FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Forcepoint UEBA:

Решение поведенческой безопасности

Ferdinando Mancini
Director, Sales Engineering

Пётр Савич
ст. инженер-консультант

FORCEPOINT UEBA

поведенческий анализатор нового поколения

ЦЕЛОСТНЫЙ НАДЗОР ЗА СОТРУДНИКАМИ

Коммуникации

О чём они говорят?

С кем общаются?

Источники: Email, чат, голос

Система

Чем занимаются в сетях?

Какие системы используют?

Источники: SIEM, компьютер, веб-навигация, входы, публикация файлов

Кадровые службы

Какова их мотивация?

Откуда берутся дурные намерения?

Источники: собеседования по эффективности, Active Directory

Физический доступ

Каково физическое поведение?

Куда и когда они перемещаются?

Источники: СКД, поездки

ПОВЕДЕНЧЕСКАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЛЮДИ **СОБЫТИЯ**

СЦЕНАРИИ

“Пунктирные линии” между моделями событий/сущностей, измерение рисковых показателей

АНАЛИЗ СОБЫТИЙ : «Что они делают»

Обогащение событий интересующими характеристиками, скоринг по редкости, персональная или групповая нормализация

ЗАГРУЗКА и ОБОГАЩЕНИЕ СОБЫТИЙ
(потоковая или пакетная через API)

АНАЛИЗ СУЩНОСТЕЙ : «Кто они»

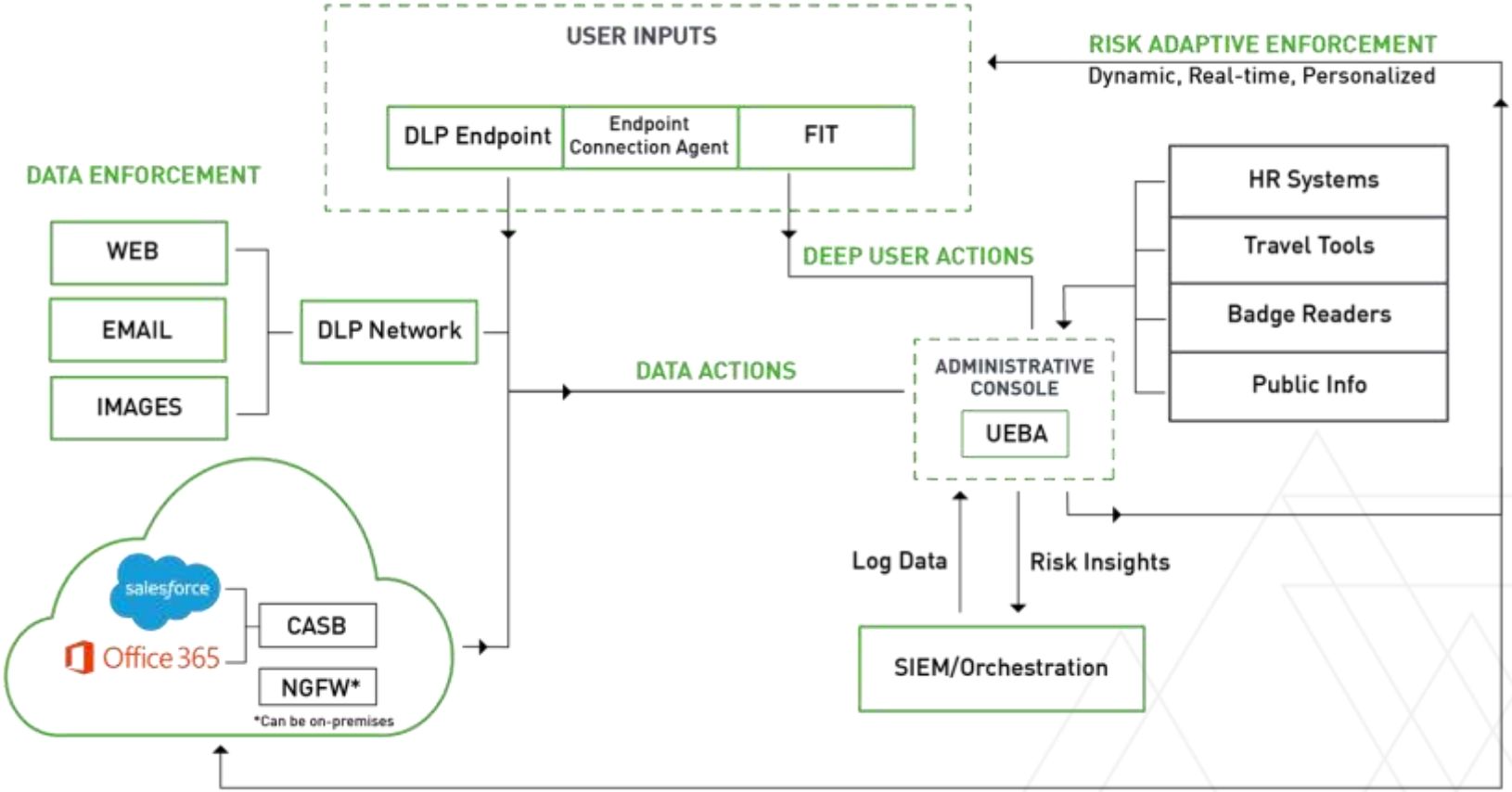
скоринг по статическим признакам сущностей

Характеристики **Атрибуты**

СБОР АТРИБУТОВ и ХАРАКТЕРИСТИК
(из Кадровых Служб, Active Directory, CMDB)

Что они делают ← **ПОНИМАНИЕ ИНСАЙДЕРОВ** → **Кем они являются**

РОЛЬ UEBA В ЛИНЕЙКЕ FORCEPOINT



ИСТОЧНИКИ ДАННЫХ И ИНТЕГРАЦИИ

SIEM

splunk> ArcSight IBM Radar RSA NetWitness

Коммуникации

Exchange SYMPHONY Bloomberg Skype for Business

Системные журналы

Windows Linux

DLP

FORCEPOINT Symantec DIGITAL GUARDIAN McAfee

Агенты на компьютере

FORCEPOINT DIGITAL GUARDIAN dtex

Информация

workday. salesforce Active Directory

Веб-шлюзы

BLUE COAT Symantec CISCO f5 FORCEPOINT

Перемещение данных

Print Logs, Removable Device Logs (Windows, Endpoint)

«КОРОБОЧНЫЕ» ПРИМЕНЕНИЯ

	Вынос данных	Кража паролей	Злонамеренный пользователь	Нежелательное поведение	Незаконное поведение
Модели	• Внутреннее перемещение данных • Внешнее перемещение данных • Файловые операции • Разведывание данных • Сокрытие от систем контроля • Кадровый риск	• Вредоносный код • Компрометированная аутентификация • Фишинг • Отклонение от базовой конфигурации • Вредоносные сайты и ресурсы	• Сетевая разведка • Системное администрирование • Вредоносная аутентификация • Исследование вредоносных действий • Отклонение от базовой конфигурации • Физический доступ • Запрос на привилегированный доступ • Кадровый риск	• Сексуальные домогательства • Насилие на рабочем месте • Непристойное содержимое • Уходящий сотрудник • Снижение продуктивности • Расслабленная работа • Финансовые трудности • Отрицательный настрой • Кадровый риск	• Конфликт интересов • Утечка информации • Корпоративный шпионаж • Доносительство • Уклонение от расследования • Кадровый риск
Источники данных	• Web Proxy • Windows • Linux • User Activity Monitoring • Email • Chat • Network Flow Logs • SharePoint • Web Server Logs • HR	• Web Proxy • Windows • Linux • User Activity Monitoring • Email • Chat • Network Flow Logs • VPN • Firewall • Anti-Virus • HR • Voice	• Web Proxy • Windows • Linux • User Activity Monitoring • Email • Chat • Network Flow Logs • VPN • Badge Data • Voice • HR	• Web Proxy • Email • Chat • Network Flow Logs • HR • Voice	• Web Proxy • Email • Chat • Firewall • HR • Voice • DLP

АРХИТЕКТУРА

Производительность

Мощность каждого уровня наращивается вертикально и/или горизонтально. Балансировка мощности на уровне UI, хранения и загрузки данных.

Требования

ОС: RedHat Enterprise или CentOS

Хранение: Master Data Service и Ingest (загрузка) требуют скоростного хранилища: от 5,000 IOPS

Развертывание

Appliance. Производительный сервер 1U или 2U (с твердотельными дисками)

Виртуализация: Развертывание на инфраструктуре виртуализации заказчика

Amazon AWS: Each node executes within its own instance in an Amazon AWS Virtual Private Cloud.

ПРОБЛЕМАТИКА SIEM: АНОМАЛИИ НЕИНФОРМАТИВНЫ

UEBA 1-го поколения:

- Надстройка для SIEM
- Аномалии в миллиардах событий

Результат

- Тысячи событий => Сотни аномалий
- Это был человек или машина?
- Что вообще с этим делать?
  - Аномалии – «наводка», но не «фактура»
  - Подробности и обстоятельства утеряны
  - Приходится искать правду в других продуктах и инструментах

“Продукт класса UEBA, который лишь "разбирает логи", может упустить важное, особенно на бесконтрольных устройствах пользователей… Внутренние собеседования, данные поездок, активность в соц. сетях и другая неструктурированная информация может быть весьма полезна при выявлении и оценке рискового поведения сотрудников.”

– Gartner, Декабрь 2016

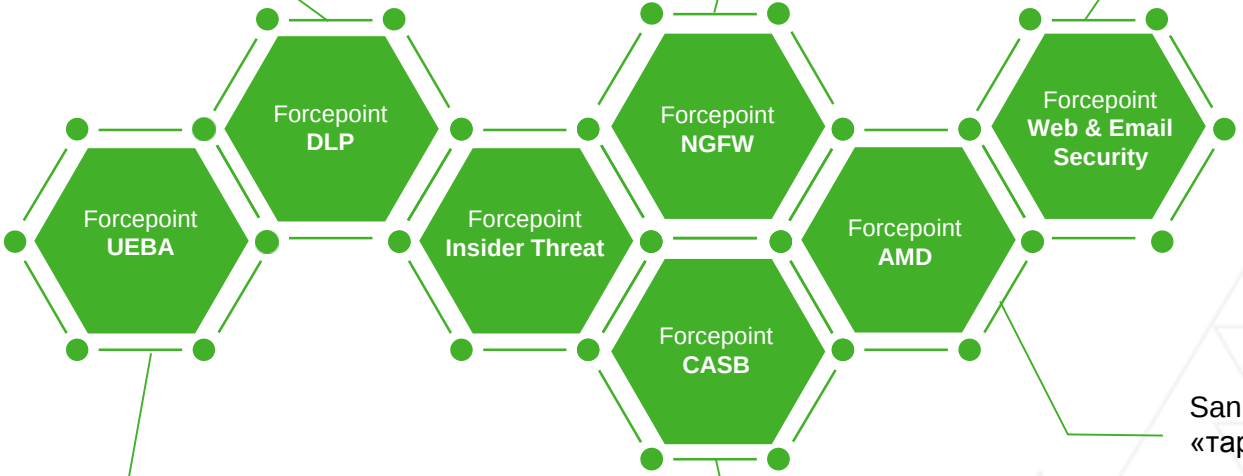
Демонстрация

ТЕХНОЛОГИЧЕСКИЕ ОТЛИЧИЯ FORCEPOINT UËBA

Охват	Разбор структурированных данных (атрибуты, метаданные, поля таблиц) и *неструктурированных данных (файлы, документы, контент, сообщения)*: не упустить ничего
Контекст	Акцент на поведении, не только аномалий, с чёткой индикацией и обоснованием нежелательности поведения. Анализ настроения и естественная языковая обработка
Гибкость	Лёгкость создания и подстройки рисковых моделей под конкретные нужды предприятия, любые практические применения
Эффективность	Тщательный и всесторонний анализ на единой платформе с быстрым переходом от «сигнала» к расследованию «фактуры»

ВАЖНО: не загружает обновления из Интернета, можно изолировать

НАВИГАТОР ПО ПРОДУКТАМ FORCEPOINT



Stonesoft. Никогда не ломается (почти)

Промышленная DLP

Шлюзы Web/Email

Sanbox, защита от
«таргетированных» атак

Поведенческий анализ.
Надстройка над SIEM и
всеми остальными

Защитный брокер для Office365, SAP и др.
DLP для мобильных устройств

Спасибо

