kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Сергей Повышев

Старший менеджер-руководитель направления «Управление информационной безопасности», ПАО «Северсталь»

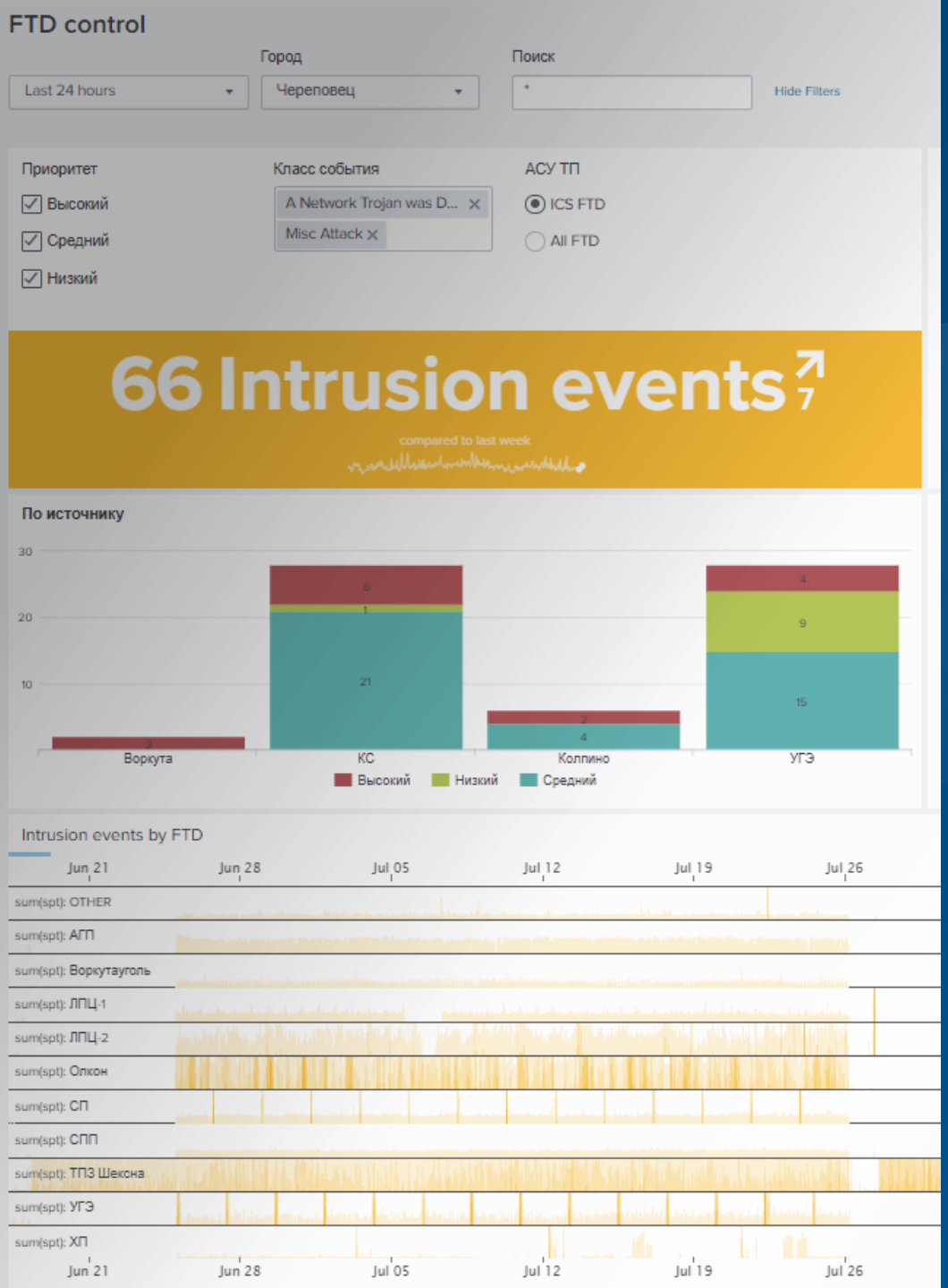
#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Мониторинг информационной безопасности в АСУ ТП. Поиск иголки в стоге сена

Повышев Сергей Алексеевич

Сентябрь 2020. Сочи



Содержание

- Система мониторинга: Ожидание vs Реальность
- Ландшафт проблем
- Неэффективные сценарии
- Ключевые факторы успеха
- Эффективные сценарии
- Будущее мониторинга

Система мониторинга. Ожидание vs Реальность

Северсталь

Эксплуатационный мониторинг DATAPK средний уровень			Эксплуатационный мониторинг DATAPK базовый уровень			Эксплуатационный мониторинг KICS	
248			276			53	
728	470	186	95	502	341	40	34

Предприятие	Изменение АСУ	Изменение ОЗ	В/А	Н/Д	Сбой ОЗ	Предупреждение
ТПЗ-Шексна	33	220	38	70	13	29
ДП	2	78	7	81	21	12
Колпино	38	378	29	31	4	27
Сталеплавильное	407	1,991	201	149	125	99
УГЭ	114	1,063	293	13	20	69
Воркутауголь	10	138	62	36	0	33
ЛПЦ1	158	318	31	71	15	96
ЛПЦ2	1,233	592	59	17	26	63
ПХЛ	137	807	30	64	28	131
АГП	100	1,017	51	144	26	320
Сортопрокатное	30	240	56	50	13	51
Карельский окатыш	13	153	28	51	0	75
Олкон	100	55	26	104	0	25
Общее	–	10	511	15	–	9

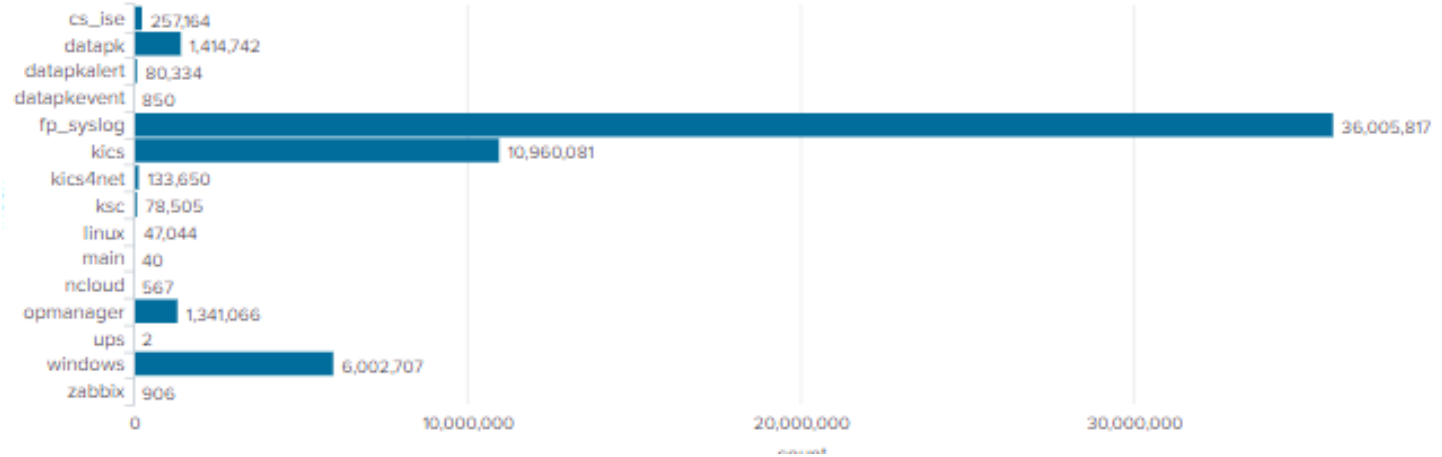
>80 тыс. инцидентов для разбора

>140 сценариев выявления инцидентов

>30 типов источников событий

>2700 объектов, охваченных мониторингом

1 аналитик и 2,4 FTE для сопровождения



>60 млн. событий в сутки

Ландшафт проблем. Не повторяйте ошибки

Северсталь

Проблемы:

Высокие трудозатраты на анализ событий и разбор инцидентов ИБ:

- Большое количество **False-Positive**:
  - Отсутствие WhiteList в средствах защиты и SIEM перед началом внедрения системы мониторинга
  - Отсутствие настроенных профилей безопасности для объектов защиты, что приводит к неэффективным сценариям
- Анализ событий со всех устройств в сети АСУТП, а не с критичных объектов защиты
- Некорректные критерии отнесения событий ИБ к инцидентам

Процесс внедрения систем мониторинга затягивается:

- Процесс настройки объектов защиты не автоматизирован
- Отсутствие процесса asset-менеджмента в системах АСУ ТП
- Необходимость перезагрузки объектов защиты, которые непрерывно задействованы в технологическом процессе.

Быстрая деградация системы без поддержки по причине постоянных изменений инфраструктуры АСУТП:

- Запоздалый процесс передачи систем мониторинга на сопровождение внутренним службам
- Отсутствие требуемых навыков работы в LINUX среде у обслуживающего персонала
- Отсутствие процесса постоянной актуализации текущих эталонных состояний объектов защиты

Инфраструктура АСУТП меняется каждый день!

Нарушение целостности и доступности событий с объектов защиты :

- События на СЗИ перезаписываются раз в сутки из-за большого объема информации.
- Использование UDP протокола для доставки событий с объектов защиты, что вызывало потерю части событий
- Не готовность инфраструктуры к передаваемому объёму информации. RSPAN перегружает сеть

- Не учтены требования к железу с учётом будущих апгрейдов
- Конкуренция за ресурсы на одном железе сенсоров нескольких вендоров

- Наличие НДВ в СрЗИ, использование OpenSource пакетов с библиотеками позволяющими выполнять произвольные команды на удалённых машинах и кражу аутентификационных данных

Неэффективные сценарии

Брутфорс

- Взаимодействие объектов по UDP – задержки в обработке информации вызывают брутфорс

Сканирование сети

- Легитимные сканирования при межконтроллерном взаимодействии

ARP-спуфинг

- Взаимодействие между ПЛК при поиске адреса получателя

Некоррелированные сценарии Windows

- Одно событие не даёт картины о вмешательстве в систему.
- Изменение конфигураций не критичных ОЗ

Изменение конфигураций не критичных ОЗ

- Ввиду огромного количества контролируемых объектов, нет возможности в ежедневной корректировке конфигураций и принятия их за эталонные, без резолюции УИБ. Необходимо контролировать только значимые объекты

Сценарии по контролю неизменяемости сети

- АСУ ТП не статична, изменения происходят постоянно

Ключевые факторы успеха

Люди	Отдельный аналитик АСУ ТП
Процессы	Утверждённые KPI по защищённости АСУ ТП
	RACI матрица распределения ролей между ИТ и ИБ по сопровождению системы мониторинга + регламент
	Корректировка ДИ, разработка новых ЛНА
	Ввод в эксплуатацию новых ОЗ в защищенном исполнении
Технологии	Основной упор на мониторинг критичных ОЗ и безагентный сбор журналов
	Asset-management с правильной архитектурой под АСУ ТП
	Создание эффективных сценариев на базе профилей безопасности по критичным ОЗ и прикладном ПО

Отдельный аналитик АСУ ТП

Активное участие в расследовании инцидентов и аналитике событий с источников АСУ ТП, обогащение событий необходимой информацией.

Разработка новых и корректировка существующих сценариев и контролей без привлечения третьих лиц. Оперативное изменение сценариев.

Внедрение KPI по сопровождению систем мониторинга обслуживающему персоналу

Северсталь

Повышение вовлеченности обслуживающего персонала в выполнении операций по повышению защищенности АСУ ТП
Согласовано и утверждено 16 KPI по сопровождению мониторинга

Операционные:

№	Показатель	Целевой показатель на 20 год%	Факт на 01.04.20	Факт на 3.07.2020
	% АРМов и серверов на которых работает активный сбор конфигураций WinRM, WMI, HTTPS	80%	38,00%	55,00%
5	% управляемого АСО на которых работает активный сбор по протоколу SNMP	80%	48,00%	51,50%
6	% АРМов и серверов на которых работает пассивный сбор по syslog	80%	22,00%	39,00%
7	% управляемого АСО на которых работает пассивный сбор для syslog	80%	32,00%	33,50%
17	% физических АРМов, серверов, из занесеных в CMDB	90%	99,00%	99,00%
ТОГ	**% выполнения сводного показателя по защищенности**	**80,45%**	**35,86%**	**45,41%**

Тактические:

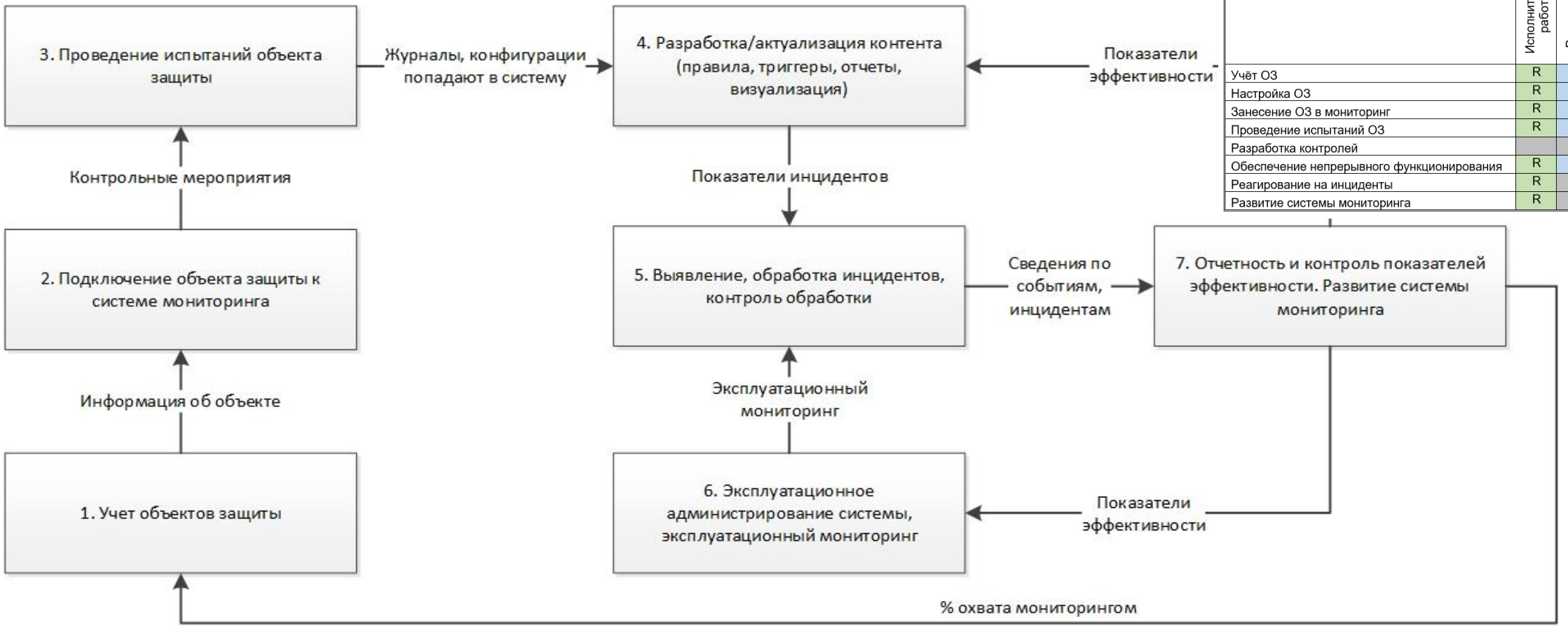
- доля инцидентов выявленных автоматически по отношению к инцидентам, выявленным вручную;
- % ложных срабатываний при автоматическом выявлении;
- % инцидентов обработанных в регламентированные сроки;
- % повторных инцидентов.

Стратегические:

- количество простоев по причине киберинцидентов;
- compliance требований регуляторов;
- общее количество подтвержденных инцидентов в системе;
- доля сотрудников привлечённых к ответственности к не привлечённым по инцидентам ИБ.

RACI матрица распределения ролей между ИТ и ИБ по сопровождению системы мониторинга

- **Разработана матрица RACI по сопровождению системы мониторинга**



Процесс	Исполнитель работ	Рук-ль исп. работ	Менеджер УИБ	Ст. менеджер УИБ
Учёт ОЗ	R	A	I	
Настройка ОЗ	R	A		
Занесение ОЗ в мониторинг	R	A	C	
Проведение испытаний ОЗ	R	A	C	
Разработка контролей			R	A
Обеспечение непрерывного функционирования	R	A		
Реагирование на инциденты	R		R	A
Развитие системы мониторинга	R		R	A

Структура ЛНА по расследованию и выявлению инцидентов

Положение о системе управления инцидентами информационной безопасности

- *Организация работы*

Регламент по обработке инцидентов информационной безопасности

- Сценарии реагирования на инциденты (IRM) и план восстановления (DRP)
  - *Инструкции*
- Альбомы дашбордов (SIEM)
  - *Визуализация*

Регламент по взаимодействию с НКЦКИ

- *Compliance*

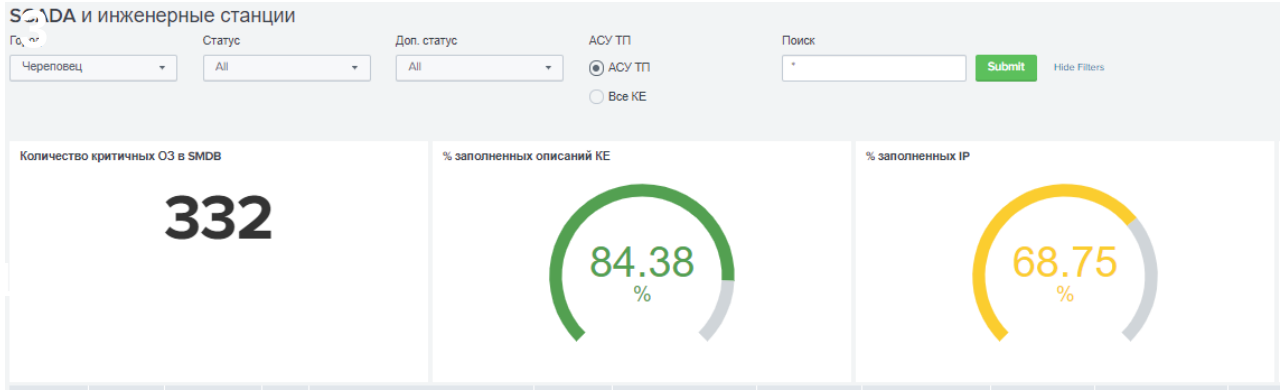
Регламент по сопровождению систем мониторинга ИБ АСУ ТП

- *Ответственность*

Основной упор на мониторинг критичных ОЗ

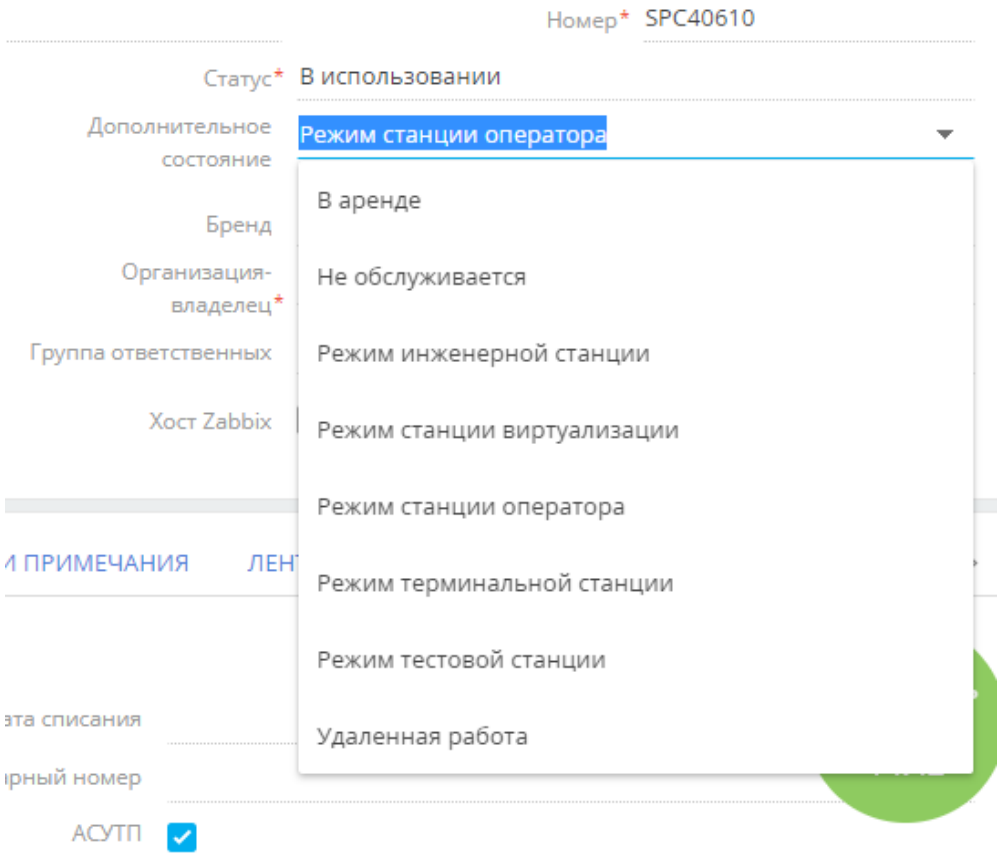
Критичные хосты:

- Станции операторов (SCADA)
- Инженерные станции (программирование PLC)
- Сервера в DMZ АСУТП
- Активное сетевое оборудование



Разрабатываются контроли в соответствии с профилями безопасности на каждый тип объекта защиты

Выделены критичные объекты на уровне CMDB (корректировка структуры БД)



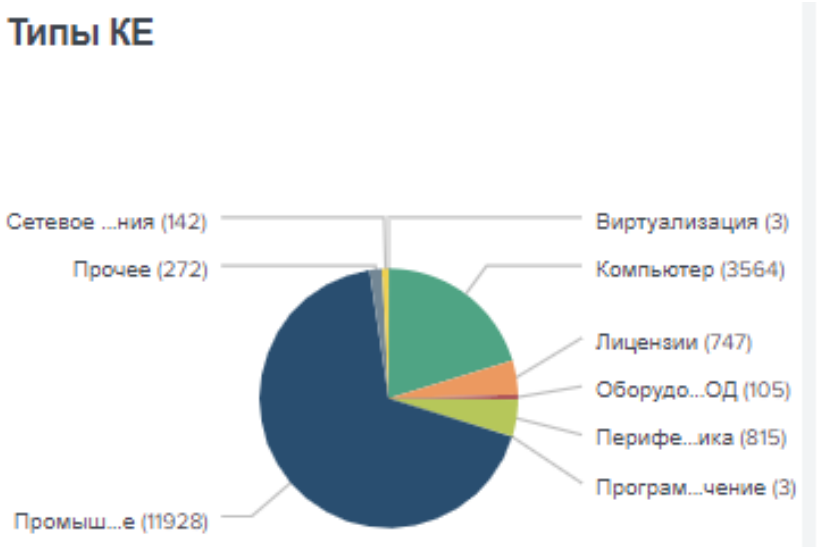
Asset-management с правильной архитектурой под АСУ ТП

Создано отдельное пространство в CMDB для АСУ ТП

- Оборудование и сети разбиты по категориям, цехам, агрегатам
- Идёт процесс актуализации сведений об объектах АСУ ТП, включая ключевые параметры: имя, IP-адрес, MAC-адрес, АСУ ТП.

Настроена интеграция АСУ ТП с CMDB

- Данные из CMDB синхронизируются с SIEM и СрЗИ



Ввод в эксплуатацию новых ОЗ в защищенном исполнении

Северсталь

Использование пакета автоматизации по настройке ОЗ

Контроль поступления событий от объекта
Скрипты для генерации событий

Контроль заведения объекта в систему мониторинга
Эксплуатационный мониторинг

Контроль предоставления прав пользователям
WinEvent ID

Контроль сетевой активности
WL, ASA

Контроль установки средств АВЗ
SQL запросы к KSC

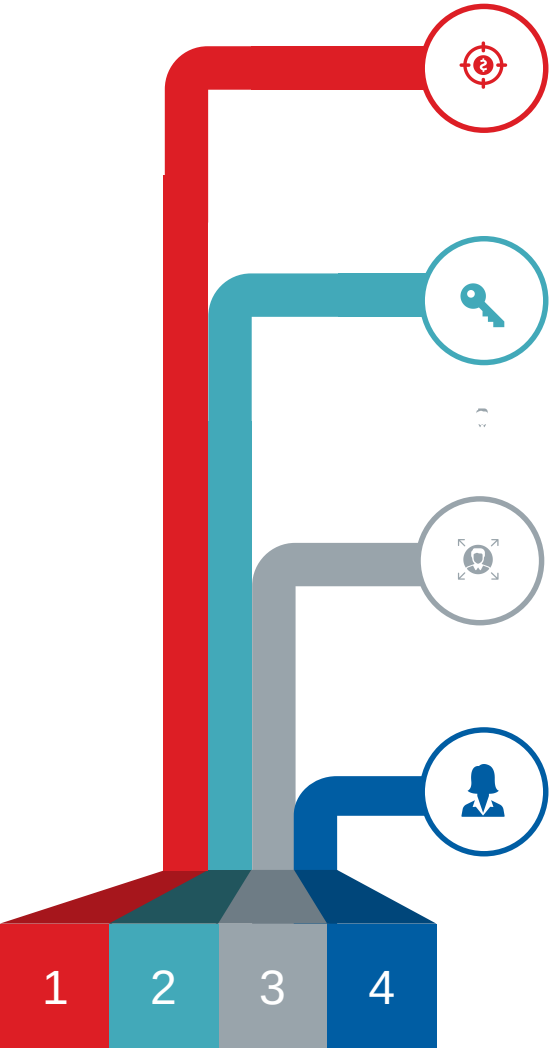
*** Обязанности по настройке защищённого исполнения закреплены в регламентах и ДИ**

Эффективные сценарии выявления инцидентов

Северсталь

- Контроль подключения внешних устройств
- Контроль подключения новых узлов
- Контроль изменения защищённого профиля SCADA
- Контроль изменения проектов SCADA, PLC
- Эффективные настройки NGFW
- Контроль подключения подрядчиков

Контроль внешних устройств



- Контроль подключения USB
- *DriverFrameworks-UserMode and UserPnp*
- *Microsoft-Windows-DeviceSetupManager / Admin*
- *Microsoft-Windows-DeviceSetupManager / Operational*
- *Microsoft-Windows-Kernel-PnP/Device Configuration*
- *Microsoft-Windows-Kernel-PnPConfig/Configuration*
- *Security*

- PermissionID

Связь по PermissionID событий, временных меток подключения и отключения устройства

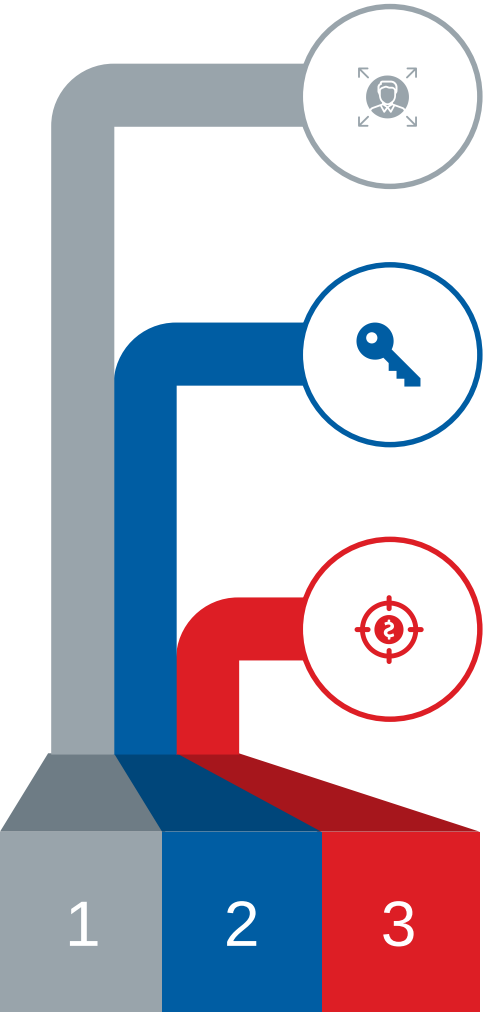
- Определение класса, вендора и продукта устройства

Определение принадлежности устройства по 16-битным идентификаторам VID (Vendor ID) и PID (Product ID) – обратить внимание на пары VID/PID для открытых проектов(BadUSB).
12D1 - Huawei Technologies Co., Ltd.
04E8 - Samsung Electronics Co., Ltd
05AC - Apple, Inc.

- Связь s/n устройства в событии с s/n из MDM

определение пользователя мобильного устройства

Контроль подключения новых узлов в технологической сети



- Однозначное определение легитимности обнаруженного устройства
  GET-запрос **https://localhost:8060/api/json/maps/getLayer2ScanDetails?apiKey=key** при появлении события обнаружения ассета о результатах сканирования

- Связь временной метки обнаружения asset и площадки с временными метками изменения статуса портов на АСО
  _time (GigabitEthernet1/0/36:up) = _time (Event_4000005003)
  Возможность оперативной блокировки подключенного устройства в автоматическом режиме

- Артефакты обнаружение нового asset в сети:
  MAC адрес на порту АСО при сканировании сети OpManager:

```
port 24, ifindex 24 has changed its state to used, having mac '1C:1B:0D:7D:93:E1'
```

_time	Place	msg	smac	IP	Name	Info
2020-08-17 12:48:32	АГП	Обнаружено новое устройство с адресом 192.168.	08:00:06:71:	192.168.	Устройство 566	ОЗ занесён в DATAPK :АСУ ТП линий сушки шлама №3 КОШ

Контроль изменения защищённого профиля SCADA
На примере WinCC(ver. 6 - 7.5)

Северсталь

контроли

- Контроль установки неподписанных драйверов
  HKEY_CURRENT_USER\Policies\Microsoft\Driver Signing\ BehaviorOnFailedVerify = 0

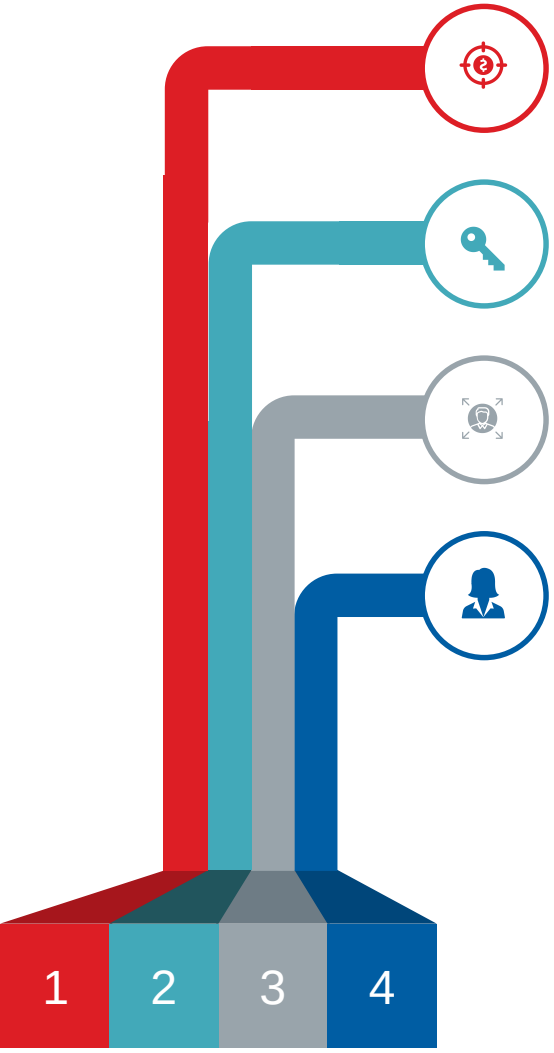
- Контроль отключения функции Data Execution Prevention :
  Control Panel -> System -> Advanced -> Performance -> Settings -> Data Execution Prevention -> Turn on DEP for all programs and services expect those I select

- Контроль изменения учетных записей WinCC
  select PW_USER.ID, PW_USER.name,PW_USER.EXPTIME from '+ RTRIM(@dbname) +'.dbo.PW_USER where PW_USER.ID >= 1000 Order by PW_USER.name'

- Контроль включения удаленного управления (CCDDiagAgent.exe):
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\CCDDiagAgent.exe

- Контроль использования SSL для работы WebNavigator и WebUX
  Event_4000002601 technology="Nic“ HTTP

Контроль изменения проектов SCADA, PLC



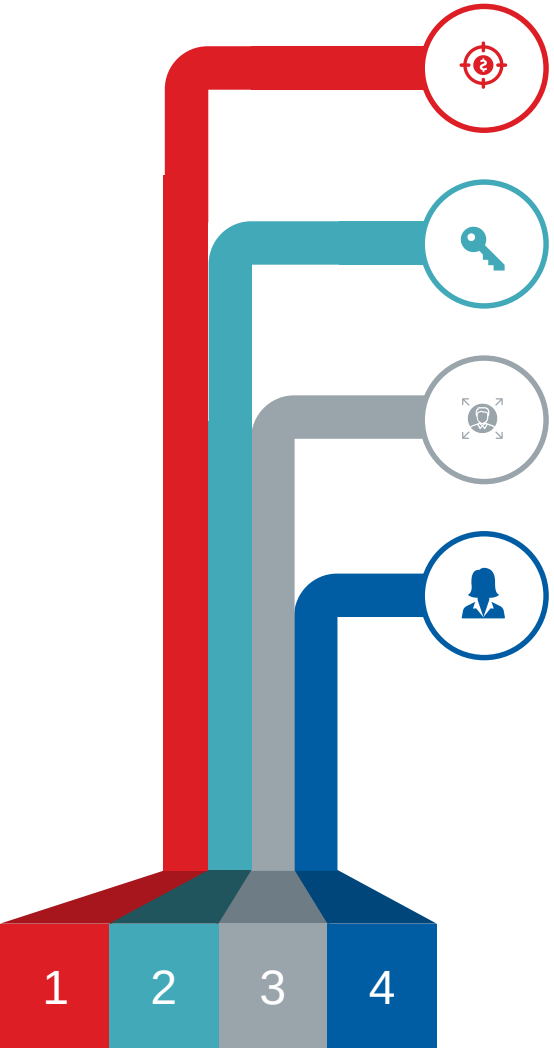
- **Version identifier**
  контроль изменения проекта по заявке в ServiseDeck (связь поля Version identifier с номером заявки)

- **DAM/DBF**
  контроль ручных корректировок БД минуя оболочку Versiondog

- **Versiondog Users**
  контроль изменения прав пользователей на редактирование проектов

- **Command Control**
  контроль системных команд, от инженерных станций, минуя Versiondog

Эффективные настройки NGFW

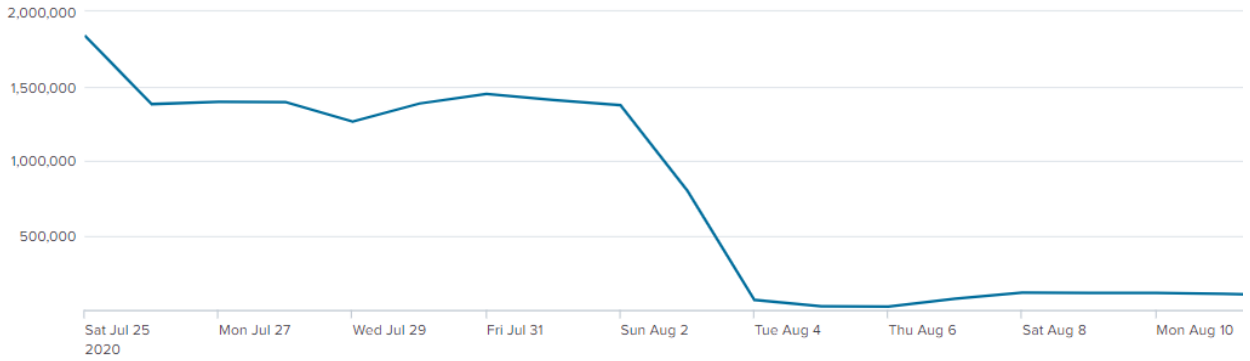


- **loggining**
  настройка передачи IPS ACL, health, audit событий в SIEM для дальнейшей корреляции и упрощения ведения расследований

- **Intrusion Prevention Policy**
  использование layer механизмов совместно с FP recomendation

- **Network Access Policy $ White Listing**
  внесение в NAP средств эксплуатационного мониторинга инфраструктуры

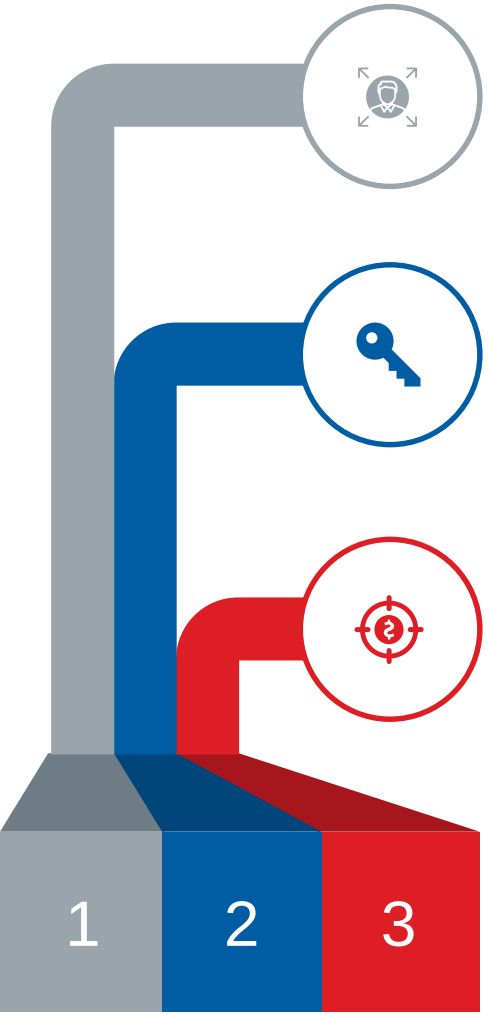
- **Network Discovery**
  аудит сетей при первом подключении к NGFW



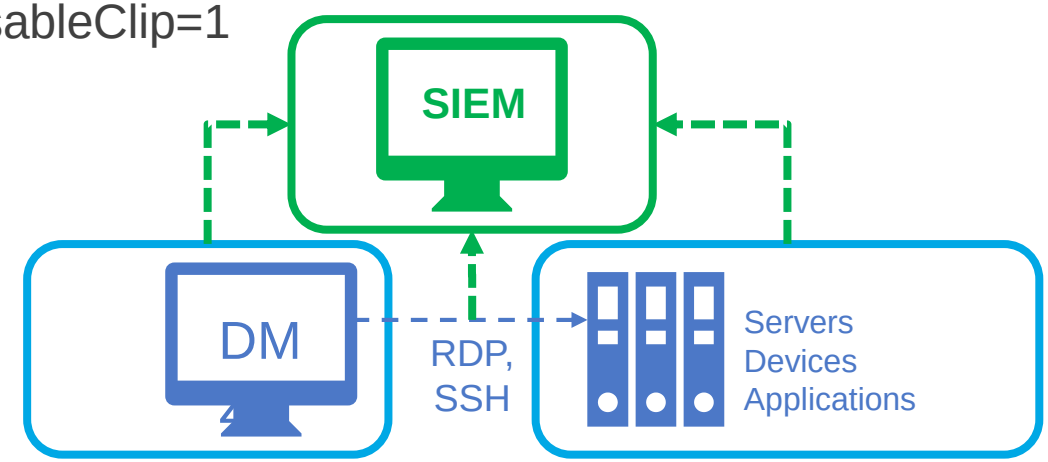
в 10 раз

Уменьшение false-positive

Контроль подключения подрядчиков



- Контроль добавления ТС в выделенный OU
  с привязкой добавления пользователей в глобальные/локальные группы администрирования
- Контроль изменения локальных групп администрирования, добавления новых пользователей, статусах их подключений и времени работы на серверах в выделенном OU
  Сравнение подключаемого пользователя с выгрузкой пользователей из SAP HR
- Контроль состояния буфера обмена
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\fDisableClip=1



Будущее мониторинга

Выявление антифрода в АСУ ТП

Корректировка отдачи дорогостоящих материалов

Корректировка показателей расхода энергоресурсов с целью победы в производственном соревновании

Корректировка скорости прокатки стана с целью выполнения плана, не смотря на ухудшение качества продукции

Корректировка показателей информационных систем слежения за металлом

Спасибо
за внимание