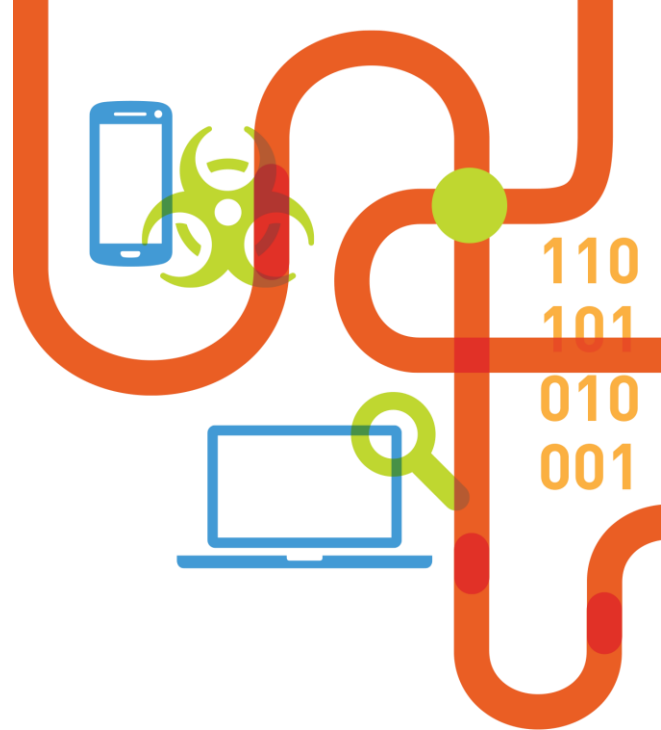




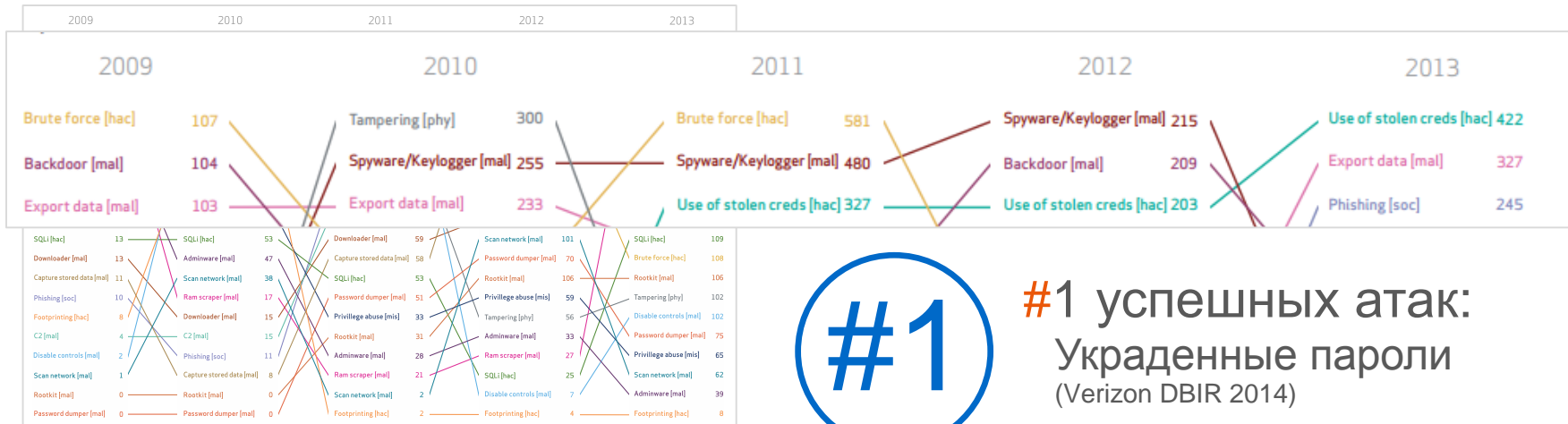
# USERINSIGHT

Эффективное обнаружение и расследование атак на пользователей

Softprom by ERC | [rapid7@softprom.com](mailto:rapid7@softprom.com) | [www.softprom.com](http://www.softprom.com)



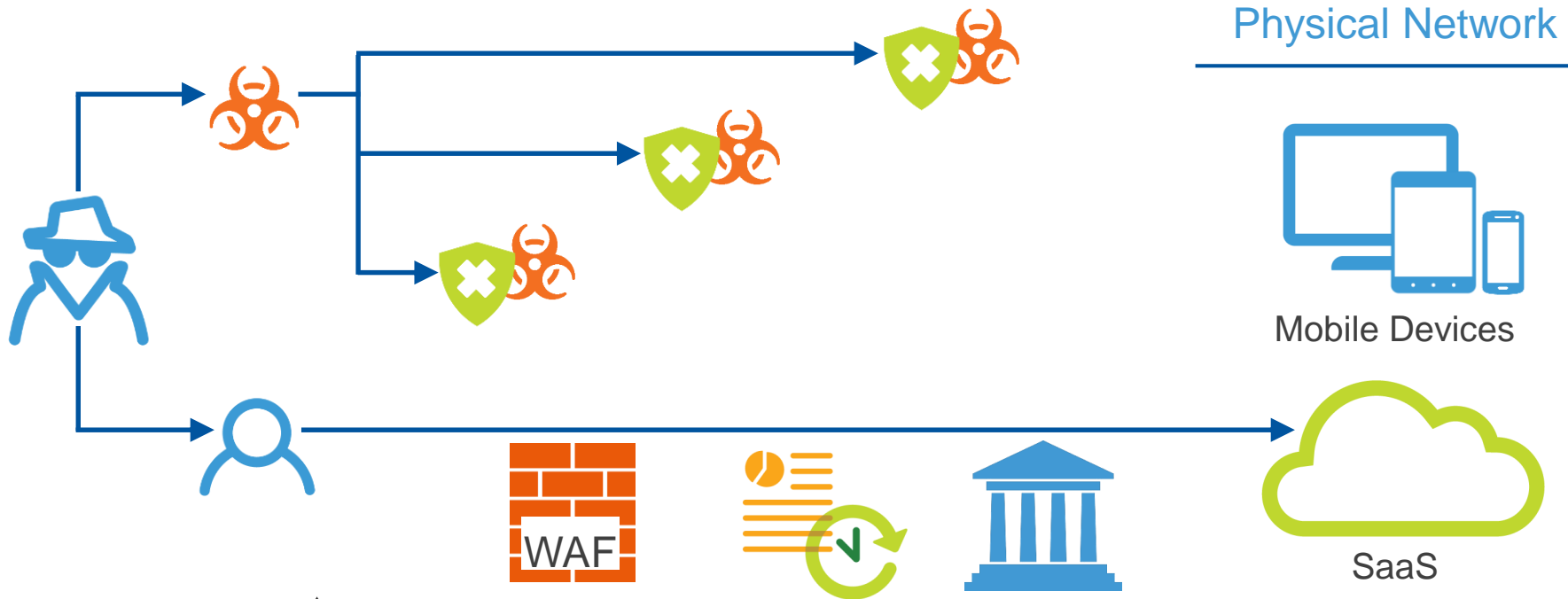
# Атаки на пользователей: Векторы атак



## “Пользователи остаются самым слабым звеном в защите”

Gartner 2013

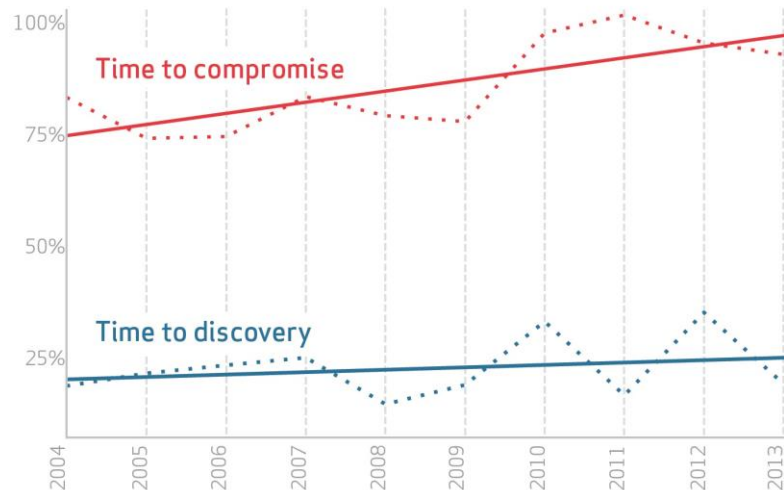
# Современные технологии защиты не контролируют ключевой вектор атак



# Атакующие проникают в сеть быстрее чем их обнаруживают...

Figure 13.

Percent of breaches where time to compromise (red)/time to discovery (blue) was days or less



“«Плохие парни» редко должны уложиться 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

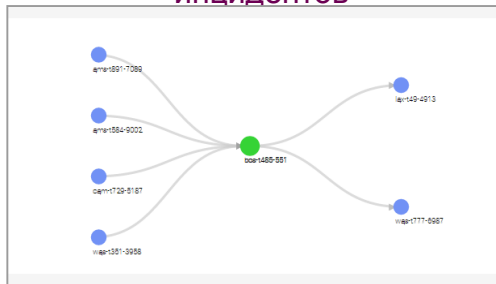
Эффективное обнаружение атак



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

## Расследование

Быстрое расследование инцидентов



- Быстрое расследование инцидентов.
- Определение VCEX 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.



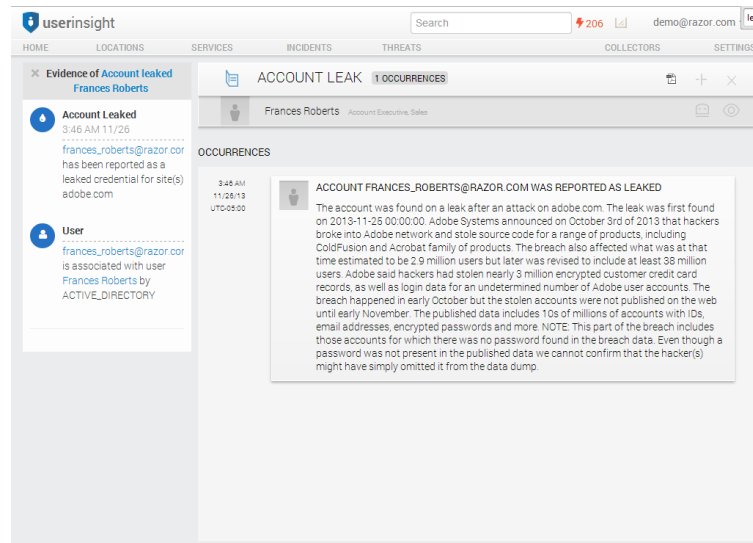
# UserInsight: Встроенное обнаружение признаков компрометации





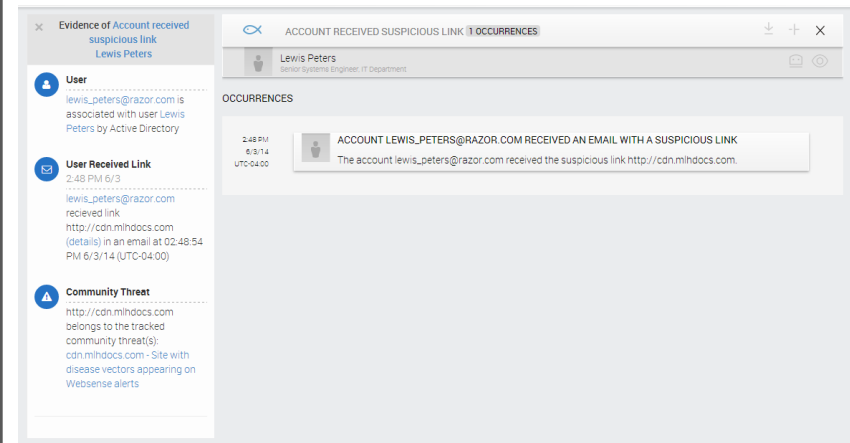
# Обнаружение скомпрометированных аккаунтов

- 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 обнаруживает скомпрометированные аккаунты в крупных утечках



# Обнаружение попыток фишинга

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



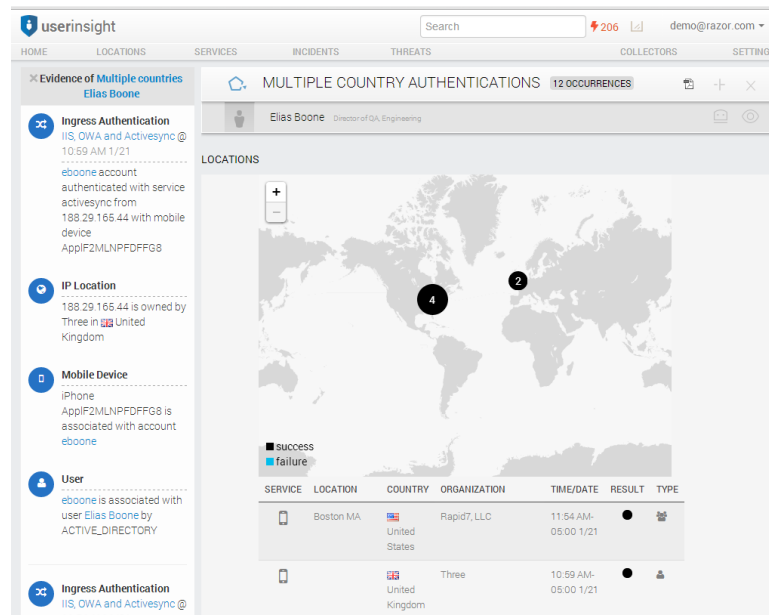
# UserInsight: Встроенное обнаружение признаков компрометации

userinsight

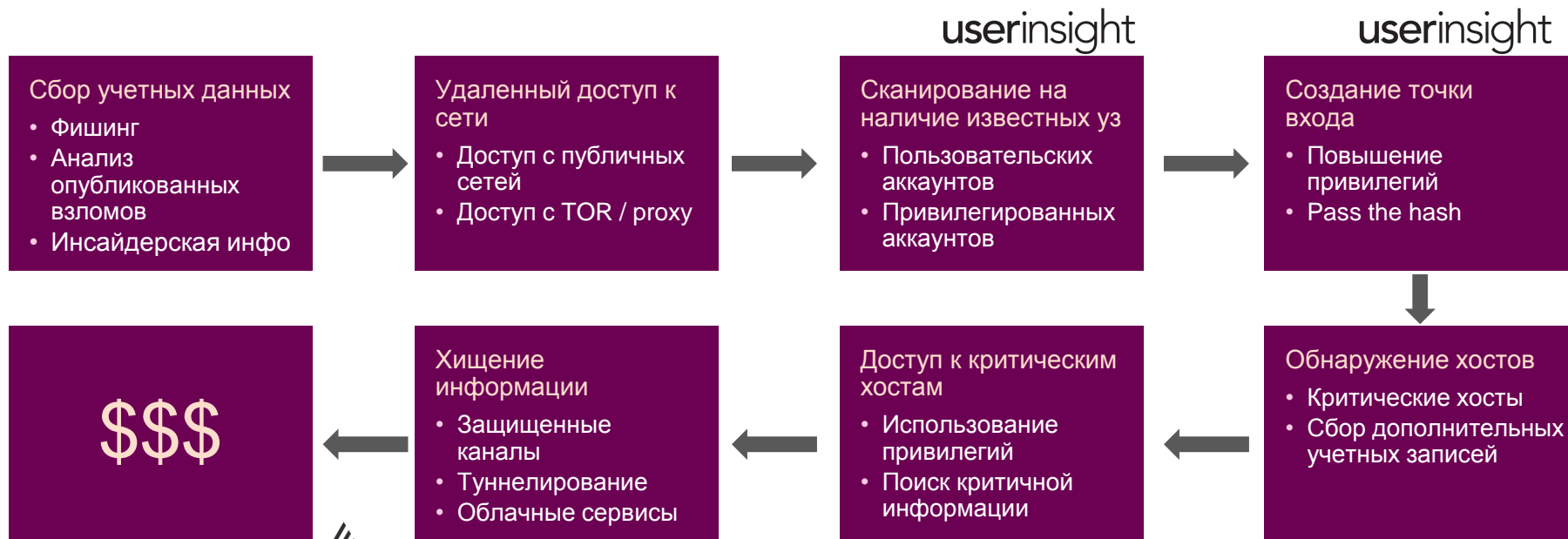


# Обнаружение доступа злоумышленника к сети.

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



# UserInsight: Встроенное обнаружение признаков компрометации



# 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

The screenshot displays the UserInsight web application interface. The top navigation bar includes 'HOME', 'LOCATIONS', 'SERVICES', 'INCIDENTS', 'THREATS', 'COLLECTORS', and 'SETTINGS'. A search bar and a user profile 'lital.asher@rapid7.com' are also visible. The main content area is titled 'Evidence of Honey user authentication Samuel Bailey'. It shows two sections: 'Asset Accessed' and 'User'. The 'Asset Accessed' section indicates that 'sbailey successfully accessed lax-t590-8988 using ntmspp at 03:03:07 PM 4/22/14 (UTC-04:00)'. The 'User' section shows 'sbailey is associated with user Samuel Bailey by Active Directory'. Below these sections, a table lists 'OCCURRENCES' of 'HONEY USER AUTHENTICATION' for 'Samuel Bailey'. The table has columns for 'Time', 'Event', and 'Details'. The events listed are 'ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET LAX-T590-8988' and 'ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET WAS-1777-6987.TOR.RAZOR.COM'. The details for each event state: 'Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset lax-t590-8988' or 'Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset was-1777-6987.tor.razor.com from asset lax-t590-8988'.

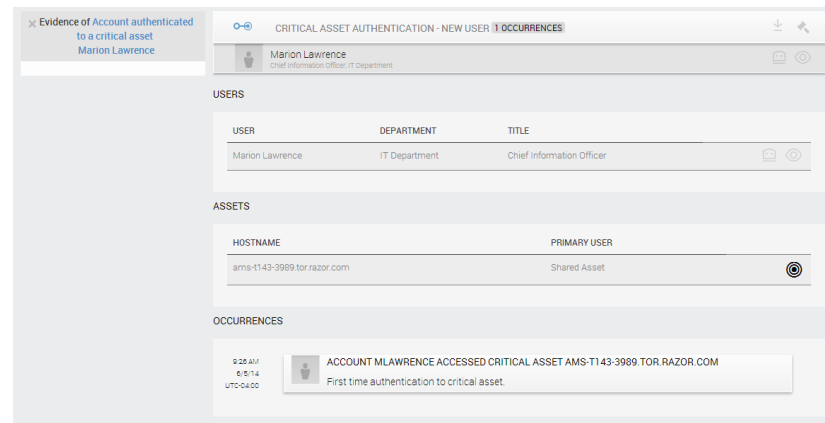
Time	Event	Details
3:03 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET LAX-T590-8988	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset lax-t590-8988
3:30 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET LAX-T590-8988	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset lax-t590-8988
3:34 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET WAS-1777-6987.TOR.RAZOR.COM	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset was-1777-6987.tor.razor.com from asset lax-t590-8988
3:34 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET WAS-1777-6987.TOR.RAZOR.COM	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset was-1777-6987.tor.razor.com from asset lax-t590-8988
3:12 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET LAX-T590-8988	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset lax-t590-8988
3:08 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET LAX-T590-8988	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset lax-t590-8988
3:08 PM 4/22/14 UTC-04:00	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET WAS-1777-6987.TOR.RAZOR.COM	Account sbailey for honey user Samuel Bailey had a successful authentication attempt on asset was-1777-6987.tor.razor.com from asset lax-t590-8988
3:07 PM	ATTEMPTED AUTHENTICATION TO HONEY USER ACCOUNT SBAILEY ON ASSET WAS-1777-	

# UserInsight: Встроенное обнаружение признаков компрометации



# 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

The screenshot displays the UserInsight interface with a sidebar on the left and a main content area on the right. The sidebar shows a search bar and a list of items under 'Evidence of Log deletion' for 'Doris Rogers', including 'Cleared Logs' and 'User'. The main content area is titled 'DETECTION EVASION - EVENT LOG DELETION / 4 OCCURRENCES' and shows details for 'Doris Rogers' (Regional Channel Manager, Channel Sales). It includes sections for 'USERS', 'ASSETS', and 'OCCURRENCES'. The 'OCCURRENCES' section lists four events where 'ACCOUNT DROGERS CLEARED EVENT LOGS' on the asset 'laxt607-5235.tor.razor.com'.

USER	DEPARTMENT	TITLE
Doris Rogers	Channel Sales	Regional Channel Manager

HOSTNAME	PRIMARY USER
laxt607-5235.tor.razor.com	Doris Rogers

TIME	EVENT
11:16 AM 5/14/14 UTC-04:00	ACCOUNT DROGERS CLEARED EVENT LOGS Account drogers cleared the event logs on asset laxt607-5235.tor.razor.com.
6:00 PM 5/13/14 UTC-04:00	ACCOUNT DROGERS CLEARED EVENT LOGS Account drogers cleared the event logs on asset laxt607-5235.tor.razor.com.
5:54 PM 5/13/14 UTC-04:00	ACCOUNT DROGERS CLEARED EVENT LOGS Account drogers cleared the event logs on asset laxt607-5235.tor.razor.com.
11:38 AM 5/13/14 UTC-04:00	ACCOUNT DROGERS CLEARED EVENT LOGS Account drogers cleared the event logs on asset laxt607-5235.tor.razor.com.

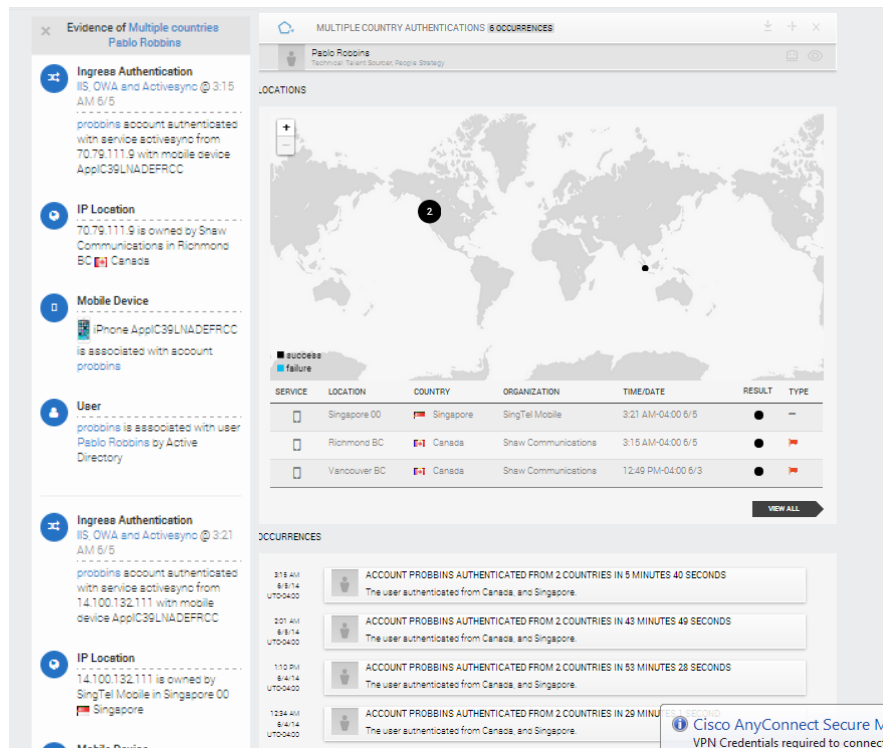
©2014 - RAPID7, LLC ALL RIGHTS RESERVED.

userinsight

РАССЛЕДОВАНИЕ


# Легкое принятие решений

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




# Автоматическое сопоставление данных о угрозах пользователям и хостах

- Сбор информации о уязвимостях хостов (с помощью Nexpose)






 MFSA2014-29 Firefox: Privilege escalation using WebIDL-implemented APIs (CVE-2014-1510)

THREATS

TYPE	NAME	SOURCE	DESCRIPTION
EXPLOIT	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution		This exploit dynamically creates a xpi addon file. The resulting bootstrapped Firefox addon is presented to the victim via a web page. The victim's Firefox browser will pop a dialog asking if they trust the addon. Once the user clicks "install", the addon is installed and executes the payload with full user permissions. As of Firefox 4, this will work without a restart as the addon is marked to be "bootstrapped". As the addon will execute the payload after each Firefox restart, an option can be given to automatically uninstall the addon once the payload has been executed. On Firefox 22.0 - 27.0, CVE-2014-1510 allows us to skip the first half of the permissions prompt.

USERS

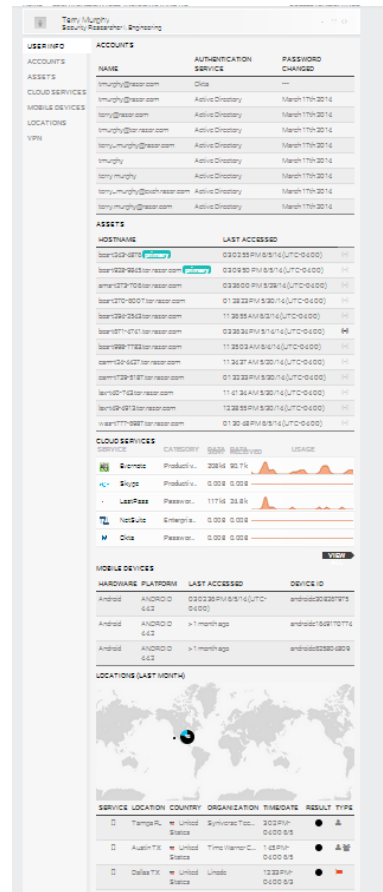
<< < 1 2 > >>

NAME	DEPARTMENT	ASSET
Alan Gonzales	Security Solutions	ams-4734-1037.tor.razor.com 
Alan Gonzales	Security Solutions	bos-1639-7279.tor.razor.com 
Albert Morris	IT Department	bos-1808-4083.tor.razor.com 
Alfonso Vaughn	Sales Operations	cam-1560-8309.tor.razor.com 
Allison Meyer	Security Solutions	ams-1801-8759.tor.razor.com 

LEAVE FEED

# Контроль всех активностей пользователей

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



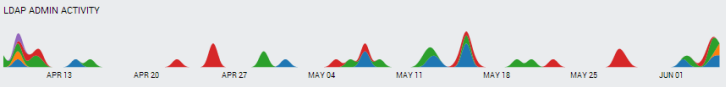
userinsight

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

LDAP ADMIN ACTIVITY

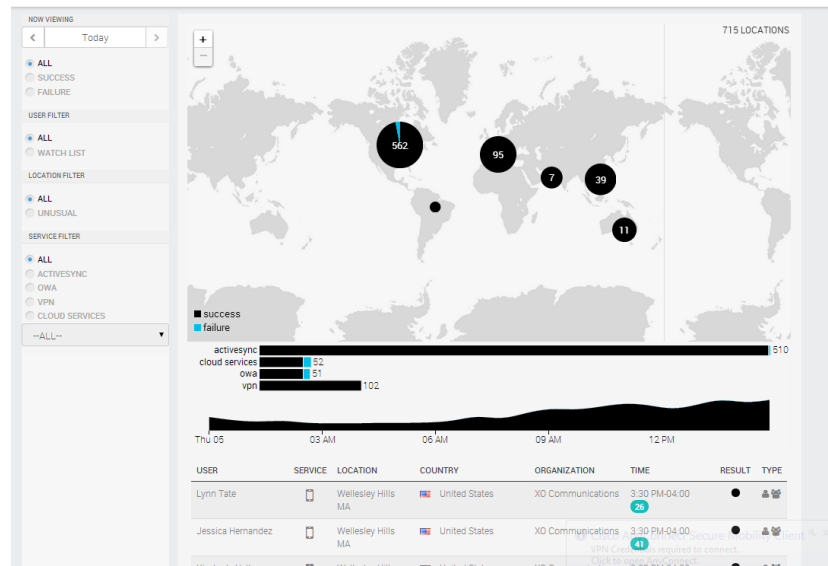


The dashboard features a timeline from April 13 to June 01 with colored peaks indicating activity levels. A filter section on the left allows searching by user and selecting event types: Password Reset (blue), Account Enabled (orange), Computer Account Created (green), Group Modified (red), and Account Created (purple).

TIME/DATE	ACTION	SOURCE	TARGET
09:46:16 AM 6/5/14 (UTC-04:00)	An attempt was made to reset an account's password.	smorris0	Ralph Ward
09:45:34 AM 6/5/14 (UTC-04:00)	A user account was enabled.	smorris0	Ralph Ward
02:19:04 PM 6/4/14 (UTC-04:00)	A computer account was created.	tgonzales0	was-1377-56765
12:27:03 PM 6/4/14 (UTC-04:00)	A computer account was created.	omullins	ams-111-9715
11:26:49 AM 6/4/14 (UTC-04:00)	An attempt was made to reset an account's password.	smorris0	Edward Thompson (Admin)
05:10:52 PM 6/3/14 (UTC-04:00)	A member was added to the security-enabled local group vds-updates in domain tor.	gmorgan	Jason Hall
02:37:41 PM 6/2/14 (UTC-04:00)	A computer account was created.	omullins	cam-1185-25205
08:55:50 AM 6/2/14 (UTC-04:00)	An attempt was made to reset an account's password.	ethompson0	Shannon Ramsey
07:25:11 PM 6/2/14 (UTC-04:00)	A member was added to the security-enabled global group vcreators in domain tor.	fcampbell	Gloria Morgan
06:34:36 PM 5/27/14 (UTC-04:00)	A member was added to the security-enabled local group vdomina in domain tor.	fcampbell	Pedro Hart
06:12:50 PM 5/27/14 (UTC-04:00)	A member was added to the security-enabled local group nagios-access in domain tor.	tgonzales0	Sarah Lee
03:36:41 PM 5/22/14 (UTC-04:00)	A member was added to the security-enabled local group r7_productowners in domain tor.	tgonzales0	Sue Snyder
08:10:45 PM 5/20/14 (UTC-04:00)	A computer account was created.	omullins	bois-1169-23725
05:14:05 PM 5/19/14 (UTC-04:00)	A computer account was created.	omullins	was-1424-2193
04:23:18 PM 5/16/14 (UTC-04:00)	A member was added to the security-enabled local group presales rapid7 lab admin in domain tor.	slee0	Mindy Linosley
06:18:24 PM 5/15/14 (UTC-04:00)	A computer account was created.	omullins	aus-1194-59005
04:49:59 PM 5/15/14 (UTC-04:00)	An attempt was made to reset an account's password.	smorris0	Service Desk
04:44:45 PM 5/15/14 (UTC-04:00)	An attempt was made to reset an account's password.	smorris0	Service Desk
04:38:22 PM 5/15/14 (UTC-04:00)	An attempt was made to reset an account's password.	smorris0	Service Desk

# 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 сервисами 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

Shared Accounts		
TARGET ACCOUNT	SOURCE ACCOUNTS	LAST SEEN
dmulins (Debert Mullins)	3	May 23rd 2014
razor-wm (Razor-WM nut)	3	June 9th 2014
vgonzales (Virginia Gonzalez)	3	May 2nd 2014
ethompson0 (Edward Thompson (Admin))	2	June 4th 2014
sanders0 (Sandra Anderson (Admin))	2	June 3rd 2014
slee0 (Sarah Lee (Admin))	2	June 4th 2014
administrator (administrator)	2	June 4th 2014

Exploitable Vulnerabilities		
TITLE	TOTAL USERS	TOTAL ASSETS
MS14-017: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution	182	174
MS14-012: Cumulative Security Update for Internet Explorer (2925418)	142	419
MFSA2014-29 Firefox: Privilege escalation using WebGL implemented API	96	125
MFSA2014-29 Firefox: Privilege escalation using WebGL implemented API	96	125
Vulnerability (VMSA-2014-0054) (CVE-2014-0160)	56	80
MS13-090: Cumulative Security Update of Active Kill Bits (2903986)	46	325
MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution	45	269
Java CPU June 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	33	73
Java CPU June 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	33	73
Java CPU June 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	33	73
Java CPU June 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	33	73
Java CPU June 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	33	73
Java CPU June 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	33	73
MS13-081: Vulnerabilities in Windows Kernel/Mode Drivers Could Allow Remote Code Execution	31	319
Java CPU June 2013 Java Runtime Environment Serviceability vulnerability (CVE-2013-0286)	30	62
Java CPU April 2013 Java Runtime Environment 2D vulnerability (CVE-2013-0286)	23	56
Java CPU April 2013 Java Runtime Environment Libraries vulnerability (CVE-2013-0286)	21	45
Java CPU April 2013 Java Runtime Environment Deployment vulnerability (CVE-2013-0286)	21	46

# userinsight

## Расследование

Быстрое расследование  
инцидентов



## Контроль

Простая оценка рисков



## Обнаружение

Эффективное обнаружение  
атак



# BACKUP SLIDES

# Почему UserInsight лучше SIEM?



# Почему UserInsight может заменить SIEM?

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

---

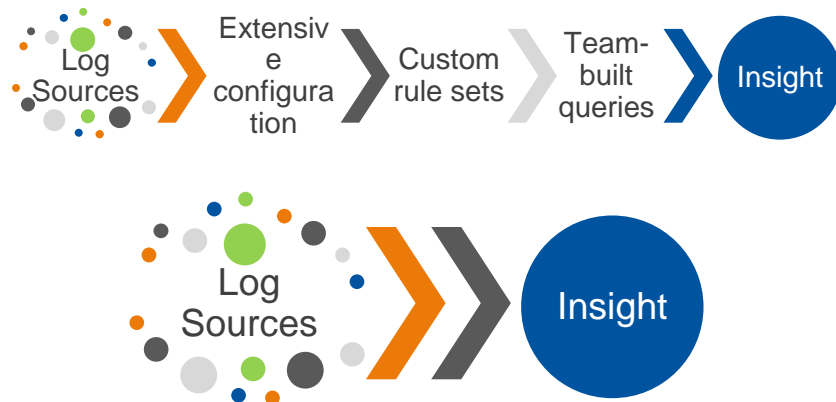
«Мы отдел ИБ состоящей из 2х человек. Раньше мы использовали локальную SIEM, но сейчас мы отказались от этого решения, так как для нас важно максимально использовать ресурсы для обеспечения безопасности и мы не можем выделить отдельного человека для контроля и настройки SIEM для получения релевантных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

---

Marketing company

# 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.



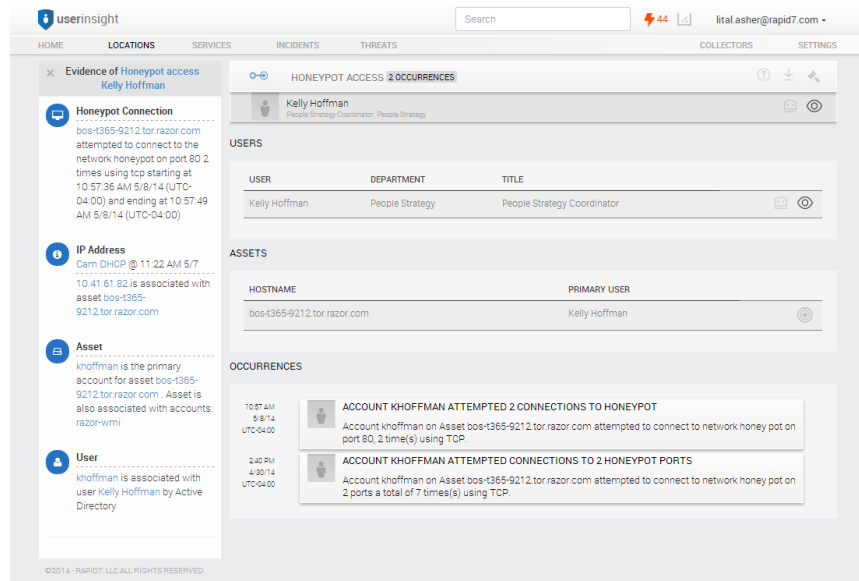
---

“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.”

---

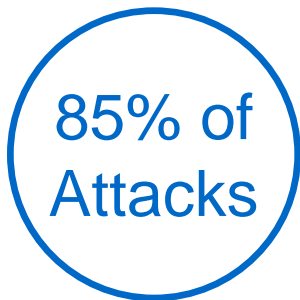
# Обнаружает сканирование сетей злоумышленником для поиска хостов

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





# 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  
длительным

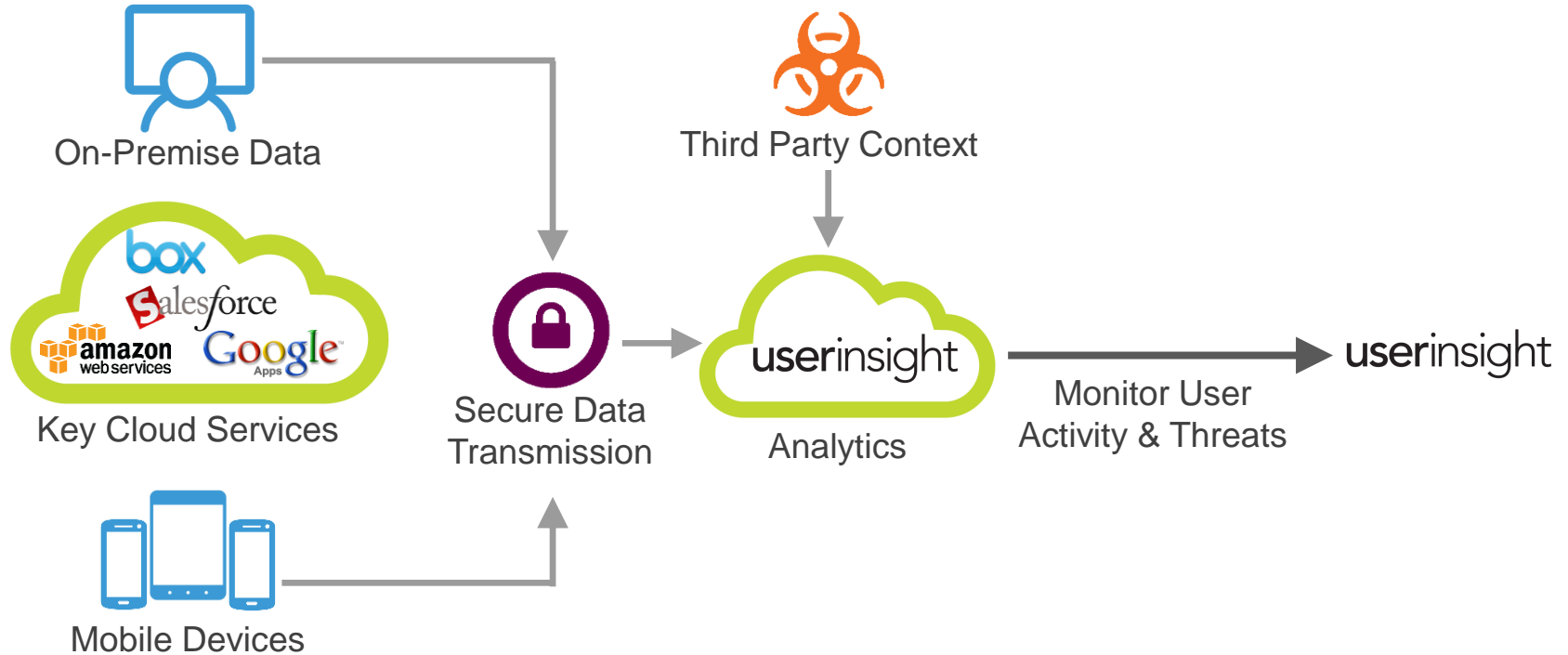
Ponemon Institute LLC,  
2014



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

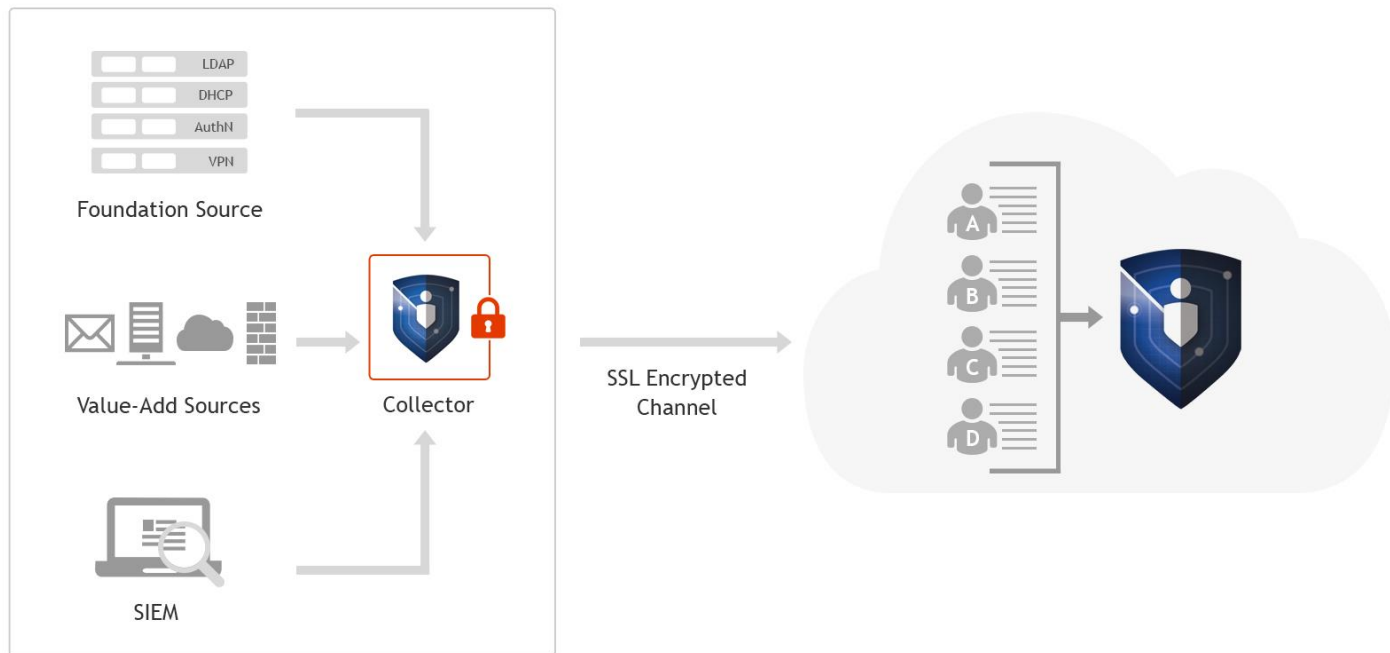
Ponemon Institute LLC,  
2014

# UserInsight – Sources of Data



# UserInsight – как это работает

CUSTOMER NETWORK



# THANK YOU

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

Rapid7@softprom.com | [www.softprom.com](http://www.softprom.com)