



Автоматизация реагирования на инциденты ИБ

Александр Бондаренко
Генеральный директор, R-Vision

Про антиспам





СКОРОСТЬ РЕАКЦИИ

On average, how much time elapsed between the initial compromise and detection (i.e., the dwell time)? How long from detection to remediation?

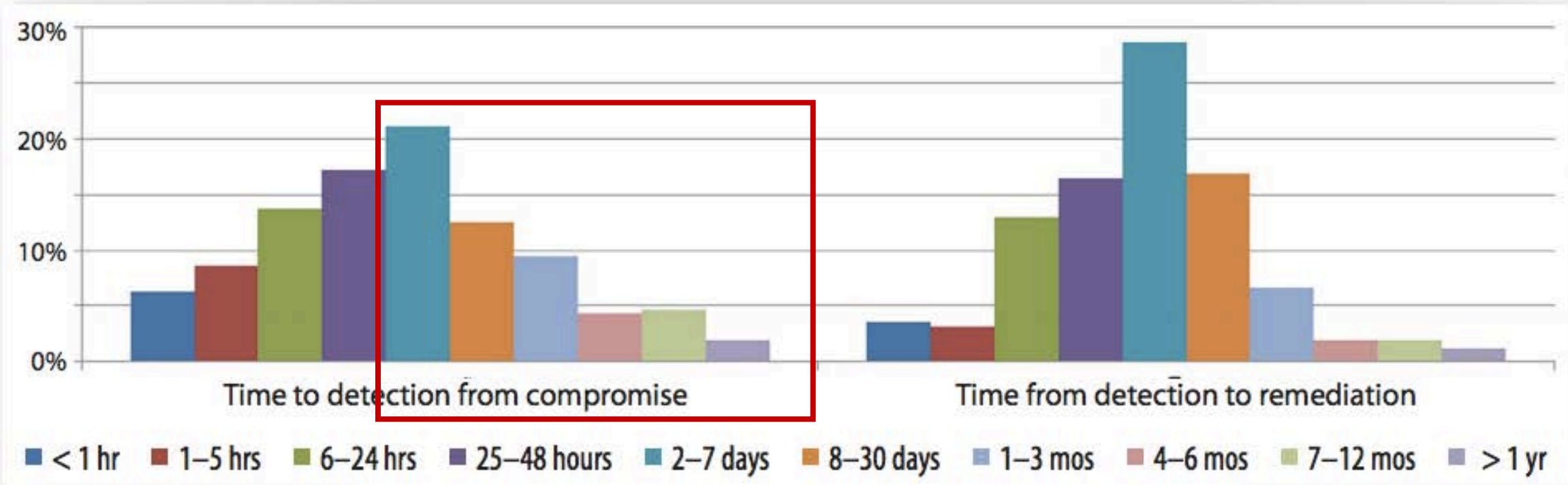
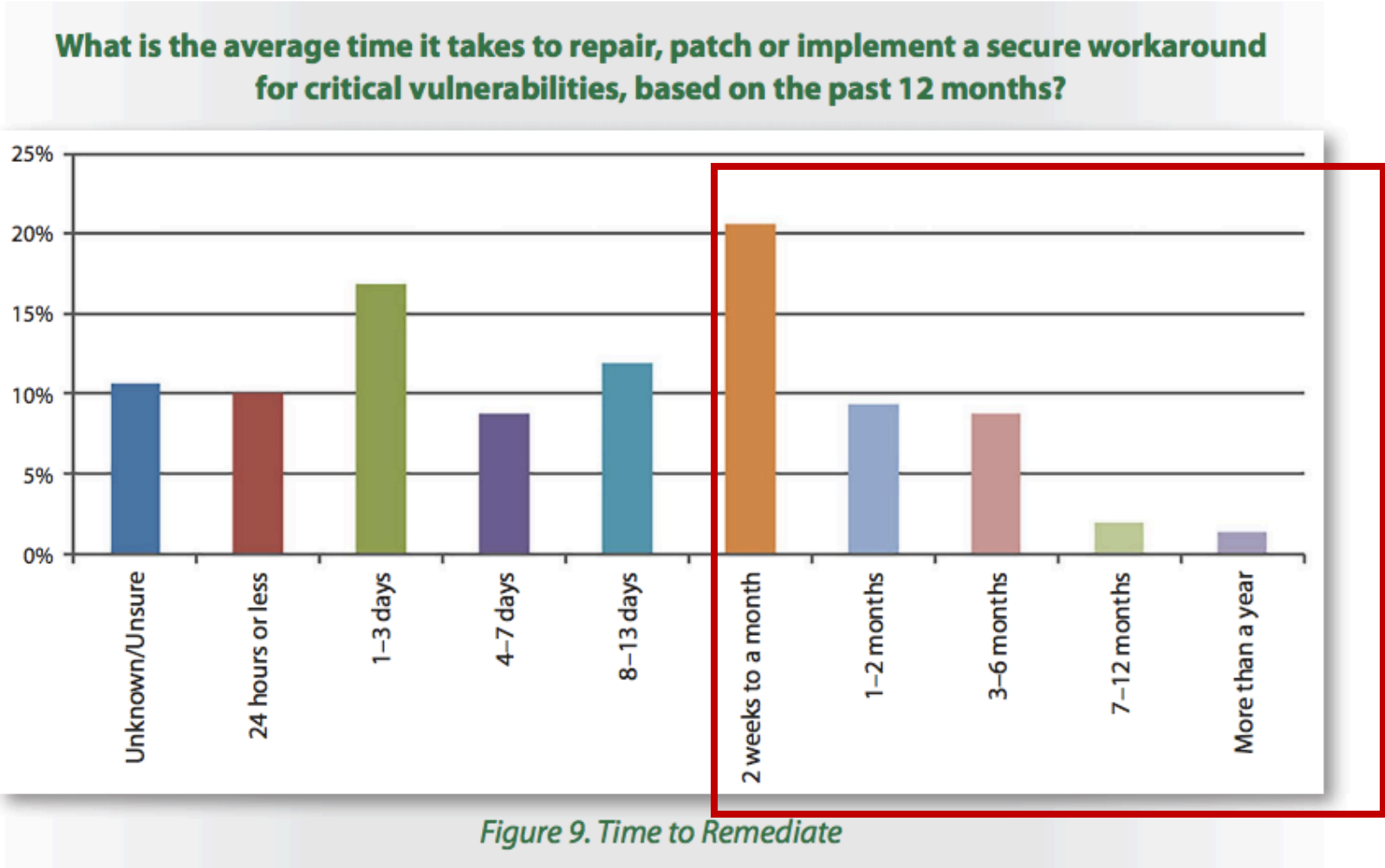


Figure 8. Time to Detection and Time from Detection to Response

ВРЕМЯ «ЖИЗНИ» УЯЗВИМОСТИ



ВРЕМЯ «ЖИЗНИ» УЯЗВИМОСТИ

Рис. 17. Доля устройств с известными уязвимостями в процентах (с распределением по годам)



Почему ?

Роботы



Бизнес

Экономика

Финансы

Мнения

Политика

Технологии

Недвижимость

Авто

Менеджмент

Стиль жизни

USD 57.545 Евро 61.33 ММВБ 2148.48 PTC 1176.11 S&P 500 2349.25 Brent 55.74 Золото 1242.2

Робот-юрист заменит 3000 сотрудников Сбербанка

12 января 18:39 Обновлено в 21:17 Интерфакс



Робот-юрист, который начал работать в Сбербанке в 2016 г., позволит кредитной организации высвободить 3000 рабочих мест по юридической специальности в текущем году. С таким заявлением выступил зампред правления Сбербанка Вадим Кулик на Гайдаровском форуме.

«Буквально в IV квартале мы запустили робота-юриста, который может нам из бумаг писать исковые заявления - один из примеров работающих роботов. Фактически на текущий момент это означает, что практически все иски, которые пишутся у нас по физическим лицам, полностью перейдут на этих роботов в течение этого полугодия», - пояснил он.

По его словам, многие высвобождаемые сотрудники Сбербанка будут задействованы в программе переобучения. «И если, соответственно, мы не можем их применить, то дальше, естественно, начинаются сокращения», - добавил он.

Кулик признал, что получается непростая ситуация. «Это большая проблема, потому как чем

Главное

Популярное

Президентские управления обменяются департаментами

«Северсталь» предупредила о рисках для бизнесменов в России

Tele2 сократит персонал и изменит структуру в регионах

«Победа» наймет охрану в аэропортах для защиты от агрессивных пассажиров

Российские легкоатлеты должны вернуться

По экспертным оценкам **доля операций, совершаемых роботами** на Нью-Йоркской фондовой бирже NYSE, составляет порядка **70%**, на срочной секции FORTS Московской биржи — **90%** сделок выполняются алгоритмическими роботами, а при торговле акциями на ММВБ около **60%** сделок выполняют «машины».

ТЕХНОЛОГИИ НА СЛУЖБЕ У ХАКЕРОВ

Computer Viruses

Artificial Intelligence

Computer Programming

Can artificial intelligence be implemented in computer viruses? Has anyone done it yet?

Has any one created an Artificially Intelligent Computer virus , which can modify its signature to avoid detection from an Anti Virus. A computer virus which can stop all its infectious activities and go into the state of incubation when a full system scan is going on through an Anti Virus. What is the possibility of seeing such computer viruses in near future ?

Crims using anti-virus exclusion lists to send malware to where it can do most damage

When vendors tell you what to whitelist, crims are reading too

7 Dec 2016 at 07:32, Darren Pauli



Advanced malware writers are using anti-virus exclusion lists to better target victims, researchers say.

The Twitter Bot That Sounds Just Like Me

Hackers can use artificial intelligence to mimic their —and entice them to click on malicious links.

**Мы воюем с
«машинами»!**



..... И

проигрываем

GAME OVER



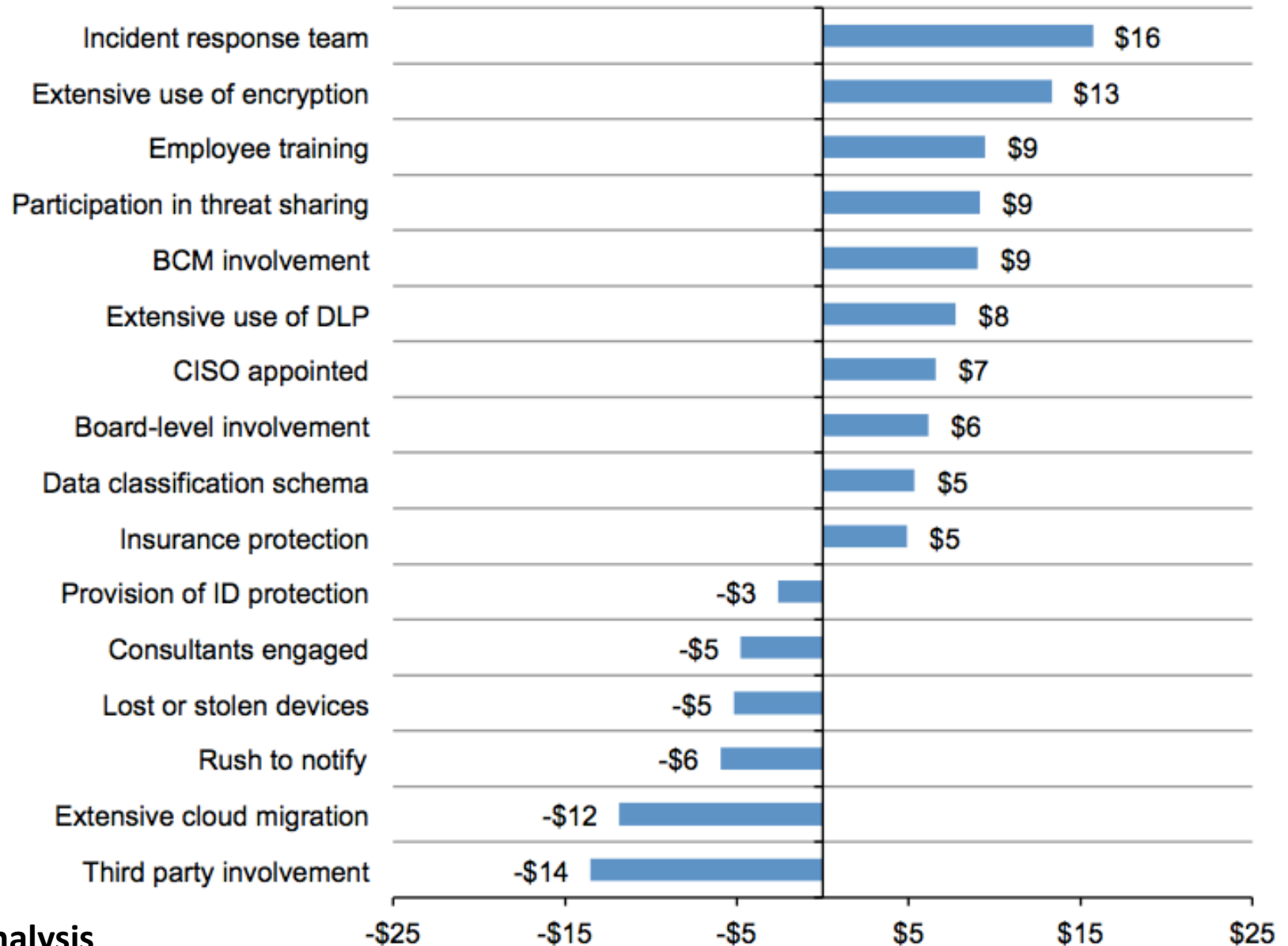


**Преступность определяется не
наличием воров...**

"Organizations are shifting security budgets from prevention to prediction, detection and response, and security vendors need to be capture this shifting spend"

Gartner, 2016

Figure 8. Impact of 16 factors on the per capita cost of data breach
 Consolidated view (n=383), measured in US\$



> 60 %

времени на «бумажную» работу

What do you believe are the key impediments to effective IR at your organization?

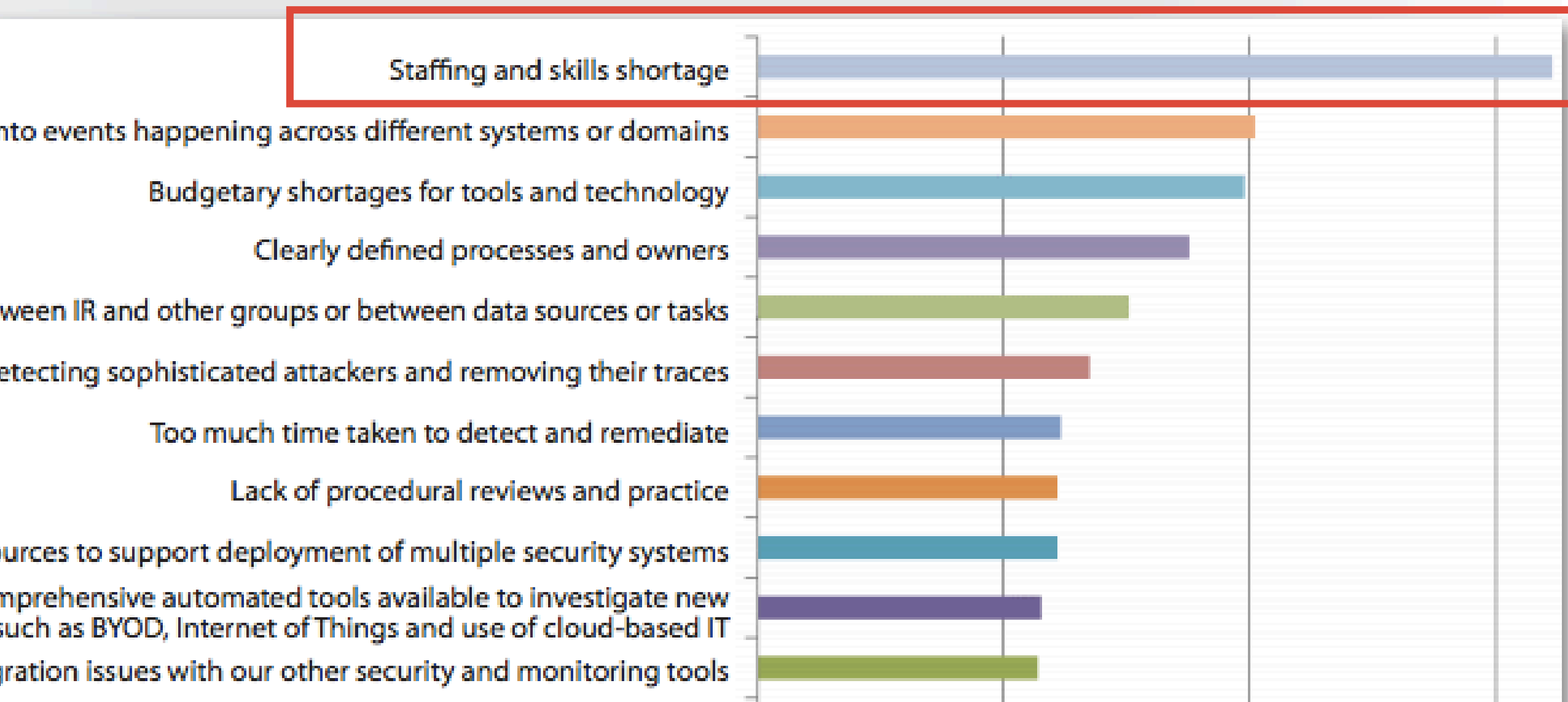
Select up to five choices in any order.



Figure 13. Impediments to Effective IR Teams

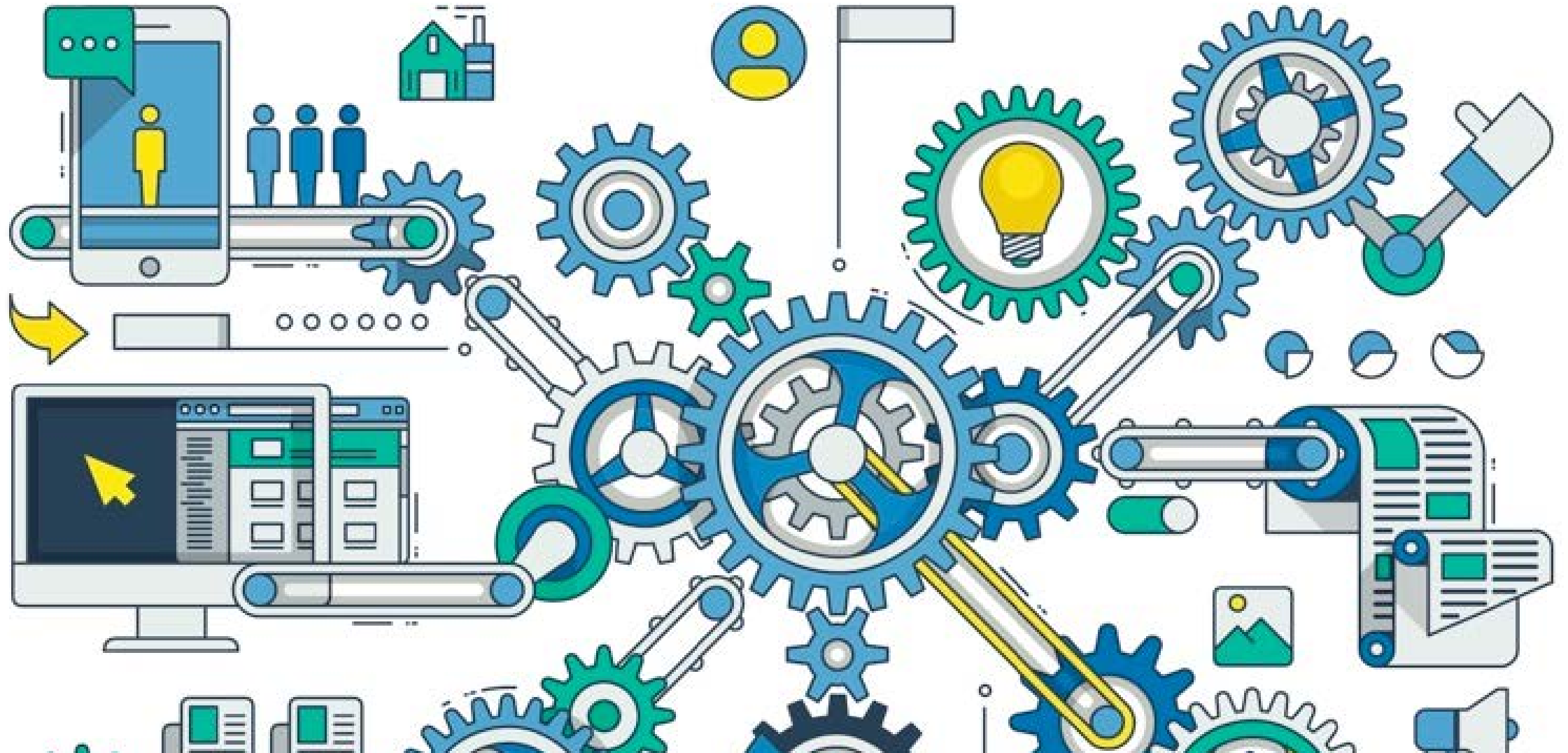
What do you believe are the key impediments to effective IR at your organization?

Select up to five choices in any order.



ВЫВОДЫ ?

Автоматизация или поражение



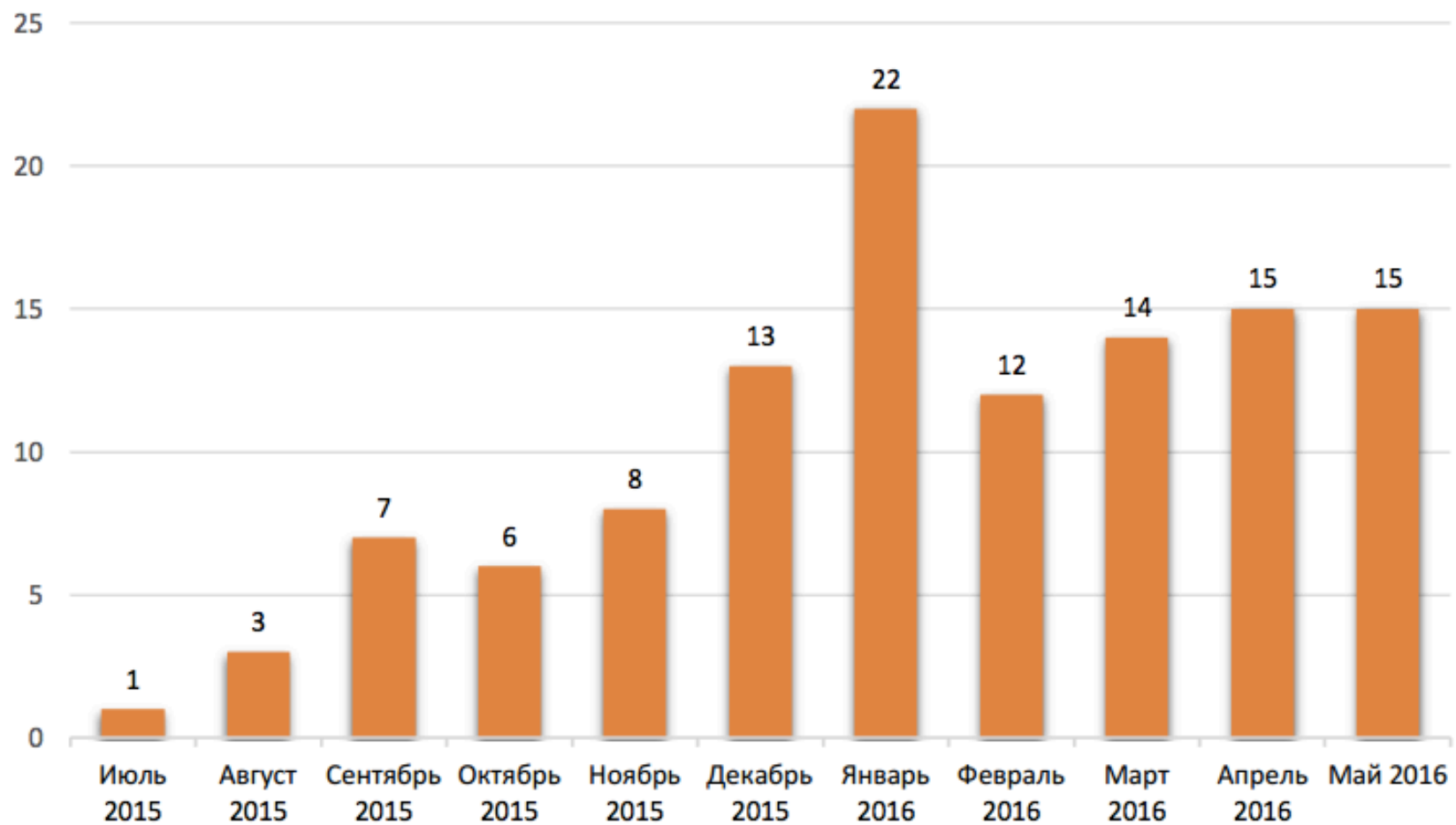


Рисунок 4 – Количество бюллетеней, рассылаемых FinCERT, по месяцам



Варианты автоматизации

№ 1 СКРИПТЫ

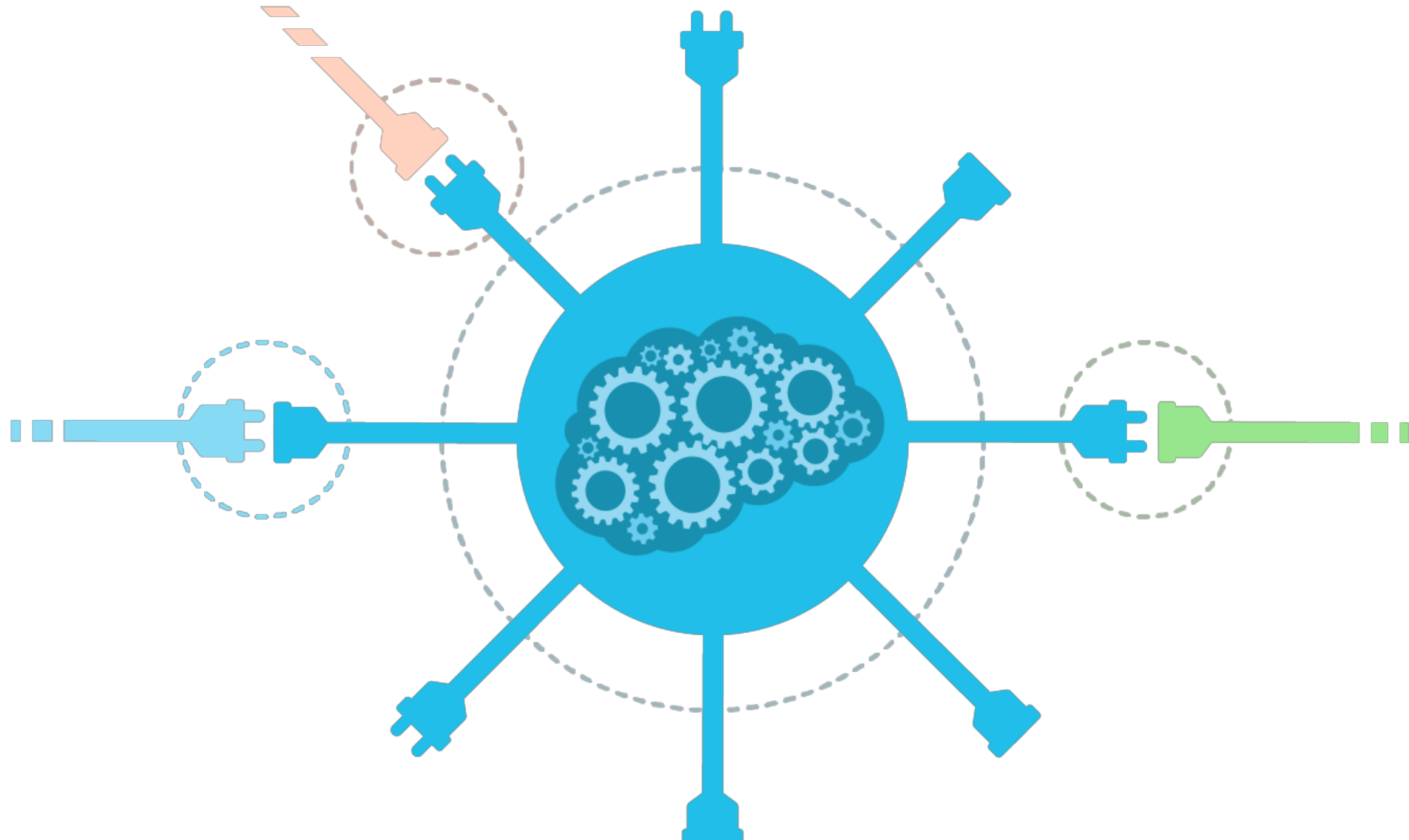
```
ui_print(" - Mounting system partition...");
run_program("/sbin/busybox", "mount", "/system");
run_program("/sbin/busybox", "mount", "-o", "rw,remount",
"/system", "/system");
run_program("/sbin/busybox", "mount", "-o", "rw,remount", "/",
"/");
ui_print(" - Setting up...");
package_extract_dir("system", "/system");
ui_print(" - Fixing permissions...");
set_perm(0, 0, 0755, "/system/bin/bse");
set_perm_recursive(0, 0, 0755, 0755, "/system/etc/init.d");
set_perm_recursive(0, 0, 0755, 0755, "/system/etc/startup");
ui_print(" - Unmounting system partition...");
```

СКРИПТЫ


- **Все пишем сами**
- **Знания уходят вместе с людьми**
- **Дешево**

```
ui_print(" - Mounting system partition...");
run_program("/bin/yx", "mount", "/system");
run_program("/sbin/busybox", "mount", "-o", "rw,remount",
"/system", "/system");
run_program("/sbin/busybox", "mount", "-o", "rw,remount", "/",
"/");
ui_print(" - Setting up...");
padding_ext(" - Setting up...");
ui_print(" - Fixing permissions...");
set_perm(0, 0, 0755, "/system/bin/bse");
set_perm_recursive(0, 0, 0755, 0755, "/system/etc/init.d");
set_perm_recursive(0, 0, 0755, 0755, "/system/etc/startup");
ui_print(" - Mounting system partition...");
```

№ 2 ИНТЕГРАЦИИ РЕШЕНИЙ



№ 2 ИНТЕГРАЦИИ РЕШЕНИЙ

- **Требования определяем заранее**
 - **У производителей с этим плохо**
- 





Александр Бондаренко
Генеральный директор,
R-Vision

bondarenko@rvision.pro