

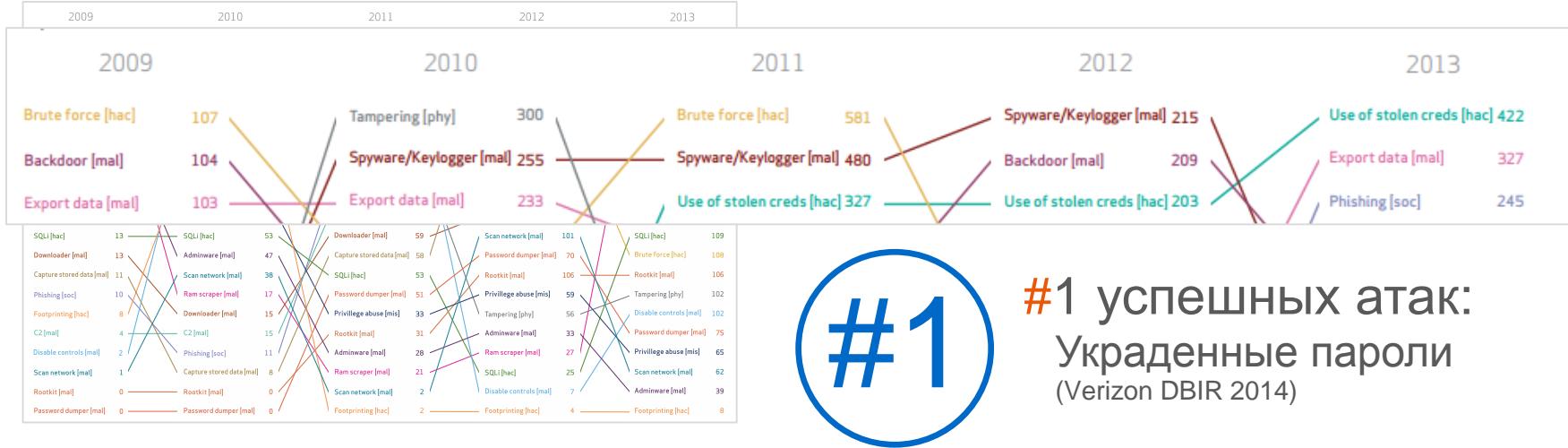


USERINSIGHT



Эффективное обнаружение и расследование атак на пользователей

Атаки на пользователей: Векторы атак

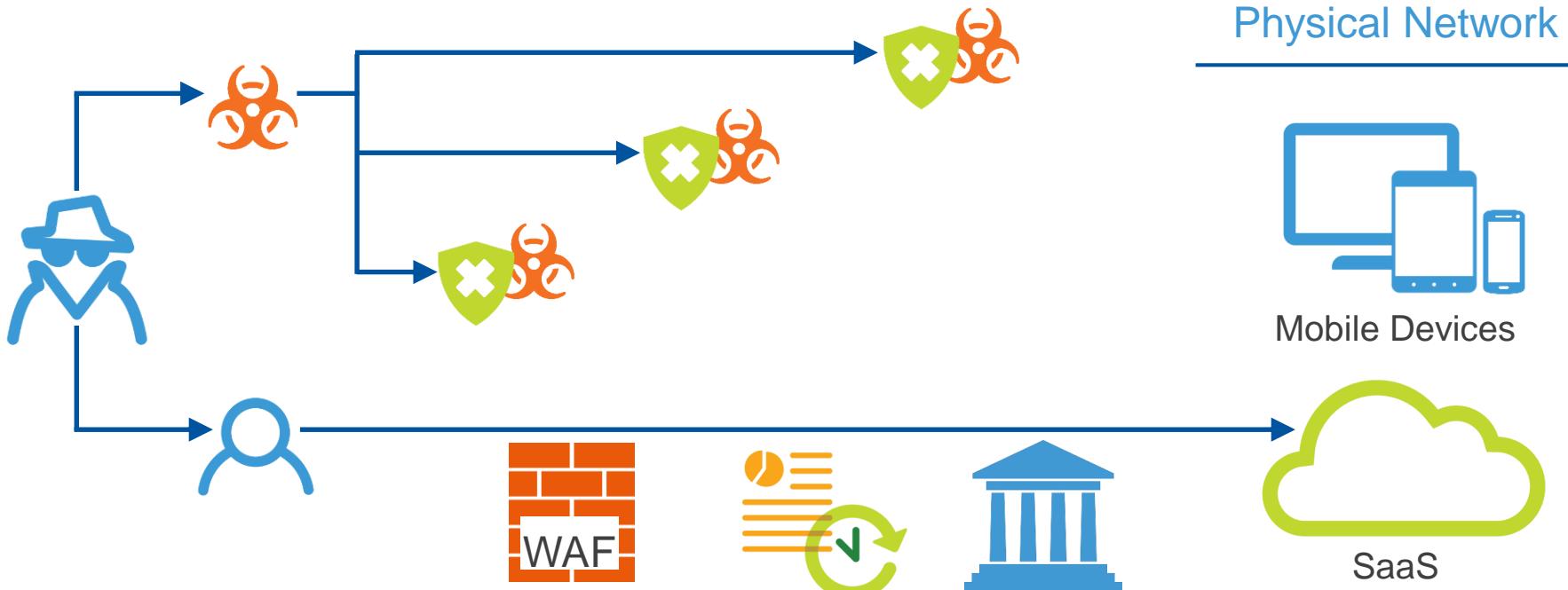


#1 успешных атак:
Украденные пароли
(Verizon DBIR 2014)

“Пользователи остаются самым слабым звеном в защите”

Gartner 2013

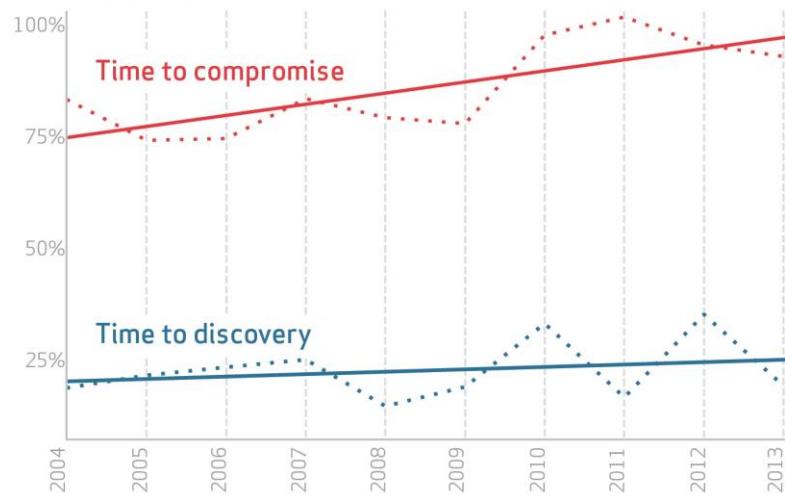
Современные технологии защиты не контролируют ключевой вектор атак



Атакующие проникают в сеть быстрее чем их обнаруживают...

Figure 13.

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



- 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

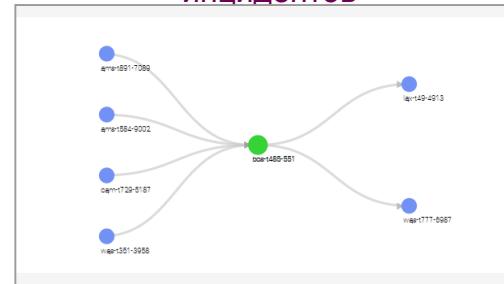
Эффективное обнаружение атак



- Обнаружает действия 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 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.



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 скомпроментированные аккаунты в крупных утечках

The screenshot shows the UserInsight platform interface. At the top, there's a navigation bar with tabs for HOME, LOCATIONS, SERVICES, INCIDENTS, THREATS, COLLECTORS, and SETTINGS. A search bar and a notification for 206 new items are also at the top. The main content area has a sidebar on the left with a list of detected incidents:

- Evidence of Account leaked** (Frances Roberts):
 - Account Leaked**: 3:46 AM 11/26. The email frances.roberts@razor.com has been reported as a leaked credential for site(s) adobe.com.
 - User**: frances.roberts@razor.com is associated with user Frances Roberts by ACTIVE_DIRECTORY.

On the right, there's a detailed view of the first incident under the heading "ACCOUNT LEAK 1 OCCURRENCE". It shows a table with one row for Frances Roberts, Account Executive, Sales. Below this is a section titled "OCCURRENCES" with a single entry:

Date	Description
3:46 AM 11/26/13 UTC-05:00	ACCOUNT FRANCES_ROBERTS@RAZOR.COM WAS REPORTED AS LEAKED

The description details the breach: "The account was found on a leak after an attack on adobe.com. The leak was first found on 2013-11-25 00:00:00. Adobe Systems announced on October 3rd of 2013 that hackers broke into its servers and stole source code for a range of products including ColdFusion and Acrobat family of products. The breach also affected what was at that time estimated to be 3.0 million users but later was revised to include at least 30 million users. Adobe said hackers had stolen nearly 3 million encrypted customer credit card records, as well as login data for an undetermined number of Adobe user accounts. The breach happened in early October but the stolen accounts were not published on the web until early November. The published data includes 10s of millions of accounts with IDs, email addresses, encrypted passwords and more. NOTE: This part of the breach includes those accounts for which there was no password found in the breach data. Even though a password was not present in the published data we cannot confirm that the hacker(s) might have simply omitted it from the data dump."

Обнаружение попыток фишинга

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

The screenshot shows a user interface for monitoring account activity. At the top, a header reads "Evidence of Account received suspicious link Lewis Peters". Below this, under the "User" section, it says "lewis_peters@razor.com is associated with user Lewis Peters by Active Directory". Under the "User Received Link" section, there is a log entry: "2:48 PM 6/3 lewis_peters@razor.com received link http://cdn.mihdocs.com (details) in an email at 02:48:54 PM 6/3/14 (UTC-04:00)". Under the "Community Threat" section, it states "http://cdn.mihdocs.com belongs to the tracked community threat(s): cdn.mihdocs.com - Site with disease vectors appearing on Websense alerts". To the right, a separate window titled "ACCOUNT RECEIVED SUSPICIOUS LINK 1 OCCURRENCE" shows a single occurrence for "Lewis Peters" with the same details: "lewis_peters@razor.com received an email with a suspicious link http://cdn.mihdocs.com".

UserInsight: Встроенное обнаружение признаков компрометации



Обнаружение доступа злоумышленника к сети.

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

The screenshot displays the UserInsight application interface. At the top, there are navigation tabs: HOME, LOCATIONS, SERVICES, INCIDENTS, THREATS, COLLECTORS, and SETTINGS. A search bar and user information (demo@razor.com) are also at the top. The main content area shows a list of "Evidence of Multiple countries" for "Elias Boone". The list includes:

- Ingress Authentication: IIS, OWA and ActiveSync @ 10:59 AM 1/21. Description: eboone account authenticated with service activesync from 188.29.165.44 with mobile device AppID2MLNPFDFFG8.
- IP Location: 188.29.165.44 is owned by Three in United Kingdom.
- Mobile Device: iPhone AppID2MLNPFDFFG8 is associated with account eboone.
- User: eboone is associated with user Elias Boone by ACTIVE_DIRECTORY.
- Ingress Authentication: IIS, OWA and ActiveSync @ 10:59 AM 1/21. Description: eboone account authenticated with service activesync from 188.29.165.44 with mobile device AppID2MLNPFDFFG8.

Below this is a "LOCATIONS" section featuring a world map with four red dots labeled 1, 2, 3, and 4, corresponding to the IP locations listed above. A legend indicates "SUCCESS" (green) and "failure" (red). A table at the bottom lists the details for each event:

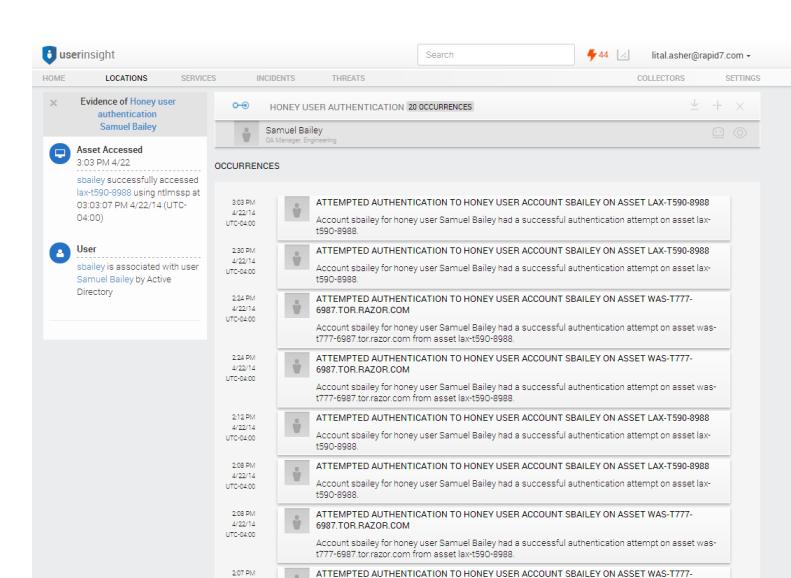
SERVICE	LOCATION	COUNTRY	ORGANIZATION	TIME/DATE	RESULT	TYPE
iPhone	Boston MA	United States	Rapid7, LLC	11:54 AM-05:00 1/21	●	device
iPhone	Three	United Kingdom		10:59 AM-05:00 1/21	●	device

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



UserInsight: Встроенное обнаружение признаков компрометации



Detect Attacker's Access Critical Assets

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

The screenshot displays a user interface for monitoring critical asset access. At the top, a header bar indicates 'Evidence of Account authenticated to a critical asset' and 'Marion Lawrence'. Below this, a title 'CRITICAL ASSET AUTHENTICATION - NEW USER 1 OCCURRENCES' is shown, along with Marion Lawrence's profile: 'Marion Lawrence, Chief Information Officer, IT Department'. A 'USERS' section lists Marion Lawrence with her department and title. An 'ASSETS' section shows a host named 'ams-t143-3989 tor.razor.com' associated with a 'Shared Asset'. In the 'OCCURRENCES' section, a log entry from '6/5/14 UTC-04:00' details the event: 'ACCOUNT MLAWRENCE ACCESSED CRITICAL ASSET AMS-T143-3989 TOR.RAZOR.COM' and notes it as 'First time authentication to critical asset.'

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 for monitoring event log deletion. At the top, a header bar shows 'DETECTION EVASION - EVENT LOG DELETION 4 OCCURRENCES'. Below this, a summary section for 'Doris Rogers' (Regional Channel Manager, Channel Sales) lists her user details and associated assets. The main area is divided into sections for 'USERS' and 'ASSETS', both of which show a single entry for Doris Rogers. The 'OCCURRENCES' section contains four log entries, each detailing an account droger clearing event logs on specific assets at specific times.

HOSTNAME	PRIMARY USER
lax-t607-5235.tor.razor.com	Doris Rogers

TIME	ACCOUNT DROGERS CLEARED EVENT LOGS
11:54 AM 5/14/14 UTC-04:00	Account drogers cleared the event logs on asset lax-t607-5235.tor.razor.com.
6:00 PM 5/13/14 UTC-04:00	Account drogers cleared the event logs on asset lax-t607-5235.tor.razor.com.
6:54 PM 5/13/14 UTC-04:00	Account drogers cleared the event logs on asset lax-t607-5235.tor.razor.com.
11:38 AM 5/13/14 UTC-04:00	Account drogers cleared the event logs on asset lax-t607-5235.tor.razor.com.

userinsight

РАССЛЕДОВАНИЕ

Легкое принятие решений

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

The screenshot displays a user interface for investigating a security incident. At the top, a header bar shows the user's name, Pablo Robbins, and the title "Evidence of Multiple countries". Below this is a detailed list of findings:

- Ingress Authentication**: IIS, OWA and ActiveSync @ 3:15 AM 6/5. Description: probobins account authenticated with service activesync from 70.79.111.9 with mobile device AppIC39LNADEFRC.
- IP Location**: 70.79.111.9 is owned by Shaw Communications in Richmond BC, Canada.
- Mobile Device**: iPhone AppIC39LNADEFRC is associated with account probobins.
- User**: probobins is associated with user Pablo Robbins by Active Directory.

On the right side, there is a world map titled "MULTIPLE COUNTRY AUTHENTICATIONS 6 OCCURRENCES" with a legend for "success" (green) and "failure" (red). A callout bubble highlights a location in North America. Below the map is a table of "LOCATIONS" with columns: SERVICE, LOCATION, COUNTRY, ORGANIZATION, TIME/DATE, RESULT, and TYPE. The table shows three entries:

SERVICE	LOCATION	COUNTRY	ORGANIZATION	TIME/DATE	RESULT	TYPE
IIS	Singapore 00	Singapore	SingTel Mobile	3:21 AM-04:00 6/5	●	—
IIS	Richmond BC	Canada	Shaw Communications	3:15 AM-04:00 6/5	●	✗
IIS	Vancouver BC	Canada	Shaw Communications	12:49 PM-04:00 6/3	●	✗

At the bottom, a section titled "OCCURRENCES" lists four events:

- 8:15 AM 6/14 UTC+0400: ACCOUNT PROBBINS AUTHENTICATED FROM 2 COUNTRIES IN 5 MINUTES 40 SECONDS. The user authenticated from Canada and Singapore.
- 8:20 AM 6/14 UTC+0400: ACCOUNT PROBBINS AUTHENTICATED FROM 2 COUNTRIES IN 43 MINUTES 49 SECONDS. The user authenticated from Canada and Singapore.
- 11:05 PM 6/14 UTC+0400: ACCOUNT PROBBINS AUTHENTICATED FROM 2 COUNTRIES IN 53 MINUTES 28 SECONDS. The user authenticated from Canada and Singapore.
- 11:28 AM 6/14 UTC+0400: ACCOUNT PROBBINS AUTHENTICATED FROM 2 COUNTRIES IN 29 MINUTES 44 SECONDS. The user authenticated from Canada and Singapore.

A note at the bottom right states: "Cisco AnyConnect Secure M VPN Credentials required to connect."

Автоматическое сопоставление данных о угрозах пользователях и хостах

- Сбор информации о уязвимостях хостов (с помощью Nmap)

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		
NAME	DEPARTMENT	ASSET
Alan Gonzales	Security Solutions	ams-t734-1037.tor.razor.com
Alan Gonzales	Security Solutions	bos-t639-7279.tor.razor.com
Albert Morris	IT Department	bos-t808-4083.tor.razor.com
Alfonso Vaughn	Sales Operations	cam-t560-8309.tor.razor.com
Allison Meyer	Security Solutions	ams-t801-8759.tor.razor.com

LEAVE FEEDBACK

Контроль всех активностей пользователей

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

The screenshot displays a dashboard for monitoring user activity. It includes sections for:

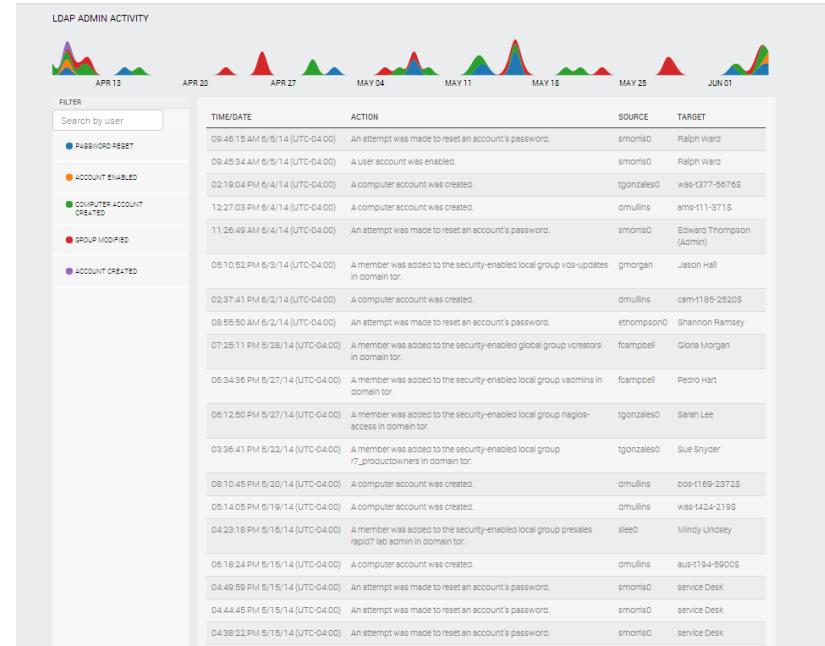
- ACCOUNTS:** Shows a list of accounts with their names, authentication services, and password change dates. Most accounts are listed under Active Directory, with one under Okta.
- ASSETS:** A list of hosts with their last access times.
- CLOUD SERVICES:** A chart showing usage statistics for various services: GitHub (Production), Slides (Production), LastPass (Personal), Notion (Enterprise), and Okta (Personal). GitHub shows the highest usage at 2014.92 kB.
- MOBILE DEVICES:** A list of devices by hardware platform, last accessed time, and device ID.
- LOCATIONS (LAST MONTH):** A world map showing the last location of devices.
- SERVICE LOCATION COUNTRY ORGANIZATION TIME DATE RESULT TYPE:** A table showing service locations, country, organization, time, date, result, and type for three entries: Tampa FL, Austin TX, and Dallas TX.

userinsight

КОНТРОЛЬ РИСКОВ

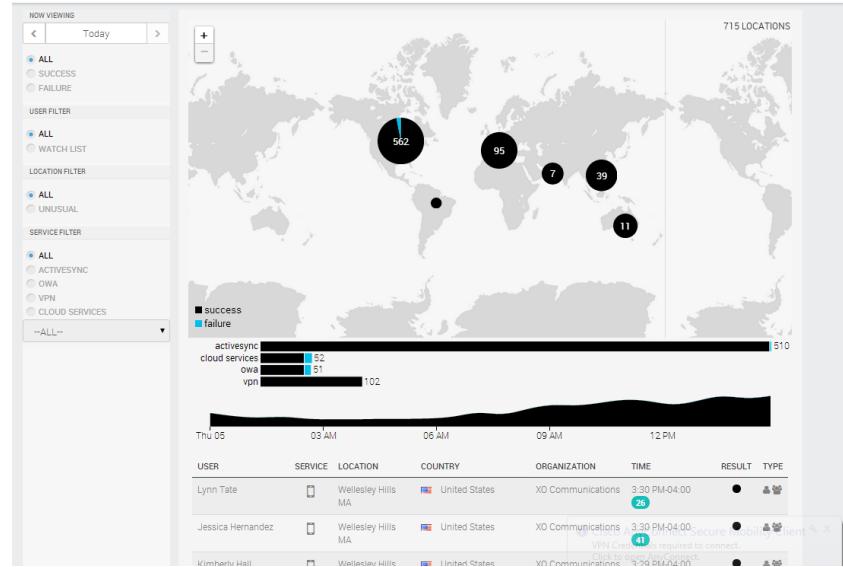
Контроль всех активностей администраторов

- 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 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
dmullins (Debby Mullins)	3	May 23rd 2014
razor-wm (Razor-WM.wm)	3	June 5th 2014
vgonzales (Virginia Gonzales)	3	May 2nd 2014
ethompson0 (Edward Thompson (Admin))	2	June 4th 2014
sanderson0 (Sandra Anderson (Admin))	2	June 3rd 2014
seid0 (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 (2925418)	152	174	
MS14-012: Cumulative Security Update for Internet Explorer (2925418)	142	419	
MSFA2014-29 Firefox: Privilege escalation using WebIDL-implemented API (2925418)	96	125	
MSFA2014-29 Firefox: Privilege escalation using WebIDL-implemented API (2925418)	96	125	
Vkware Workstation: Vulnerability (VMSA2014-0004) (CVE-2014-0160)	56	60	
MS13-080: Cumulative Security Update of ActiveX Kill Bits (2800986)	48	325	
MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2800986)	45	289	
Java CPU June 2013 Java Runtime Environment 20 vulnerability (CVE-2013-2867)	33	73	
Java CPU June 2013 Java Runtime Environment 20 vulnerability (CVE-2013-2867)	33	73	
Java CPU June 2013 Java Runtime Environment 20 vulnerability (CVE-2013-2867)	33	73	
Java CPU June 2013 Java Runtime Environment 20 vulnerability (CVE-2013-2867)	33	73	
Java CPU June 2013 Java Runtime Environment 20 vulnerability (CVE-2013-2867)	33	73	
MS13-081: Vulnerabilities in Windows Kernel Mode Drivers Could Allow Remote Code Execution (2800986)	31	319	
Java CPU June 2013 Java Runtime Environment Serviceability vulnerability (CVE-2013-2867)	30	62	
Java CPU April 2013 Java Runtime Environment 20 vulnerability (CVE-2013-2867)	23	56	
Java CPU April 2013 Java Runtime Environment Libraries vulnerability (CVE-2013-2867)	21	45	
Java CPU April 2013 Java Runtime Environment Deployment vulnerability (CVE-2013-2867)	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?

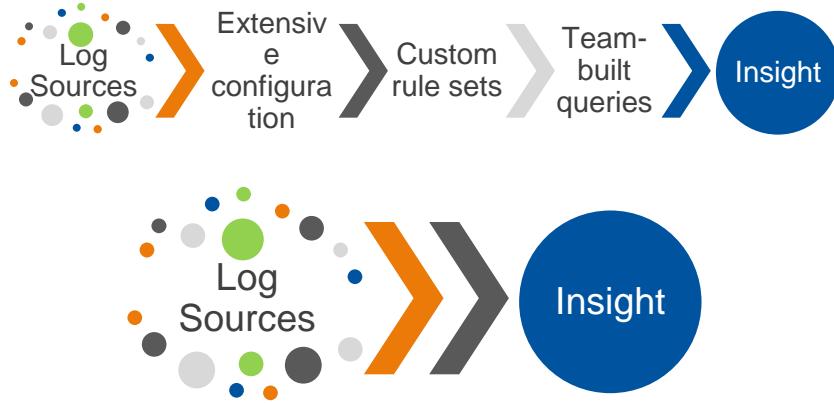
- Обнаружение атак и расследование инцидентов «из коробки»
- Поведенческий анализ «из коробки»
- Уведомления о злоупотреблениях и нарушениях политик «из коробки»

«Мы отдел ИБ состоящий из 2x 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 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.

The screenshot displays the UserInsight web application interface. At the top, there's a navigation bar with links for HOME, LOCATIONS, SERVICES, INCIDENTS, and THREATS. A search bar and user information ('lital.asher@rapid7.com') are also at the top right. The main content area shows a detailed view of a honeypot access event:

- Evidence of Honeypot access by Kelly Hoffman:** Shows a connection attempt from IP address 10.41.61.82 to a honeypot on port 80 at 10:57:36 AM on May 8, 2014.
- Honeypot Connection:** Details the connection attempt from the honeypot IP to port 80.
- IP Address:** Shows the IP address 10.41.61.82 associated with the asset 'bos-t365-9212.tor.razor.com'.
- Asset:** Details the asset 'bos-t365-9212.tor.razor.com' which is associated with account 'knoffman'.
- User:** Details the user 'knoffman' associated with the account 'Kelly Hoffman' via Active Directory.

On the right side, there are sections for **USERS** (listing 'Kelly Hoffman' with 'People Strategy' department and 'People Strategy Coordinator' title), **ASSETS** (listing the honeypot asset), and **OCCURRENCES** (listing two events: 'ACCOUNT KHOFFMAN ATTEMPTED 2 CONNECTIONS TO HONEYPOD' and 'ACCOUNT KHOFFMAN ATTEMPTED CONNECTIONS TO 2 HONEYPOD PORTS').

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

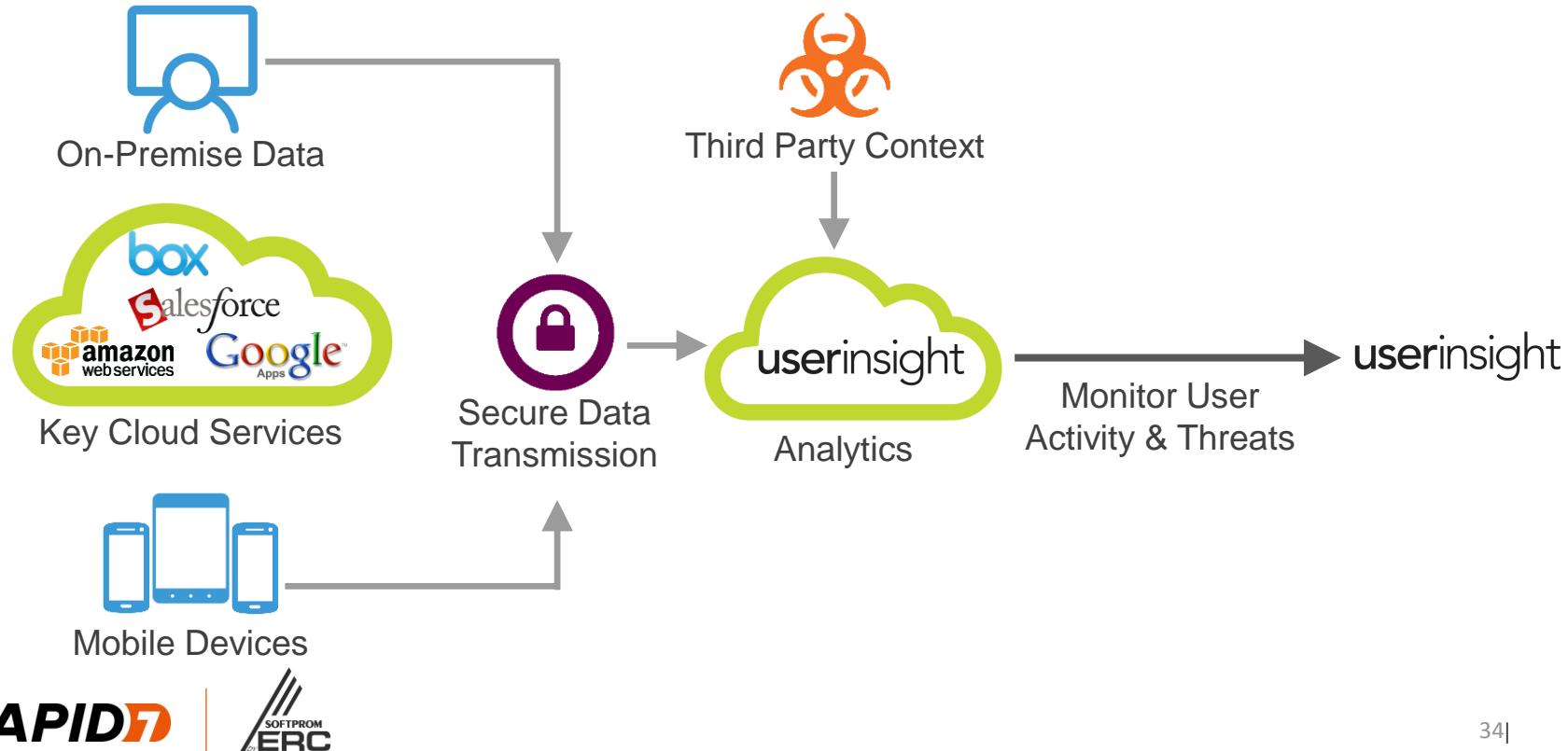
Ponemon Institute LLC,
2014



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

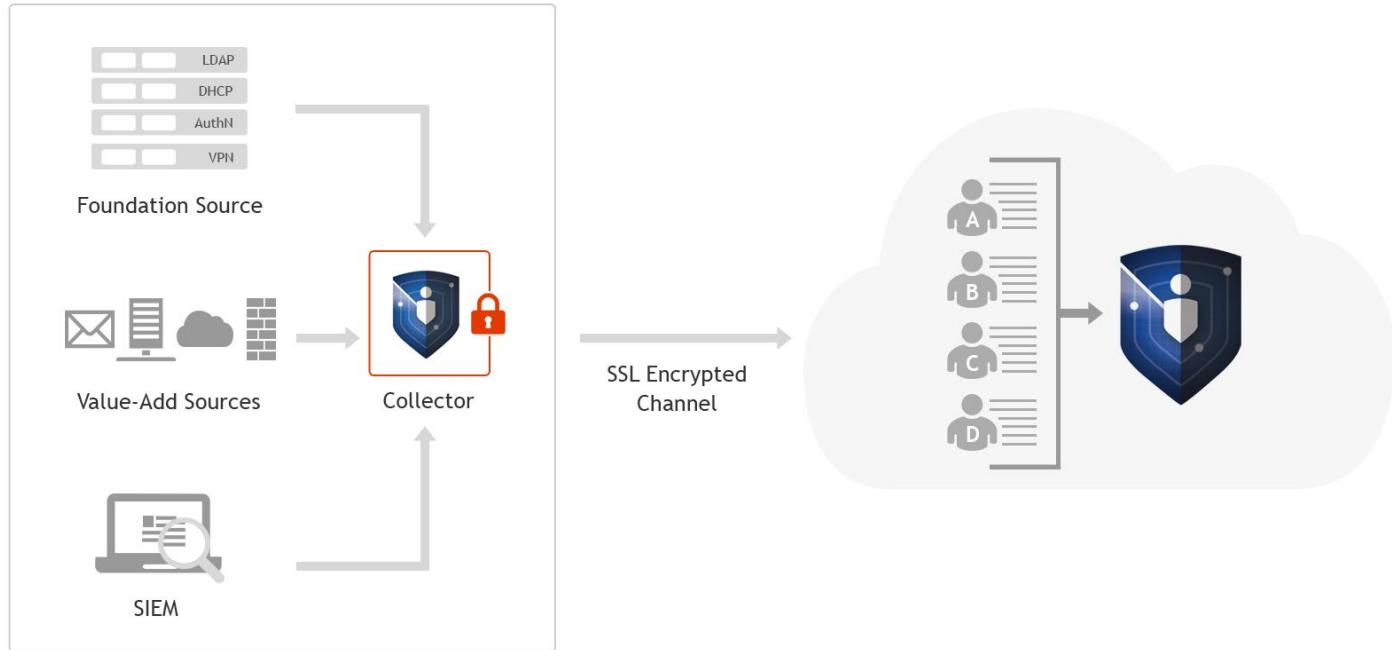
Ponemon Institute LLC,
2014

UserInsight – Sources of Data



UserInsight – как это работает

CUSTOMER NETWORK



THANK YOU

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

Rapid7@softprom.com | www.softprom.com