Практические аспекты применения системы предотвращения вторжений (IPS) FortiGate

10.08.2018

Андрей Терехов
инженер
aterekhov@fortinet.com

Сетевая безопасность и безопасность в аэропортах

Безопасность в аэропортах

Проверка билета и паспорта

Можно пройти на рейс только при наличии билета

Проверка багажа

Даже, если есть билет, с опасными вещами в багаже пройти не получится

Опциональный досмотр

При возникновении сомнений сотрудники службы безопасности могут провести дополнительный досмотр

Сетевая безопасность и безопасность в аэропортах

Безопасность в аэропортах	Сетевая безопасность
Проверка билета и паспорта	Межсетевой экран Прозрачно, в режиме реального времени
Можно пройти на рейс только при наличии билета	Проверка соединения на предмет правил контроля доступа
Проверка багажа	COB (IPS) Прозрачно, в режиме реального времени
Даже, если есть билет, с опасными вещами в багаже пройти не получится	Анализ сессии на предмет нарушений: попыток эксплуатации уязвимостей, активности вредоносного ПО
Опциональный досмотр	Сетевая песочница (Sandbox) Офлайн проверка, занимает время и вносит задержку
При возникновении сомнений сотрудники службы безопасности могут провести дополнительный досмотр	Доскональный анализ подозрительных файлов, разрешенных IPS

Но сетевая безопасность становится всё сложнее

Больше сервисов, *больше* задач,
больше операций на каждую задачу
=> *выше* **сложность работы**

=> *меньше* кандидатов

=> *дефицит* кадров *и*
усложнение работы

=> автоматизация
реагирования

Рост сложности задач обеспечения ИБ

	2007	2017
Хакерских групп	< 50	> 1,000
Производителей СЗИ	< 100	> 2,300
Тревог/День (среднее)	< 1,000	> 1,000,000
Расходы на ИБ	< $3B	> $80B

Optiv research, 7 September 2017, Dave DeWalt, General (Ret.) David Patraeus

Вызовы кибербезопасности и решения

ВЫЗОВ

- Современные продвинутые угрозы и постоянная активность злоумышленников

РЕШЕНИЕ

» Инспекция трафика решением **IPS мирового уровня**

Что аналитики подразумевают под IPS мирового уровня?

Gartner

- движок IPS 1-го поколения
- Идентификация приложения
- Идентификация контекста
- Идентификация контента
- Гибкая платформа

Gartner ввели термин **Next-Generation Intrusion Prevention Systems (NGIPS)** ещё в 2011

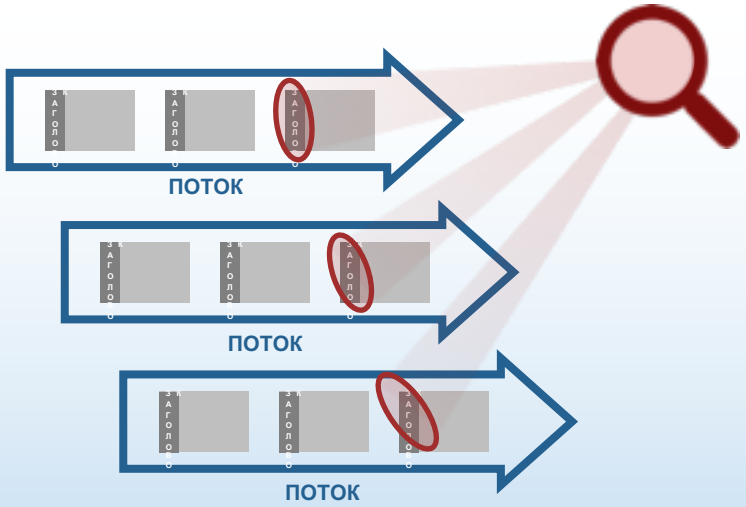
Недавно, в актуальных Магических Квадрантах, Gartner **повысили планку** для NGIPS

Gartner

- Сигнатуры
- Анализ протоколов
- Идентификация приложений и пользователей
- Идентификация контекста
- Сервис осведомленности об угрозах
- Идентификация контента
- Расширяемость
- Выявление продвинутых угроз
- Исторический анализ
- Опциональная поддержка режима L3

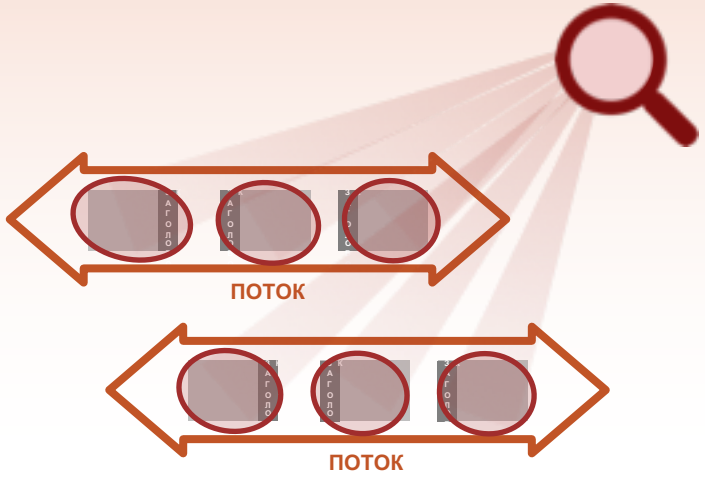
Убедитесь, что у вас используются правильные инструменты инспекции

Традиционный Межсетевой экран



- Контроль доступа
- Поверхностная проверка для определения отправителя, получателя и типа трафика
- Опасность как правило заметна с первых нескольких пакетов соединения
- Высокая скорость и пропускная способность

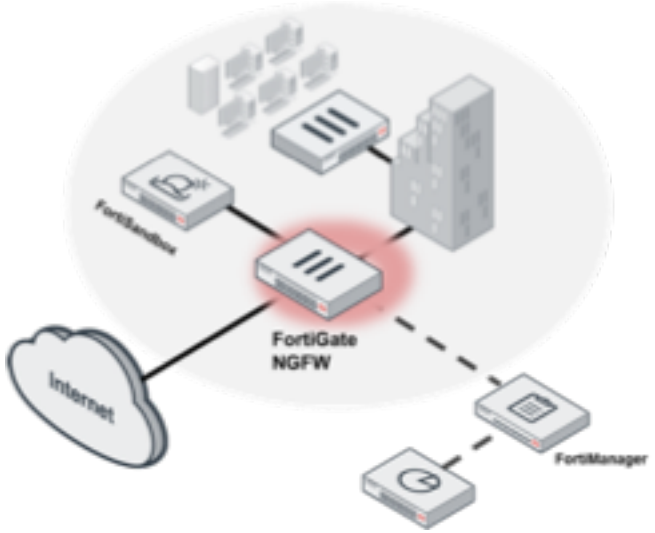
Традиционный СОВ (IPS)



- Инспекция протоколов и контента
- Глубокий анализ пакетов на предмет подозрительной нагрузки
- Риск оценивается для всего потока пакетов
- Инспекция с учетом состояния

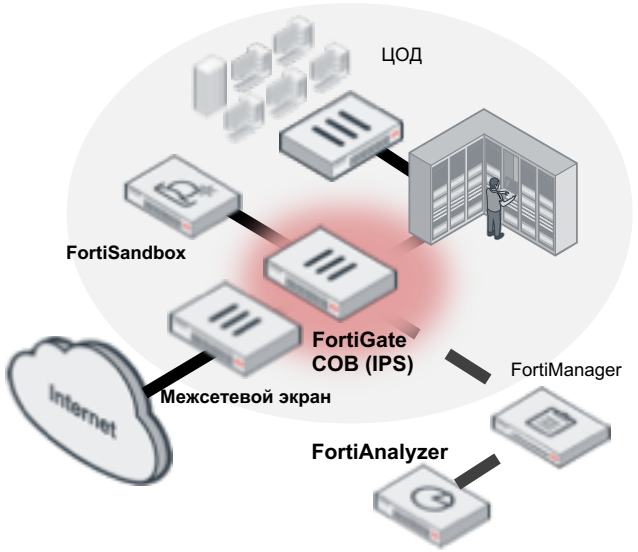
Две распространенных стратегии развертывания

IPS как часть межсетевого экрана (NGFW)



- IPS интегрирован с межсетевым экраном (NGFW)
- Мотивация - консолидация

Самостоятельный IPS



- IPS работает и управляется отдельно
- Мотивация - выделенная производительность и разделение полномочий
- Возможность применения совместно со сторонними МЭ

Вызовы кибербезопасности и решения

ВЫЗОВ

- Современные продвинутые угрозы и постоянная активность злоумышленников

РЕШЕНИЕ

» Инспекция трафика решением **IPS мирового уровня**

ВЫЗОВ

- Рост скоростей передачи данных в ЦОД

РЕШЕНИЕ

» Надёжная реализация **высокопроизводительного** IPS

Остерегайтесь влияния на производительность

Типовая деградация производительности при включении дополнительных инспекций

Как достичь высокой производительности? Ответ Fortinet

Сетевой процессор

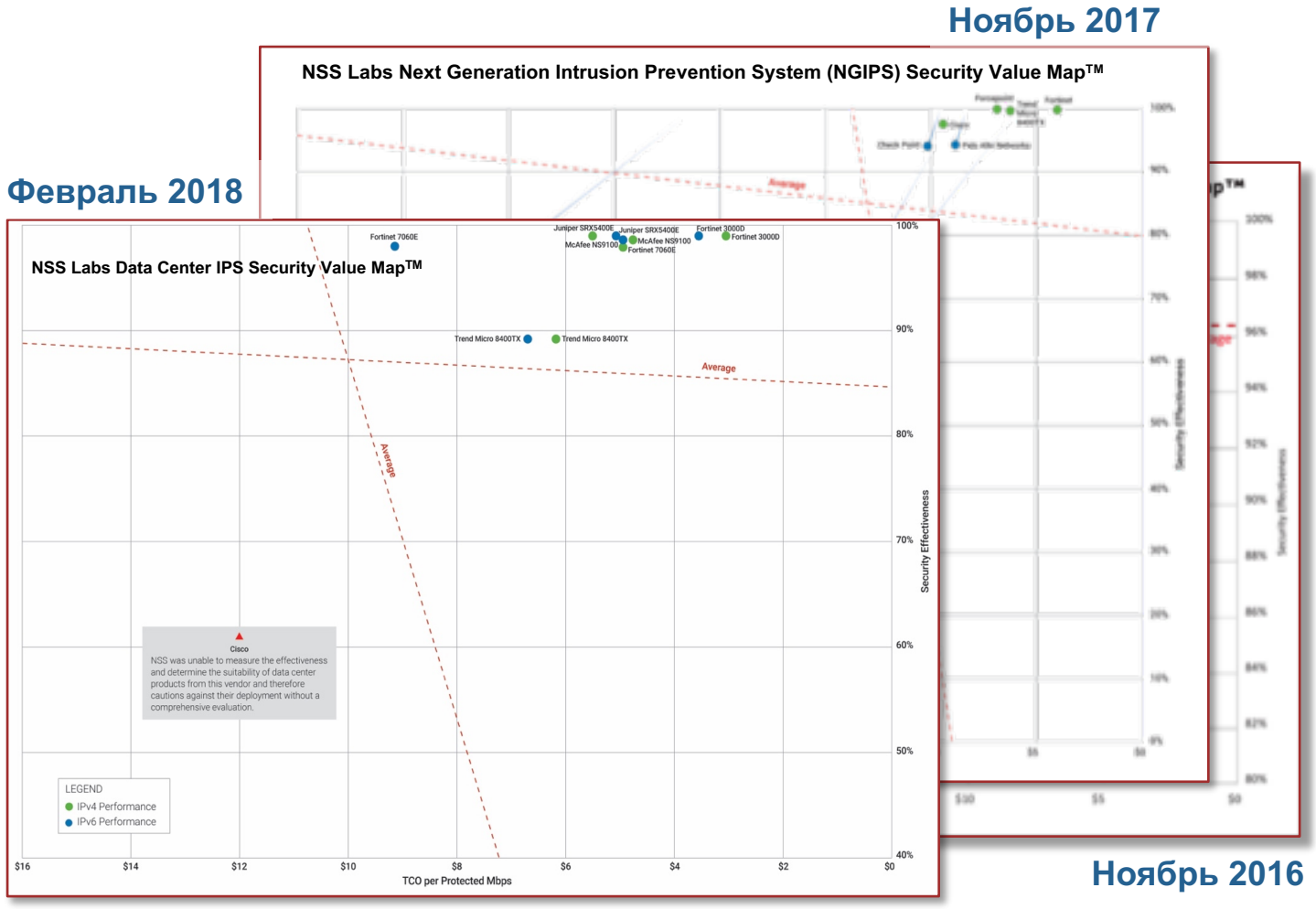
- Эффективно **повышает пропускную способность** ПАК
- Аппаратное ускорение **типовых задач МЭ**, таких как установление и контроль соединения

Контентный процессор

- Обеспечивает **высокую производительность** при включении дополнительных инспекций
- Аппаратное ускорение **глубокого анализа пакетов** - разгрузка CPU от вычислительно-интенсивных функций

Доказанная инспекция IPS мирового уровня

- Регулярные высокие результаты в сторонних сравнительных тестах
- Обратите внимание на эффективность детектирования и стоимость владения



Вызовы кибербезопасности и решения

ВЫЗОВ

- Современные продвинутые угрозы и постоянная активность злоумышленников

РЕШЕНИЕ

» Инспекция трафика решением **IPS мирового уровня**

ВЫЗОВ

- Рост скоростей передачи данных в ЦОД

РЕШЕНИЕ

» Надёжная реализация **высокопроизводительного** IPS

ВЫЗОВ

- Ограниченные ресурсы и стремление организаций к максимальной эффективности

РЕШЕНИЕ

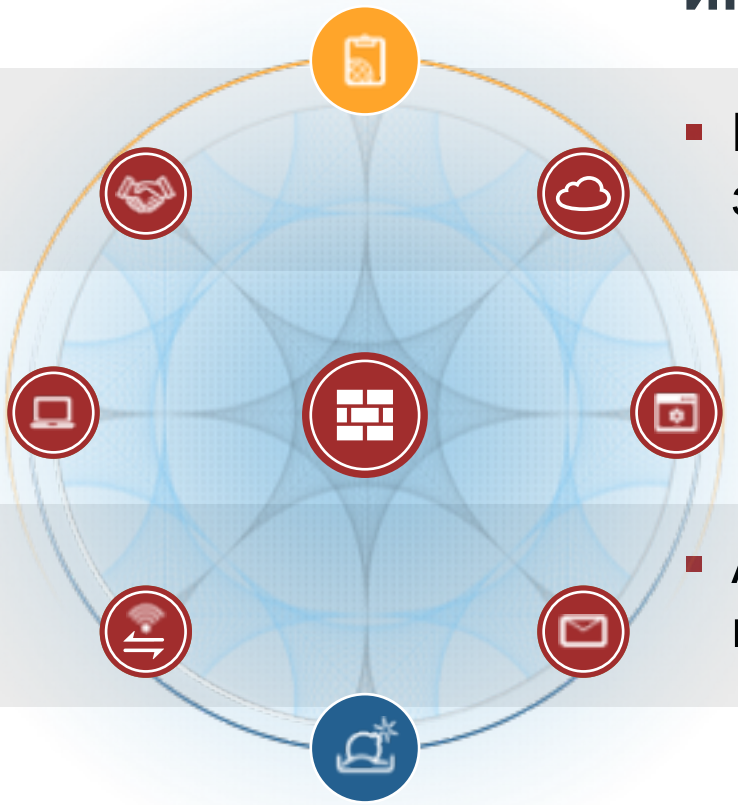
» **Инновационные возможности** IPS, выходящие за традиционные рамки

Ограничение временных ресурсов на работу со средствами защиты

Вызов

Ограничение ресурсов

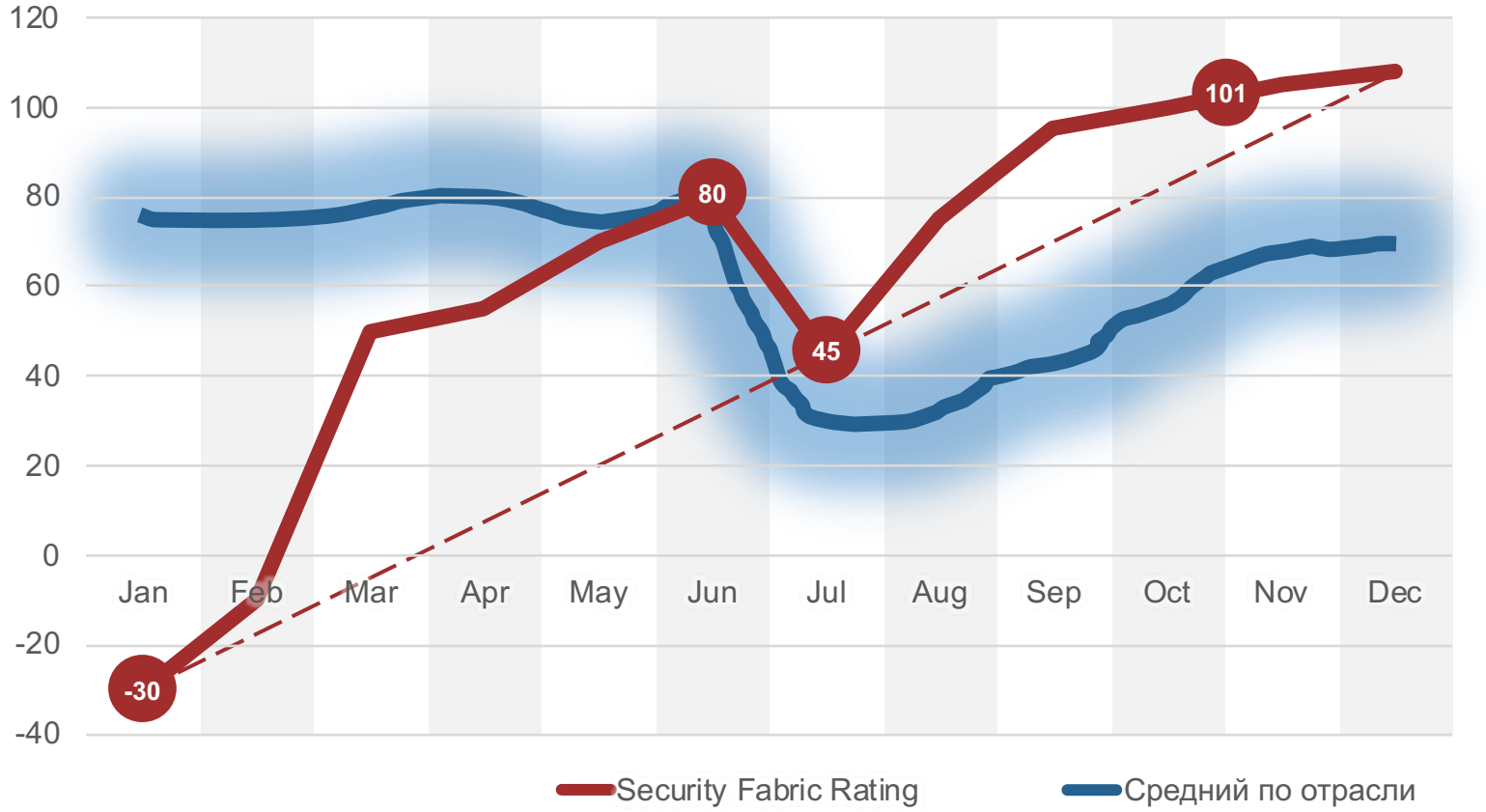
- Как нам узнать насколько хорошо мы защищены?
- Как быстро применить выводы?



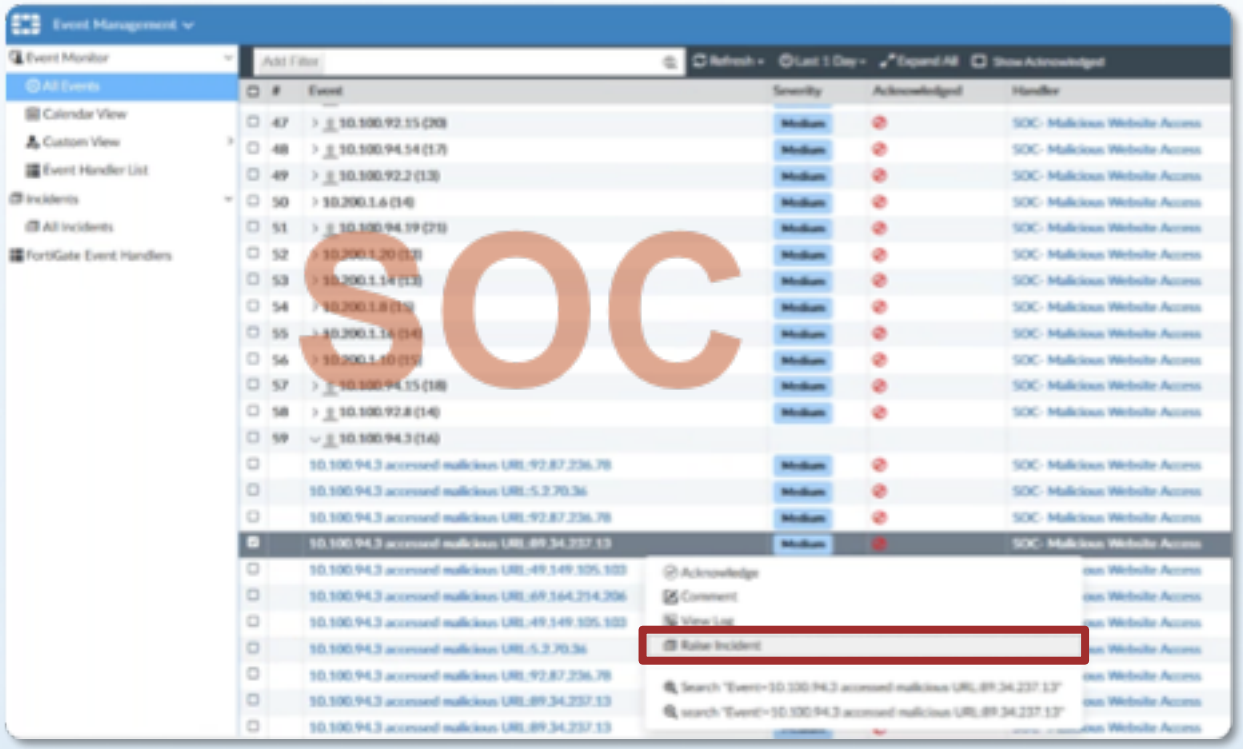
Решение - подход, интегрирующий NOC и SOC

- **Измеримая оценка** защищенности
- Автоматизация **взаимодействия подразделений**

Измеримая оценка

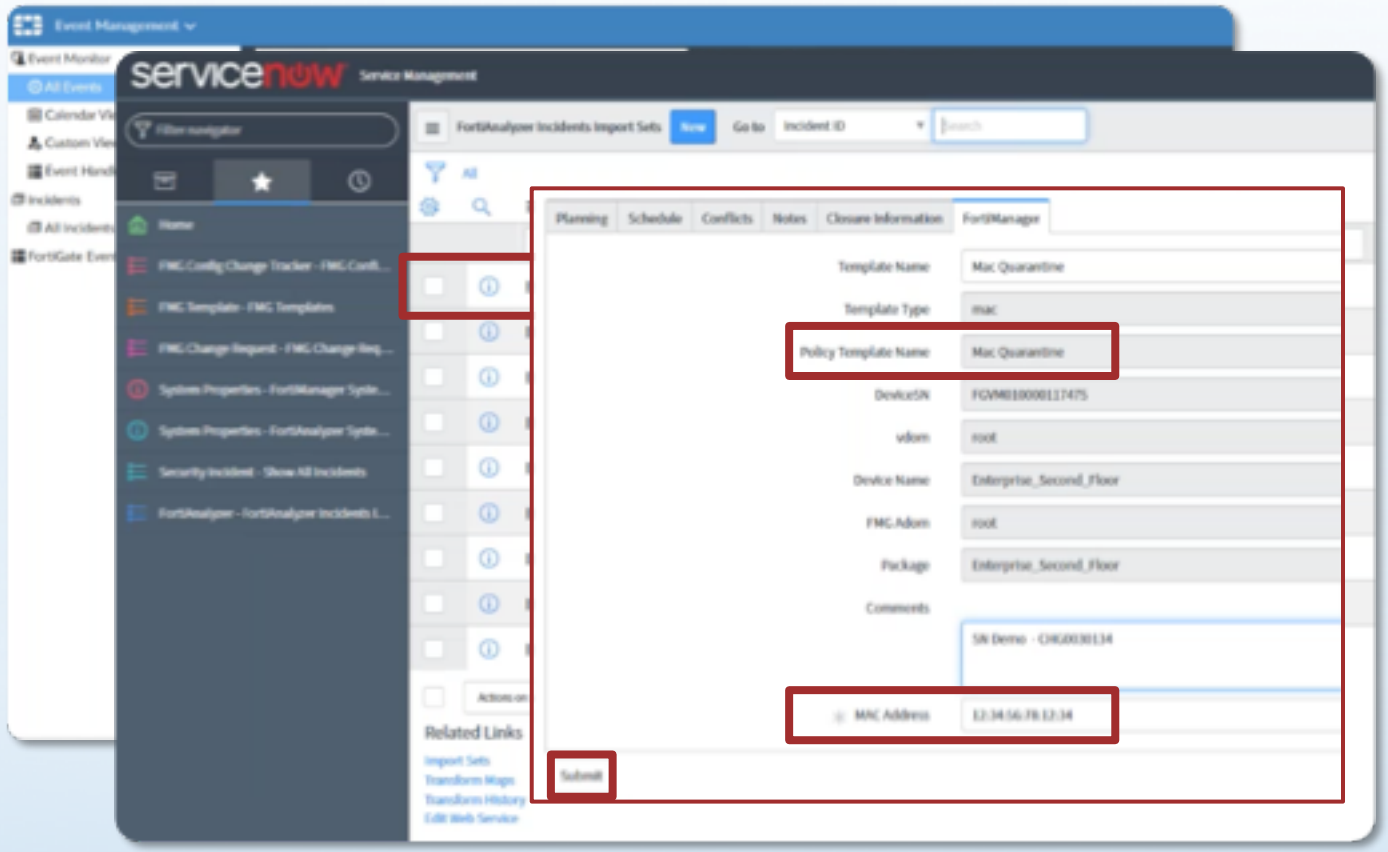


Автоматизация взаимодействия



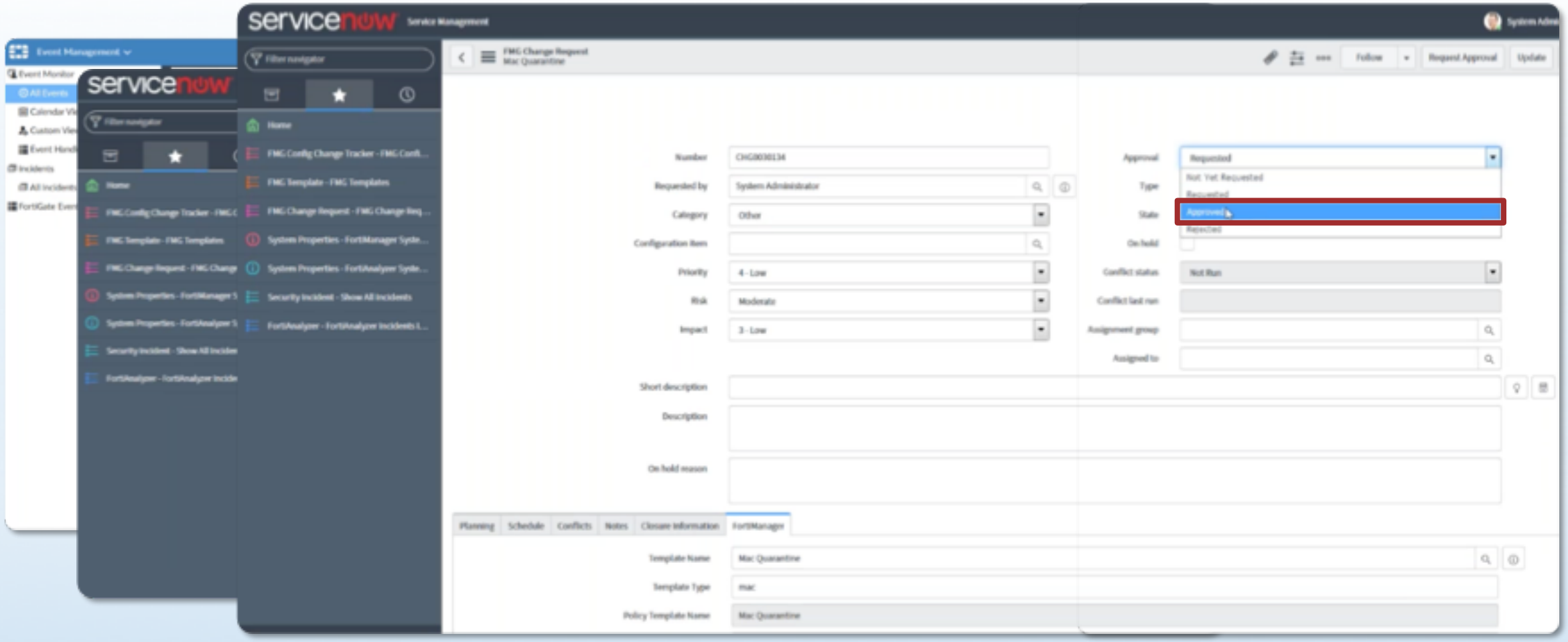
аналитик регистрирует инцидент (**SOC**), который затем направляется в ITSM

Автоматизация взаимодействия



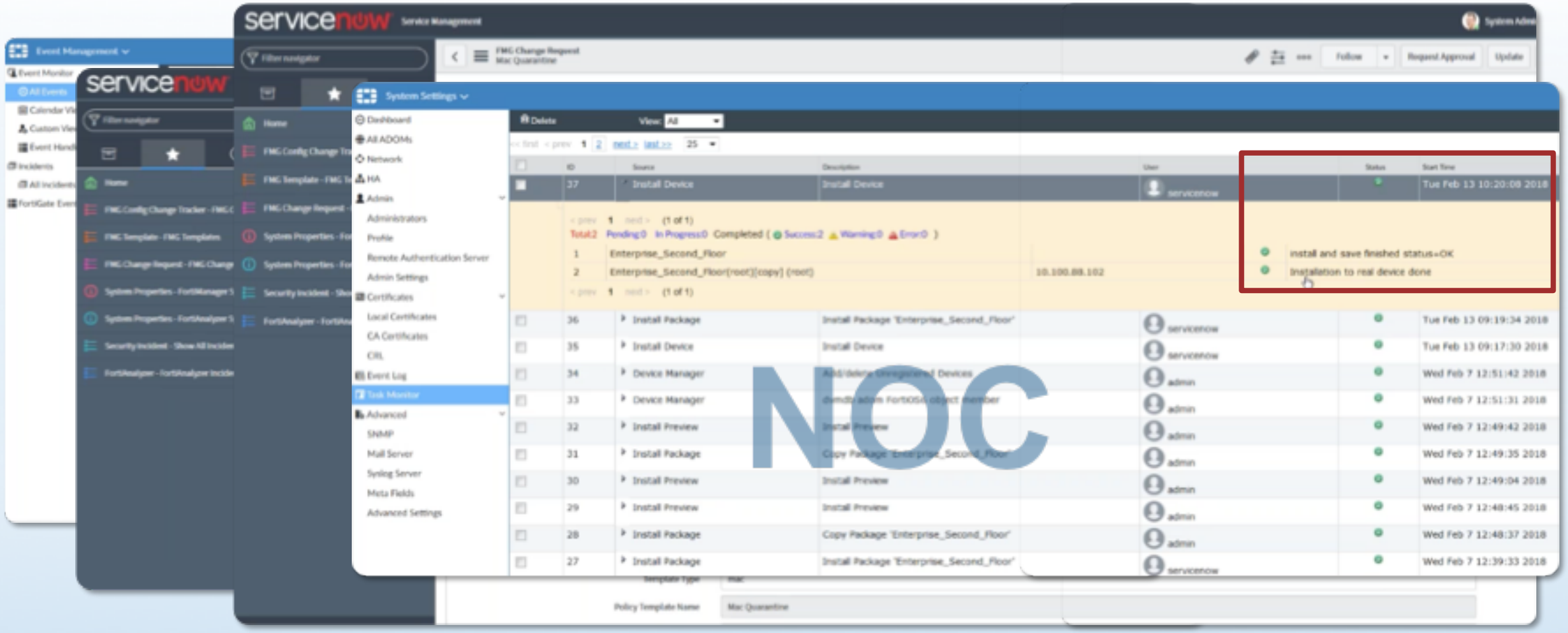
оператор ITSM принимает заявку и запрашивает требуемые действия

Автоматизация взаимодействия



руководитель подразделения одобряет запрошенное изменение в ITSM

Автоматизация взаимодействия



запрошенное изменение автоматически применяется (**NOC**) в инфраструктуре

Современные вызовы кибербезопасности - современный IPS

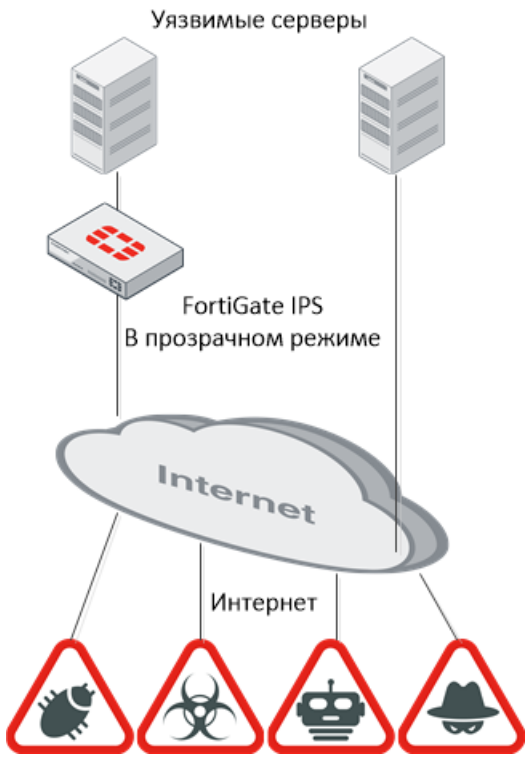
- **IPS мирового уровня**
  - » IPS должен активно развиваться, чтобы защищать от актуальных угроз
- **Высокая производительность**
  - » IPS должен обеспечивать высокую эффективность и высокую производительность одновременно
    - Следует оценивать не только брошюры (data sheets), но и сторонние тесты производительности и (в идеале) проводить тест в своей среде
- **Выход за традиционные рамки**
  - » IPS должен эволюционировать вслед за растущими требованиями организаций

Use case – защита активов, подключенных к Интернет

- Сколько в организации ПК, серверов, принтеров, телефонов, коммутаторов, …?
- А сколько виртуальных машин и контейнеров в частных и общих облаках?
- Какие виды данных обрабатываются организацией и на каких активах?
- Примеры инцидентов:
  - Equifax действительно взломали через баг в Apache Struts, но уязвимость оказалась старой
    - https://xakep.ru/2017/09/14/equifax-dejstvitelno-vzlomali-cherez-bag-v-apache-struts-no-uyazvimost-okazalas-staroj/
    - Неизвестные злоумышленники завладели личной информацией 143 млн американцев
    - Проникновение в мае 2017 года, присутствие оставалось незамеченным вплоть до конца июля 2017 года
    - Эксплуатация уязвимости CVE-2017-5638, устраненной в начале марта 2017 года
    - У компании было два или более месяца на установку обновления, однако по какой-то причине этим никто не озаботился
  - Власти Атланты потратили 2,6 млн долларов на устранение последствий атаки шифровальщика (на момент 25 апреля 2018)
    - https://xakep.ru/2018/04/25/samsam-attack-costs/
    - 23 марта 2018 года власти американского города Атланта, штат Джорджия, подверглись атаке шифровальщика
    - Вымогатели требовали от города около 55 000 долларов (в Bitcoin эквиваленте), однако выкуп так и не был выплачен.
    - По данным одной из местных компаний, занимающихся кибербезопасностью, в мае 2017 как минимум 5 серверов, принадлежащих властям Атланты, и доступных из Интернет, были заражены DoublePulsar

https://fortiguard.com/encyclopedia/ips/43745/apache-struts-2-jakarta-multipart-parser-code-execution
https://fortiguard.com/encyclopedia/ips/43963/backdoor-doublepulsar

Use case – защита активов, подключенных к Интернет



Threat	Category	Threat Level
Backdoor.DoublePulsar	IPS	Critical
Zivif.PR115-204-P-RS.Web.Cameras.Hardcoded.Password	IPS	Critical
MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	IPS	Critical
Blocked by Firewall Policy	Blocked by Firewall Policy	High
MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	IPS	High
Telnet.Login.Brute.Force	IPS	High
Mirai.Botnet	IPS	High
Android.ADB.Debug.Port.Remote.Access	IPS	Medium
Psiphon	Proxy	Medium
PPTP	Proxy	Medium
RealVNC.Server.Authentication.Bypass	IPS	Medium
Telnet.Remote.Root.Login	IPS	Low
Failed Connection Attempts	Failed Connection Attempts	Low
MS.SQL.Server.Empty.Password	IPS	Low
SSH.Client.Request.Mimicking	IPS	Low

Use case – защита активов, подключенных к Интернет

Подключение к Интернет с защитой FortiGate

Suricata CVE - Top 10

CVE ID	CNT
CVE-2012-0152	11
CAN-2001-0540	2
CVE-2001-0540	2

Export: Raw Formatted

Suricata Alert Signature - Top 10

ID	Description	CNT
2210037	SURICATA STREAM FIN recv but no session	1361
2001978	ET POLICY SSH session in progress on Expected Port	938
2006408	ET POLICY HTTP Request on Unusual Port Possibly Hostile	931
2023997	ET INFO Potentially unsafe SMBv1 protocol in use	373
2102465	GPL NETBIOS SMB-DS IPC$ share access	369
2101251	GPL TELNET Bad Login	256
2009582	ET SCAN NMAP -sS window 1024	216
2023016	ET TELNET SUSPICIOUS Path to BusyBox	142
2023017	ET TELNET SUSPICIOUS busybox shell	135
2023018	ET TELNET SUSPICIOUS busybox enable	135

Export: Raw Formatted

Прямое подключение к Интернет

Suricata CVE - Top 10

CVE ID	CNT
CVE-2001-0540	28
CVE-2012-0152	6
CAN-2001-0540	2
CVE-2002-0013 CVE-2002-0012	2
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	2
CVE-2017-5638	2
CVE-2001-0414	1
CVE-2006-2369	1
CVE-2017-5638 CVE-2017-5638	1

Suricata Alert Signature - Top 10

ID	Description	CNT
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	141928
2006408	ET POLICY HTTP Request on Unusual Port Possibly Hostile	900
2001978	ET POLICY SSH session in progress on Expected Port	614
2101251	GPL TELNET Bad Login	545
2023016	ET TELNET SUSPICIOUS Path to BusyBox	308
2023017	ET TELNET SUSPICIOUS busybox shell	305
2023018	ET TELNET SUSPICIOUS busybox enable	305
2102466	GPL NETBIOS SMB-DS IPC$ unicode share access	234
2009582	ET SCAN NMAP -sS window 1024	199
2023997	ET INFO Potentially unsafe SMBv1 protocol in use	131

Export: Raw Formatted

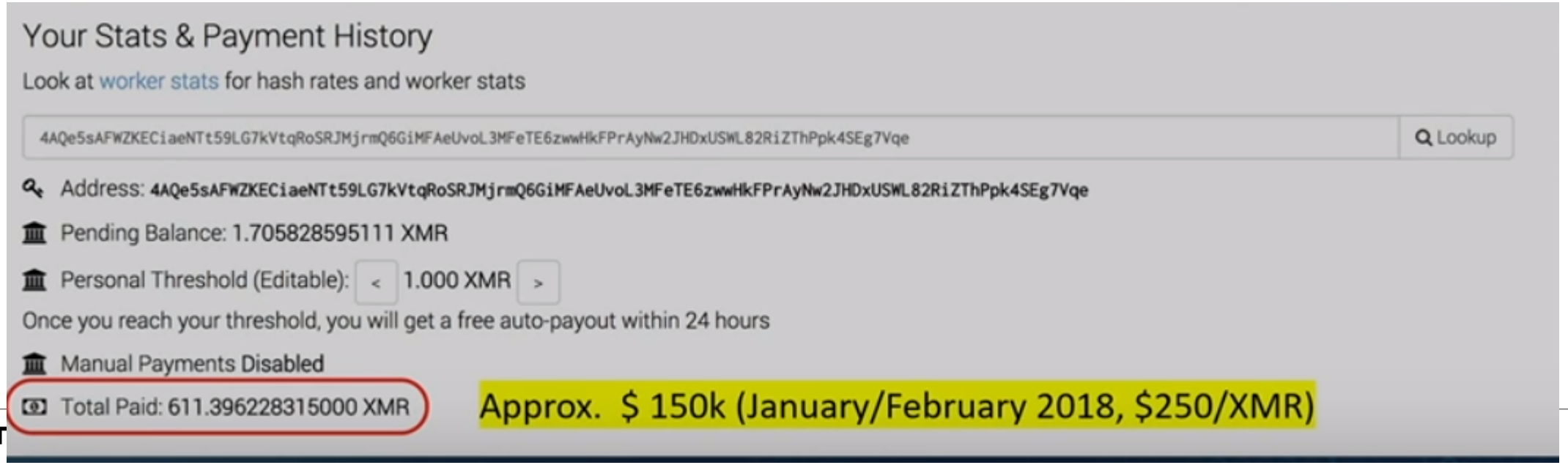
Use case – защита вычислительных ресурсов

- У кого в организации и за её пределами есть доступ к вычислительным ресурсам?
- Как осуществляется мониторинг утилизации вычислительных ресурсов (ПК, серверы, облака, Android-устройства, …)?
- Примеры инцидентов:
  - Уязвимость в Oracle WebLogic эксплуатировалась для майнинга Monero
    - https://www.securitylab.ru/news/490733.php
    - Атакующие использовали PoC-эксплоит для критической уязвимости CVE 2017-10271, затрагивающей серверы WebLogic
    - Злоумышленникам удалось добыть криптовалюту на сумму $226 тыс., больше чем требование выкупа для властей Атланты
    - “Злоумышленники имели доступ ко всей информации на серверах, но вместо того, чтобы продать ее на черном рынке, они просто установили программное обеспечение для добычи криптовалюты”
  - Майнинг криптовалюты на неиспользуемых вычислительных мощностях
    - https://lenta.ru/news/2018/07/25/bitochki/
    - В 2011 году сотрудник платежной компании Qiwi за три месяца намайнил на терминалах компании 500 тысяч биткойнов
    - Майнинг проводился во внерабочее время, что не привело к прямому ущербу, но повысило затраты на электроэнергию
    - Ежегодно только на добычу биткоина и Ethereum тратится 50,5 тераватта - это сопоставимо с годовым потреблением энергии нескольких европейских стран
    - https://coinlife.com/news/terminaly-qiwi-mogli-sovershit-ataku-51-na-blokchejn-bitkoina/

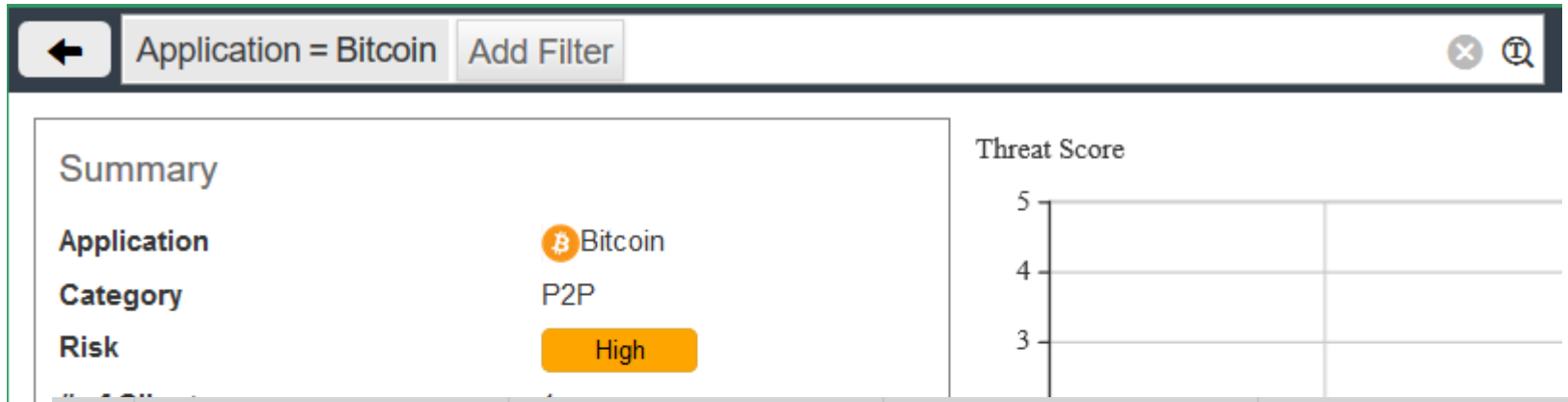
https://fortiguard.com/encyclopedia/ips/45334/oracle-weblogic-server-wls-wsat-component-code-injection
https://fortiguard.com/search?q=miner&type=app&engine=1
https://fortiguard.com/search?q=miner&type=mob&engine=1

Use case – защита вычислительных ресурсов

- У кого в организации и за её пределами есть доступ к вычислительным ресурсам?
- Как осуществляется мониторинг утилизации вычислительных ресурсов (ПК, серверы, облака, Android-устройства, …)?
- Примеры инцидентов:
  - Уязвимость в Oracle WebLogic эксплуатировалась для майнинга Monero
    - https://www.securitylab.ru/news/490733.php
    - Атакующие использовали PoC-эксплоит для критической уязвимости CVE 2017-10271, затрагивающей серверы WebLogic
    - Злоумышленникам удалось добыть криптовалюту на сумму $226 тыс., больше чем требование выкупа для властей Атланты
    - “Злоумышленники имели доступ ко всей информации на серверах, но вместо того, чтобы продать ее на черном рынке, они просто установили программное обеспечение для добычи криптовалюты”



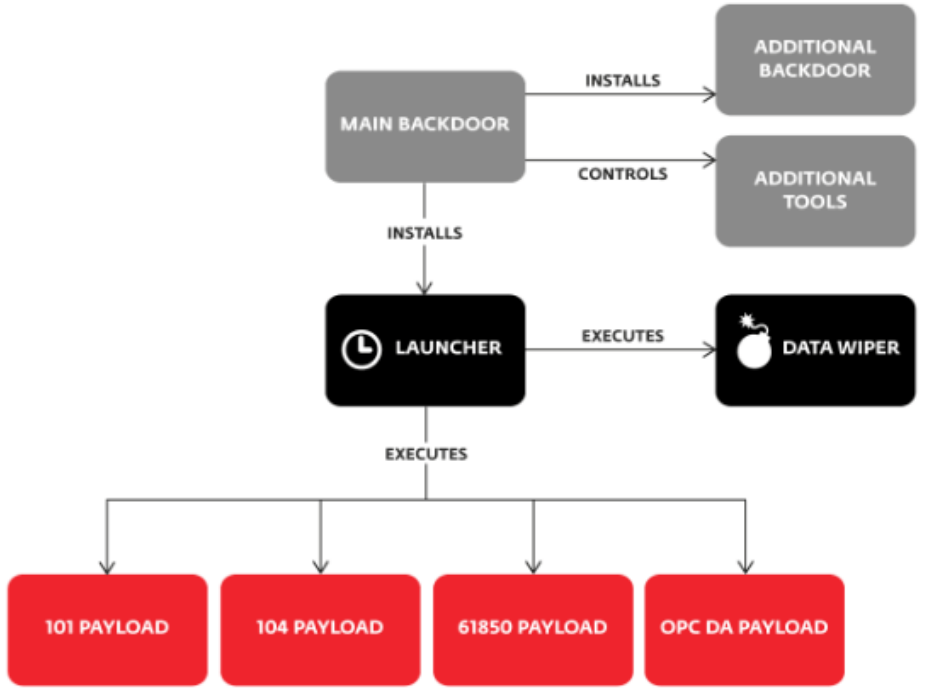
Use case – защита вычислительных ресурсов



#	Threat	Category	CVE ID	Threat Level	Threat Score(Blocked/ Allowed)	Incidents(Blocked/ Allowed)
1	coinhive.com	Malicious Websites		High	300	5
2	pool.xmr.pt	Malicious Websites		High	120	2
3	monero.lindon-pool.win	Malicious Websites		High	120	2
4	bohemianpool.com	Malicious Websites		High	60	1
5	api.viaxmr.com	Malicious Websites		High	60	1
6	api.xmr.mypool.online	Malicious Websites		High	60	1
7	api.xmrpool.xyz	Malicious Websites		High	60	1
8	ratchetmining.com	Malicious Websites		High	60	1
9	www.p00ls.net	Malicious Websites		High	60	1
10	monerohash.com	Malicious Websites		High	60	1
11	pool.xmrpool.de	Malicious Websites		High	60	1
12	malicious-url	IPS		High	30	1

Use case – защита АСУ ТП и (от) Интернета вещей

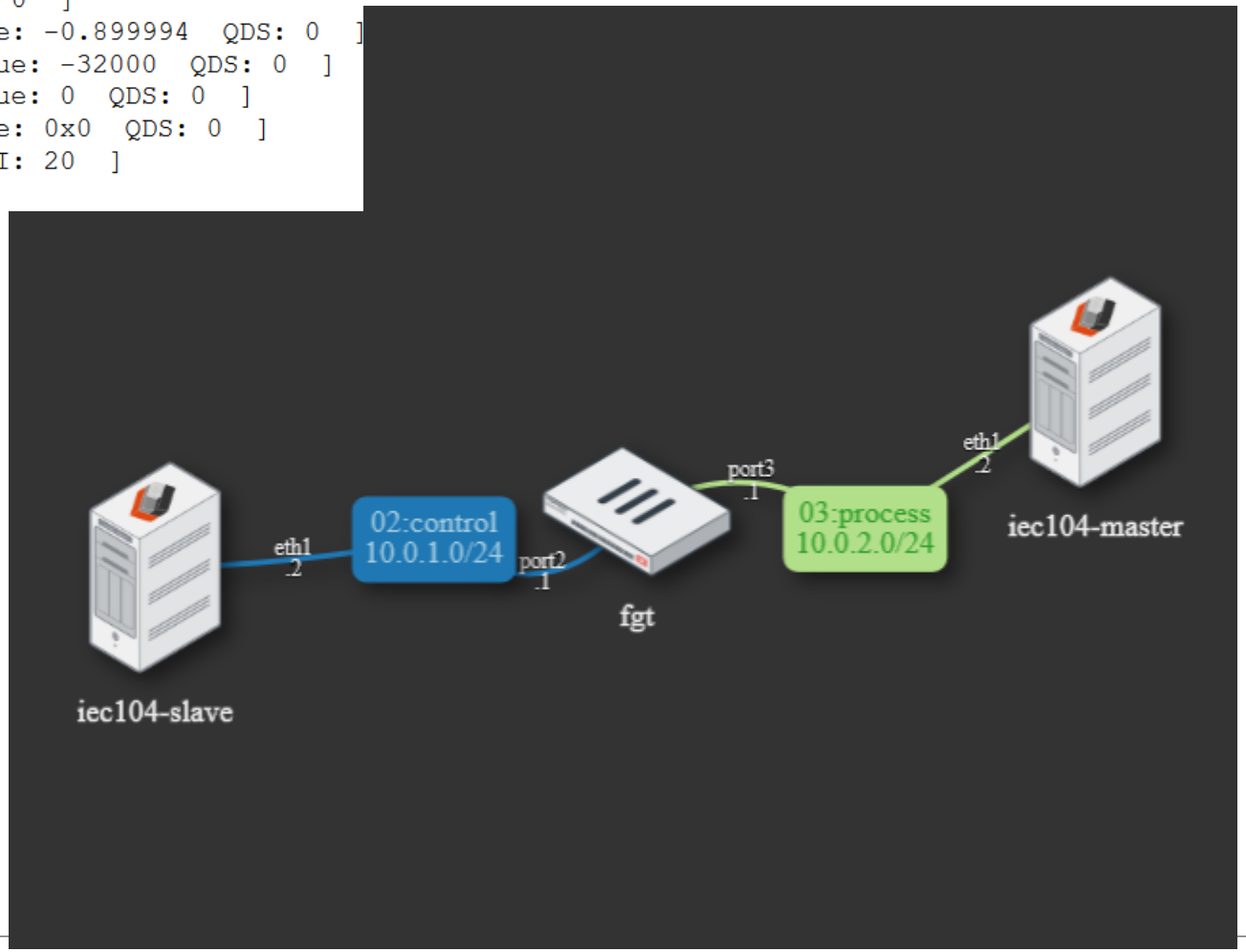
- Есть ли в организации АСУ ТП, объединены ли эти системы в единую сеть?
- Как отделена сеть АСУ ТП, как предоставляется удалённый доступ?
- Сколько в организации IoT (Smart TV, IP-камер и прочих подобных устройств)?
- Контролируется ли межсетевое взаимодействие IoT, выполняется ли обновление?
- Примеры инцидентов:
  - » Industroyer/CRASHOVERRIDE – вредоносное ПО, способн
    - https://habr.com/company/eset/blog/330730/
    - Модули для IEC 101, IEC 104, IEC 61850, OPC DA
    - Широко распространенные промышленные протоколы, которые создава
    - Главный компонент – бэкдор, используется атакующими для управлени
    - Стоит упомянуть, что большинство C&C-серверов бэкдора используют
  - » Уязвимости в камерах Dahua и HikVision
    - https://www.csoonline.com/article/3269199/security/critical-hikvision-flaw-cou
    - Удалённый доступ к видео, потенциальная компрометация
    - Dahua, CVSS 10: 2017, 2013, 2013
    - HikVision, CVSS 10: 2017, 2013
    -



https://fortiguard.com/encyclopedia/virus/7412580
https://fortiguard.com/encyclopedia/ips/39673/hikvision-dvr-rtsp-request-remote-code-execution

Use case – защита АСУ ТП и Интернета вещей

```
INFO:root:Sending:  STARTDT_ACT
INFO:root:Received: STARTDT_CON
INFO:root:Sending:  ASDU addr 1000, type 100, CoT 6, [IOA: 0  QOI: 20  ]
INFO:root:Received: ASDU addr 1000, type 100, CoT 7, [IOA: 0  QOI: 20  ]
INFO:root:Received: ASDU addr 1000, type 1, CoT 20, [IOA: 1  SIQ: 1  ]
INFO:root:Received: ASDU addr 1000, type 3, CoT 20, [IOA: 2  DIQ: 0  ]
INFO:root:Received: ASDU addr 1000, type 9, CoT 20, [IOA: 3  Value: -0.899994  QDS: 0  ]
INFO:root:Received: ASDU addr 1000, type 11, CoT 20, [IOA: 4  Value: -32000  QDS: 0  ]
INFO:root:Received: ASDU addr 1000, type 13, CoT 20, [IOA: 5  Value: 0  QDS: 0  ]
INFO:root:Received: ASDU addr 1000, type 7, CoT 20, [IOA: 6  Value: 0x0  QDS: 0  ]
INFO:root:Received: ASDU addr 1000, type 100, CoT 10, [IOA: 0  QOI: 20  ]
INFO:root:Sending:  S: (6)
```



Use case – защита АСУ ТП и Интернета вещей

```
INFO:root:Sending:  STARTDT_ACT
INFO:root:Received: STAR
INFO:root:Sending:  ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Received: ASDU
INFO:root:Sending:  S:
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.1.2	10.0.2.2	TCP	74	34620 → 2404 [SYN] Seq=0 Win=29
2	0.000564	10.0.2.2	10.0.1.2	TCP	74	2404 → 34620 [SYN, ACK] Seq=0 A
3	0.011780	10.0.1.2	10.0.2.2	TCP	66	34620 → 2404 [ACK] Seq=1 Ack=1
4	0.014626	10.0.1.2	10.0.2.2	104apci	72	<- U (STARTDT act)
5	0.015135	10.0.2.2	10.0.1.2	TCP	66	2404 → 34620 [ACK] Seq=1 Ack=7
6	0.015849	10.0.2.2	10.0.1.2	104apci	72	-> U (STARTDT con)
7	0.017039	10.0.1.2	10.0.2.2	TCP	66	34620 → 2404 [ACK] Seq=7 Ack=7
8	1.014572	10.0.1.2	10.0.2.2	104asdu	82	<- I (0,0) ASDU=1000 C_IC_NA_1
9	1.017195	10.0.2.2	10.0.1.2	104asdu	82	-> I (0,1) ASDU=1000 C_IC_NA_1
10	1.018123	10.0.1.2	10.0.2.2	TCP	66	34620 → 2404 [ACK] Seq=23 Ack=2
11	1.018685	10.0.2.2	10.0.1.2	104asdu	190	-> I (1,1) ASDU=1000 M_SP_NA_1
12	1.022367	10.0.1.2	10.0.2.2	TCP	66	34620 → 2404 [ACK] Seq=23 Ack=1
13	1.022408	10.0.1.2	10.0.2.2	104apci	72	<- S (6)
14	1.022410	10.0.1.2	10.0.2.2	TCP	66	34620 → 2404 [FIN, ACK] Seq=29
15	1.023512	10.0.2.2	10.0.1.2	TCP	66	2404 → 34620 [FIN, ACK] Seq=147

```
> Frame 11: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:03:02 (02:09:0f:00:03:02), Dst: MS-NLB-PhysServer-09_0f:00:03:01 (02:09:0f:00:03:01)
> Internet Protocol Version 4, Src: 10.0.2.2 (10.0.2.2), Dst: 10.0.1.2 (10.0.1.2)
> Transmission Control Protocol, Src Port: 2404, Dst Port: 34620, Seq: 23, Ack: 23, Len: 124
> IEC 60870-5-104-Apci: -> I (1,1)
> IEC 60870-5-104-Asdu: ASDU=1000 M_SP_NA_1 Inrogen IOA=1 'single-point information'
> IEC 60870-5-104-Apci: -> I (2,1)
> IEC 60870-5-104-Asdu: ASDU=1000 M_DP_NA_1 Inrogen IOA=2 'double-point information'
> IEC 60870-5-104-Apci: -> I (3,1)
> IEC 60870-5-104-Asdu: ASDU=1000 M_ME_NA_1 Inrogen IOA=3 'measured value, normalized value'
> IEC 60870-5-104-Apci: -> I (4,1)
> IEC 60870-5-104-Asdu: ASDU=1000 M_ME_NB_1 Inrogen IOA=4 'measured value, scaled value'
> IEC 60870-5-104-Apci: -> I (5,1)
```

Use case – защита АСУ ТП и Интернета вещей

10.0.1.2	10.0.2.2	IEC.60870.5.104_Supervisory.Functions	pass	Supervisory Functions
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.C.IC.NA.1	pass	Information Transfer.C.IC.NA.1: 01 0a 00 e8 03 00 00 00 14
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.M.BO.NA.1	pass	Information Transfer.M.BO.NA.1: 01 14 00 e8 03 06 00 00 00 00 00 00 00
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.M.ME.NC.1	pass	Information Transfer.M.ME.NC.1: 01 14 00 e8 03 05 00 00 00 00 00 00 00
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.M.ME.NB.1	pass	Information Transfer.M.ME.NB.1: 01 14 00 e8 03 04 00 00 00 83 00
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.M.ME.NA.1	pass	Information Transfer.M.ME.NA.1: 01 14 00 e8 03 03 00 00 cd 8c 00
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.M.DP.NA.1	pass	Information Transfer.M.DP.NA.1: 01 14 00 e8 03 02 00 00 00
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.M.SP.NA.1	pass	Information Transfer.M.SP.NA.1: 01 14 00 e8 03 01 00 00 01
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.C.IC.NA.1	pass	Information Transfer.C.IC.NA.1: 01 07 00 e8 03 00 00 00 14
10.0.1.2	10.0.2.2	IEC.60870.5.104_Information.Transfer.C.IC.NA.1	pass	Information Transfer.C.IC.NA.1: 01 06 00 e8 03 00 00 00 14
10.0.1.2	10.0.2.2	IEC.60870.5.104_Control.Functions.STARTDT.CON	pass	Control Functions.STARTDT.CON
10.0.1.2	10.0.2.2	IEC.60870.5.104_Control.Functions.STARTDT.ACT	pass	Control Functions.STARTDT.ACT
10.0.1.2	10.0.2.2	IEC.60870.5.104_Control.Functions.STARTDT.ACT	block	Control Functions.STARTDT.ACT
10.0.1.2	10.0.2.2	IEC.60870.5.104_Control.Functions.STARTDT.ACT	block	Control Functions.STARTDT.ACT

10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 100 , CoT= 10
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 7 , CoT= 20
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 13 , CoT= 20
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 11 , CoT= 20
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 9 , CoT= 20
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 3 , CoT= 20
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 1 , CoT= 20
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 100 , CoT= 7
10.0.1.2	10.0.2.2	IEC104.ASDU	pass	COA= 1000 , ASDU Type= 100 , CoT= 6
10.0.1.2	10.0.2.2	IEC.60870.5.104_CF	pass	CF
10.0.1.2	10.0.2.2	IEC.60870.5.104_CF	pass	CF

ВОПРОСЫ?

Fortinet@netwell.ru