



# Вера в технологии? Вера в людей? Поиски баланса

**Владимир Дрюков**  
Директор Solar JSOC

**Ростелеком**  
Солар



# #whoarewe

№1

на рынке SOC  
в России

190+

сотрудников  
Solar JSOC

72+ млрд

анализируемых  
событий ИБ в сутки

10 минут

на обнаружение  
кибератаки

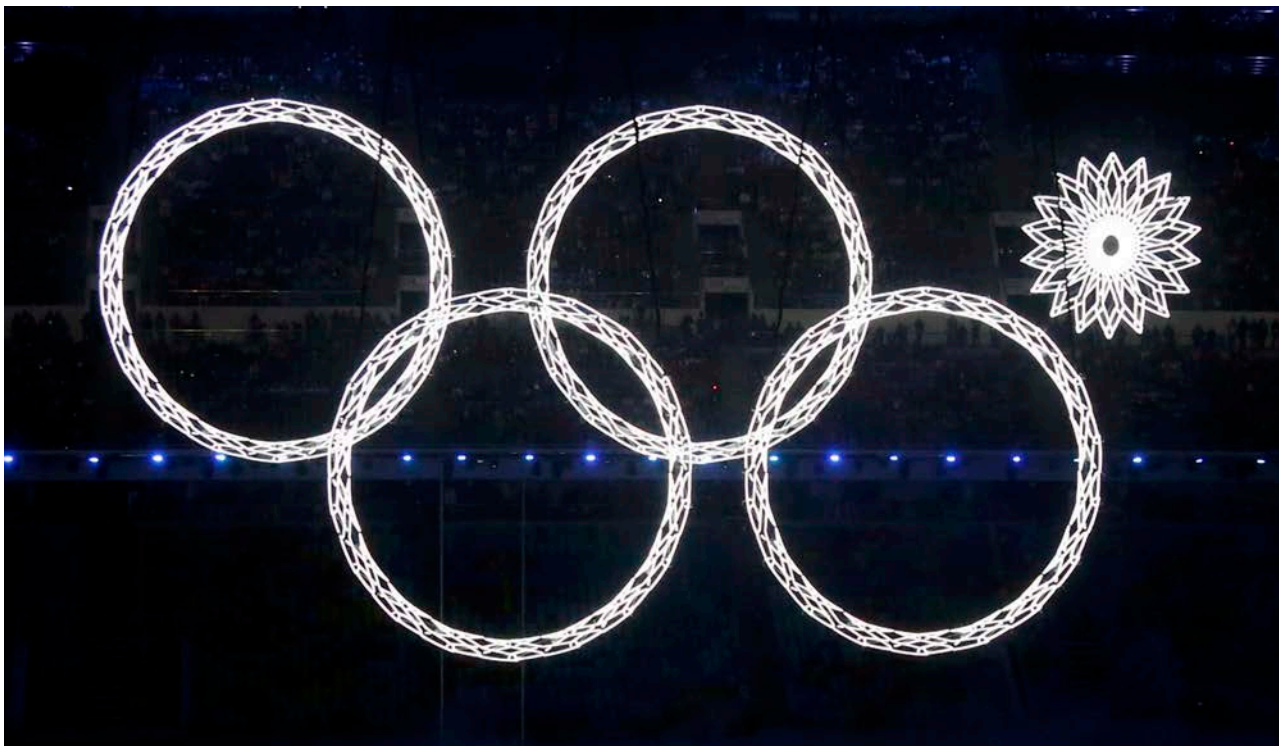
30 минут

на реагирование  
и защиту

50+

клиентов из топ-100  
российского бизнеса

# Олимпиада-2014 – кибератака?



# Олимпиада-2018 – точно кибератака

≡ WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN IN | SUBSCRIBE



ILLUSTRATION: JOAN WONG

ANDY GREENBERG

EXCERPT

SECURITY

10.17.2019 06:00 AM

## The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History

How digital detectives unraveled the mystery of Olympic Destroyer—and why the next big attack will be even harder to crack.

# Киберолимпиада 2019+



# Быстрее?



**Ростелеком**  
Солар

# Современный киберпреступник – динамика

	Публикация уязвимости	Время до разработки эксплоита	Публикация эксплоита	Время до первого использования	Первая массовая атака
<b>Shellshock</b>	12.09.2014	2 недели	24.09.2014	1 день	25.09.2014
<b>Eternal Blue</b>	n/a	n/a	14.04.2017	1 неделя	21.04.2017 12.05.2017
<b>CVE-2018-15982</b>	28.08.2018	3,5 месяца	05.12.2018	1 сутки	07.12.2018
<b>Blue Keep</b>	14.05.2019	2 месяца	25.07.2019	4 месяца	04.11.2019

# vs динамика защиты инфраструктур – патчи



- Критические уязвимости ОС – 42 дня
- Критические уязвимости прикладного ПО
  - Исправление наложенными средствами – до 20 дней
  - Устранение – от 90 дней



- Критические уязвимости ОС – от 2 месяцев
- Критические уязвимости прикладного ПО – от 120 дней
- Критические уязвимости АСУ ТП – .....

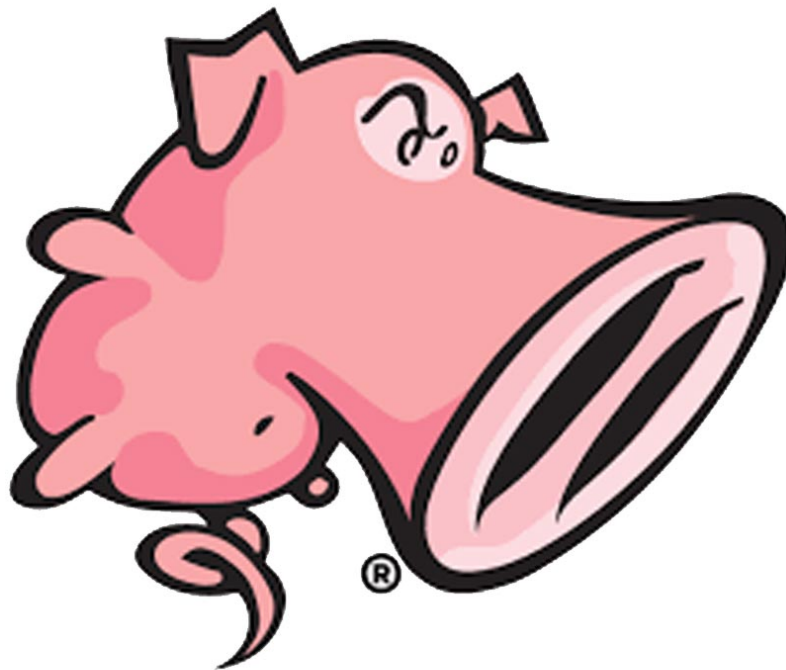


- Критические уязвимости ОС – от 4 месяцев
- Критические уязвимости прикладного ПО – ....

# Ключевое в патч-менеджменте – коммуникация



# Или сигнатуры на IDS и NTA



# Выше?



**Ростелеком**  
Солар

# Почтовый фишинг как бич нового времени

Тема: Форум iFin-2019  
Прикрепленные файлы: Письмо.html, Priglashenie.zip

Форум iFin-2019 – это центральное мероприятие в России, посвященное электронным финансам, которое проводится с 2001 года. На Форуме можно будет ознакомиться с самыми современными достижениями в области ДБО, интернет- и мобильного банкинга, финансовых маркетплейсов и экосистем, узнать о применении в дистанционном обслуживании инновационных технологий, включая демонстрацию искусственного интеллекта в банковской сфере, биометрии, вычислений в оперативной памяти, облачных технологий, открытых API, новых средств информационной безопасности и многое другое. В деловой программе Форума – всестороннее обсуждение новейших технологий и практических примеров их использования, представленных ведущими банками и разработчиками.

Участие двух представителей от кредитных организаций – бесплатное (при условии предварительной регистрации). Поспешите зарегистрироваться. Заполните анкету в приложенном архиве и перешлите нам. Вы получите два бесплатных приглашения и название Вашего банка будет размещено на официальном портале форума.

# Песочница – не панацея

- Наблюдается рост установщиков вредоносного ПО, использующих **цепочки вызовов легальных утилит**, уже расположенных на хосте:
  - Regsvr32.exe
  - Wmic.exe
  - Hh.Exe
  - и многих других утилит, исполняющих код, переданные им либо через командную строку напрямую, либо через файл, приведенный как аргумент, либо как интернет-ссылка
- В результате процесс установки вредоносного ПО разделяется между вызовами этих легальных утилит и автоматические средства детектирования **не успевают объединить** этот процесс для выявления установки ВПО в систему
- Есть примеры **обхода белых списков** за счет технологии

# Песочница – не панацея



# Повышение осведомленности сотрудников



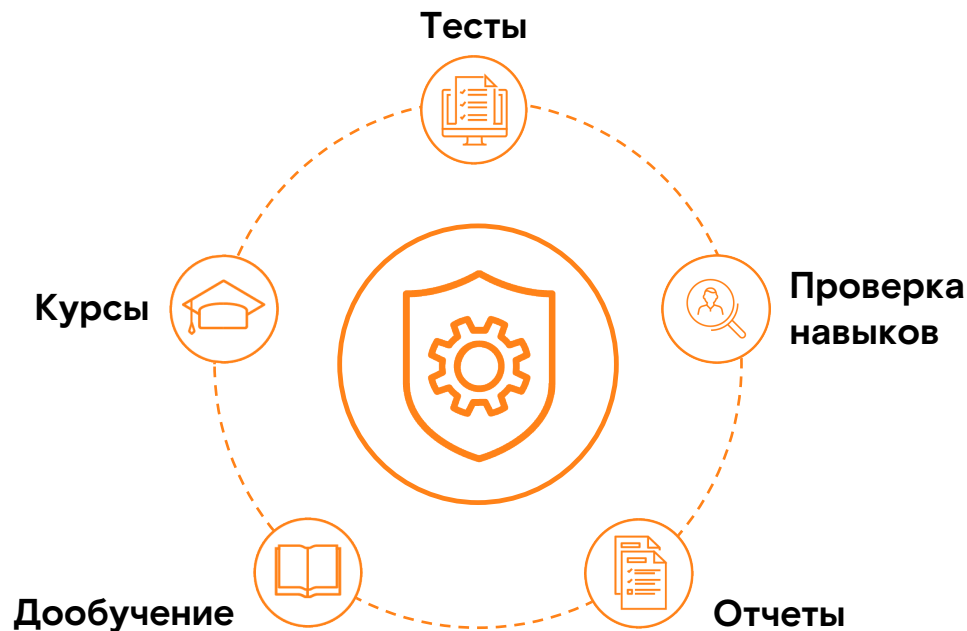
# Обучил и спишь спокойно

12

После обучения на атаки социальной инженерии поддается лишь каждый 12-й пользователь вместо каждого 7-го

64%

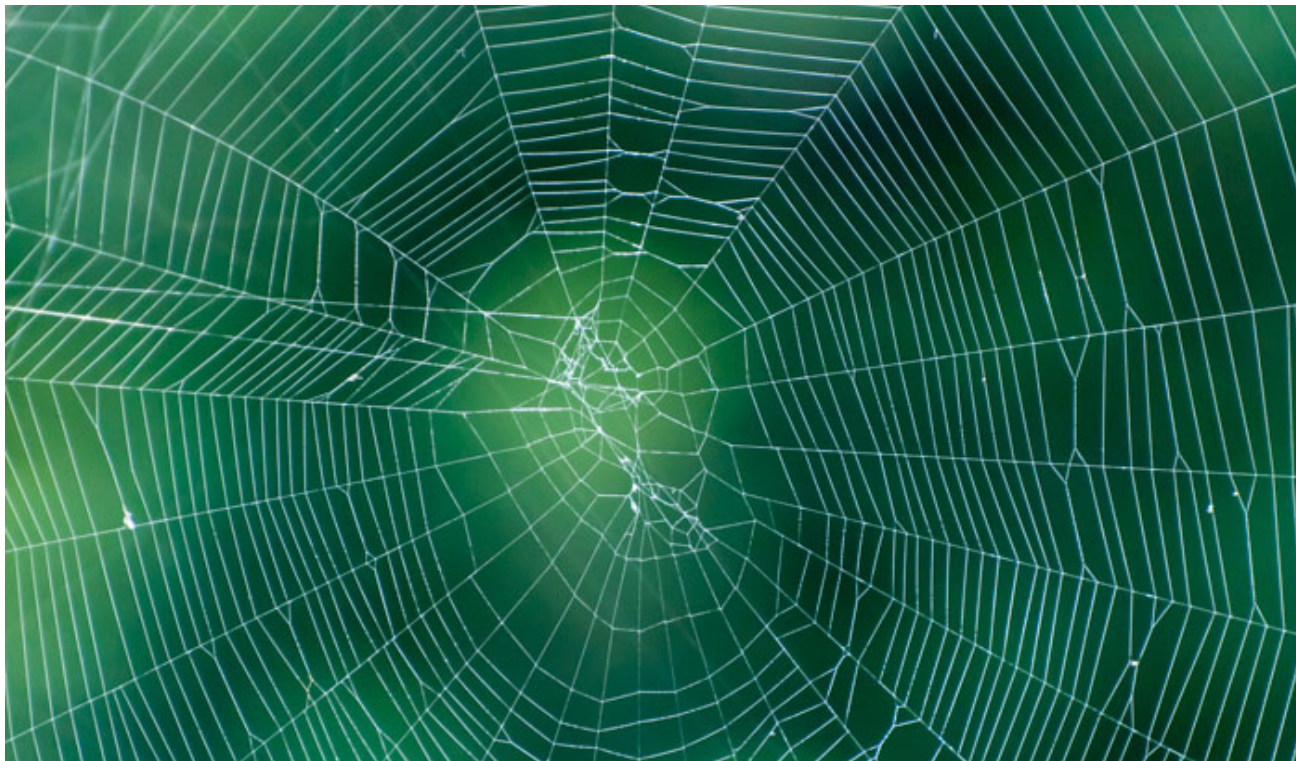
На столько обучение снижает количество кликов по фишинговым письмам



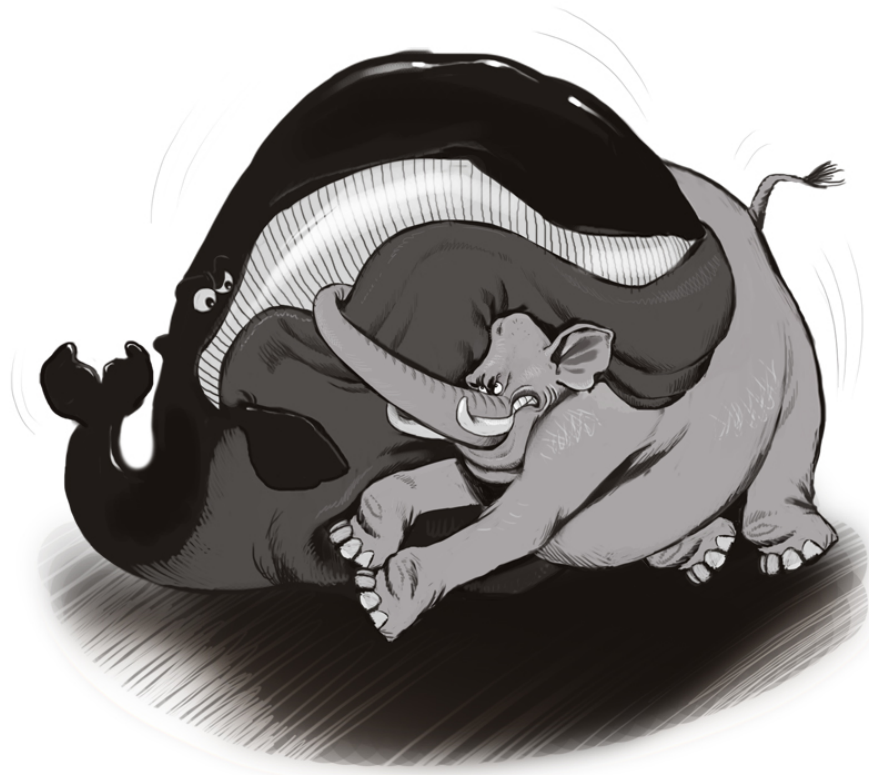
Все равно 1/12 открое



# Ключ – в обратной связи



Сильнее?

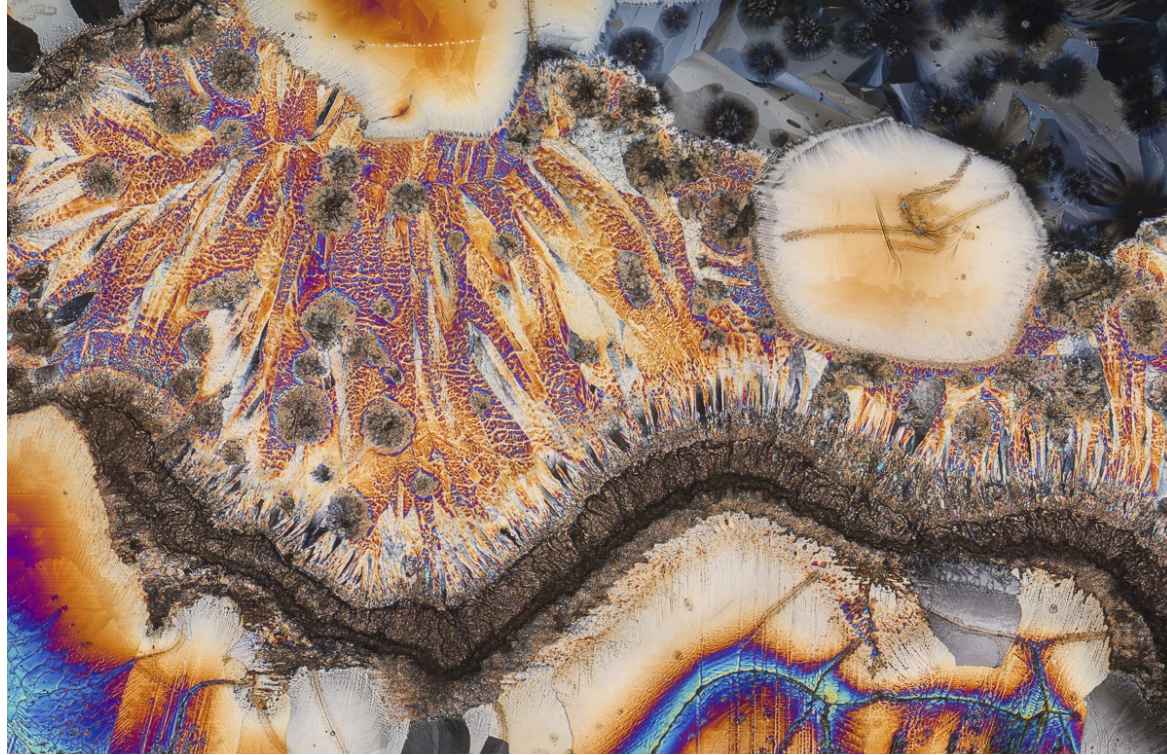


**Ростелеком**  
Солар

# Кто наш противник?



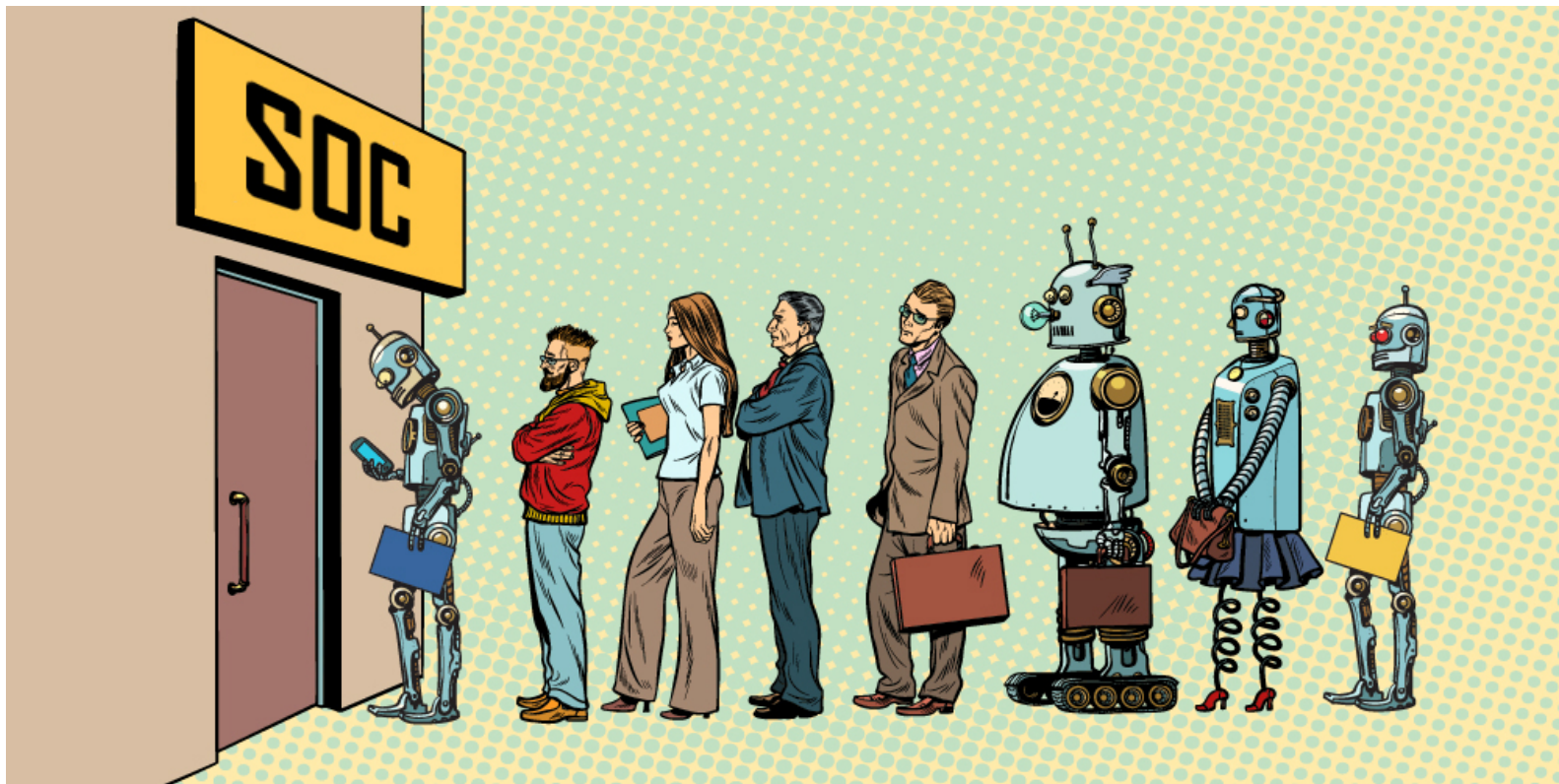
# Методы противодействия – full view



# С бесконечным объемом поддержания состояния



# Методы противодействия – технологии



# С обеспечением контекстом



# Методы противодействия – непрерывная экспертиза



# В условиях кадрового голода



# Конечно, если мы не знаем кодов...

The screenshot shows the 'cheat happens' website interface. At the top left is the logo 'ch cheat happens'. To the right, it says 'Customized For: CHEATHAPPENS MEMBER'. Below this is a navigation bar with buttons for 'Hotkeys', 'Joystick', 'Instructions', 'Help', and 'Debug'. The 'Hotkeys' button is selected, displaying a list of cheat codes for DOOM 2016. To the right of the list is a promotional image for DOOM with the text 'CLICK BOX FOR FULL TRAINER' and 'CLICK ON BOX FOR SUPPORT'. At the bottom right, there is a 'Game Not Found' button.

ch cheat happens

Customized For: CHEATHAPPENS MEMBER

DOOM 2016 MEGA TRAINER PROMO Steam Version Self Updating

Hotkeys Joystick Instructions Help Debug

Numpad 1: Mega Health  
Numpad 2: Unlimited Ammo  
Numpad 3: Fast Cooldown Weapon  
Numpad 4: Fast Chargeup Weapon  
Numpad 5: Instant Grenades  
Numpad 6: Super Armor  
Numpad 7: Easy Kills  
Numpad 8: Weapon Currency  
Numpad 9: Suit Token Currency  
Numpad 0: Float Mode  
Numpad -: Float Up  
Numpad +: Float Down  
Numpad /: Save Position  
Numpad \*: Teleport  
Numpad .: Unlimited Chainsaw  
F9: Unlimited Rune Timer

Notes

CLICK BOX FOR FULL TRAINER

CLICK ON BOX FOR SUPPORT

Game Not Found

Дешевле

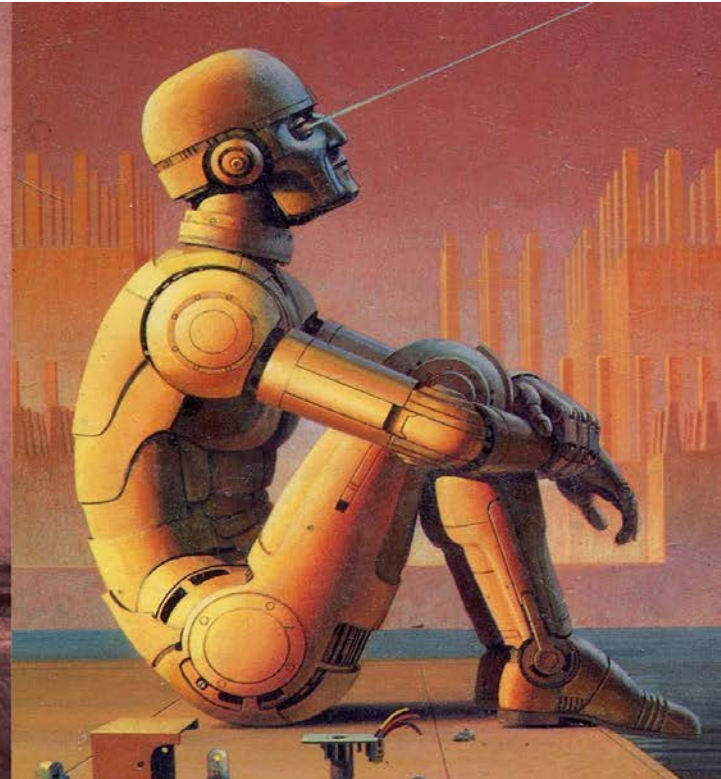


**Ростелеком**  
Солар

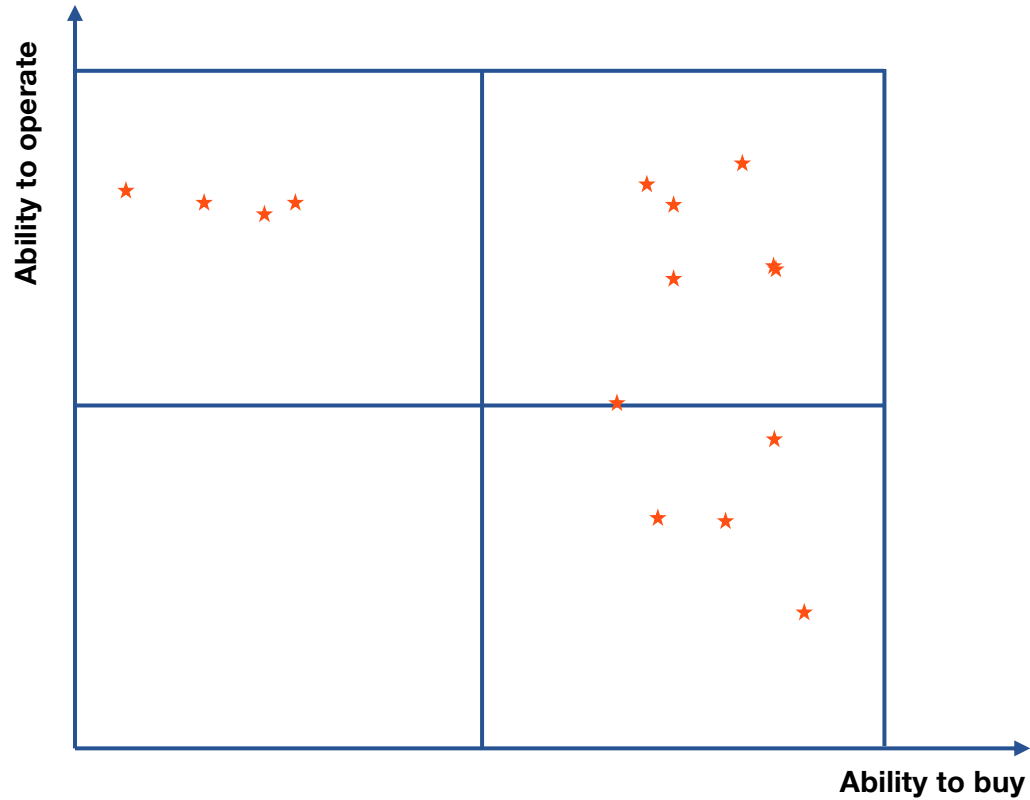
# System как замена EDR? Opensource SIEM?



# Нелегкий выбор безопасника



# Новый квадрант Gartner для SOC



# Дорогу осилит идущий



**Ростелеком**  
Солар



# Спасибо за внимание!

Владимир Дрюков  
Директор Solar JSOC

Ростелеком  
Солар

