MNEMONICA

Mastering Security Delivering Protection

ГРАДОВЕ НА БЪДЕЩЕТО

Киберсигурността в човешката ера или
човешката сигурност в дигиталната ера

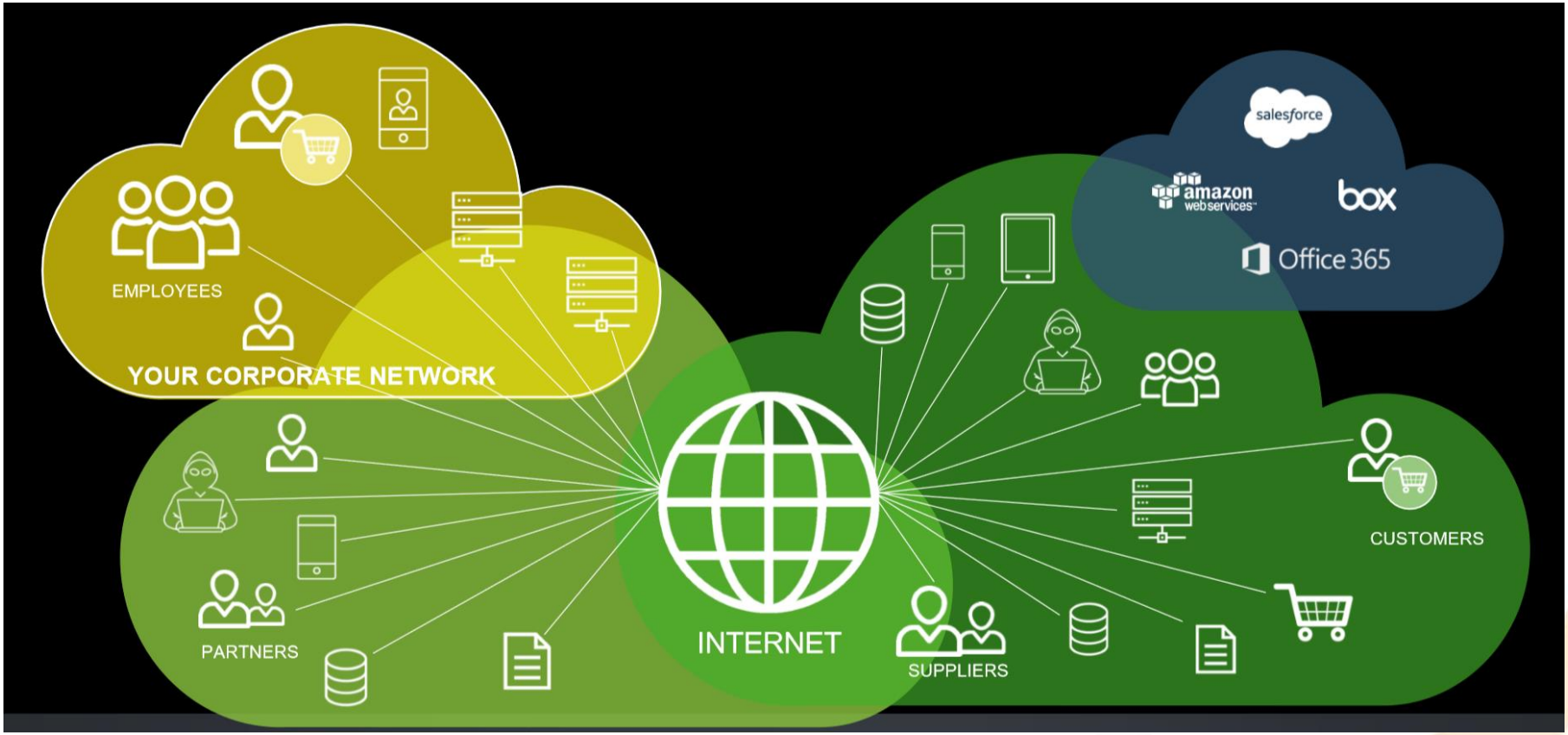
Вихрен Славчев

28.02.2019 г.

София

MNEMONICA
Mastering Security Delivering Protection

НОВАТА РАБОТНА СРЕДА



MNEMONICA
Mastering Security Delivering Protection

ПРЕДИЗВИКАТЕЛСТВА И ОСНОВНИ ПРОБЛЕМИ - ФАКТИ

- Пробиви чрез Phishing – 68%
- Пробиви чрез Malware - 66%
- Пробиви чрез Social Engineering - 46%
- Инциденти от суперпотребители – 80%
- Пробиви поради потребителски грешки – 36%
- 1 от всеки 5 потребители е готов да продаде корпоративния си достъп

MNEMONICA
Mastering Security Delivering Protection

ПРЕДИЗВИКАТЕЛСТВА И ОСНОВНИ ПРОБЛЕМИ ПРИ IOT

- По-широка употреба, по-голяма заплаха
- Незащитени IoT – задаващо се бедствие
- Недобре защитени API
- Уязвимости в системите и приложенията
- Откраднати акаунти
- Злонамерени служители
- Постоянни заплахи от ново поколение
- Загуба на информация/устройства/носители
- Недостатъчен контрол и проучване при употреба на облачни услуги

MNEMONICA
Mastering Security Delivering Protection

РАЗУМНИЯТ КОМПРОМИС

GDPR или PSD II

Сигурност или достъпност

SECURITY & COMPLIANCE

INNOVATION

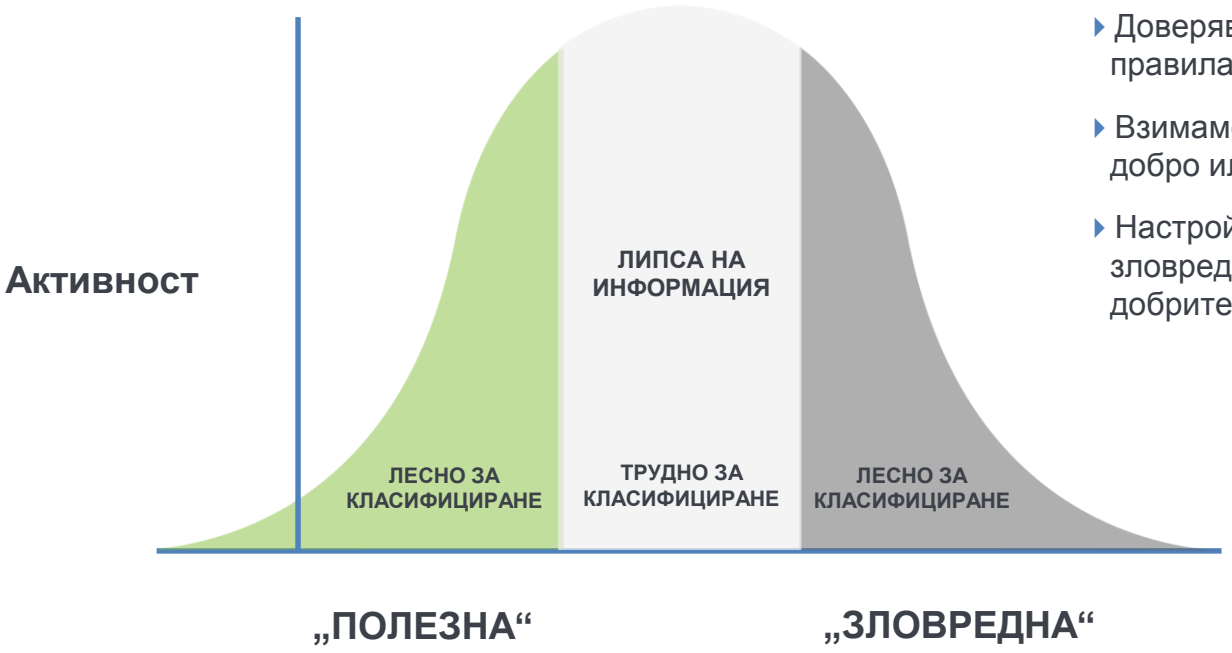
56% of business decision makers state it is **DIFFICULT** or **VERY DIFFCULT** to promote innovation while maintaining corporate security and governance

MNEMONICA
Mastering Security Delivering Protection

НОВИТЕ ЦЕЛИ

Умни градове, автоматизирани услуги и защитени данни

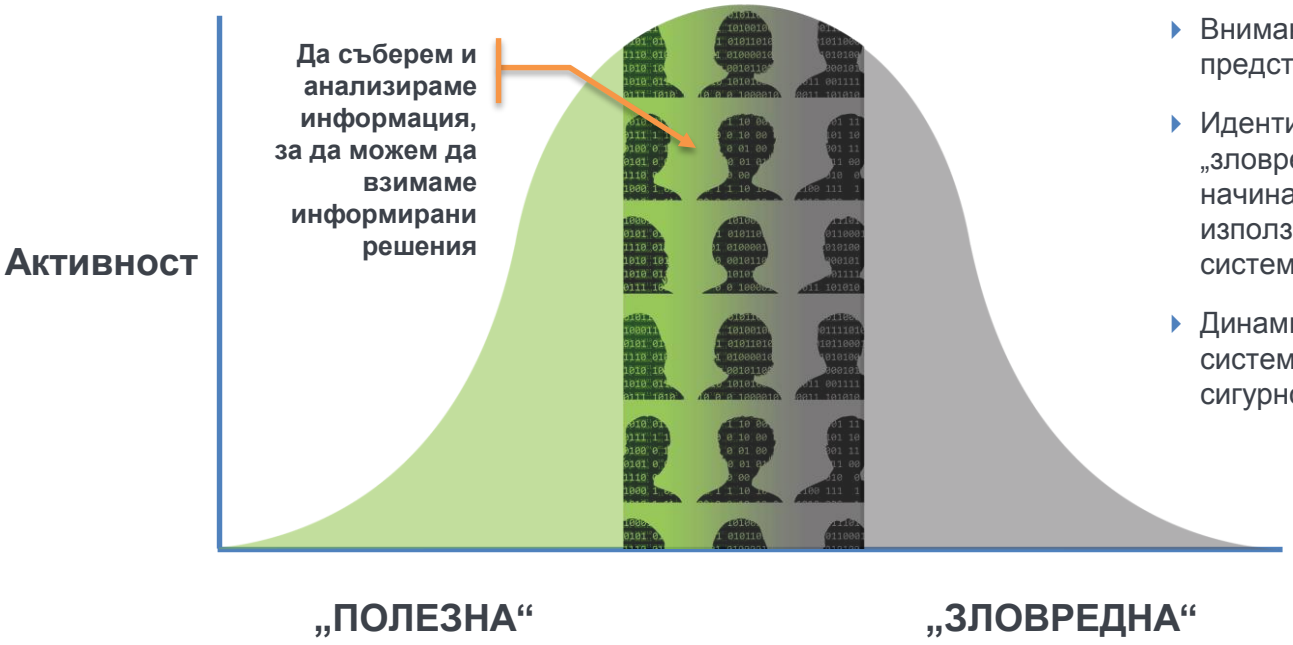
ТРАДИЦИОННИЯТ НАЧИН НА ЗАЩИТА



- Доверяваме се на статични политики и правила в една динамична среда
- Взимаме решение на момента какво е добро или не
- Настройваме си системите да спират зловредните дейности и да пропускат добрите

АБСОЛЮТНО НЕОБХОДИМО, НО НЕДОСТАТЪЧНО

КИБЕРСИГУРНОСТ ОТ НОВО ПОКОЛЕНИЕ



ФОКУС ВЪРХУ ПОВЕДЕНИЕТО

- Внимание върху действията, които представляват най-голям риск
- Идентифициране на „полезна“ и „зловредна“ активност според начина, по който потребителите използват информационните системи
- Динамичност и самообучение на системата за информационна сигурност

ПРИМЕР ЗА ПОВЕДЕНЧЕСКИ ПОДХОД

Петър, специалист „Техническа поддръжка“

Петър се опитва да се свърже с офиса в събота в 23:00 часа, за да достъпи документацията на клиент с цел извършване на планирана миграция

Традиционен подход

***Политика**: блокиране. Само дежурните могат да се свързват и то до 22:00 часа*

ЕФЕКТ ВЪРХУ ПОТРЕБИТЕЛЯ

Петър е ядосан и разочарован, тъй като не успява да спази поет ангажимент към клиент

Ще измисли заобикаляне на този проблем – ще копира занапред всичката документация локално

Нивото на сигурност е компрометирано, клиентът също е недоволен

ЕФЕКТ ВЪРХУ АДМИНИСТРАЦИЯТА

Прекият му ръководител трябва да анализира инцидента

Потенциално това може да се случва всяка вечер в продължение на месеци

В крайна сметка този тип проверка се спира

ПРИМЕР ЗА ПОВЕДЕНЧЕСКИ ПОДХОД

Петър, специалист „Техническа поддръжка“

Петър успява да се свърже с офиса и отваря необходимата му документация

Петър копира голямо количество друга техническа документация

Получава имейл от клиент с линк за сваляне на технически данни, към който Петър се свързва

Петър започва да достъпва и да копира информация от документациите на различни клиенти за адреси, имена и пароли

Високорисков профил

Политика: **наблюдение** на всички активности от компютъра на Петър и **блокиране** на всички опити за пренасяне и копиране на данни

Среднорисков профил

Политика: **криптиране** на документите, съдържащи чувствителна информация

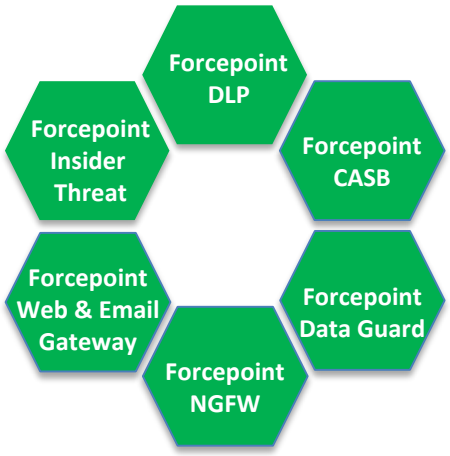
Нискорисков профил

Политика: **разрешено.** Записва се следа за събитието

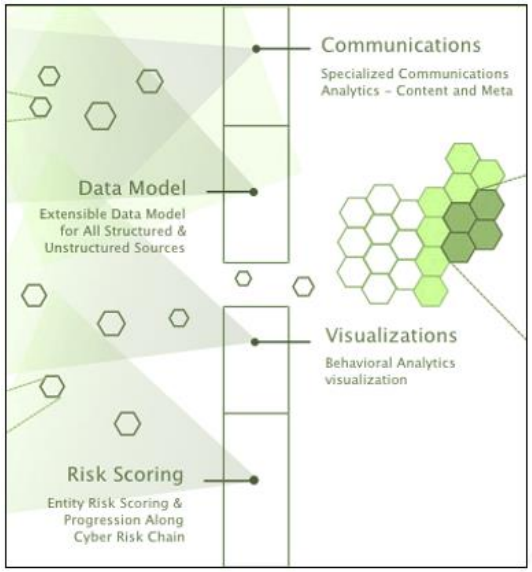
ОСНОВНИ РЕШЕНИЯ СРЕЩУ ЗАПЛАХИТЕ

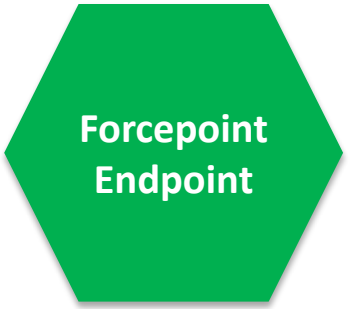
ЕКОСИСТЕМА ОТ СРЕДСТВА

ИЗТОЧНИЦИ ⟩ СИСТЕМА ЗА АНАЛИЗ ⟩ НАЛАГАНЕ НА ПОЛИТИКИ



3rd Party Data Sources





ЧОВЕКЪТ

СИСТЕМИТЕ СА ИНСТРУМЕНТ

Аналитичност

1. Dashboard за аналитик

Рейтинг на потребителите – създаден около дефинирана точкова система и с достатъчно детайли, за да позволи на аналитика да взима бързи решения

2. Времева графика по обект

Детайлна графика, която показва рисковите събития

3. Разследване

Възможност за детайлно разследване, позволяващо на аналитика да разгледа „един ден“, да набелязва, маркира събития и др.

Администрация

4. Модели

Възможност компаниите да създават техни собствени модели на риска, без да имат нужда от Data Scientist

5. Функционалности

Възможност компаниите да създават собствени правила и действия, които отговарят на техните специфични нужди

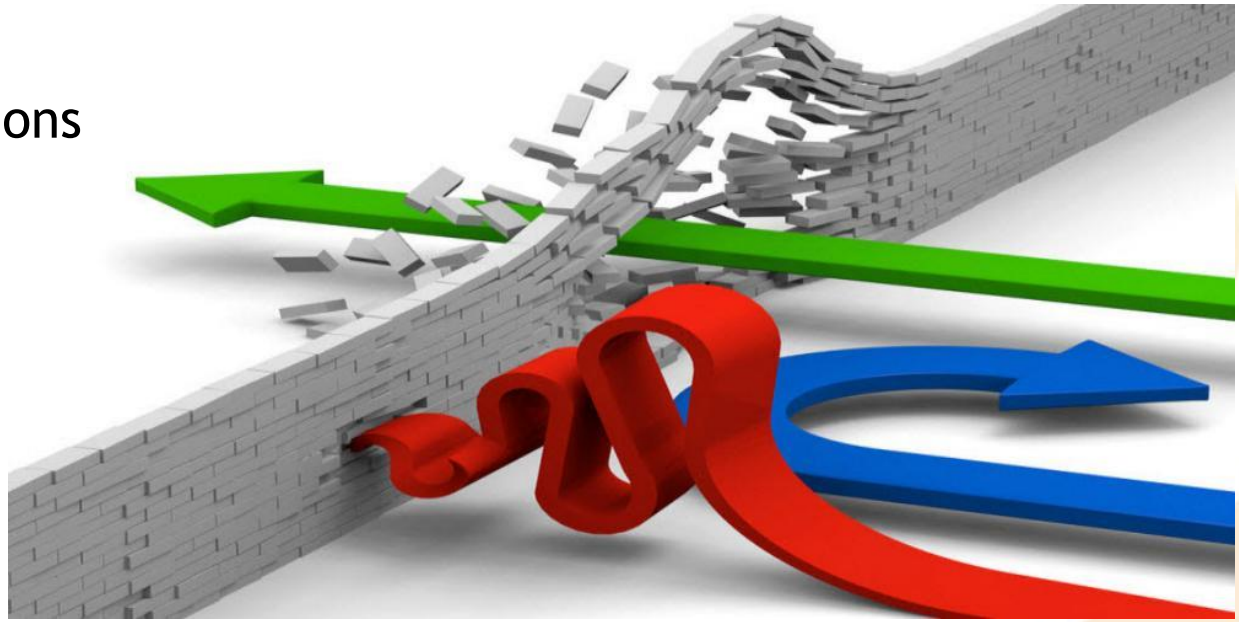
6. Лексикон

Възможност компаниите да дефинират важните за тях думи, комбинации, имена на процеси и домейни и др.

MNEMONICA
Mastering Security Delivering Protection

ПОЛЗАТА ОТ ТЕХНОЛОГИИТЕ - ТЕСТВАНЕ

- Vulnerability scanning
- Penetration testing
- Application testing
- Database testing
- Real life simulations



Благодаря!

MNEMONICA
Mastering Security Delivering Protection

„Николай Хайтов“ 12, етаж 4, офис 13
1113 София
www.mnemonica.bg

02 964 16 41
02 964 16 40

office@mnemonica.bg