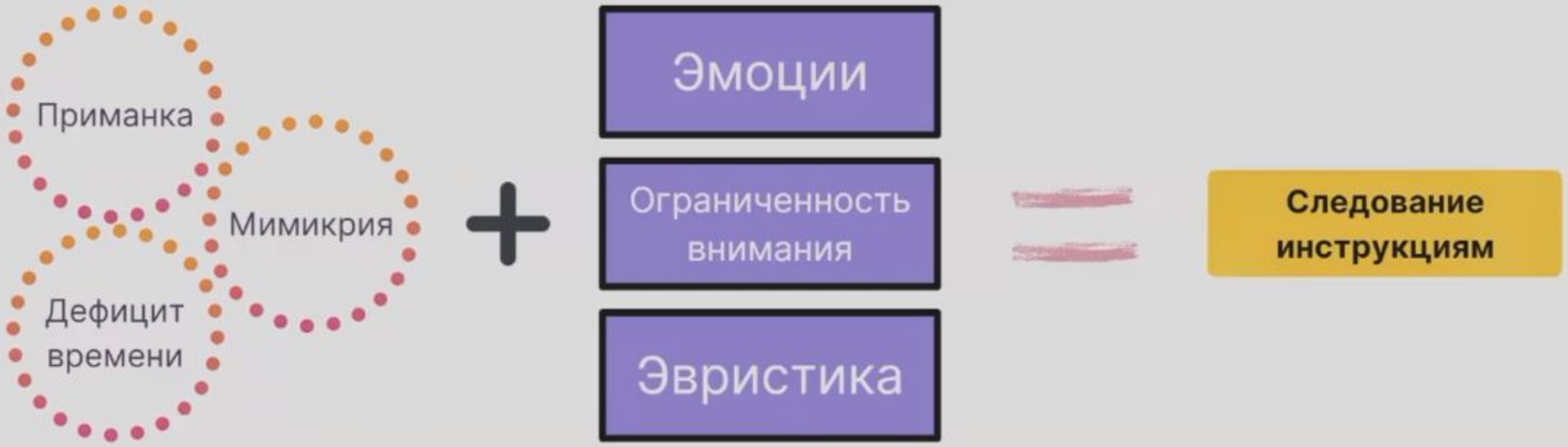
Социальная инженерия в контексте информационной безопасности — использование человеческого фактора с целью нарушения информационной безопасности системы.

Связанные области: HUMINT, OSINT, тестирование на проникновение, продажи, маркетинг, противоправная деятельность.

Виды атак типа социальная инженерия

1. Претекстинг
2. Фишинг
3. Троянский конь
4. Quid pro quo («услуга за услугу»)
5. Дорожное яблоко
6. Обратная соц. инженерия
7. Верифицированный отправитель

Претекстинг



Претекстинг

https://6click.lord-film-cam.site/2019/09/07/hakery-1995.html
4:35

"Один из героев звонит ночью в телевизионную компанию, связывается с менеджером и просит о помощи: погиб важный файл, начальник убьет, пожалуйста, дайте номер корпоративного модема. Так он и получает доступ в сеть компании."

Фишинг

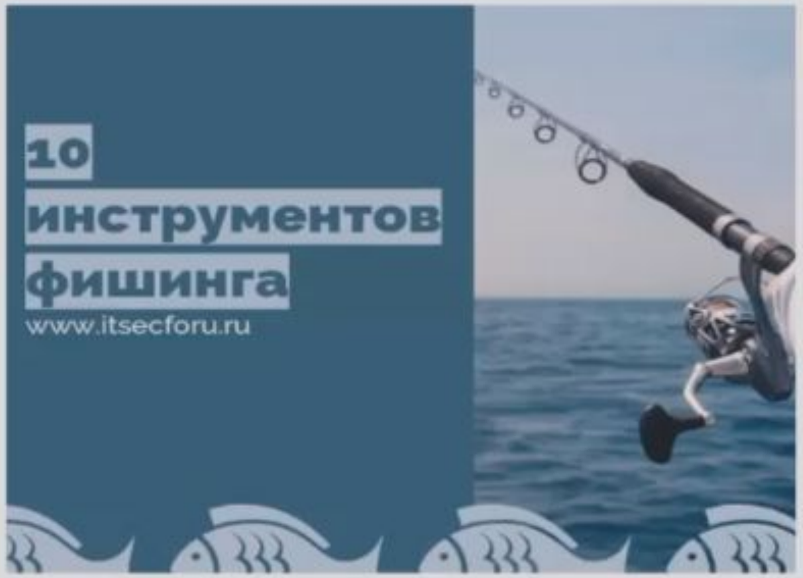
https://www.youtube.com/watch?v=TPR5Jt1cJFU
8:03

Типичный фишинг: юный герой захотел попасть в сообщество хакеров и заодно насолить своему школьному недругу.

Он создал простенький сайт по продаже того, что могло заинтересовать жертву (пищевых добавок для роста мышечной массы по совсем бросовым ценам), и тот попался — ввел данные кредитки отца.

Фишинг

1. Evilginx2
2. SETootkit
3. HiddenEye
4. King-Phisher
5. Gophish
6. Wifiphisher
7. SocialFish
8. BlackEye
9. Shellphish
10. zphisher



10 лучших инструментов для фишинга

Information Security Squad · 16 апр. 2020 г.

https://itsecforu.ru/2020/04/16/%f0%9f%8e%a310-%d0%bb%d1%83%d1%87%d1%88%d0%b8%d1%85-%d0%b8%d0%bd%d1%81%d1%82%d1%80%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d0%be%d0%b2-%d1%84%d0%b8%d1%88%d0%b8%d0%bd%d0%b3%d0%b0/?utm_source=canva&utm_medium=iframely

Фишинг

Как взломать аккаунты в социальных сетях – ZPhisher

Information Security Squad / 26 янв.

https://itsecforu.ru/2022/01/26/%F0%9F%8E%A3-%D0%BA%D0%B0%D0%BA-%D0%B2%D0%B7%D0%BB%D0%BE%D0%BC%D0%B0%D1%82%D1%8C-%D0%B0%D0%BA%D0%BA%D0%B0%D1%83%D0%BD%D1%82%D1%8B-%D0%B2-%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85/

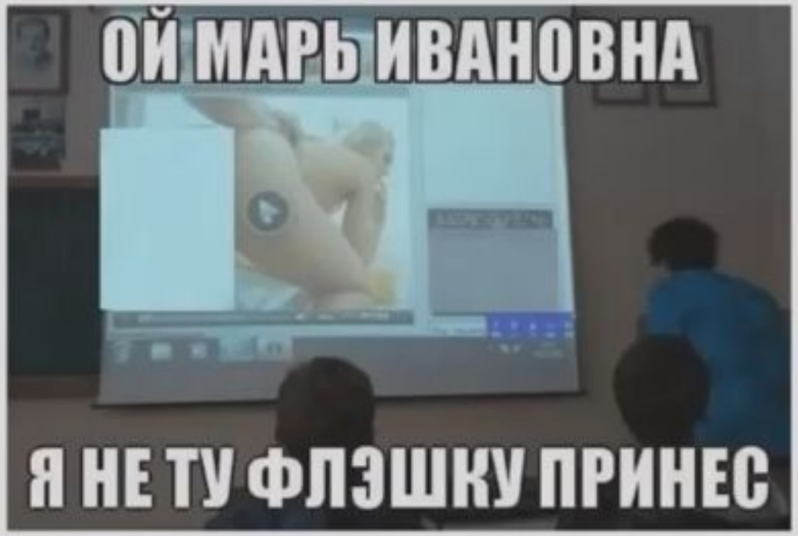
10 популярных «фишинговых» тем в 2021 году по версии Positive Technologies

По нашим оценкам, фишинг по-прежнему остается одним из главных методов атак, используемых злоумышленниками. Количество атак на частных лиц с использованием методов социальной инженерии заметно увеличилось: если ...

ptsecurity.com / Positive Technologies / 11 янв.

https://www.ptsecurity.com/ru-ru/research/analytics/10-populyarnyh-fishingovyh-tem-v-2021-godu-po-versii-positive-technologies/

Дорожное яблоко



Арт-проект с социальным подтекстом Drop Dead

Под Белгородом грибник нашел флешку с данными о погранслужбе Украины

Quid pro quo

Andrei
Здравствуйте ,я програмщик по образованию ,судя повашему ID - у вашего паблика вирус ,давайте мне свой пароль и логин ,я всё исправлю ,никакого обмана.Предоплата 100%.

Денис
О господи

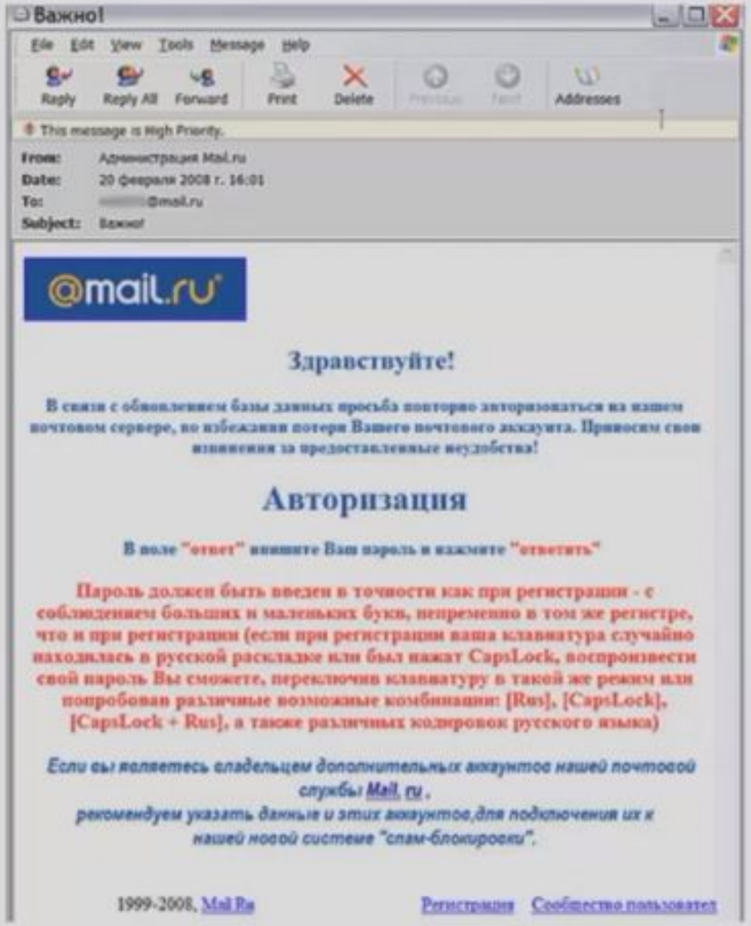
Правда?

Andrei
Да,систая правда

Чистая

Только быстро

Осталось 4часа



Важно!

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Addresses

This message is High Priority.

From: Администрация Mail.ru
Date: 20 февраля 2008 г. 16:01
To: @mail.ru
Subject: Важно!

@mail.ru

Здравствуйте!

В связи с обновлением базы данных просьба повторно авторизоваться на нашем почтовом сервере, во избежании потери Вашего почтового аккаунта. Приносим свои извинения за предоставленные неудобства!

Авторизация

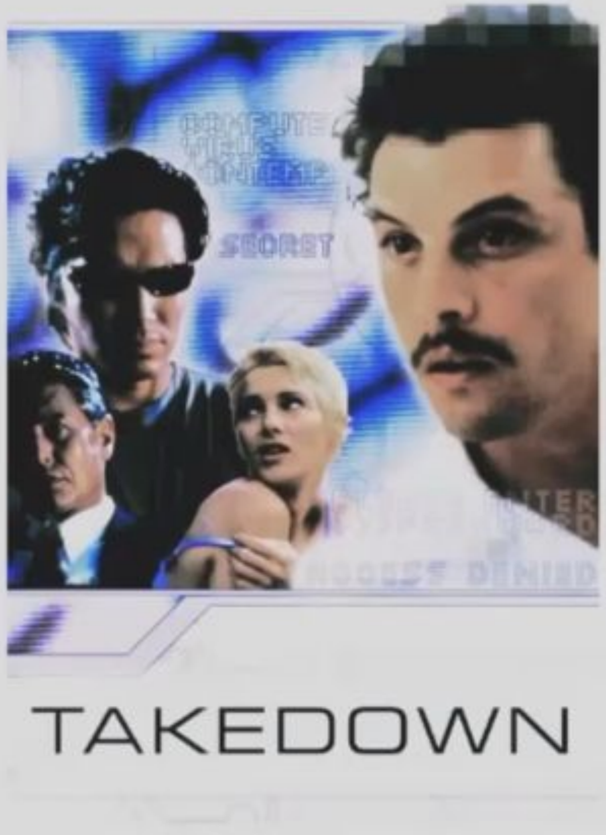
В поле "ответ" впишите Ваш пароль и нажмите "ответить"

Пароль должен быть введен в точности как при регистрации - с соблюдением больших и маленьких букв, непременно в том же регистре, что и при регистрации (если при регистрации ваша клавиатура случайно находилась в русской раскладке или был нажат CapsLock, воспроизвести свой пароль Вы сможете, переключив клавиатуру в такой же режим или попробовав различные возможные комбинации: [Rus], [CapsLock], [CapsLock + Rus], а также различных кодировок русского языка)

Если вы являетесь владельцем дополнительных аккаунтов нашей почтовой службы Mail. ru .
рекомендуем указать данные и этих аккаунтов,для подключения их к нашей новой системе "спам-блокировки".

1999-2008, Mail.Ru Регистрация Сообщество пользовател

Обратная социальная инженерия



https://6click.lord-film-cam.site/2019/09/07/vziom-2000.html
7:10
9:10

Целью обратной социальной инженерии является заставить цель саму обратиться к злоумышленнику за «помощью».

С этой целью злоумышленник может применить следующие техники:

- Диверсия: Создание обратимой неполадки на компьютере жертвы.
- Реклама: Злоумышленник подсовывает жертве объявление вида «Если возникли неполадки с компьютером, позвоните по такому-то номеру» (это в большей степени касается сотрудников, которые находятся в командировке или отпуске).

Хакеры

Митник взломал Пентагон
на компьютере с процессором меньше
2 мегагерц

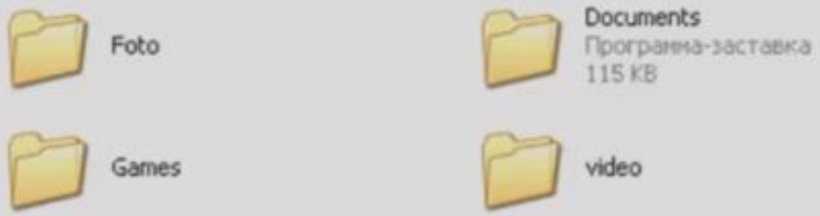
https://diletant.media/articles/26011961/

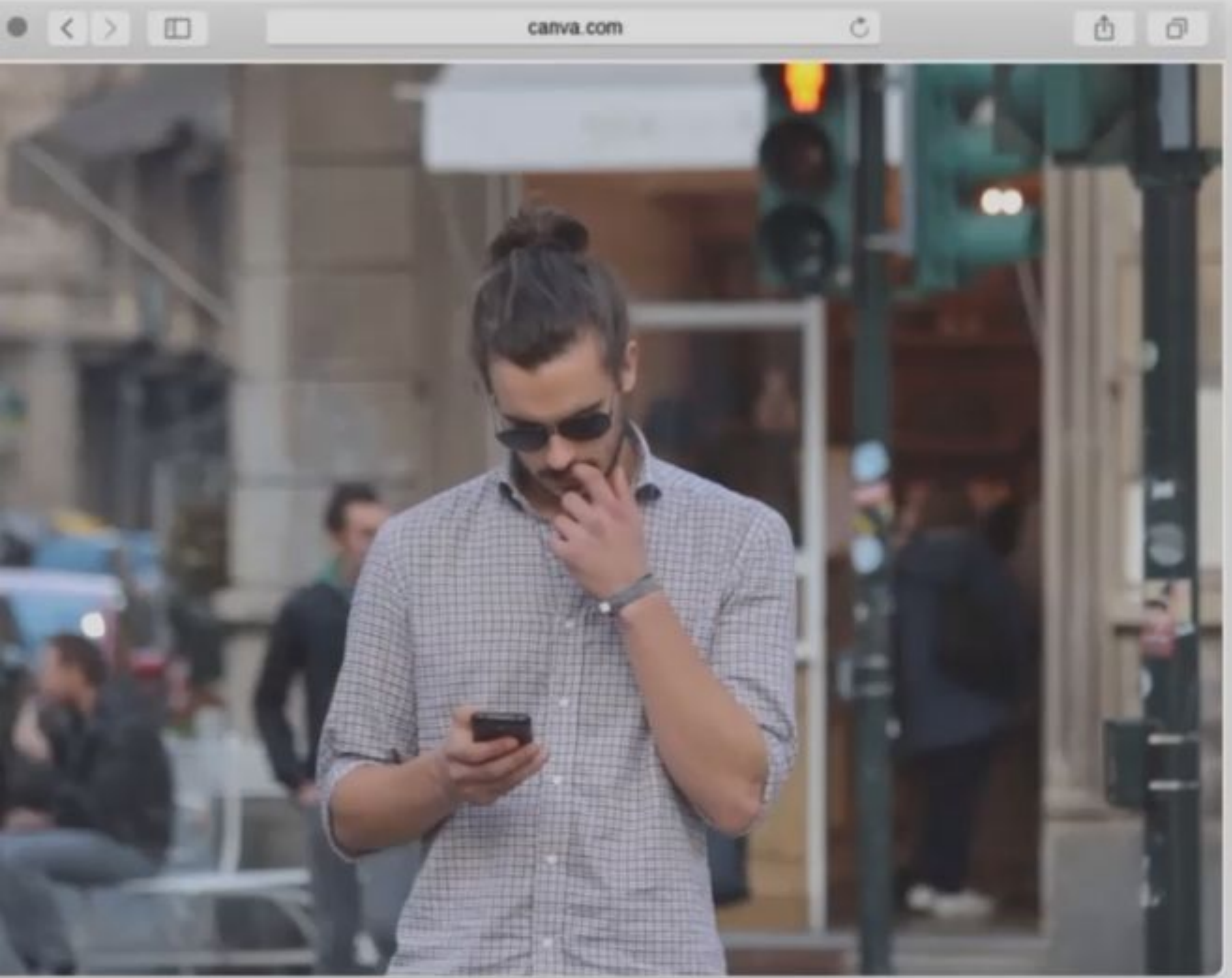
Российские пранкеры Вован и Лексус
(Владимир Кузнецов и Алексей Столяров)

https://www.gazeta.ru/politics/news/2022/03/24/17469805.shtml

Дополнительные виды

- Подмена иконки файла;
- Интригующее название файла;
- Мотивация к получению контента;
- Имитация живого общения;
- Эксплуатация страхов пользователя;





Любопытство

Поддельная подписка на рассылку

Майнинг почт

Массовая разведка

Персонализация

Как вас зовут?

Сайт не работает

Мультилендинг

Организационные меры

1

политики безопасности

2

обучение сотрудников

Над чем/как работают ИБ-специалисты методами социальной инженерии?

(на примере ЗАО "Перспективный мониторинг")

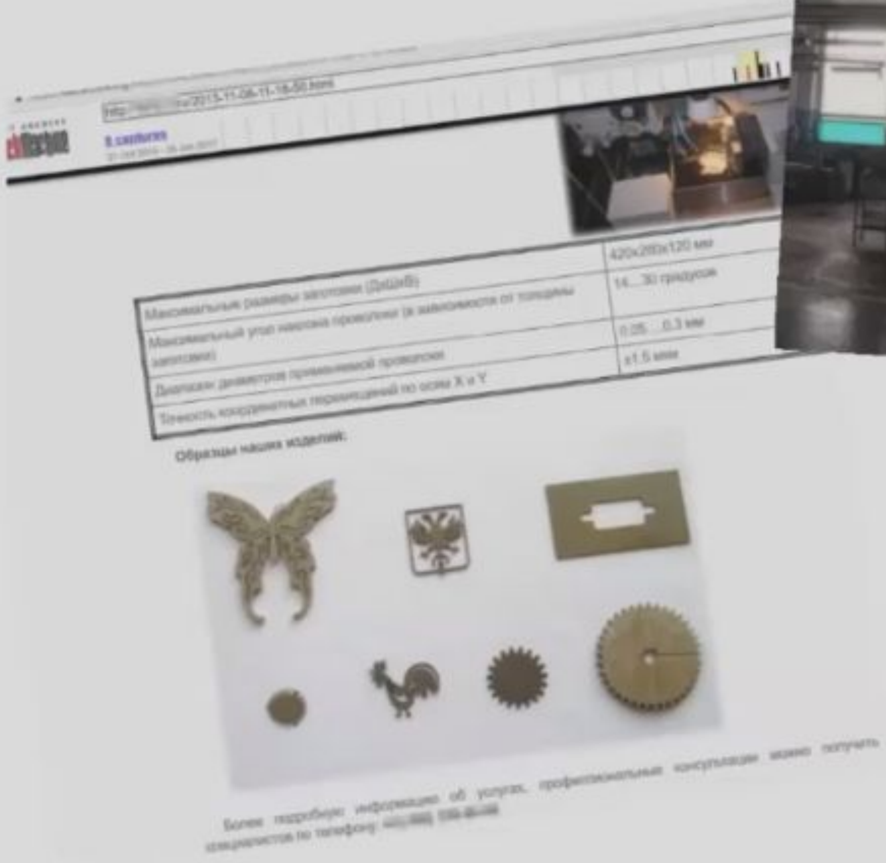
Физическая безопасность и социальная инженерия

Цель: аудит физической защищённости

Мероприятия:

- Экспертная оценка нормативных и методических документов (план повышения защищённости объекта, паспорт антитеррористической защищённости и т.п.)
- Анализ контроля доступа и внутренних правил
- Аудит технических средств (систем контроля и управления доступом, видеонаблюдения, периметральной охраны и сигнализации)
- Аудит физической охраны объектов

Физическая безопасность и социальная инженерия



Экономическая безопасность и социальная инженерия

Цель: противодействие мошеннической деятельности

Методология: симуляция действий злоумышленника / жертвы

Приёмы:	**Мероприятия:**
Обман	Контрольная закупка
Обман	Контрольная поставка
Обман	Тайный покупатель

Цель: получение конкурентного преимущества

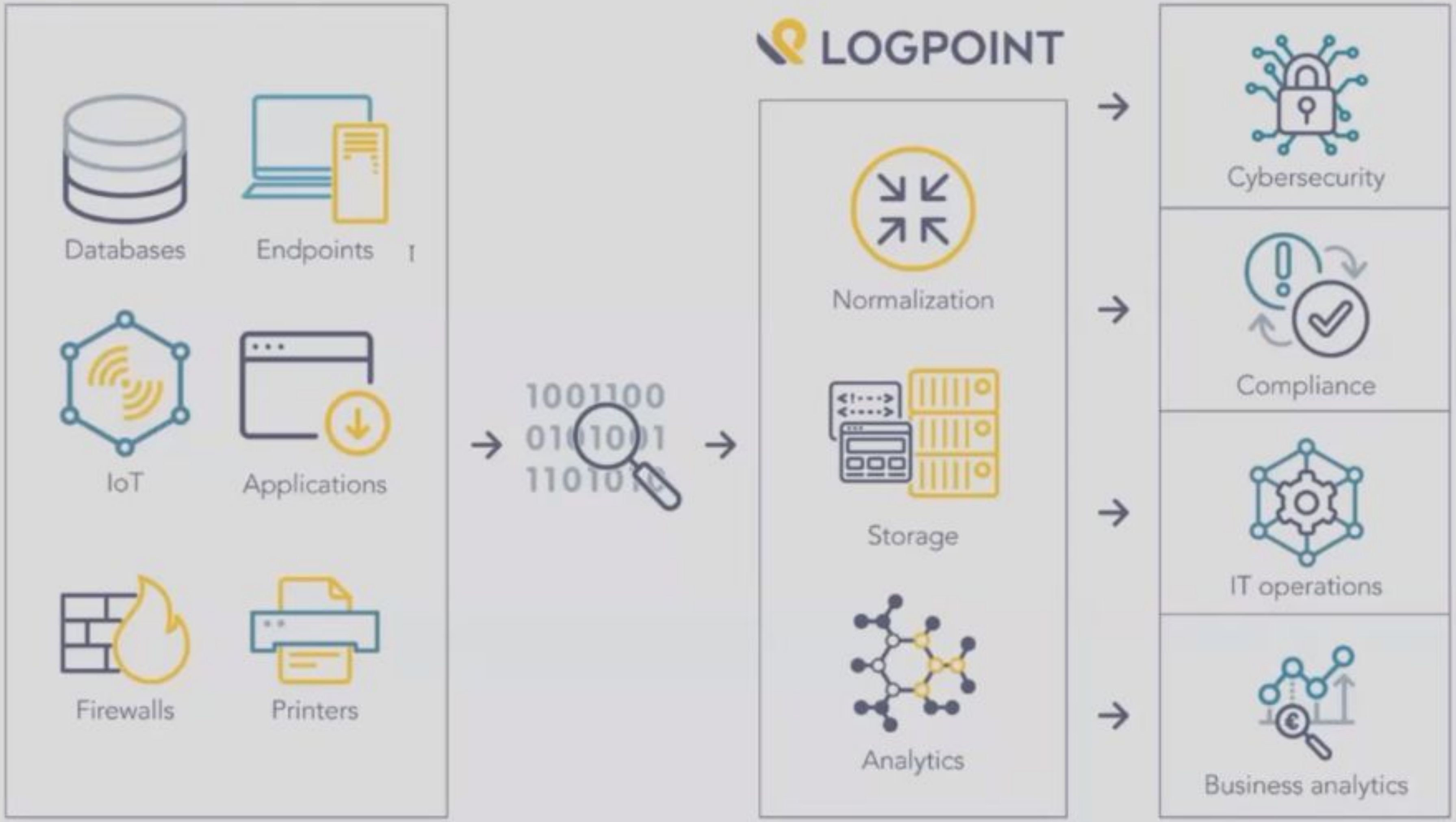
Методология: конкурентная разведка

Информационная безопасность и социальная инженерия

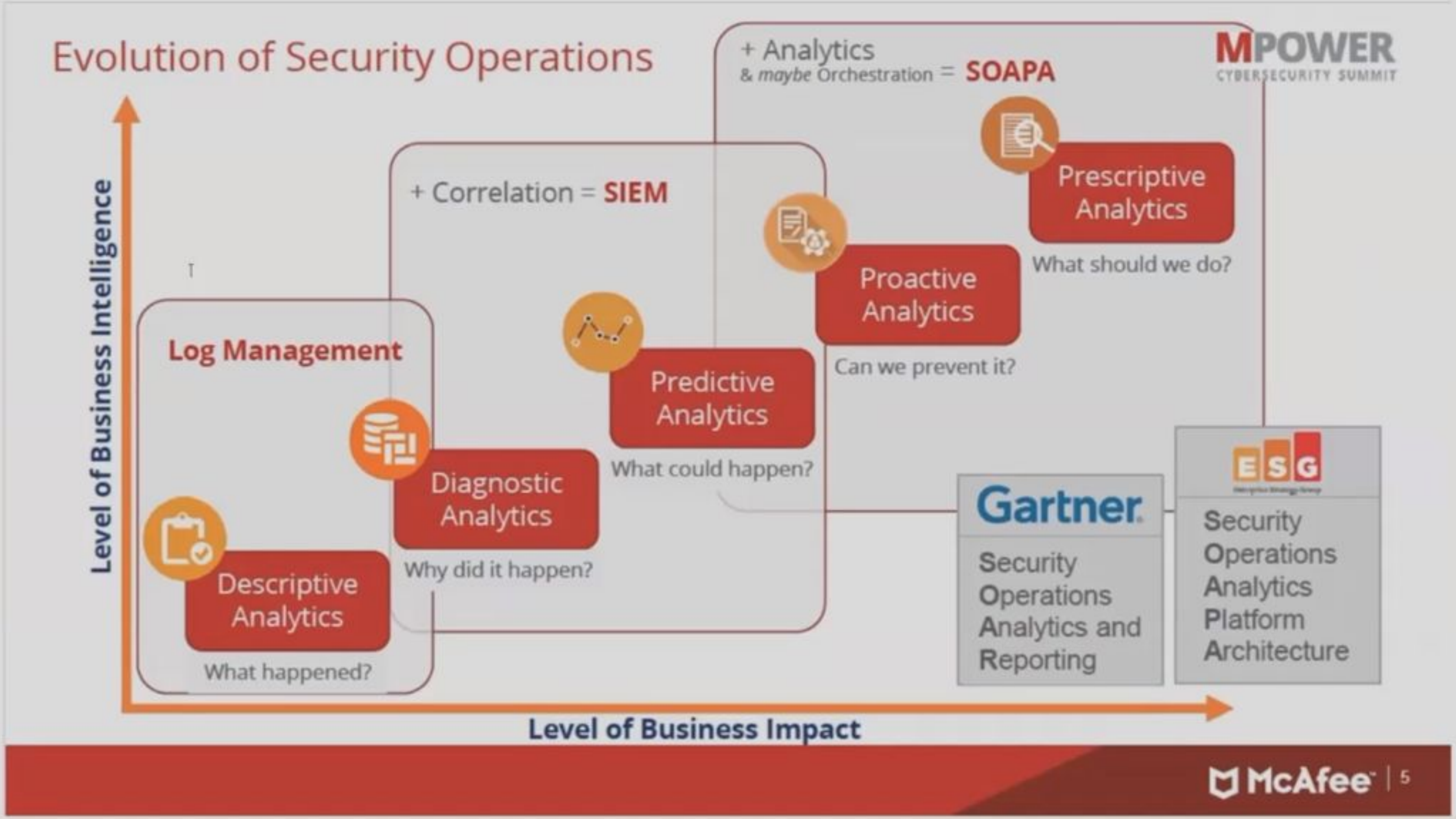
Аудит информационной безопасности:

- Проверка возможности получения доступа к конфиденциальной информации
- Проверка возможности получения доступа к информационным системам (в том числе, физического)
- Проверка эффективности работы IDS/IPS, DLP и прочих СЗИ
- Проверка работы служб информационной и внутренней безопасности
- Проверка осведомлённости сотрудников в вопросах ИБ

SIEM at a glance



SOAR



Evolution of Security Operations
MPOWER
CYBERSECURITY SUMMIT
+ Analytics
& maybe Orchestration = SOAPA
+ Correlation = SIEM
Log Management
Level of Business Intelligence
Descriptive Analytics
What happened?
Diagnostic Analytics
Why did it happen?
Predictive Analytics
What could happen?
Proactive Analytics
Can we prevent it?
Prescriptive Analytics
What should we do?
Gartner
Security Operations Analytics and Reporting
ESG
Security Operations Analytics Platform Architecture
Level of Business Impact
McAfee
5

Security Incident Response

упрощает проведение идентификации инцидентов.
Еще он занимается импортированием информации из применяемых решений, а также отвечает за кастомизацию процессов.

Vulnerability Response

- анализ зависимостей;
- оценка воздействия на бизнес-процессы, а также простоев;
- внесение необходимых изменений;
- проверка выполненных изменений

Threat Intelligence

Необходим для обнаружения индикаторов возможной компрометации и отслеживания угроз на глубоких уровнях

Блокировка внешних носителей

Контроль возможных утечек данных через внешние устройства и ограничение доступа к различным типам

- флешки,
- модемы,
- принтеры,
- жесткие диски

Тематика докладов

1. Автоматизация фишинговых атак. Программные решения для проведения фишинговых атак.
2. SET, CATPHISH и иные инструменты социальной инженерии, встроенные в Kali Linux
3. Суть и назначение SIEM и SOAR систем. Их роль в противодействии социальной инженерии.