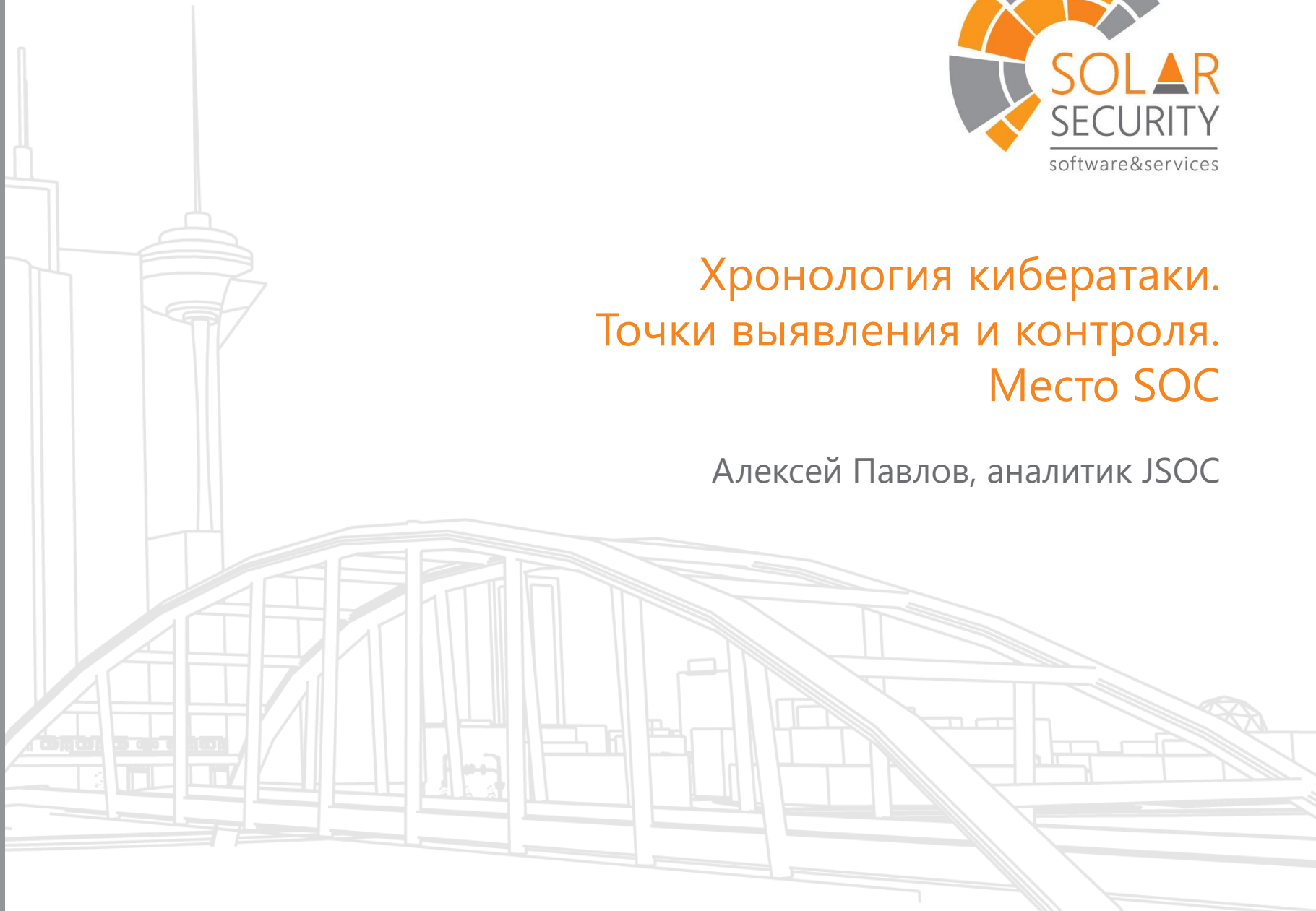




Хронология кибератаки. Точки выявления и контроля. Место SOC

Алексей Павлов, аналитик JSOC



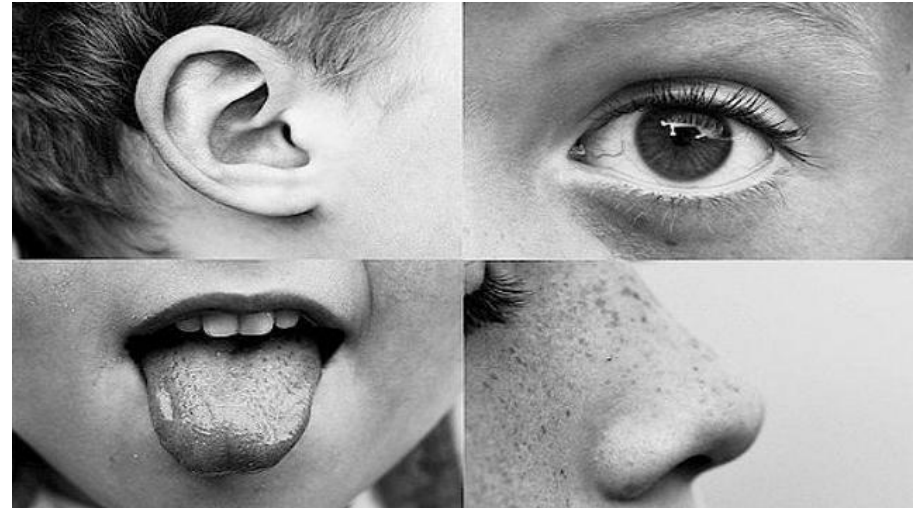
Поиск цифрового следа на всех этапах атаки

- ❖ Проникновение в инфраструктуру
- ❖ Повышение привилегий
- ❖ Получение доступа к ключевым системам (ERP, CRM, АБС, процессинг)
- ❖ Хищение информации, вывод денежных средств



4 чувства для поиска злоумышленника

- ❖ Сетевые коммуникации (включая локальные)
- ❖ Аутентификация в ОС и приложениях
- ❖ Работа с ключевыми файлами и объектами ОС
- ❖ Операции с приложениями/сервисами



Шаг первый: Точка входа в инфраструктуру



Социальная инженерия

Распространение вредоносов

Штатные механизмы передачи данных

Взлом VPN

...



Точка входа в инфраструктуру

Индикаторы

Социальная инженерия

- Mail AV
- Репутационные базы
- Последующая активность на рабочей станции

Распространение вредоносов

- Репутационные базы
- Контроль процессов/файлов/реестра на критичных машинах

Штатные механизмы передачи данных

- AV / Mail AV

Взлом VPN

- Логи VPN
- Профили пользователей



Шаг второй: Обустройство. Типовые шаги

Массовая
рассылка писем
с вредоносами

Повышение
привилегий

Callback:
получение
команд от
управляющих
серверов

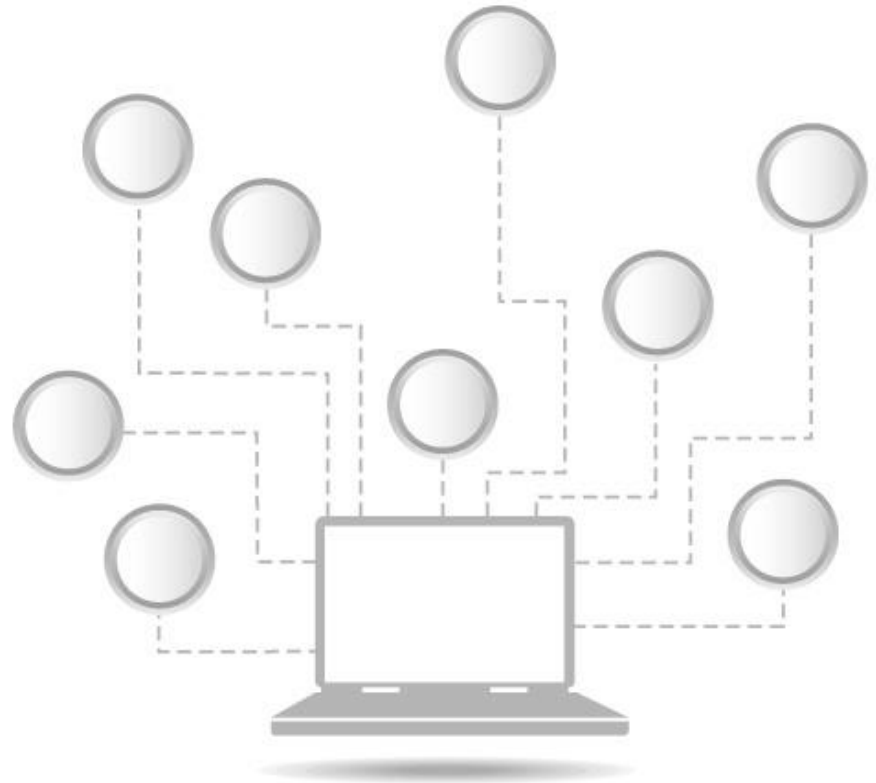
RemoteAdmi
nTools

Сканирование
хостов, портов



Получение доступа
к целевой рабочей станции

- ❖ Opensource базы
- ❖ Репутационные базы вендоров
- ❖ Информация с СЗИ
- ❖ Собственная информация JSOC
- ❖ Технологические партнеры
- ❖ Партнерства с CERT



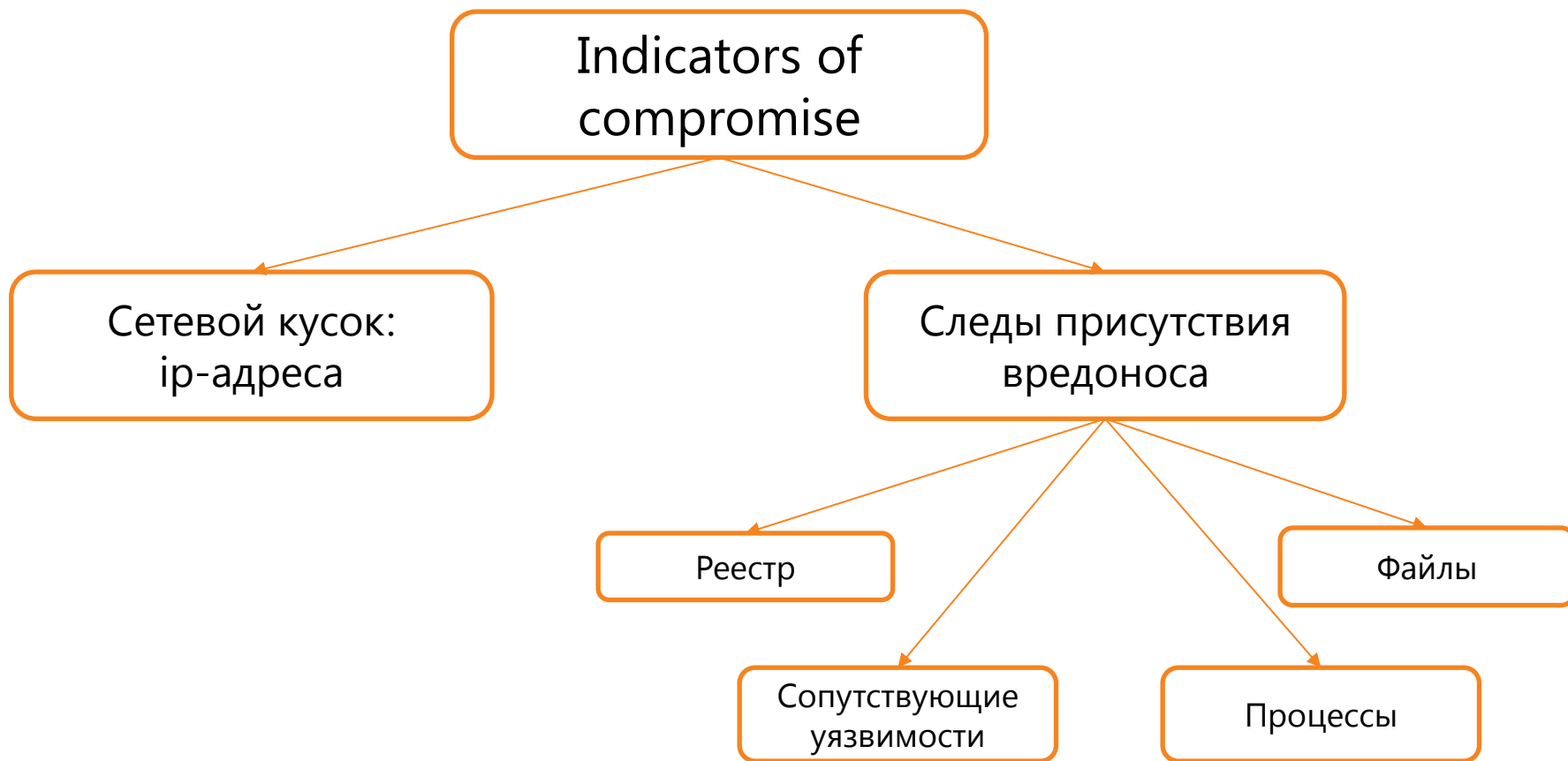


Анализ ИОС

Ретроспективный
анализ

Оповещение
Заказчиков

Добавление
сигнатур



Источники:

- ❖ Контроллеры домена
- ❖ Сетевые устройства – МСЭ, Прокси
- ❖ Локальные логи

Сценарии срабатывания:

- ❖ Встроенная категоризация сетевых устройств
- ❖ Алерты по известным портам

Расследование:

- ❖ Анализ сетевой активности
- ❖ Проверка запускаемых процессов (если хост подключен)

Эскалация:

- ❖ Ночное время
- ❖ Критичные хосты



Кейс: Remote admin tools

18 Jul 2015 03:08:02 MSK Зафиксирован инцидент: Запуск RemoteAdminTools на хосте

Исходные данные:

- ❖ Машина руководителя отдела
- ❖ Локальные логи недоступны

Расследование:

- ❖ Оповещение аналитика
- ❖ Согласование с Заказчиком подключения машины к JSOC
- ❖ Подключение хоста. Для организации ретроспективного анализа – в agent properties «startatend=false»

Кейс: Remote admin tools

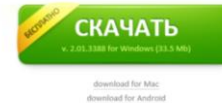
Пример уведомления

Зафиксирован инцидент "Исходящая активность RemoteAdminTools на хосте"

1. Название инцидента:	Исходящая активность <u>RemoteAdminTools</u> на хосте
2. Дата и время инцидента:	18 Jul 2015 03:08:02 MSK
3. Подробное описание инцидента:	<p>На хосте [REDACTED] (ip-адрес [REDACTED]) зафиксирован запуск средств удаленного администрирования <u>ушрс</u> по категоризация bluecoat.</p> <p>Попытки доступа на ip-адрес 173.193.202.79 блокируются ACL.</p> <p>Данная активность на хосте выявлена впервые. Активного пользователя на хосте в момент инцидента выявить не удалось. Последняя активность была зарегистрирована 17 июля в 18.59, учетная запись: [REDACTED]</p>
4. Каким образом обнаружен инцидент:	Анализ событий Bluecoat.
5. Причина возникновения:	Использование средств удаленного доступа/администрирования на хосте.
6. Информация об источнике события:	<p>===== Информация о системе ===== Хост инициатора: [REDACTED] Сетевая зона: [REDACTED]_user1_vlan100_10.0.0.0</p> <p>===== Информация о пользователе ===== ФИО: [REDACTED] Должность: Начальник Управления Организация: [REDACTED] Подразделение: Управление администрации и делопроизводства Телефон: [REDACTED]</p>
7. Информация о цели события:	inetnum: 173.193.202.79 netname: vuupc.com country: Brazil
8. Рекомендация по расследованию ответственному:	Проверить легитимность использования средств удаленного администрирования. В случае отрицательного результата удалить запрещенное ПО.
9. Примечание:	<u>Ушрс</u> это программа для удаленного доступа к компьютеру/рабочему столу с другого компьютера или мобильного устройства, подключенного к интернету. На некоторых ресурсах эту программу причисляют к <u>зловредам</u> .

- ❖ 17 Jul 2015 17:23:44 MSK Запуск MediaGet
- ❖ 17 Jul 2015 18:59:14 MSK Логаут пользователя, блокировка компьютера
- ❖ 18 Jul 2015 03:07:57 MSK Запуск процесса vuurc.exe
- ❖ 18 Jul 2015 03:08:02 MSK Инцидент
- ❖ 18 Jul 2015 03:26:00 MSK Оповещение аналитика по телефону
- ❖ 18 Jul 2015 03:32:48 MSK Оповещение от 1-й линии в сторону Заказчика
- ❖ 18 Jul 2015 03:55:00 MSK подключение машины к ArcSight

MediaGet - ищи, качай, смотри!
Самое простое приложение в сети Интернет для поиска и скачивания файлов



Kaspersky not-a-virus:Downloader.Win32.MediaGet.dxo

Microsoft ✔

Name	Destination Process Name	File Name	Device Custom String3	Device Custom String5
A new process has been created.	C:\Windows\System32\PING.EXE	ping_ya.ru	0x10c64	0x10f58
A new process has been created.	C:\Windows\System32\cmd.exe	"C:\WINDOWS\system32\cmd.exe"	0x10f58	0x2cc

Шаг третий: контроль за целевой станцией



Операции в
домене

Отклонение от
профиля,
несоответствия
учетных данных

Изменения на
критичных
хостах –
процессы,
файлы, реестр

❖ Skeleton key – использование любой учетной записи в домене без пароля

1. Upload the Skeleton Key DLL file to a staging directory on a jump host in the victim's network. CTU researchers have observed three filenames associated with the Skeleton Key DLL file: ole64.dll, ole.dll, and msuta64.dll. Windows systems include a legitimate ole32.dll file, but it is not related to this malware.
2. Attempt to access the administrative shares on the domain controllers using a list of stolen domain administrator credentials.
3. If the stolen credentials are no longer valid, use password theft tools to extract clear text domain administrator passwords from one of the following locations, which suggest a familiarity with the victim's environment:
 - memory of another accessible server on the victim's network
 - domain administrators' workstations
 - targeted domain controllers
4. Use valid domain administrator credentials to copy the Skeleton Key DLL to C:\WINDOWS\system32\ on the target domain controllers.
5. Use the **PsExec** utility to run the Skeleton Key DLL remotely on the target domain controllers using the rundll32 command. The threat actor's chosen password is formatted as an NTLM password hash rather than provided in clear text. After Skeleton Key is deployed, the threat actor can authenticate as any user using the threat actor's configured NTLM password hash:


```
psexec -accepteula \\%TARGET-DC% rundll32 <DLL filename> ii <NTLM password hash>
```
6. Delete the Skeleton Key DLL file from C:\WINDOWS\system32\ on the targeted domain controllers.
7. Delete the Skeleton Key DLL file from the staging directory on the jump host.
8. Test for successful Skeleton Key deployment using "net use" commands with an AD account and the password that corresponds to the configured NTLM hash.

ATTRIBUTE	VALUE OR DESCRIPTION
Filename	ole64.dll
MD5	bf45086e6334f647fda33576e2a05826
SHA1	5083b17ccc50dd0557dfc544f84e2ab55d6acd92
Compile time	2014-02-19 09:31:29
Deployed	As required (typically downloaded using malware and then deleted after use)
File size	49664 bytes
Sections	.text, .rdata, .data, .pdata, .rsrc, .reloc
Exports	ii (installs the patch) uu (uninstalls the patch) DllEntryPoint (default DLL entry point)

ATTRIBUTE	VALUE OR DESCRIPTION
Filename	msuta64.dll
MD5	66da7ed621149975f6e643b4f9886cfd
SHA1	ad61e8daeeba43e442514b177a1b41ad4b7c6727
Compile time	2012-09-20 08:07:12
Deployed	2013-09-29 07:58:16
File size	50688 bytes
Sections	.text, .rdata, .data, .pdata, .rsrc, .reloc
Exports	i (installs the patch) u (uninstalls the patch) DllEntryPoint (default DLL entry point)

Шаг Четвертый: поход за информацией, деньгами



Аутентификации
в нерабочее
время

Использование
технологических
УЗ

Нестандартные
механизмы
подключения
к БД

Изменения на
критичных
серверах –
процессы,
файлы, реестр

1. Определение систем зоны риска:


- ❖ Возможность финансовых операций
- ❖ Чувствительные к публикации данные
- ❖ Интересны для конкурентов

2. Выделение критичных сотрудников:

- ❖ ИТ и ИБ – администраторы
- ❖ Владельцы систем
- ❖ Профильные отделы компаний
- ❖ Руководители

3. Приоритезация срабатываний:

- ❖ Частотность (массовый инцидент)
- ❖ Системы зоны риска
- ❖ Критичные пользователи



Спасибо!
Вопросы?

Павлов Алексей
av.pavlov@solarsecurity.ru

+7 (916) 178 98 90