



КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ



06 декабря 2018 г.  
г. Астана

# Автоматизация реагирования на инциденты информационной безопасности

---

Игорь Сметанев

Коммерческий директор R-Vision  
[Smetanev@rvision.pro](mailto:Smetanev@rvision.pro)

#CODEIB



# С чем сталкивается среднестатистический CISO?

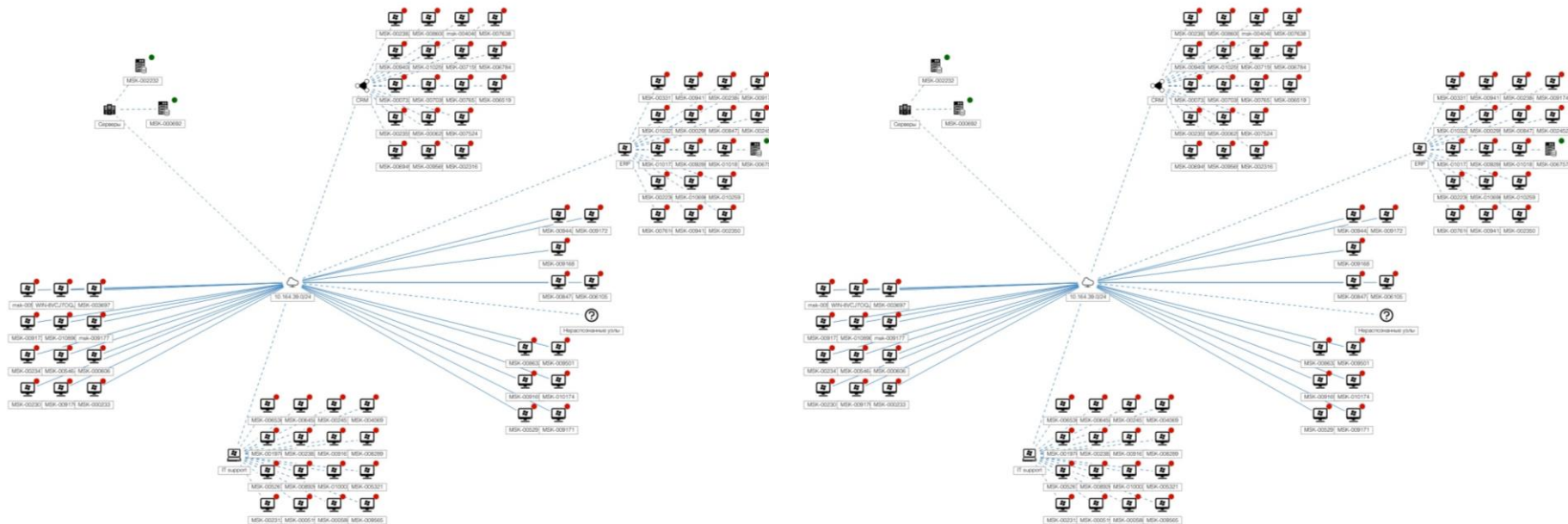
# Не хватает людей



- ✓ Администрирование
- ✓ Отчетность
- ✓ Аудиты и compliance
- ✓ Реагирование на инциденты

• 2-3 специалиста

# Гетерогенная инфраструктура



- критичность информационных систем
- критичность простоя бизнеса
- критичность потери информации

# «Зоопарк» средств защиты

 KASPERSKY Lab



INFOWATCH®

POSITIVE TECHNOLOGIES

 MICRO FOCUS

 QUINERS .COM

 АПФ OKB

 АЛТАКС  
C O O T



Symantec™

 | GROUP | IB |  
GLOBAL CYBER SECURITY COMPANY



КОД БЕЗОПАСНОСТИ



Qualys®

 McAfee™  
Together is power.

# Инциденты ИБ, требующие реагирования

- **Примеры типов инцидентов**

Компрометация ключевой информации, персональных идентификаторов, паролей	Внешние атаки/вторжения (DDoS, др.)	Сбои в работе программного обеспечения АИС
Компрометация ключа ЭП работника Организации	Выявления атак типа «отказ в обслуживании»	Недоступность критичных систем
Несанкционированное создание, удаление, блокировка, разблокировка учетных записей	Выявления попыток осуществления вторжений и сетевых атак	Выявленные уязвимости в информационных системах
Утрата работником персонального идентификатора (ТМ, Smart-карт)	Ошибки в логике работы IPS	Несанкционированное изменение ПО АРМ пользователей
Передача другим лицам пользовательских идентификаторов и паролей	.....	Несанкционированный запуск программных процессов
.....	.....	.....
.....	.....	.....

Инциденты влияют на бизнес!

Автоматизируем то, что можно  
автоматизировать

# Дирижирование безопасности



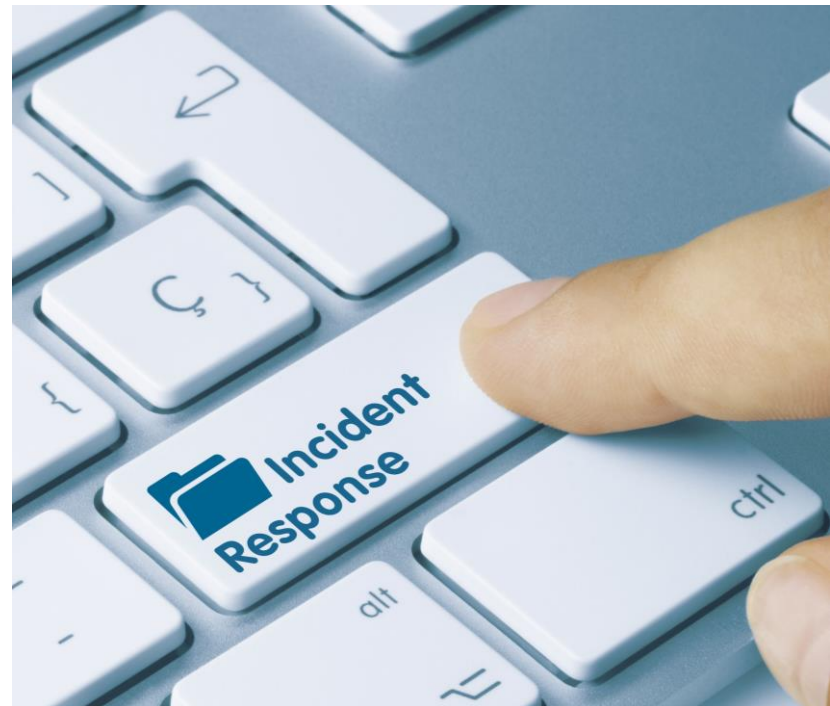


IRP  
(Incident Response Platform)

или SOAR  
(Security Orchestration Automation  
& Response)

# Реагирование на инциденты в 1 клик

- ✓ Агрегация данных по активам, инцидентам, уязвимостям
- ✓ Целостная картина по инциденту
- ✓ Автоматические сценарии реагирования по каждому типу инцидента – (roadmap инцидента)
- ✓ Автоматизация действий по реагированию
- ✓ Информационный обмен данными, отправка сведений по инцидентам в CERT



# Контроль ИТ-активов



RVision **Активы** Инциденты Уязвимости Система защиты Аудит и контроль Риски Задачи Отчеты Настройки admin

Организация Бизнес-процесс Информация Оборудование Группа ИТ-активов ПО Сеть Домены Персонал Помещение

Имя устройства	Домен / Рабочая г...	IP-адрес	Операционная сис...	Тип	S:...	S:AV	S:I...	S:...	S:FW	Количество...	Уязв...	Количество инцид...
192.168.23.83		192.168.23.83		Нераспознанный узел	⊙	⊙	⊙	⊙	⊙			
192.168.23.9		192.168.23.9		Нераспознанный узел	⊙	⊙	⊙	⊙	⊙			
BRW008092A51484		192.168.23.252		Нераспознанный узел	⊙	⊙	⊙	⊙	⊙			
centos6		192.168.23.34	CentOS release 6.7 ...	Почтовый сервер	⊙	⊙	⊙	⊙	⊙			
DC2	rmlab.local	192.168.23.5	Microsoft Windows S...	Контроллер домена...	⊙	⊙	⊙	⊙	⊙			
debian-srv		192.168.23.39, 192....	Debian GNU/Linux 7...	Роутер	⊙	⊙	⊙	⊙	⊙			
DEBIAN-SRV		192.168.23.35		Нераспознанный узел	⊙	⊙	⊙	⊙	⊙			
debian-srv-25228		192.168.100.35	Linux	Сервер Linux / Unix	⊙	⊙	⊙	⊙	⊙			
EXCHSRV	rmlab.local	192.168.23.22	Microsoft Windows S...	Почтовый сервер	⊙	⊙	⊙	⊙	⊙			
HYPER-SRV test description	rmlab.local	192.168.23.200	Microsoft Windows S...	Сервер базы данных	⊙	⊙	⊙	⊙	⊙			
mainsrv		192.168.23.8	Ubuntu 14.04.2 LTS	Сервер Linux / Unix	⊙	⊙	⊙	⊙	⊙			
NOTE		192.168.23.227		Нераспознанный узел	⊙	⊙	⊙	⊙	⊙			
R1		192.168.100.1, 192....	Cisco IOS Software ...	Роутер	⊙	⊙	⊙	⊙	⊙			
REDCHECK2	rmlab.local	192.168.23.67	Microsoft Windows S...	Сервер базы данных	⊙	⊙	⊙	⊙	⊙			
rhel7-srv1		192.168.23.31	Red Hat Enterprise L...	Почтовый сервер	⊙	⊙	⊙	⊙	⊙			1
rvision		192.168.23.155	Ubuntu 14.04.3 LTS	Сервер Linux / Unix	⊙	⊙	⊙	⊙	⊙			
WIN2K3-64-R2	rmlab.local	192.168.23.53	Microsoft Windows S...	Сервер Windows	⊙	⊙	⊙	⊙	⊙			1
WIN2K8-SRV2-2	rmlab.local	192.168.23.16	Microsoft Windows S...	Сервер Windows	⊙	⊙	⊙	⊙	⊙			2
WIN7-32-RUS-1	rmlab.local	192.168.23.91	Microsoft Windows 7...	Рабочая станция Wi...	⊙	⊙	⊙	⊙	⊙			6
WIN7-64-ENG	rmlab.local	192.168.23.225	Microsoft Windows 7	Рабочая станция Wi...	⊙	⊙	⊙	⊙	⊙			1
WIN7-DESK-2	rmlab.local	192.168.23.193	Microsoft Windows 7...	Рабочая станция Wi...	⊙	⊙	⊙	⊙	⊙			1
WIN8-PRO	rmlab.local	192.168.23.174	Microsoi: Windows 8...	Рабочая станция Wi...	⊙	⊙	⊙	⊙	⊙			
WIN-SC		192.168.23.23		Нераспознанный узел	⊙	⊙	⊙	⊙	⊙			1
WIN-TK316AELVQL	rmlab.local	192.168.23.3	Microsoft Windows S...	Контроллер домена...	⊙	⊙	⊙	⊙	⊙			2

**Запустить сканирование**

Исключить из сканирования

Имя устройства:  
192.168.100.17

+ IP-адрес      MAC-адрес  
x 192.168.100.17

Домен / Рабочая группа:  
▼

Операционная система:  
▼

Виртуальная машина:  
Нет ▼

Тип узла:  
Нераспознанный узел ▼

Статус:  
▼

Группы ИТ-активов:  
▼

Владелец актива:  
▼

Администратор безопасности:  
▼

Аудитор безопасности:  
▼

Менеджер по контролю соответствия:  
▼

Теги:  
▼

Город:  
▼

# Управление уязвимостями

Все уязвимости CRM x Серверы x АСУТП x

Идентифика...	Уровень	Название	Прогресс	Количество хост...	Источник
NS-111754		Deprecated / Disabled Plugins in Scan Policy - Notice	99% выполнено	68 ⇄	Nessus
NS-105788		VMware Tools 10.x < 10.2.0 Multiple Vulnerabilities (VMSA-2018-...	93% выполнено	14 ⇄	Nessus
NS-110990		Security Updates for Microsoft .NET Framework (July 2018)	90% выполнено	10 ⇄	Nessus
NS-83298		SSL Certificate Chain Contains Certificates Expiring Soon	90% выполнено	30 ⇄	Nessus
NS-42981		SSL Certificate Expiry - Future Expiry	90% выполнено	30 ⇄	Nessus
NS-71262		Reputation of Linux Executables: Never seen process(es)	89% выполнено	19 ⇄	Nessus
NS-110981		KB4338824: Windows 8.1 and Windows Server 2012 R2 July 20...	89% выполнено	9 ⇄	Nessus
NS-110991		Security Updates for Internet Explorer (July 2018)	89% выполнено	9 ⇄	Nessus
NS-103131		Windows 8.1 and Windows Server 2012 R2 September 2017 Se...	88% выполнено	8 ⇄	Nessus
NS-78432		MS14-057: Vulnerabilities in .NET Framework Could Allow Remo...	86% выполнено	7 ⇄	Nessus
NS-110484		KB4284878: Windows 8.1 and Windows Server 2012 R2 June 20...	83% выполнено	6 ⇄	Nessus
NS-110494		Security Updates for Internet Explorer (June 2018)	83% выполнено	6 ⇄	Nessus
NS-108295		Security Updates for Internet Explorer (March 2018)	83% выполнено	12 ⇄	Nessus
NS-105188		Security Updates for Internet Explorer (December 2017)	80% выполнено	10 ⇄	Nessus
NS-11153		Service Detection (HELP Request)	80% выполнено	10 ⇄	Nessus
NS-105185		Windows 8.1 and Windows Server 2012 R2 December 2017 Sec...	80% выполнено	10 ⇄	Nessus
NS-104894		Security Updates for Internet Explorer (November 2017)	78% выполнено	9 ⇄	Nessus
NS-106800		KB4074597: Windows 8.1 and Windows Server 2012 R2 Februar...	77% выполнено	13 ⇄	Nessus
NS-106804		Security Updates for Internet Explorer (February 2018)	77% выполнено	13 ⇄	Nessus
NS-105546		Security Updates for Internet Explorer (January 2018)	77% выполнено	13 ⇄	Nessus
NS-12634		Authenticated Check : OS Name and Installed Package Enumera...	75% выполнено	4 ⇄	Nessus
NS-107220		Google Chrome < 65.0.3325.146 Multiple Vulnerabilities	75% выполнено	4 ⇄	Nessus
NS-44657		Linux Daemons with Broken Links to Executables	75% выполнено	16 ⇄	Nessus



Дата обнаружения [UTC+03:00]

09.08.2018 23:44:15

Дата открытия [UTC+03:00]

10.08.2018 08:57:01

Дата последнего обновления [UTC+03:00]

08.09.2018 00:24:55

Прогресс устранения уязвимости:

90%

Источник:

Nessus

Описание:

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Связанные активы:

Тип	Количество
Сети	5 ⇄
Группы активов	7 ⇄

Связанное оборудование (показать все):

Тип	Количество
Сервер Windows	13 ⇄
Сервер Linux / Unix	6 ⇄

# Управление инцидентами



Все внутренние инциденты Внешние инциденты Критичные инциденты Инциденты в работе Инциденты DoS/DDoS Инциденты за ноябрь 2017 KFP JSOC Bot-Trek Инциденты ArcSight Инциденты ВПО

ID	Тип инцидента	Дата создания инци...	Категория	Статус инцидента	Уровень инцидента	Ответственный
17-11-216	Несанкционированная передача (утечка) информа...	2 ноября 2017 г., 11:55	Общий инцидент	Закрыт		Роман Семенов (rsemenov@rvlab.net)
17-11-3655	Несанкционированный доступ к информации	23 ноября 2017 г., 23:42	Событие безопасности	Открыт		
17-11-3682	Внедрение вредоносного кода	26 ноября 2017 г., 00:10	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-3713	Внедрение вредоносного кода	26 ноября 2017 г., 00:12	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-2287	Нарушение доступности онлайн-сервисов органи...	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Михаил Симонов (msimonov@rvlab.net)
17-11-2290	Сбой / отказ в работе программного обеспечения	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Алексей Иванов (aivanov@rvlab.net)
17-11-219	Внедрение вредоносного кода	2 ноября 2017 г., 11:55	Общий инцидент	Закрыт		Мозгов Михаил (mmozgov@rvlab.net)
17-11-2288	Компрометация средств аутентификации / авториз...	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Иван Петров (ipetrov@rvlab.net)
17-11-220	Компрометация средств аутентификации / авториз...	2 ноября 2017 г., 11:55	Общий инцидент	Закрыт		Михаил Симонов (msimonov@rvlab.net)
17-11-2291	Несанкционированная печать конфиденциальной ...	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-245	Подозрение на инцидент (событие ИБ)	2 ноября 2017 г., 11:55	JSOC Инцидент	Обработка		Николай Ручкин (nruchkin@rvlab.net)
17-11-244	Подозрение на инцидент (событие ИБ)	2 ноября 2017 г., 11:55	JSOC Инцидент	Обработка		Петр Ложкин (plozkin@rvlab.net)
17-11-117	Внедрение вредоносного кода	2 ноября 2017 г., 11:54	Общий инцидент	Закрыт		Joseph, Reece (a794659@rvlab.net)
17-11-116	Нарушение доступности онлайн-сервисов органи...	2 ноября 2017 г., 11:54	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-1512	Несанкционированная печать конфиденциальной ...	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-2316	Внедрение вредоносного кода	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Мозгов Михаил (mmozgov@rvlab.net)
17-11-241	Внедрение вредоносного кода	2 ноября 2017 г., 11:55	Общий инцидент (подробно)	Закрыт		Алексей Иванов (aivanov@rvlab.net)
17-11-115	Внедрение вредоносного кода	2 ноября 2017 г., 11:54	Общий инцидент	Закрыт		Алексей Иванов (aivanov@rvlab.net)
17-11-1510	Несанкционированная (подозрительная) активность	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Иван Дмитриев (dmitriev@rvlab.net)
17-11-1508	Нарушение доступности онлайн-сервисов органи...	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Михаил Симонов (msimonov@rvlab.net)
17-11-1509	Компрометация средств аутентификации / авториз...	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Иван Петров (ipetrov@rvlab.net)
17-11-1511	Сбой / отказ в работе программного обеспечения	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Алексей Иванов (aivanov@rvlab.net)
17-11-2315	Несанкционированная печать конфиденциальной ...	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Николай Ручкин (nruchkin@rvlab.net)
17-11-2317	Нарушение доступности онлайн-сервисов органи...	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Михаил Симонов (msimonov@rvlab.net)
17-11-1503	Сбой / отказ в работе программного обеспечения	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-1504	Несанкционированная печать конфиденциальной ...	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Роман Семенов (rsemenov@rvlab.net)
17-11-2312	Компрометация средств аутентификации / авториз...	2 ноября 2017 г., 12:17	Общий инцидент	Закрыт		Gill, Sigourney (a179606@rvlab.net)
17-11-50	Несанкционированная печать конфиденциальной ...	2 ноября 2017 г., 11:54	Общий инцидент	Закрыт		Александр Невский (anevsky@rvlab.net)
17-11-1505	Внедрение вредоносного кода	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Петр Ложкин (plozkin@rvlab.net)
17-11-1506	Нарушение доступности онлайн-сервисов органи...	2 ноября 2017 г., 12:08	Общий инцидент	Закрыт		Николай Ручкин (nruchkin@rvlab.net)

## В архив

ID: 17-11-117

Категория: Общий инцидент

Тип инцидента: Внедрение вредоносного кода

Способ реализации: Внедрение вредоносного кода по сети

Статус инцидента: Закрыт

Прогресс реализации действий по реагированию: 0%

Ответственный: Joseph, Reece (a794659@rvlab.net)

Уровень инцидента: Высокий

Дата создания инцидента [UTC+03:00]: 02.11.2017 11:54:44

Дата выявления инцидента [UTC+03:00]:

Дата возникновения инцидента [UTC+03:00]:

Плановая дата устранения [UTC+03:00]: 10.10.2017 11:50:00

Дата завершения разбирательства [UTC+03:00]:

Уровень ущерба (качественная оценка):

Уровень ущерба (количественная оценка):

# Сценарии реагирования

Управление инцидентами

- Категории инцидентов
- Типы инцидентов
- Циклы обработки инцидентов
- Поля инцидентов
- Шаблоны инцидентов
- Уровни критичности
- Действия по инциденту
- Сценарии реагирования**
- Правила корреляции
- Интеграция с внешними системами
  - Справочники

Система защиты

- Типы и атрибуты документов
  - Каталоги защитных мер
- Метрики

Аудит и контроль

- Справочники
- Требования
- Контрольные проверки

Все сценарии

- Вирусная эпидемия
- Закрытие событий-иб
- Запрос информации
- Запрос событий ArcSight
- Корректирующие действия
- Проверка Windows-машины скриптами
- Проверка затронутых узлов скриптами
- Проверка сетевых настроек затронутых узлов
- Реагирование на появление хоста с запрещенным ПО
- Сценарий реагирования на сообщении о потенциальном вредоносе
- Эскалация

Плейбуки для демонстрации

- Доступ к подозрительному контенту/узлу
- Заражение вирусом-шифровальщиком**
- Компрометация доменной учетной записи

Реагирование на DDoS

- Не тестовый DDoS
- Отправить сообщение администратору

Реагирование на инциденты DLP

- Инциденты от DLP системы

Реагирование на обнаружение ПО для пентестов

- Атака обнаружена из иностранного государства
- Атака обнаружена из РФ
- Геолокация IP-адреса

Поиск...

1	Значение поля	Способ реализации	"Заражение вирусом-шифровальщиком"
2	Значение поля	Краткое описание инцидента	Заражение вирусом-шифровальщиком

Настройка критериев:

Любой из критериев должен сработать

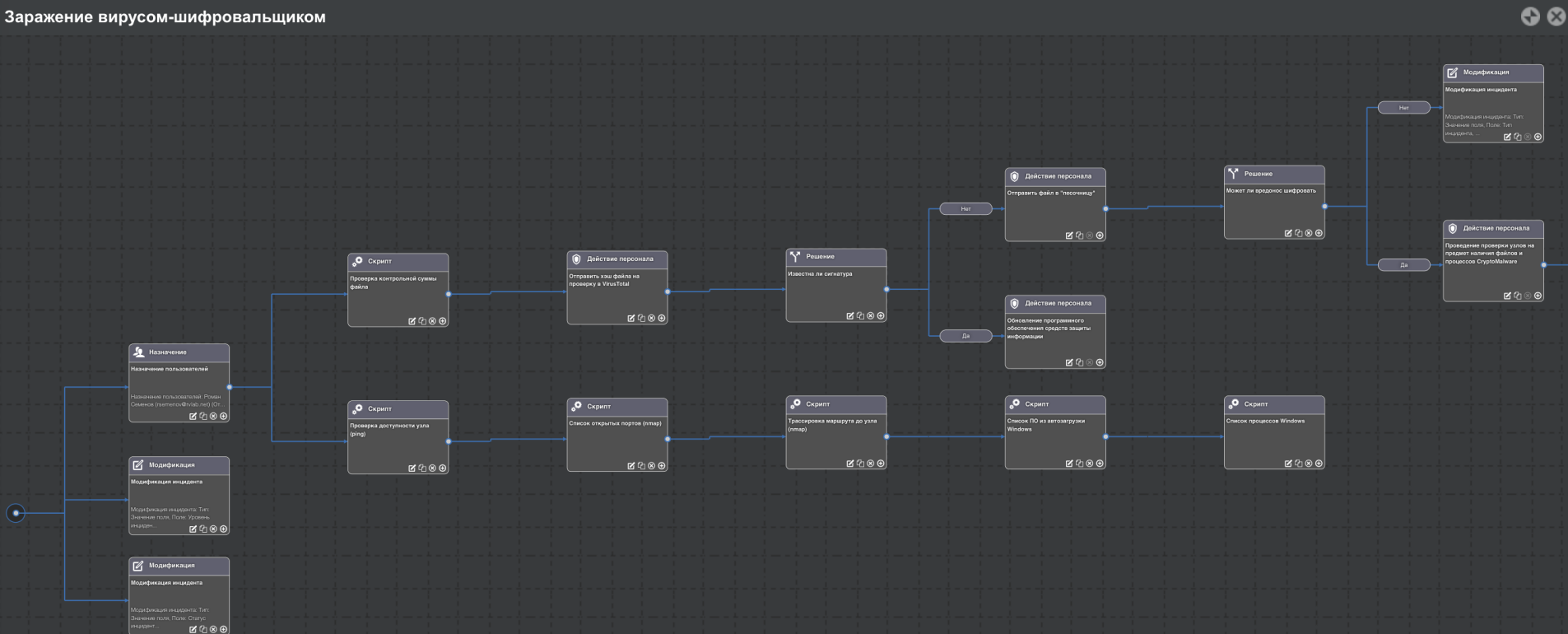
Действия по инциденту:

Добавить | Изменить | Удалить |

№	Наименование
(1)	Назначение пользователей Назначение пользователей: Роман Семенов (rsemenov@rvlab.net) (Ответственный за инцидент*), Петр Ложкин (plozkin@rvlab.net) (Участник (изменение)*), Николай Ручкин (nruchkin@rvlab.net) (Участник (изменение)*)
(1)	Модификация инцидента Модификация инцидента: Тип: Значение поля, Поле: Уровень инцидента, Значение: "Критичный"
(1)	Модификация инцидента Модификация инцидента:

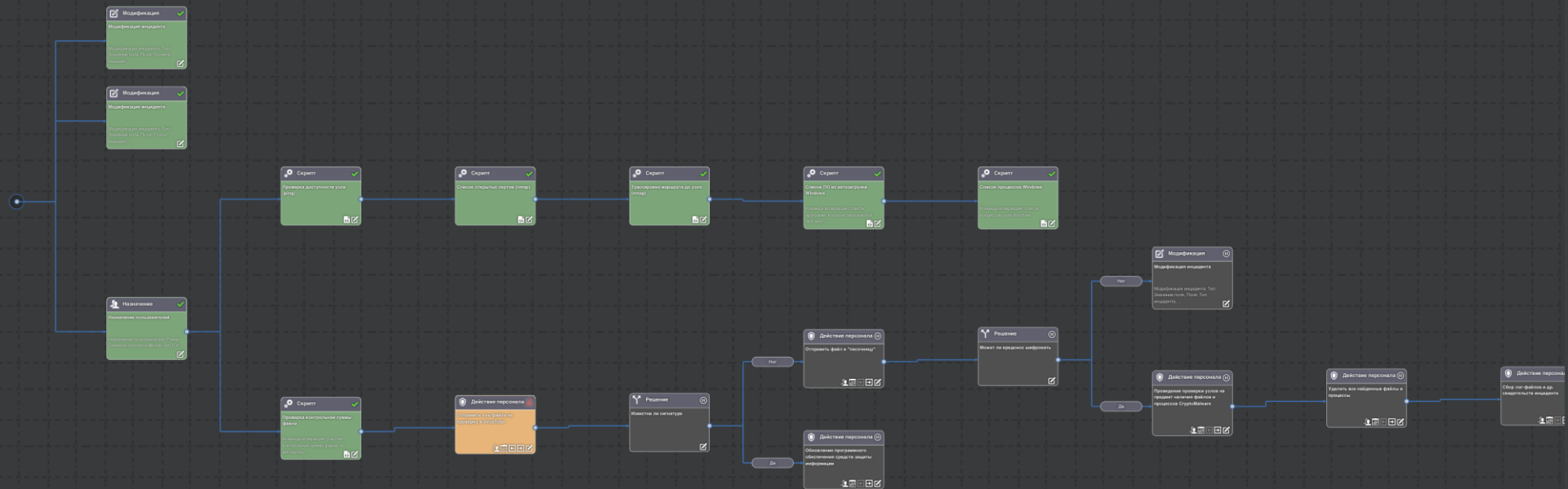
# Сценарии реагирования

## Заражение вирусом-шифровальщиком



# Сценарии реагирования

18-05-33: Внедрение вредоносного кода





# Скрипты автоматизации

Общие	Наименование	Тип	
Мой профиль	Вместо <abc.txt> укажите название требуемого файла.		
Документация	▼ <b>Сбор данных по оборудованию</b>		
Сведения об организации	Геолокация IP адреса (ipinfo.io)	R-Vision	
Лицензия	Конфигурация сетевого оборудования Cisco	Cisco	Команда возвращает конфигурацию сетевого оборудования Cisco
Пользователи системы	Конфигурация сетевого оборудования Juniper	Juniper	Команда возвращает конфигурацию сетевого оборудования Juniper
Роли пользователей	Настройки сети Linux	sh script	Команда возвращает настройки сети узла Linux
Обновление	Настройки сети Windows	Power Shell	Команда возвращает настройки сети узла Windows
Настройка почты	Проверка доступности узла (ping)	R-Vision	
Журнал	Системная дата Linux	sh script	Команда возвращает текущую дату и время узла Linux
Шаблоны отчетов	Список ПО из автозагрузки Windows	Power Shell	Команда возвращает список программ, которые запускаются при загрузке ОС Windows из следующих веток реестра: HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce HKCU\Software\Microsoft\Windows\CurrentVersion\Run HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce HKU\ProgID\Software\Microsoft\Windows\CurrentVersion\Run systemdrive\Documents and Settings\All Users\Start Menu\Programs\Startup systemdrive\Documents and Settings\username\Start Menu\Programs\Startup
Политики автогенерации отчетов	Список открытых портов (nmap)	R-Vision	
Консоль	Список подключенных USB устройств Linux	sh script	Команда производит чтение списка подключенных USB устройств на ОС Linux.
<b>Управление активами</b>	Список подключенных USB устройств Windows	Power Shell	Команда производит чтение класса WMI Win32_USBControllerDevice и преобразует результат в удобный для чтения вид.
▶ Учетные записи			
▶ Справочники			
Поля описания активов			
Жизненный цикл активов			
Внешние системы			
Архитектура			
<b>Скрипты автоматизации</b>			
▶ Политики инвентаризации			
Политики управления уязвимостями			

Группа:  
Сбор данных по оборудованию

Наименование скрипта:  
Список ПО из автозагрузки Windows

Тип:  
Power Shell

Учетная запись для выполнения команды:  
[dropdown]

Таймаут для выполнения команды (в секундах):  
[dropdown]

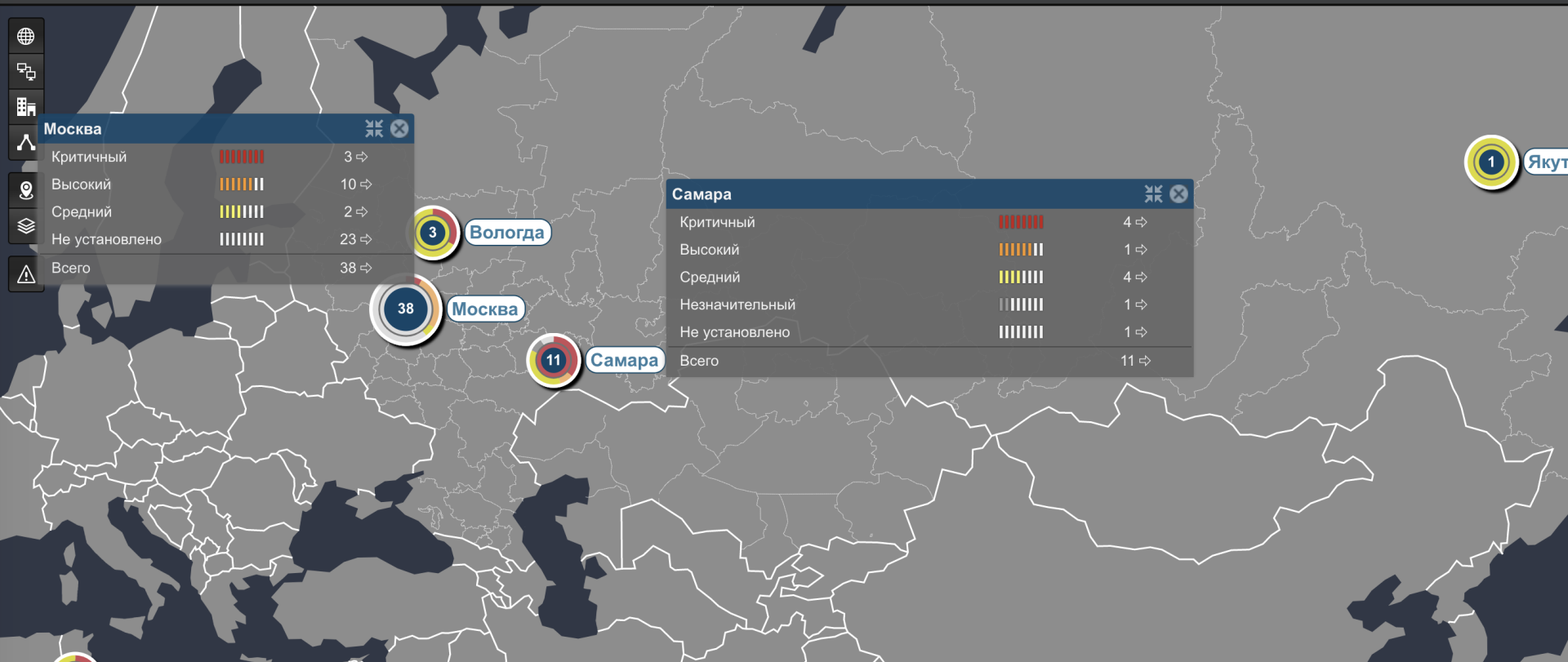
Записать результат в поле

Загрузить файл для выполнения:  
[input] **Выберите файл**

Код скрипта:  
Get-WmiObject Win32\_StartupCommand | Format-List

Описание:  
Команда возвращает список программ, которые запускаются при загрузке ОС Windows из следующих веток реестра:

# Визуализация инцидентов



## Инциденты по подразделениям



## Инциденты по объектам инфраструктуры



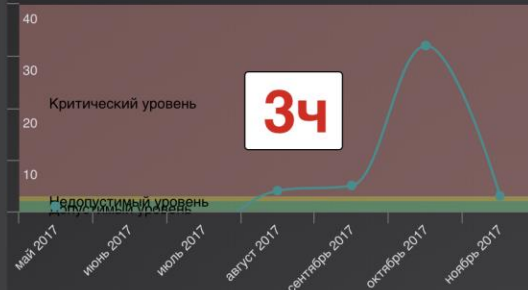
## Инциденты по статусам обработки

Цикл обработки: Типовой цикл обработки инцидентов

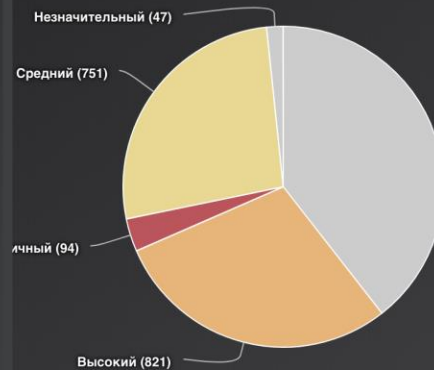


## Метрика: Среднее время реагирования

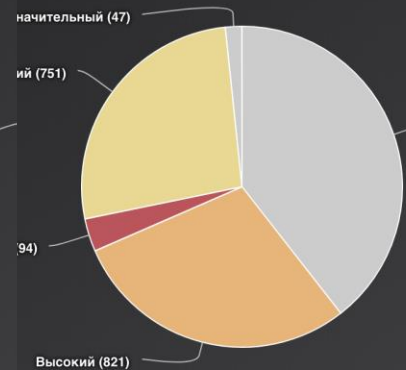
Период отображения: 01.05.2017 - 30.11.2017 | Тип инцидента: Все типы | Все инциденты | Уровень критичности: Все уровни



## Инциденты в работе



## Инциденты в работе



# Мониторинг состояния ИБ

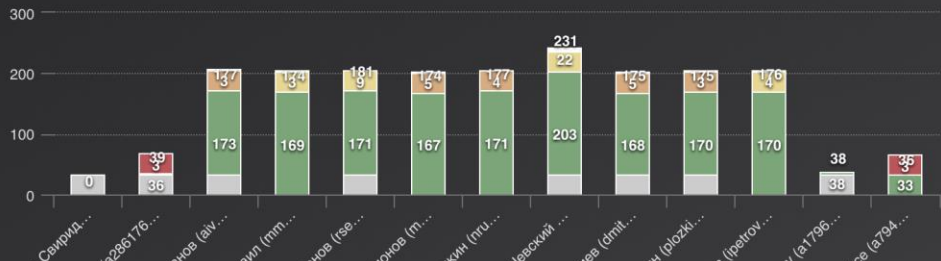
## История инцидентов

Период отображения: 19.01.2017 - 28.02.2018



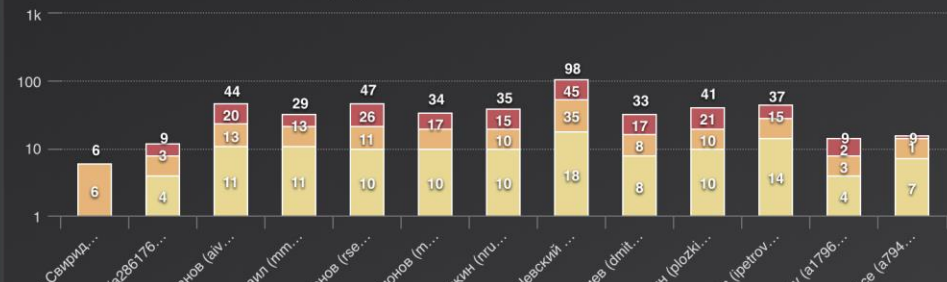
## Инциденты по ответственным (статус)

Цикл обработки: Типовой цикл обработки инцидентов  
Период отображения: 15.02.2017 - 03.12.2018



## Инциденты по ответственным (уровень критичности)

Период отображения: 14.02.2017 - 03.12.2018



# Результат

◆ Повышение скорости реагирования

◆ Минимизация потенциального ущерба и простоя бизнеса

◆ Уменьшение влияния человеческого фактора

◆ Повышение эффективности работы команды подразделения ИБ

◆ Полная картина о состоянии ИБ, учет мероприятий, накопление информации

◆ Поддержка принятия управленческих решений



# R-Vision IRP: кейсы

- ✓ Создание SOC/CERT, ситуационного центра
- ✓ Автоматизация управления жизненным циклом инцидентов ИБ
- ✓ Организация и обеспечение совместной работы группы реагирования
- ✓ Организация сервиса по обмену инцидентами ИБ
- ✓ Контроль ИТ-активов
- ✓ Централизованный сбор, накопление и хранение в единой системе всех инцидентов ИБ с возможностью последующего анализа при расследованиях
- ✓ Автоматизация реагирования на инциденты ИБ, включая активные технические меры
- ✓ Предоставление дополнительного сервиса MSSP провайдером



тенденция надолго ...

# Кадровый дефицит

## TOP 10 TECHNOLOGY TRENDS IMPACTING HIRING

These trends are increasing demand for skills across all types of IT roles.

- Cybersecurity/Data Security
- Cloud Solutions/Technologies
- Data Analysis/Visualization
- Big Data
- Internet of Things (IoT)
- Business Intelligence
- Artificial Intelligence
- Machine Learning
- Virtualization/Software Defined Infrastructure
- Converged Infrastructure

## Hot Jobs Index

Overview for Most Significant Roles Worldwide

	Future Importance	Hiring difficulty	Long-term growth
Security Management Specialist	Very high	Not difficult	High
Network Engineer/Architect	High	Not difficult	Low
Cyber/Information Security Engineer/Analyst	High	Not difficult	High
IoT Designer/Developer/Engineer	High	Not difficult	High
Business Intelligence Architect/Developer	High	Difficult	High
Software Developer/Engineer	High	Not difficult	Moderate
Machine Learning Designer/Developer/Engineer	High	Not difficult	Very high
Data Engineer	Medium	Difficult	High
Transformation Consultant	Medium	Not difficult	Moderate
Business Intelligence Analyst	Medium	Not difficult	High
Change Management	Medium	Not difficult	High
Mobile Applications Developer	Medium	Difficult	Moderate
Web Developer	Medium	Difficult	Moderate
Network/Systems Administrator	Low	Very difficult	Low
Systems Analyst	Low	Difficult	Low
Database Architect	Low	Difficult	Low
Data Scientist	Low	Not difficult	High
Computer Support Specialist	Low	Not difficult	Low



Но выход всегда есть



# Благодарю за внимание!

[www.rvision.pro](http://www.rvision.pro) | [sales@rvision.pro](mailto:sales@rvision.pro) | 8 (800) 350 77 57

Подписывайтесь на наш бесплатный дайджест ИБ: [rvision.pro/blog](http://rvision.pro/blog)