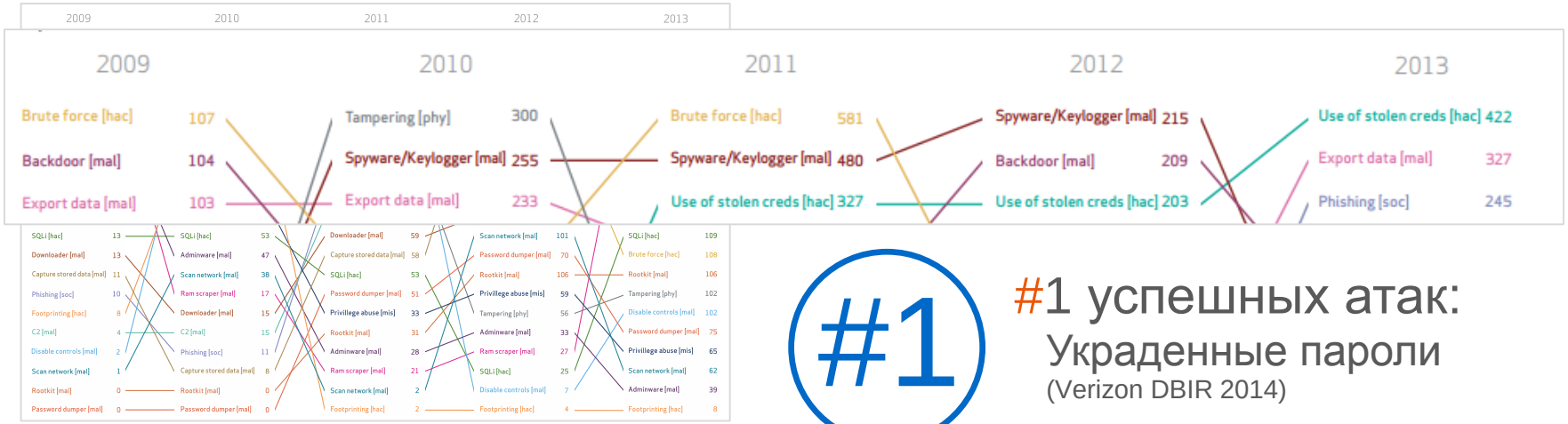
RAPID7

USERINSIGHT

Эффективное обнаружение и расследование атак на пользователей

Softprom by ERC | rapid7@softprom.com | www.softprom.com

Атаки на пользователей: Векторы атак



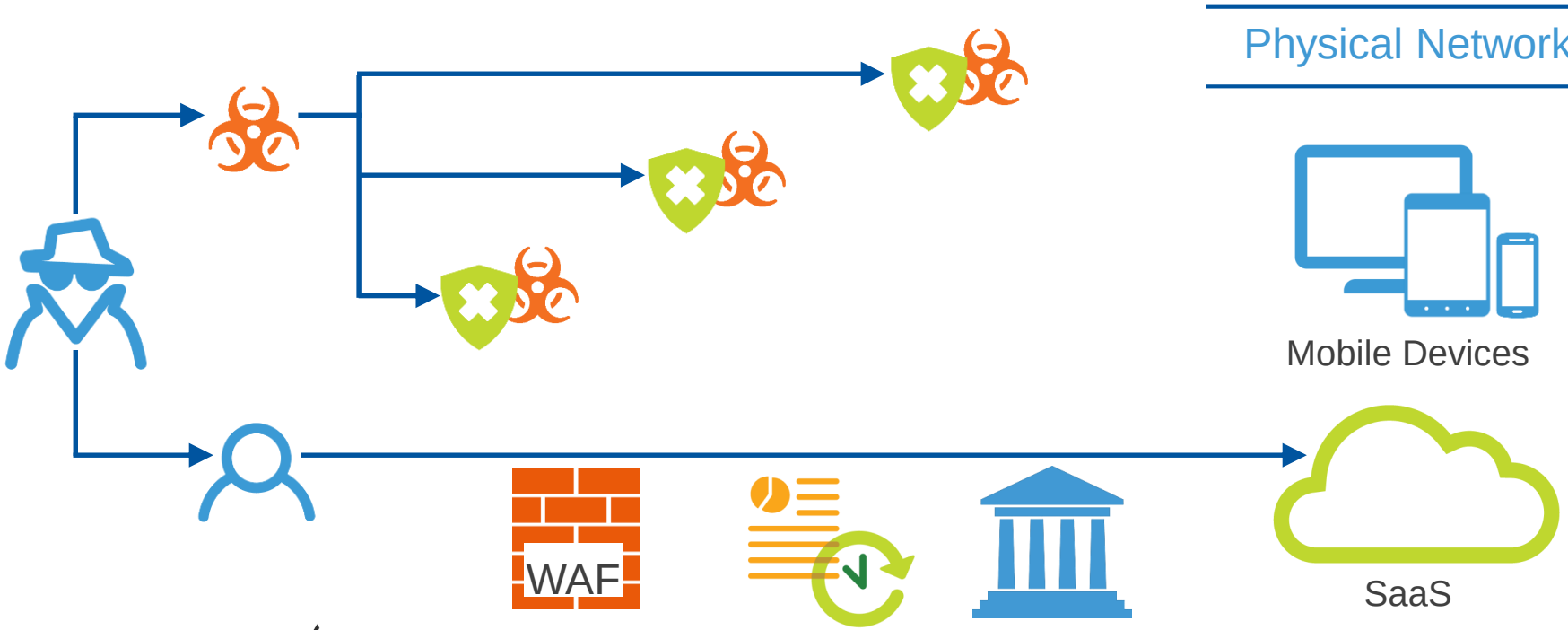
#1

#1 успешных атак:
Украденные пароли
(Verizon DBIR 2014)

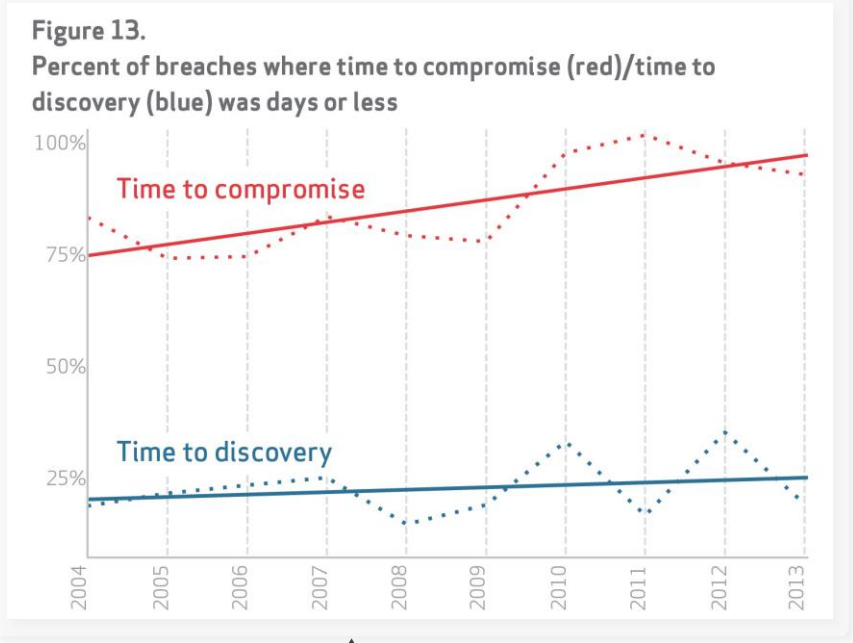
“Пользователи остаются самым слабым звеном в защите”

Gartner 2013

Современные технологии защиты не контролируют ключевой вектор атак



Атакующие проникают в сеть быстрее чем их обнаружают…



- 2014 Data Breach Report, Verizon

"«Плохие парни» редко должны уложится в дни чтобы сделать их работу, в то время когда «Хорошим парням» удается справиться за недели или месяцы."

- 2014 Data Breach Report, Verizon

Обнаружение и расследование атак на пользователей

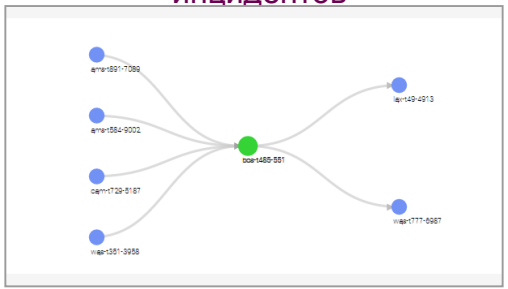
Обнаружение

Эффективное обнаружение атак

- Обнаружает действия злоумышленуика и его продвижение по сети
- Обнаружение без трудозатрат! Нет необходимости в создании и поддержке правил срабатывания.

Расследование

Быстрое расследование инцидентов



- Быстрое расследование инцидентов.
- Определение ВСЕХ участников инцидента
- Корреляция инцидентов со всеми связанными событиями.

Контроль

Простая оценка рисков

- Анализ использования пользователями локальных и облачных сервисов
- Отслеживание всей активности администраторов.
- Поведенческий анализ пользователей в корпоративных облачных сервисах.

userinsight

ОБНАРУЖЕНИЕ

Атака на пользователей “Kill Chain”: Наиболее часто используемая методика доступа и продвижения по сети.

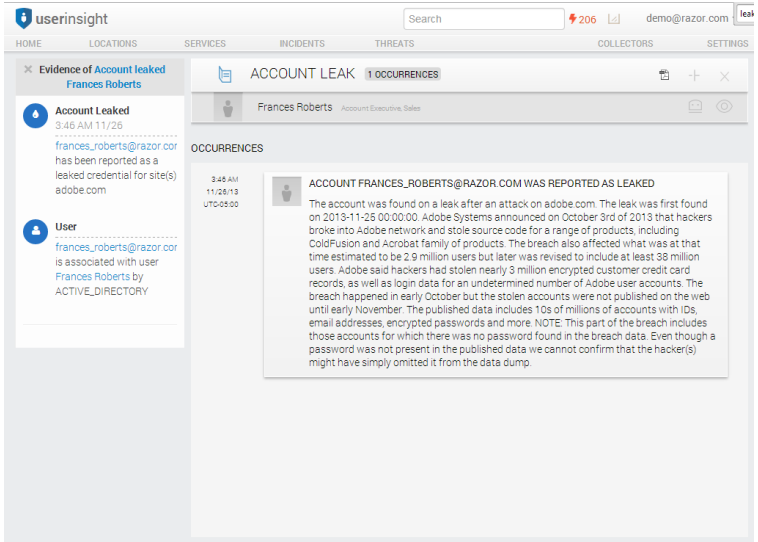
RAPID7 | SOFTPROM ERC

UserInsight: Встроенное обнаружение признаков компрометации

RAPID7 | SOFTPROM ERC

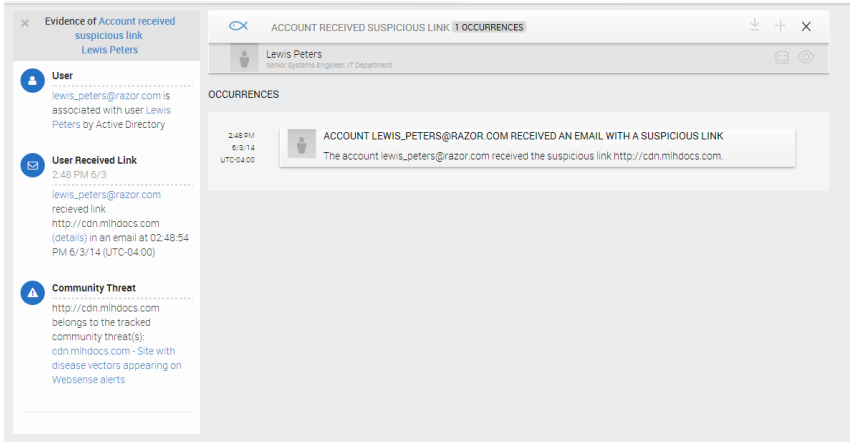
Обнаружение скомпрометированных аккаунтов

- Украденные аккаунты – самая частая точка входа для хакера
- Легкий способ украсть аккаунт – использовать данные утекшие с других сервисов (таких как eBay, Adobe, Linkedin и др.)
- UserInsight обнаружает скомпроментированные аккаунты в крупных утечках

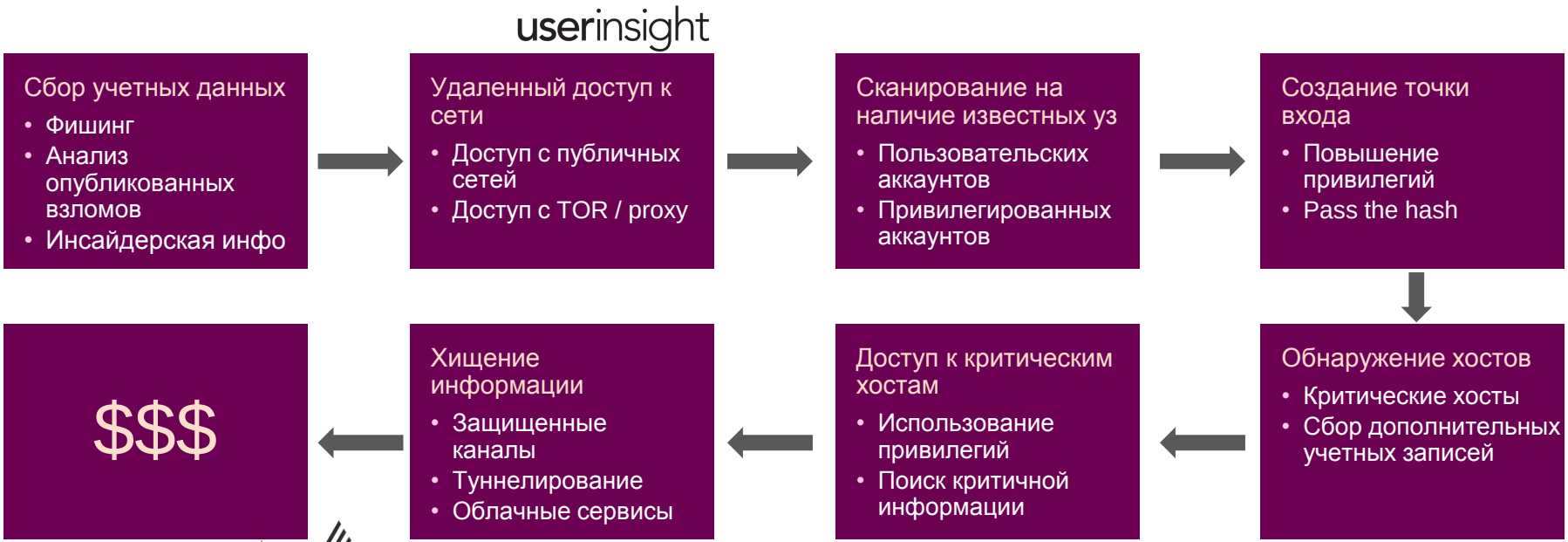


Обнаружение попыток фишинга

- Фишинг: 3я по популярности методология атак (Verizon DBIR 2014)
- UserInsight уведомляет в случае получения пользователями подозрительных ссылок.
- Позволяет выявлять схожие случаи фишинга/направленных фишинговых атак



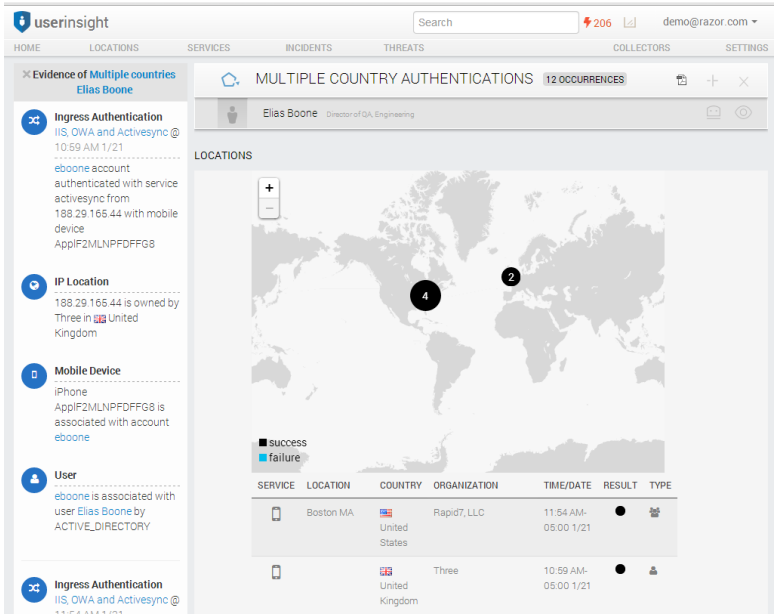
UserInsight: Встроенное обнаружение признаков компрометации



RAPID7 | SOFTPROM ERC

Обнаружение доступа злоумышленника к сети.

- UserInsight определяет географические данные подключившегося к VPN или облачному сервису устройства
- UserInsight Уведомляет в случае использования TOR/Proxy

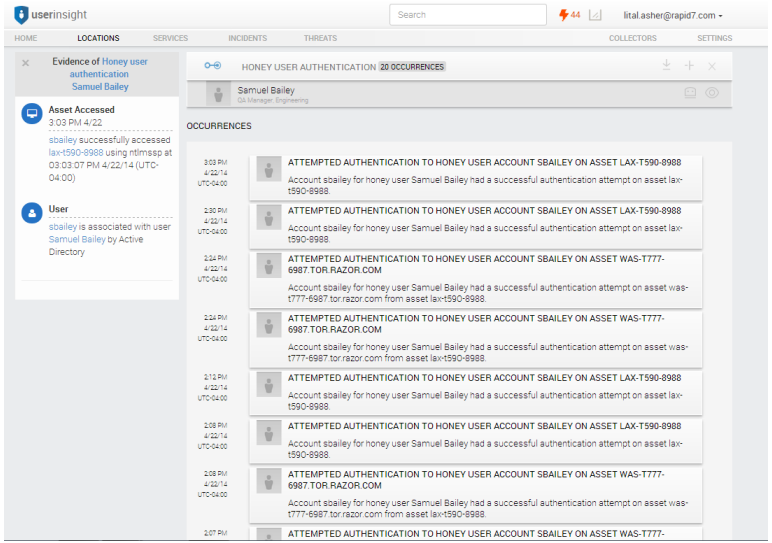


UserInsight: Встроенное обнаружение признаков компрометации

RAPID7 | SOFTPROM ERC

Определяет попытки злоумышленника собрать дополнительные учетные данные

- Дополнительные аккаунты позволяют злоумышленнику получить доступ к чувствительным данным и системам
- UserInsight определяет попытки злоумышленника получить новые доступы и привилегии:
  - Определяет сканирование LDAP (с помощью honey user)
  - Определяет повышение привилегий
  - Контролирует добавление новых администраторов
  - Определяет разблокировку ранее заблокированных аккаунтов
  - Определяет нецелевое использование сервисных аккаунтов

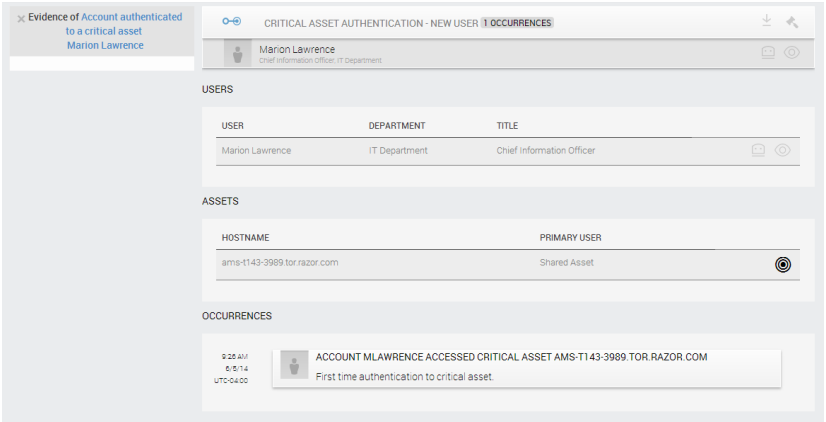


UserInsight: Встроенное обнаружение признаков компрометации

RAPID7 | SOFTPROM ERC

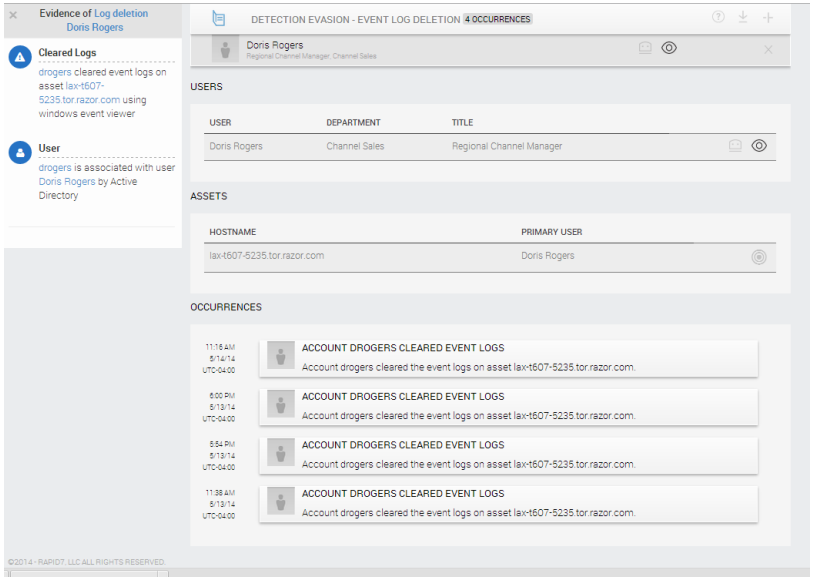
Detect Attacker’s Access Critical Assets

- UserInsight уведомляет в случае подключения нового пользователя или устройства к критическим хостам.



Определяет попытки спрятать активность

- Часто злоумышленники, в случае успеха очищают за собой логи, чтобы скрыть свою активность
- UserInsight определяет и сигнализирует о подобной активности

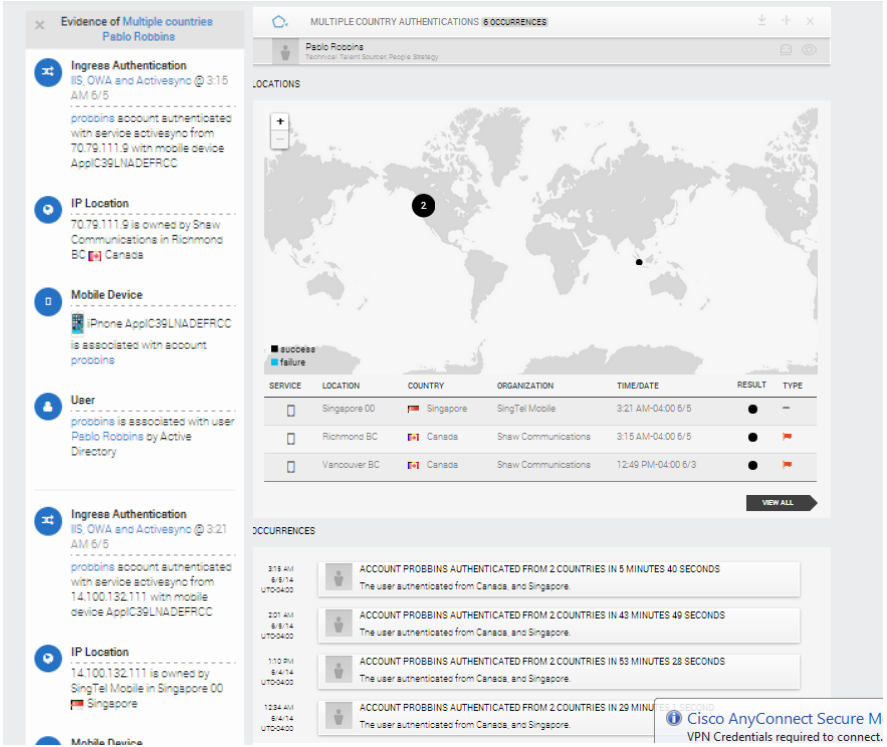


userinsight

РАССЛЕДОВАНИЕ

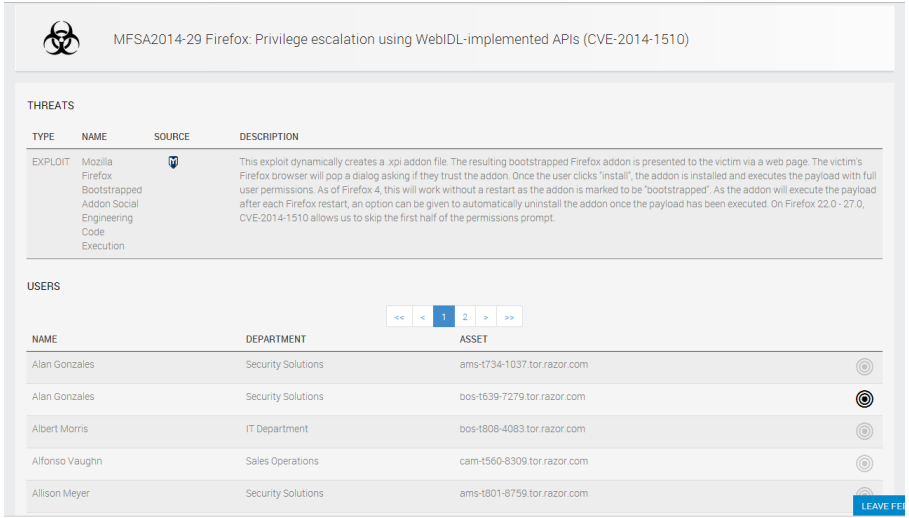
Легкое принятие решений

- Сбор доказательств по каждому инциденту
- Низкий уровень ложных срабатываний
- Автоматический поиск событий



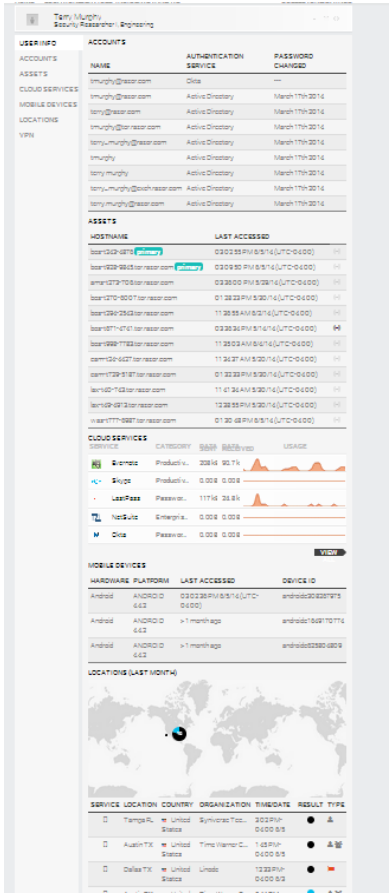
Автоматическое сопоставление данных о угрозах пользователях и хостах

- Сбор информации о уязвимостях хостов (с помощью Nexpose)



Контроль всех активностей пользователей

- Видимость всей релевантной информации о пользовательской активности – используемые хосты, корпоративные сервисы, устройства, облачные сервисы, геолокация и др.

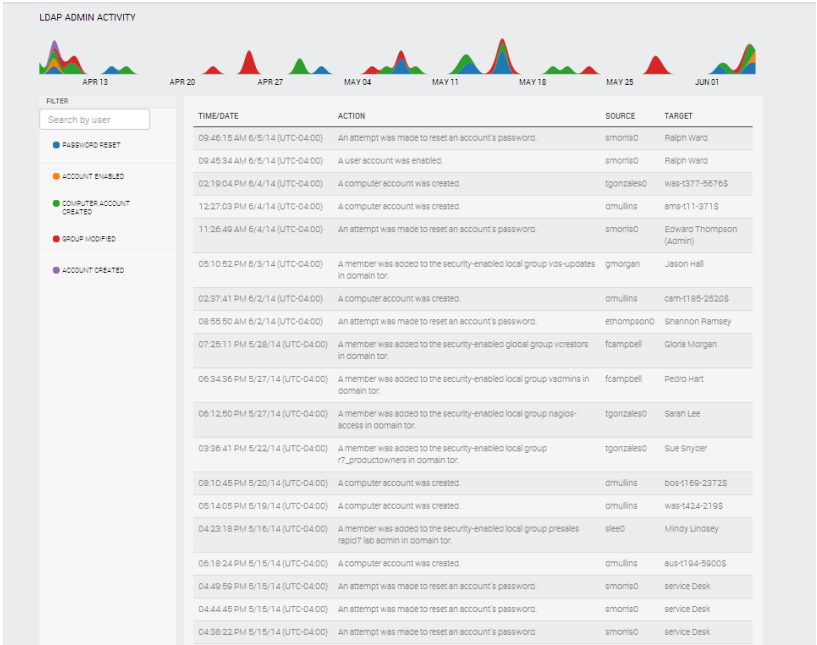


userinsight

КОНТРОЛЬ РИСКОВ

Контроль всех активностей администраторов

- 88% инцидентов с разглашением информации инсайдером совершились благодаря злоупотреблением привилегий (Verizon DBIR)
- Контролируйте поведение критических аккаунтов для выявления атак.
- Реагируйте на подозрительные действия администраторов

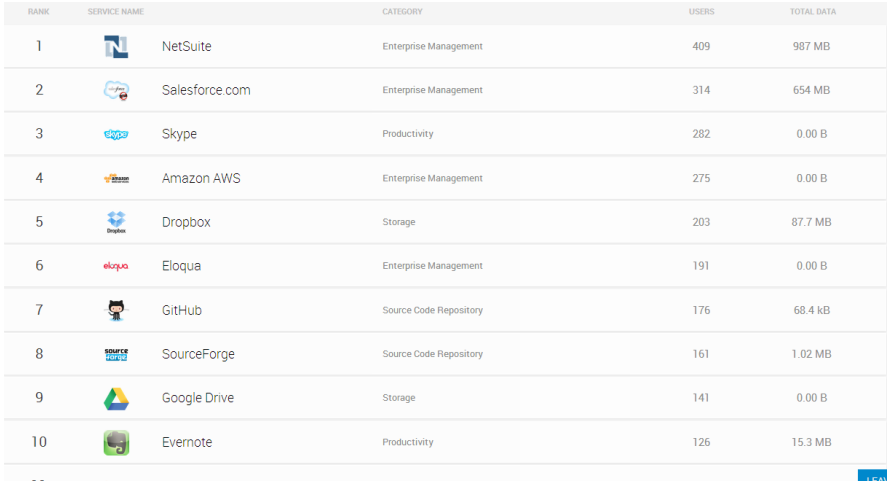


Контроль локаций подключения

- Обзор успешных/ неуспешных аутентификаций к VPN / owa / Activesync / cloud services и др.
- Контроль подключений из неизвестных и/или необычных местоположений

Узнайте какими облачными севисами пользуются ваши сотрудники

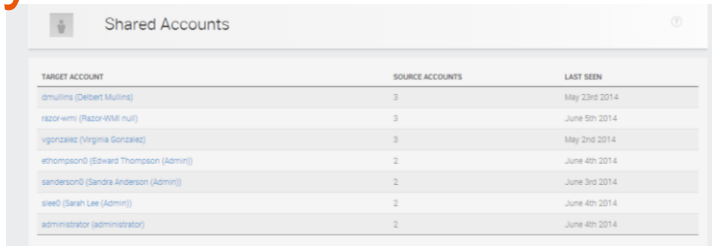
- Как и когда был использован облачный сервис
- Тесная интеграция с AWS, salesforce.com, Google Apps, box.com and Okta, выявляет компроментацию аккаунтов

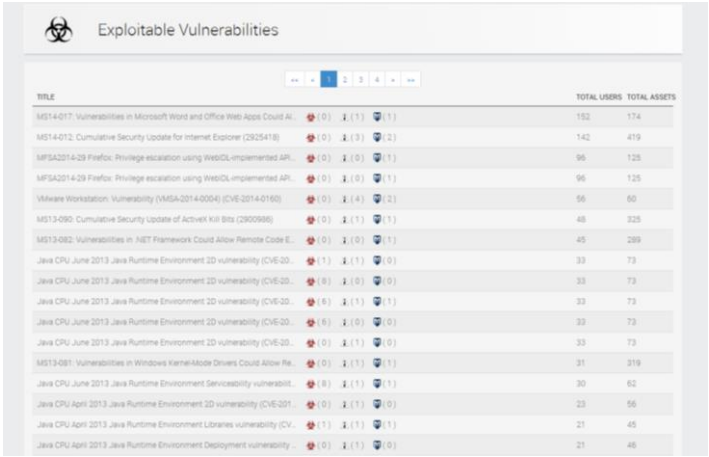


RANK	SERVICE NAME	CATEGORY	USERS	TOTAL DATA
1	NetSuite	Enterprise Management	409	987 MB
2	Salesforce.com	Enterprise Management	314	654 MB
3	Skype	Productivity	282	0.00 B
4	Amazon AWS	Enterprise Management	275	0.00 B
5	Dropbox	Storage	203	87.7 MB
6	Eloqua	Enterprise Management	191	0.00 B
7	GitHub	Source Code Repository	176	68.4 kB
8	SourceForge	Source Code Repository	161	1.02 MB
9	Google Drive	Storage	141	0.00 B
10	Evernote	Productivity	126	15.3 MB

Выявляйте нарушения политик, злоупотребление правами, уязвимости

- Аккаунты с неистекающими паролями
- Общие или связанные аккаунты
- Избыточные привилегии





userinsight

Расследование

Быстрое расследование инцидентов

Контроль

Простая оценка рисков

Обнаружение

Эффективное обнаружение атак

RAPID7 | SOFTPROM ERC

BACKUP SLIDES

Почему UserInsight лучшеSIEM?

Почему UserInsight может заменить SIEM?

- Обнаружение атак и расследование инцидентов «из коробки»
- Поведенческий анализ «из коробки»
- Уведомления о злоупотреблениях и нарушениях политик «из коробки»

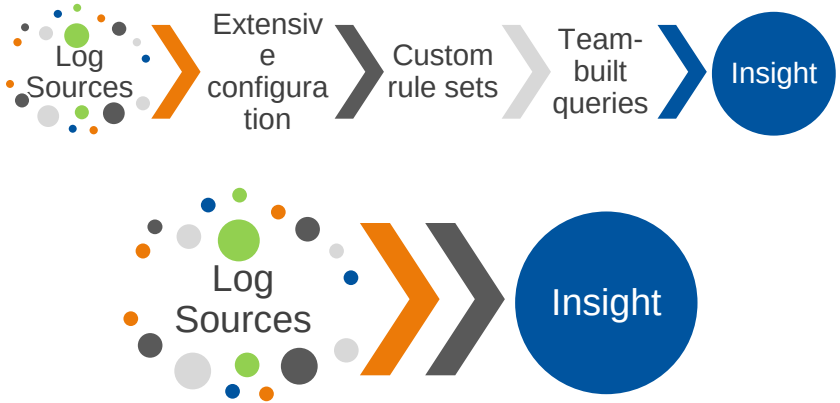
«Мы отдел ИБ состоящей из 2х человек. Раньше мы использовали локальную SIEM, но сейчас мы отказались от этого решения, так как для нас важно максимально использовать ресурсы для обеспечения безопасности и мы не можем выделить отдельного человека для контроля и настройки SIEM для получения релевантных данных”

Marketing company

RAPID7 | SOFTPROM ERC

Почему UserInsight нужен компаниям у которых уже есть SIEM?

- Увеличение эффективности: снижает необходимость написания правил корреляции в SIEM
- Видит события, которые недоступны SIEM: продвижение злоумышленника, использование аккаунтов неавторизованными людьми, и др.
- Сокращает время на расследование инцидентов: откуда началась атака, как злоумышленник пытался проникнуть в сеть, какие аккаунты пострадали от действий злоумышленника.

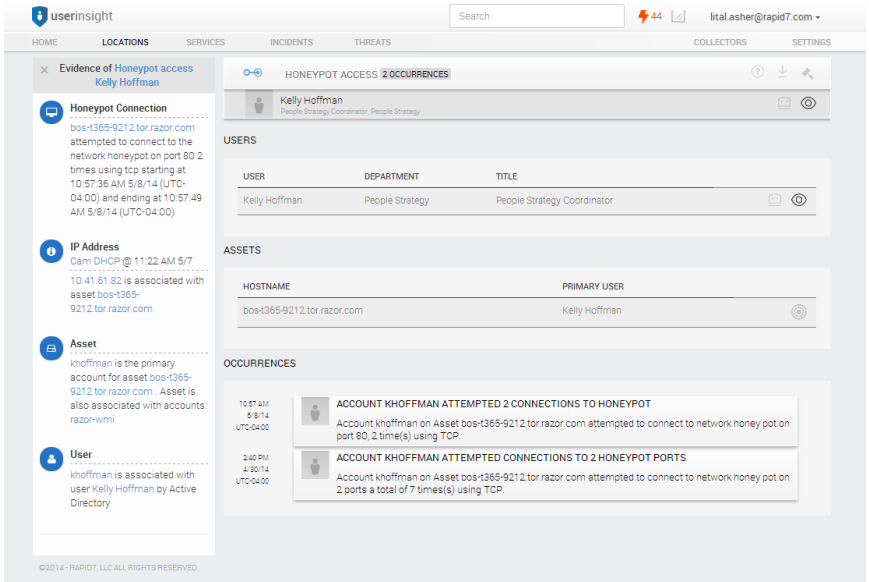


"Мы используем LogRhythm, но не при работе очень трудно получить контекст получаемых данных. UserInsight выявляет события, которые мы не смогли выявить с помощью корреляции в SIEM."

Non-profit association

Обнаружает сканирование сетей злоумышленником для поиска хостов

- Коллектор honeypot, в UserInsight обнаружает сканирование хостов, чтобы вовремя пресечь действия злоумышленников и не дать им обнаружить критические хосты.



RAPID7 | SOFTPROM ERC

Обнаружение атак и расследование инцидентов занимает слишком много времени!

Обнаружение 85% атак занимает недели, 13% атак обнаружается спустя месяцы

Verizon DBIR 2014

86% специалистов по безопасности считают расследование инцидентов слишком длятельным

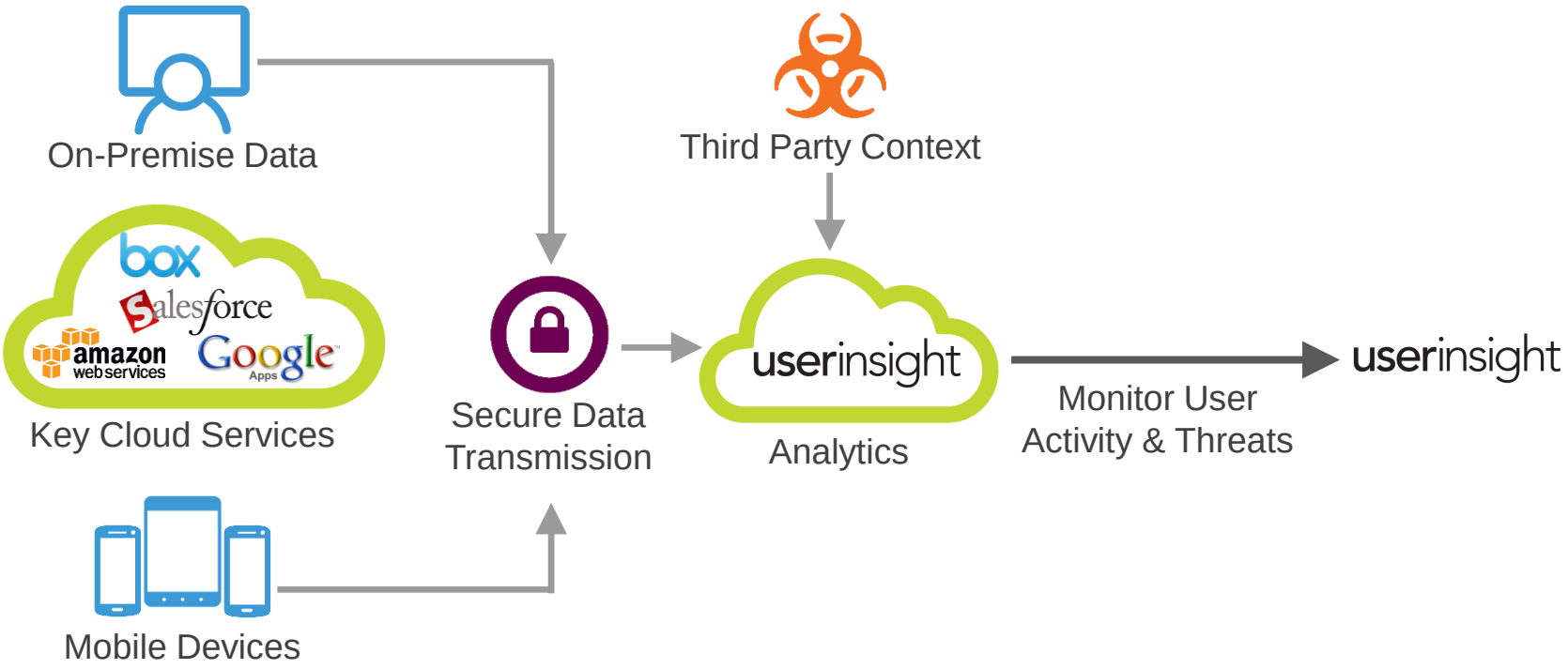
Ponemon Institute LLC, 2014

76% специалистов по безопасности считают что для более эффективного расследования решениям не хватает интеграции между собой.

Ponemon Institute LLC, 2014

RAPID7 | SOFTPROM ERC

UserInsight – Sources of Data



UserInsight – как это работает

THANK YOU

Softprom by ERC – официальный дистрибьютор компании Rapid7 на территории стран СНГ.

Rapid7@softprom.com | www.softprom.com