Управление техническими уязвимостями в 3 клика

Николай Казанцев

Начальник отдела ИБ

ООО НТФФ ПОЛИСАН

О чем?

vulnerability management

Управление уязвимостями — это «циклическая практика выявления, классификации, приоритезации, исправления и снижения» уязвимостей программного обеспечения. Управление уязвимостями является неотъемлемой частью компьютерной и сетевой безопасности, и его не следует путать с оценкой уязвимостей.

Поработал с

OpenVAS

Open Vulnerability Assessment Scanner

Qualys®

MAXPATROL

nessus®
Professional

XSpider

REDCheck

ScanOVAL

OWASP
Zed Attack Proxy

BURPSUITE

NMAP

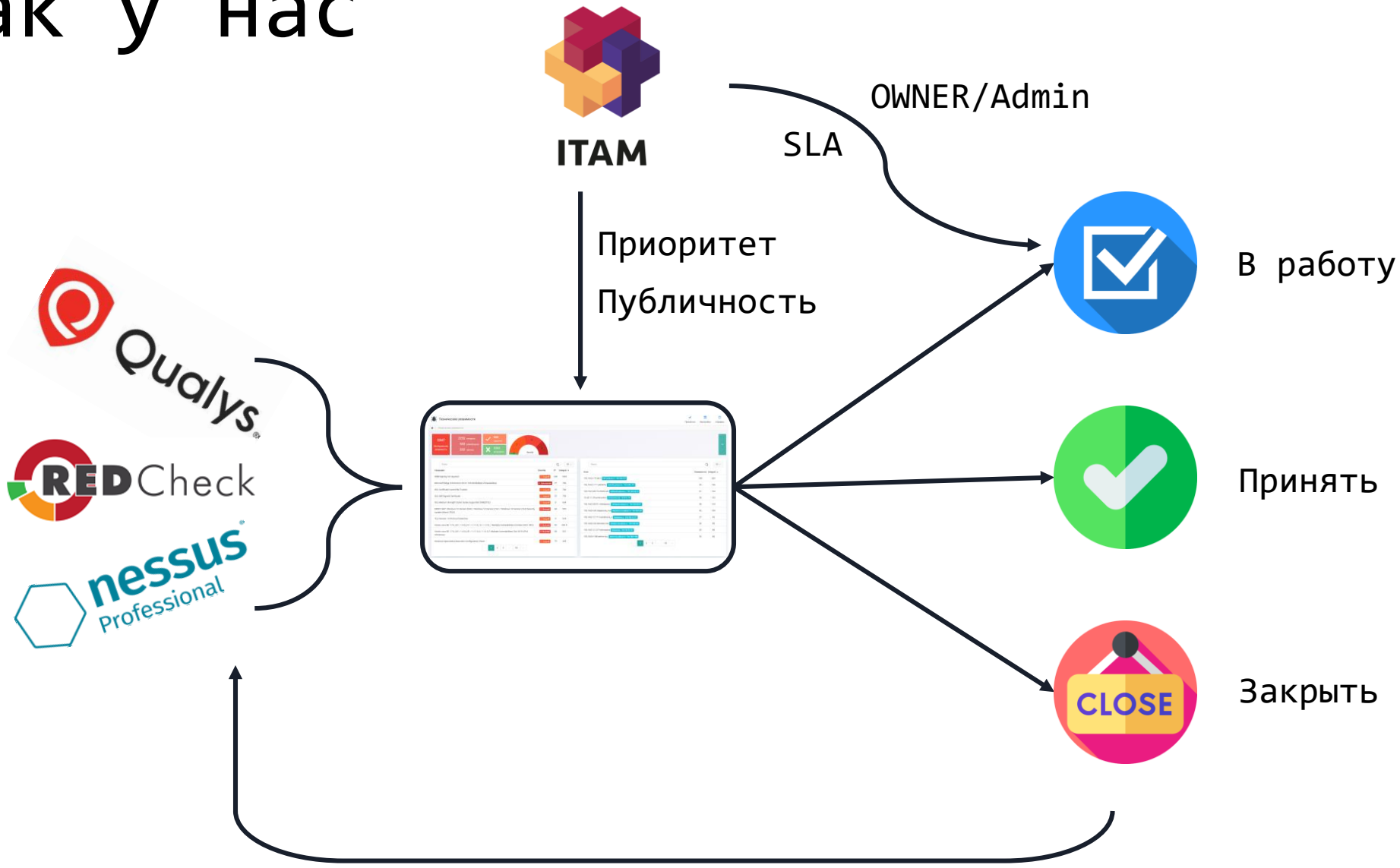
Как бывает

- Скан
- Скан – задача
- Скан – анализ – задача
- Скан – анализ – задача – контроль
- Скан – обогащение – анализ – задача – контроль

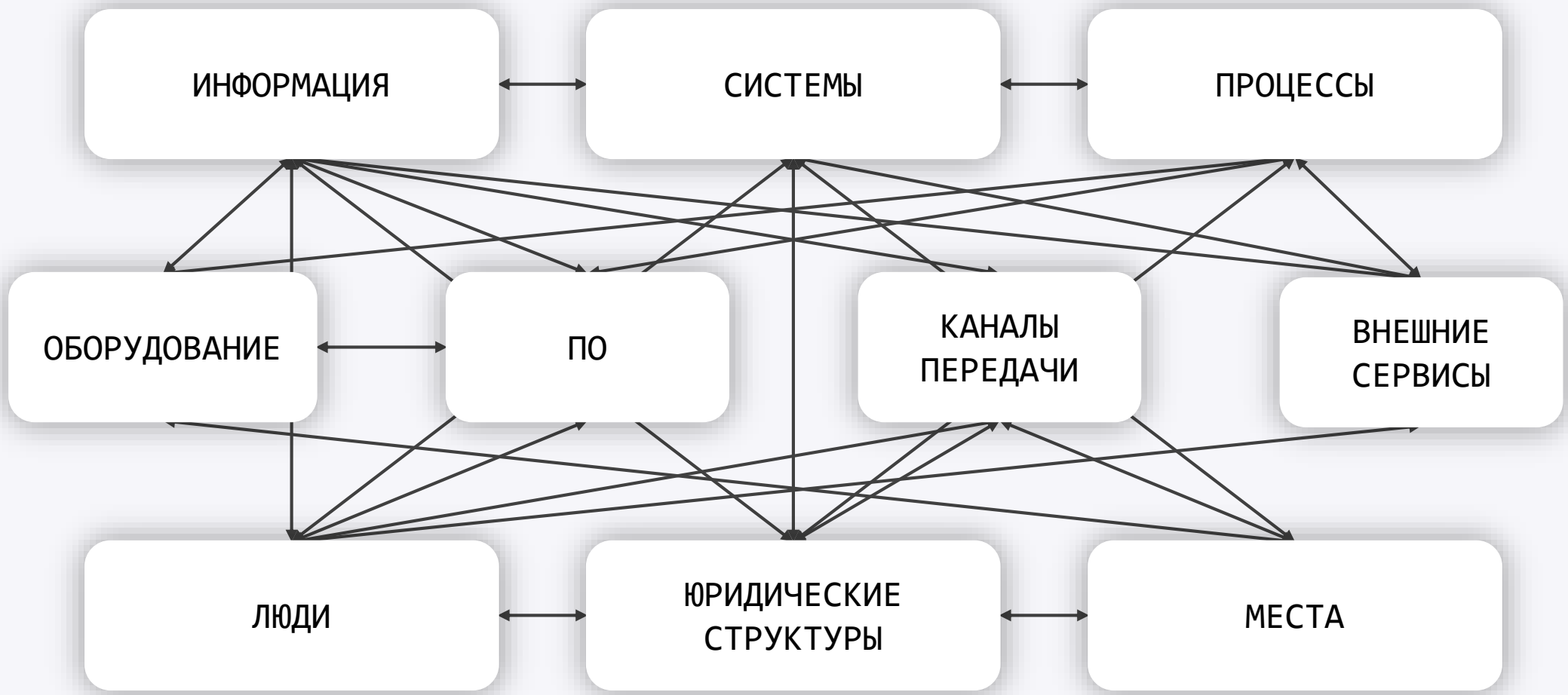
Как бывает

- Скан
- Скан – задача
- Скан – анализ – задача
- Скан – анализ – задача – контроль
- Скан – обогащение – анализ – задача – контроль

Как у нас

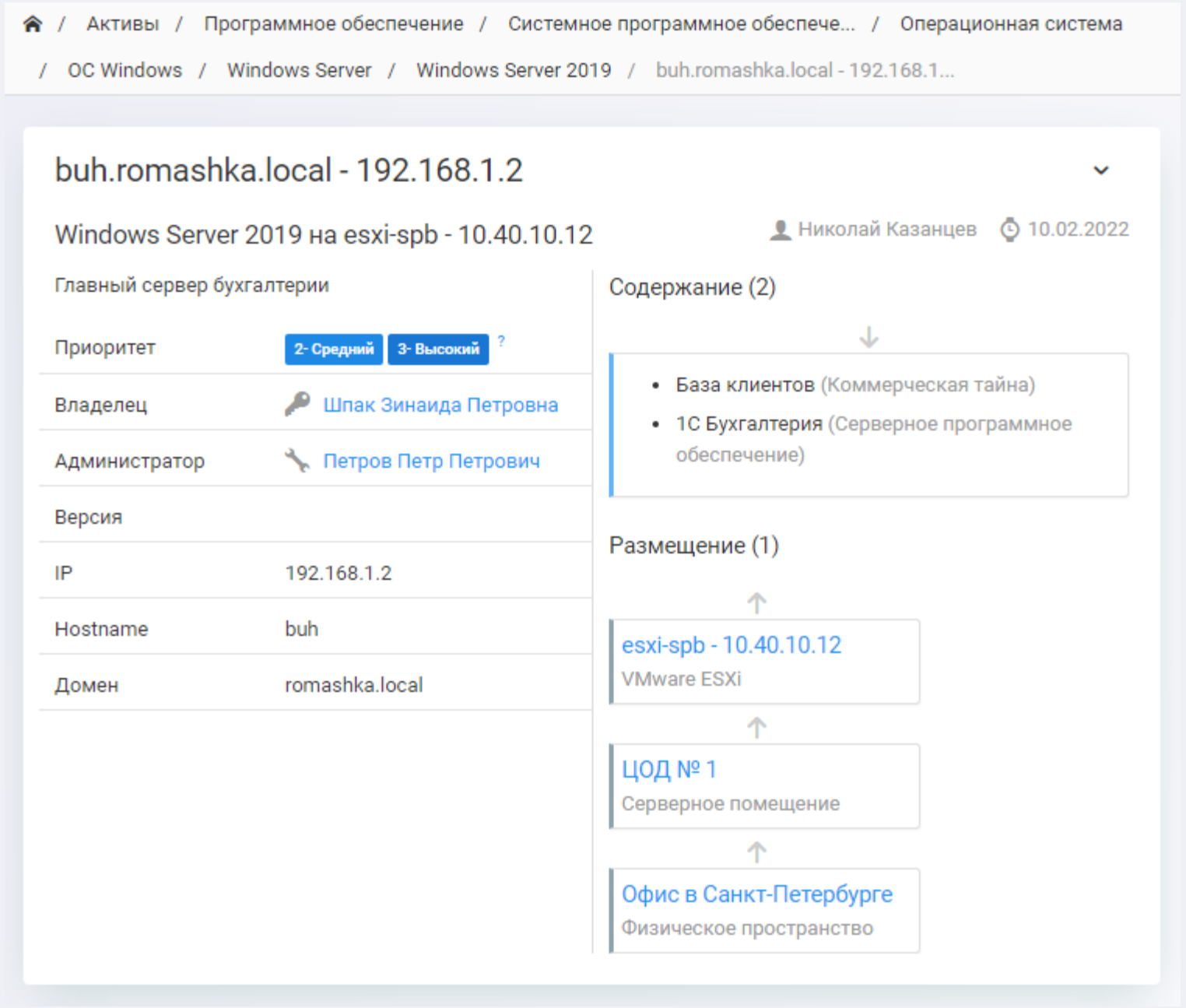

ITAM
OWNER/Admin
SLA
Приоритет
Публичность
Qualys
REDCheck
nessus
Professional
В работу
Принять
CLOSE
Закрыть

Что такое активы

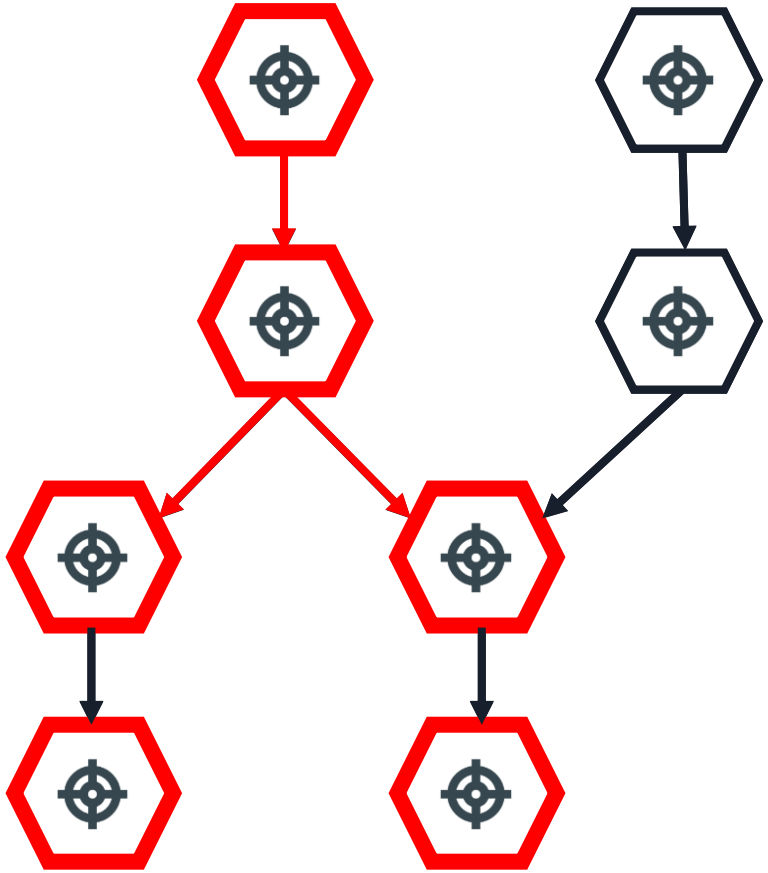


Связи

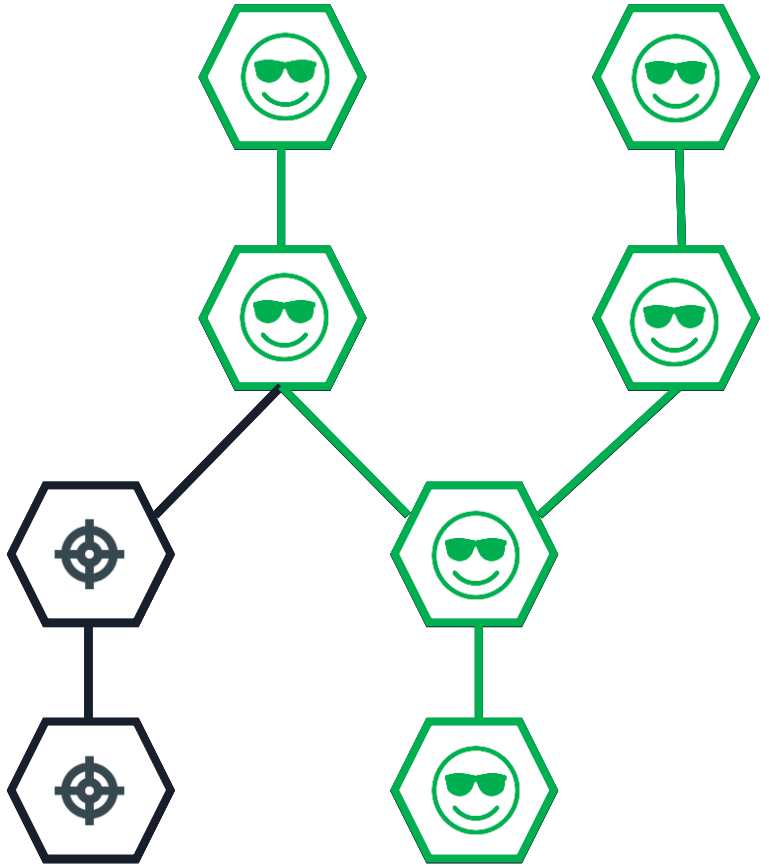
\ Информация



1.Приоритет

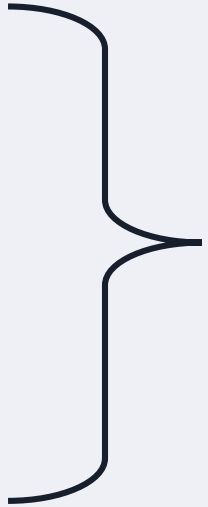


2.Владелец



Интегральная уязвимость

- Критичность уязвимости
- Количество уязвимых хостов
- Количество уязвимостей на хосте
- Приоритет актива
- Публичность актива
- Связи актива



- Приоритезация
- SLA

- Формула риска для хоста:

SUM(Vulns severity) x |0,5 * MAX(Asset priority)| x |1,5*[Asset publicity]|

- Формула риска для уязвимости

[Vuln severity] x |COUNT(IP)| x |0,5 * MAX(Asset priority)| * |1.5*COUNT(Public Assets)|

ГЛАВНАЯ
МОИ ДЕЛА
КАТАЛОГИ
ТРЕБОВАНИЯ
ТИПЫ АКТИВОВ
АКТИВЫ
УГРОЗЫ
УЯЗВИМОСТИ
РИСКИ
ЗАЩИТНЫЕ МЕРЫ
ЗАДАЧИ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ГЛОБАЛЬНЫЕ НАСТРОЙКИ

Технические уязвимости

Принятые | Настройки | Справка

/ Технические уязвимости

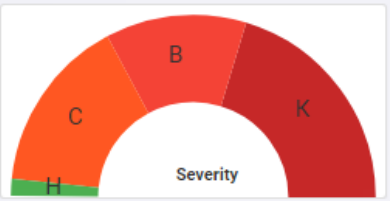
882 Интегральная уязвимость

350 открыт
132 типа
49 хостов

7 Задач в работе
3 просрочена

43 принято

7 устранено



Поиск | 10

Название	Severity	IP	Integral ▲
SSL Certificate Cannot Be Trusted	2 - Средний	30	62
Microsoft Edge (Chromium) 99.0.1150.30 Multiple Vulnerabilities	4 - Критический	11	48
SSL Self-Signed Certificate	2 - Средний	24	48
Microsoft XML Parser (MSXML) and XML Core Services Unsupported	4 - Критический	6	28
TLS Version 1.0 Protocol Detection	2 - Средний	12	24
SSL Medium Strength Cipher Suites Supported (SWEET32)	2 - Средний	11	22
Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)	3 - Высокий	7	21
Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)	3 - Высокий	7	21
Microsoft Teams 1.3.0.13000 Remote Code Execution	2 - Средний	10	20
Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)	2 - Средний	9	20

‹ 1 2 3 ... 14 ›

Поиск | 10

Host	Уязвимости	Integral ▲
192.168.6.135	47	159
192.168.12.171 kuznetsova_o kuznetsova_o - 192.168.12.171	28	99
192.168.12.127 kishmareva kishmareva - 192.168.12.127	34	93
10.33.31.78 dankina dankina.mycorp.local - 10.33.31.78	24	56
10.33.31.134 varenichenko varenichenko.mycorp.local - 10.33.31.134	22	52
192.168.12.234 andreeva-au andreeva-au.mycorp.local - 192.168.12.234	18	41
10.33.31.71 petrov petrov.mycorp.local - 10.33.31.71	16	36
10.33.31.147 makarevich makarevich.mycorp.local - 10.33.31.147	12	31
192.168.12.168 kolodjaznyi kolodjaznyi.mycorp.local - 192.168.12.168	13	29
192.168.12.199 akimov akimov.mycorp.local - 192.168.12.199	12	28

‹ 1 2 3 ... 5 ›

ГЛАВНАЯ
МОИ ДЕЛА
КАТАЛОГИ
ТРЕБОВАНИЯ
ТИПЫ АКТИВОВ
АКТИВЫ
УГРОЗЫ
УЯЗВИМОСТИ
РИСКИ
ЗАЩИТНЫЕ МЕРЫ
ЗАДАЧИ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ГЛОБАЛЬНЫЕ НАСТРОЙКИ

Технические уязвимости

Принятые | Настройки | Справка

/ Технические уязвимости

882 Интегральная уязвимость

9 открыт
1 тип
9 хостов

1 Задач в работе

0 принято

0 устранено

Создать задачу | Принять все | Закрыть все

Windows Speculative Execution Configuration Check

№ nessus_132101 | Статус Открыто | CVSS 5.4 | CVSS3 6.4 | IP 9 | Severity 2 - Средний | Integral 18

Группа Windows

The remote host has not properly mitigated a series of known speculative execution vulnerabilities. It, therefore, may be affected by :
- Branch Target Injection (BTI) (CVE-2017-5715)
- Bounds Check Bypass (BCB) (CVE-2017-5753)
- Rogue Data Cache Load (RDCL) (CVE-2017-5754)
- Rogue System Register Read (RSRE) (CVE-2018-3640)
- Speculative Store Bypass (SSB) (CVE-2018-3639)
- L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)
- Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091)
- Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126)
- Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127)
- Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130)
- TSX Asynchronous Abort (TAA) (CVE-2019-11135)

Дополнительные материалы

http://www.nessus.org/u?8902cebb
http://www.nessus.org/u?6a005ed4

Решение

Apply vendor recommended settings.

Поиск

Host	Уязвимости	Integral
192.168.12.127 kishmareva kishmareva - 192.168.12.127	34	93
10.33.31.78 dankina dankina.mycorp.local - 10.33.31.78	24	56
10.33.31.134 varenichenko varenichenko.mycorp.local - 10.33.31.134	22	52
192.168.12.234 andreeva-au andreeva-au.mycorp.local - 192.168.12.234	18	41
10.33.31.71 petrov petrov.mycorp.local - 10.33.31.71	16	36
192.168.12.199 akimov akimov.mycorp.local - 192.168.12.199	12	28
192.168.12.128 iushkova iushkova.mycorp.local - 192.168.12.128	10	24
192.168.12.211 semichuk-pc semichuk-pc - 192.168.12.211	6	15
10.33.31.87 ivanov ivanov.mycorp.local - 10.33.31.87	2	6

ГЛАВНАЯ
МОИ ДЕЛА
КАТАЛОГИ
ТРЕБОВАНИЯ
ТИПЫ АКТИВОВ
АКТИВЫ
УГРОЗЫ
УЯЗВИМОСТИ
РИСКИ
ЗАЩИТНЫЕ МЕРЫ
ЗАДАЧИ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ГЛОБАЛЬНЫЕ НАСТРОЙКИ

Технические уязвимости

Принятые | Настройки | Справка

/ Технические уязвимости

882 Интегральная уязвимость

24 открыта
24 типа
1 хост

0 Задач в работе

1 принято

0 устранено

Поиск

10

Название	Severity	IP	Integral
SSL Certificate Cannot Be Trusted	2 - Средний	30	62
Microsoft Edge (Chromium) 99.0.1150.30 Multiple Vulnerabilities	4 - Критический	11	48
SSL Self-Signed Certificate	2 - Средний	24	48
Microsoft XML Parser (MSXML) and XML Core Services Unsupported	4 - Критический	6	28
TLS Version 1.0 Protocol Detection	2 - Средний	12	24
SSL Medium Strength Cipher Suites Supported (SWEET32)	2 - Средний	11	22
Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)	3 - Высокий	7	21
Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)	3 - Высокий	7	21
Microsoft Teams 1.3.0.13000 Remote Code Execution	2 - Средний	10	20
Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)	2 - Средний	9	20

‹ 1 2 3 ›

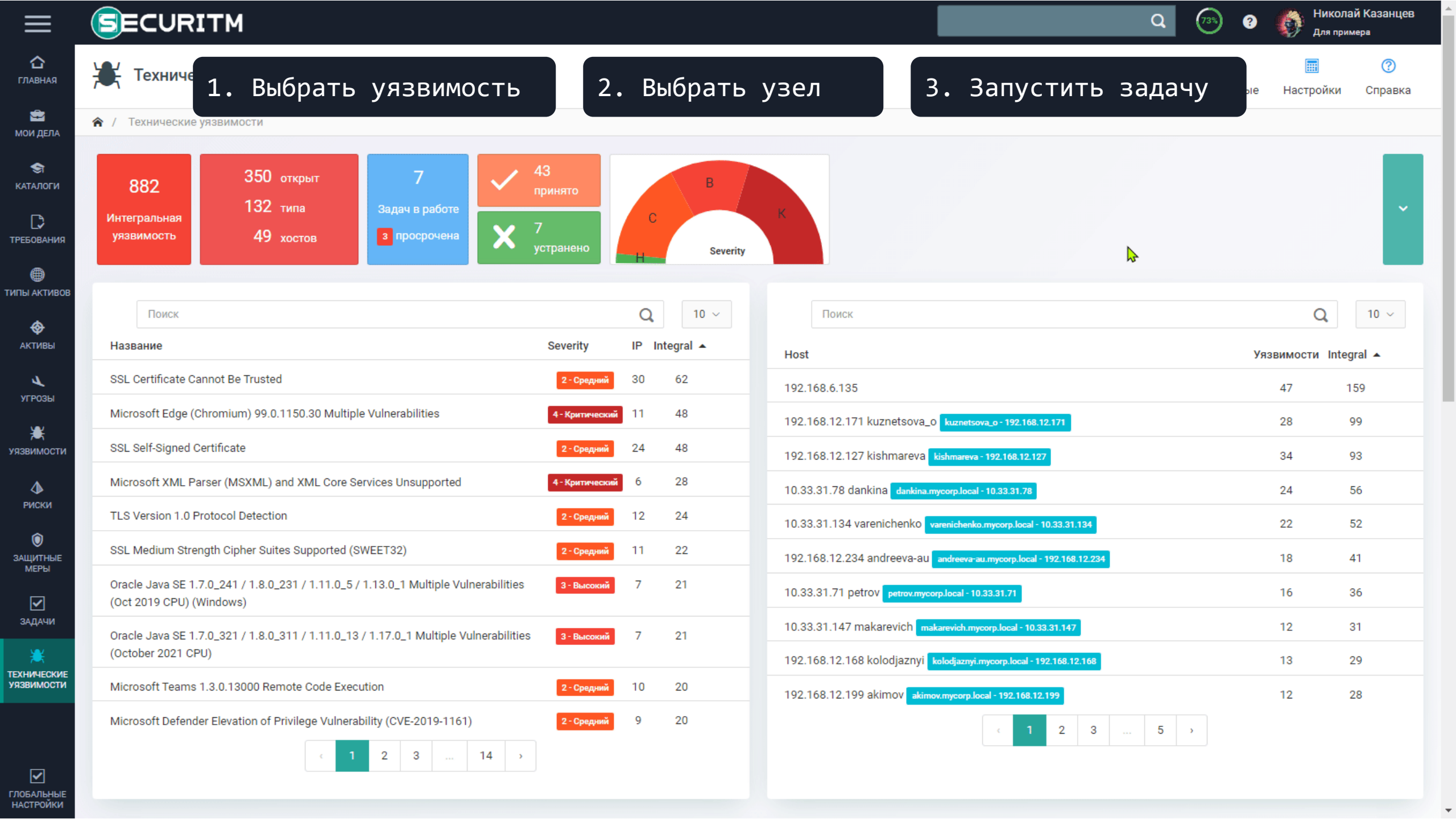
Создать задачу

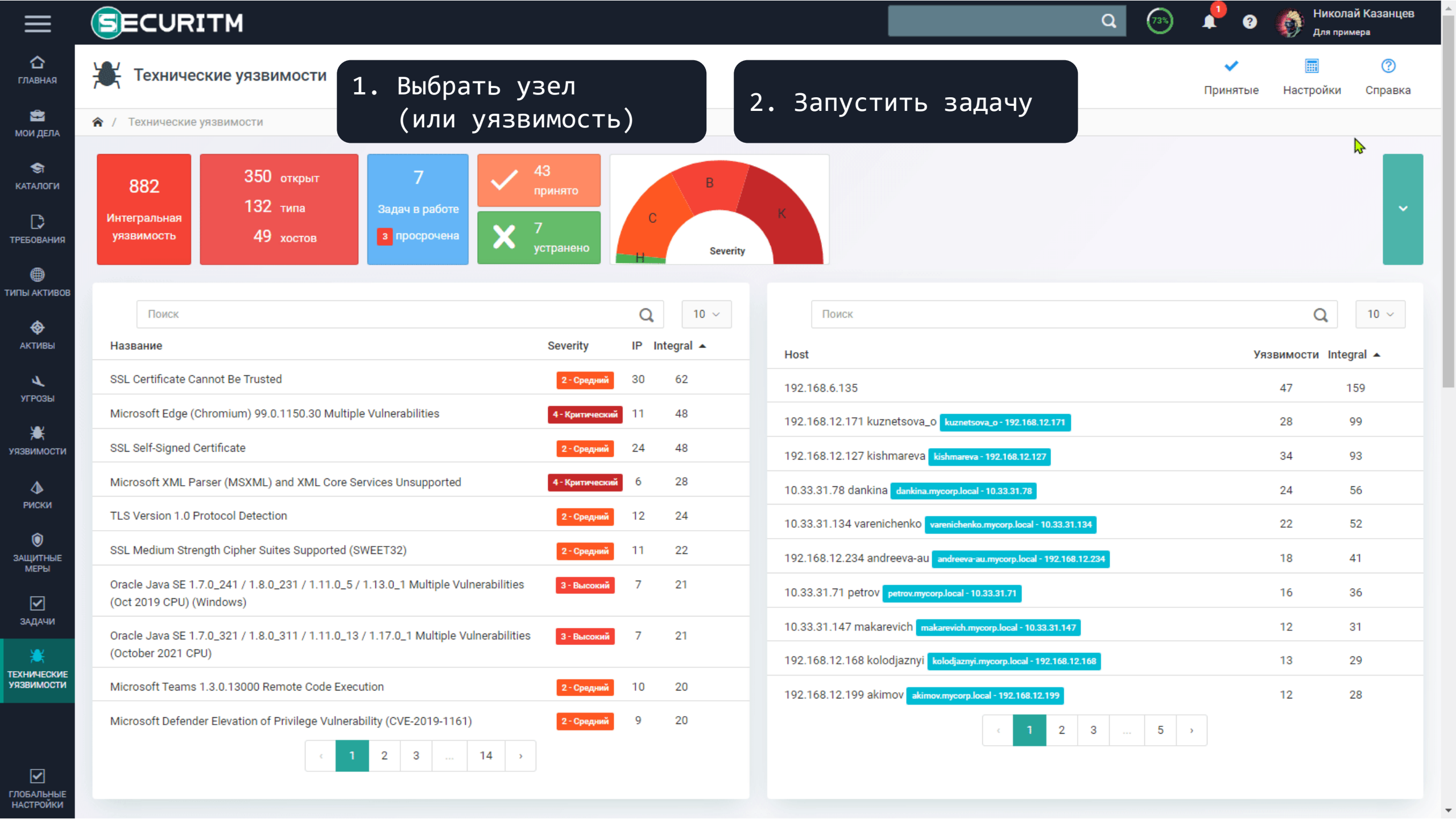
10.33.31.78 dankina

Приоритет 2- Средний | Уязвимостей 24 | Integral 56 | 20.04.2022 | 20.04.2022

Связанные активы

Название
Windows 10 dankina.mycorp.local - 10.33.31.78 20.04.2022 Отдел ИТ


SECURITM
Николай Казанцев
Для примера
1. Выбрать уязвимость
2. Выбрать узел
3. Запустить задачу
Настройки
Справка
ГЛАВНАЯ
МОИ ДЕЛА
КАТАЛОГИ
ТРЕБОВАНИЯ
ТИПЫ АКТИВОВ
АКТИВЫ
УГРОЗЫ
УЯЗВИМОСТИ
РИСКИ
ЗАЩИТНЫЕ МЕРЫ
ЗАДАЧИ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ГЛОБАЛЬНЫЕ НАСТРОЙКИ
Технические уязвимости
882
Интегральная уязвимость
350 открыт
132 типа
49 хостов
7
Задач в работе
3 просрочена
43
принято
7
устранено
B
C
K
H
Severity
Поиск
10
Название
Severity
IP
Integral
SSL Certificate Cannot Be Trusted
2 - Средний
30
62
Microsoft Edge (Chromium) 99.0.1150.30 Multiple Vulnerabilities
4 - Критический
11
48
SSL Self-Signed Certificate
2 - Средний
24
48
Microsoft XML Parser (MSXML) and XML Core Services Unsupported
4 - Критический
6
28
TLS Version 1.0 Protocol Detection
2 - Средний
12
24
SSL Medium Strength Cipher Suites Supported (SWEET32)
2 - Средний
11
22
Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)
3 - Высокий
7
21
Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)
3 - Высокий
7
21
Microsoft Teams 1.3.0.13000 Remote Code Execution
2 - Средний
10
20
Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)
2 - Средний
9
20
1
2
3
14
Поиск
10
Host
Уязвимости
Integral
192.168.6.135
47
159
192.168.12.171 kuznetsova_o
kuznetsova_o - 192.168.12.171
28
99
192.168.12.127 kishmareva
kishmareva - 192.168.12.127
34
93
10.33.31.78 dankina
dankina.mycorp.local - 10.33.31.78
24
56
10.33.31.134 varenichenko
varenichenko.mycorp.local - 10.33.31.134
22
52
192.168.12.234 andreeva-au
andreeva-au.mycorp.local - 192.168.12.234
18
41
10.33.31.71 petrov
petrov.mycorp.local - 10.33.31.71
16
36
10.33.31.147 makarevich
makarevich.mycorp.local - 10.33.31.147
12
31
192.168.12.168 kolodjaznyi
kolodjaznyi.mycorp.local - 192.168.12.168
13
29
192.168.12.199 akimov
akimov.mycorp.local - 192.168.12.199
12
28
1
2
3
5


SECURITM
Николай Казанцев
Для примера
ГЛАВНАЯ
МОИ ДЕЛА
КАТАЛОГИ
ТРЕБОВАНИЯ
ТИПЫ АКТИВОВ
АКТИВЫ
УГРОЗЫ
УЯЗВИМОСТИ
РИСКИ
ЗАЩИТНЫЕ МЕРЫ
ЗАДАЧИ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ГЛОБАЛЬНЫЕ НАСТРОЙКИ
Технические уязвимости
1. Выбрать узел (или уязвимость)
2. Запустить задачу
Принятые
Настройки
Справка
Технические уязвимости
882
Интегральная уязвимость
350 открыт
132 типа
49 хостов
7
Задач в работе
3 просрочена
43
принято
7
устранено
B
C
K
H
Severity
Поиск
10
Название
Severity
IP
Integral
SSL Certificate Cannot Be Trusted
2 - Средний
30
62
Microsoft Edge (Chromium) 99.0.1150.30 Multiple Vulnerabilities
4 - Критический
11
48
SSL Self-Signed Certificate
2 - Средний
24
48
Microsoft XML Parser (MSXML) and XML Core Services Unsupported
4 - Критический
6
28
TLS Version 1.0 Protocol Detection
2 - Средний
12
24
SSL Medium Strength Cipher Suites Supported (SWEET32)
2 - Средний
11
22
Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)
3 - Высокий
7
21
Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)
3 - Высокий
7
21
Microsoft Teams 1.3.0.13000 Remote Code Execution
2 - Средний
10
20
Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)
2 - Средний
9
20
1
2
3
14
Поиск
10
Host
Уязвимости
Integral
192.168.6.135
47
159
192.168.12.171 kuznetsova_o
kuznetsova_o - 192.168.12.171
28
99
192.168.12.127 kishmareva
kishmareva - 192.168.12.127
34
93
10.33.31.78 dankina
dankina.mycorp.local - 10.33.31.78
24
56
10.33.31.134 varenichenko
varenichenko.mycorp.local - 10.33.31.134
22
52
192.168.12.234 andreeva-au
andreeva-au.mycorp.local - 192.168.12.234
18
41
10.33.31.71 petrov
petrov.mycorp.local - 10.33.31.71
16
36
10.33.31.147 makarevich
makarevich.mycorp.local - 10.33.31.147
12
31
192.168.12.168 kolodjaznyi
kolodjaznyi.mycorp.local - 192.168.12.168
13
29
192.168.12.199 akimov
akimov.mycorp.local - 192.168.12.199
12
28
1
2
3
5

Принятие уязвимостей

* Принятие рисков эксплуатации конкретных технических уязвимостей

ГЛАВНАЯ
МОИ ДЕЛА
КАТАЛОГИ
ТРЕБОВАНИЯ
ТИПЫ АКТИВОВ
АКТИВЫ
УГРОЗЫ
УЯЗВИМОСТИ
РИСКИ
ЗАЩИТНЫЕ МЕРЫ
ЗАДАЧИ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ГЛОБАЛЬНЫЕ НАСТРОЙКИ

Технические уязвимости

Принятые | Настройки | Справка

/ Технические уязвимости

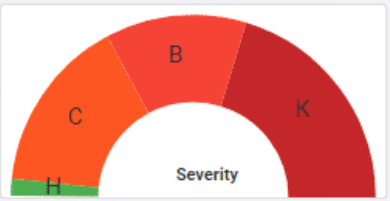
882 Интегральная уязвимость

350 открыт
132 типа
49 хостов

8 Задач в работе
3 просрочена

43 принято

7 устранено



Поиск | 10

Название	Severity	IP	Integral
SSL Certificate Cannot Be Trusted	2 - Средний	30	62
Microsoft Edge (Chromium) 99.0.1150.30 Multiple Vulnerabilities	4 - Критический	11	48
SSL Self-Signed Certificate	2 - Средний	24	48
Microsoft XML Parser (MSXML) and XML Core Services Unsupported	4 - Критический	6	28
TLS Version 1.0 Protocol Detection	2 - Средний	12	24
SSL Medium Strength Cipher Suites Supported (SWEET32)	2 - Средний	11	22
Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)	3 - Высокий	7	21
Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)	3 - Высокий	7	21
Microsoft Teams 1.3.0.13000 Remote Code Execution	2 - Средний	10	20
Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)	2 - Средний	9	20

‹ 1 2 3 ... 14 ›

Поиск | 10

Host	Уязвимости	Integral
192.168.6.135	47	159
192.168.12.171 kuznetsova_o kuznetsova_o - 192.168.12.171	28	99
192.168.12.127 kishmareva kishmareva - 192.168.12.127	34	93
10.33.31.78 dankina dankina.mycorp.local - 10.33.31.78	24	56
10.33.31.134 varenichenko varenichenko.mycorp.local - 10.33.31.134	22	52
192.168.12.234 andreeva-au andreeva-au.mycorp.local - 192.168.12.234	18	41
10.33.31.71 petrov petrov.mycorp.local - 10.33.31.71	16	36
10.33.31.147 makarevich makarevich.mycorp.local - 10.33.31.147	12	31
192.168.12.168 kolodjaznyi kolodjaznyi.mycorp.local - 192.168.12.168	13	29
192.168.12.199 akimov akimov.mycorp.local - 192.168.12.199	12	28

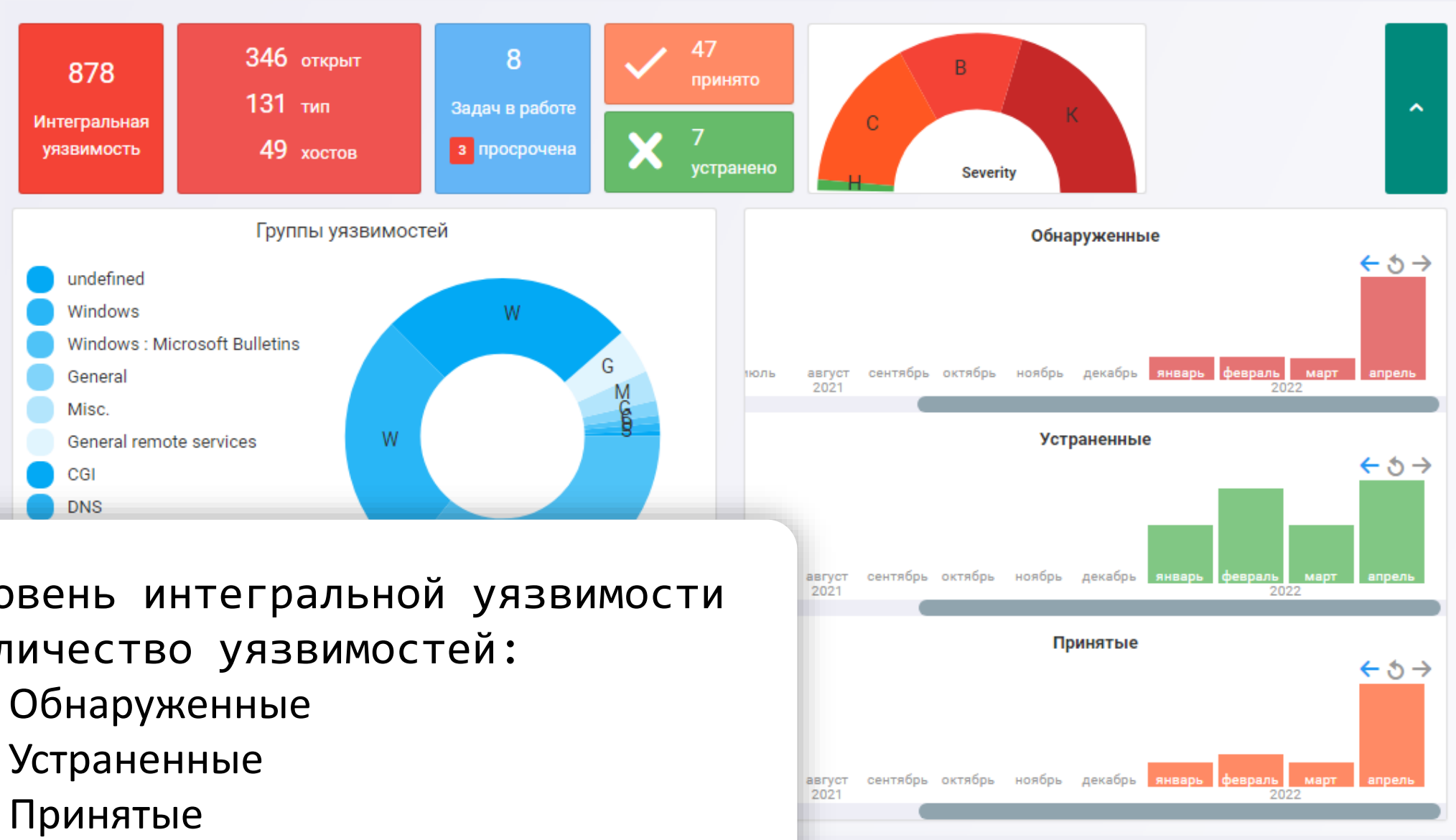
‹ 1 2 3 ... 5 ›

Profit

1. Все данные в 1 месте
2. Обогащение данных из реестра активов
3. Умная приоритезация (integral)
4. Принятие рисков
5. Авто-задачи, с ответственными, SLA, напоминаниями и отчётностью

1. Фокусировка на главном
2. Экономия времени
3. Отчетность

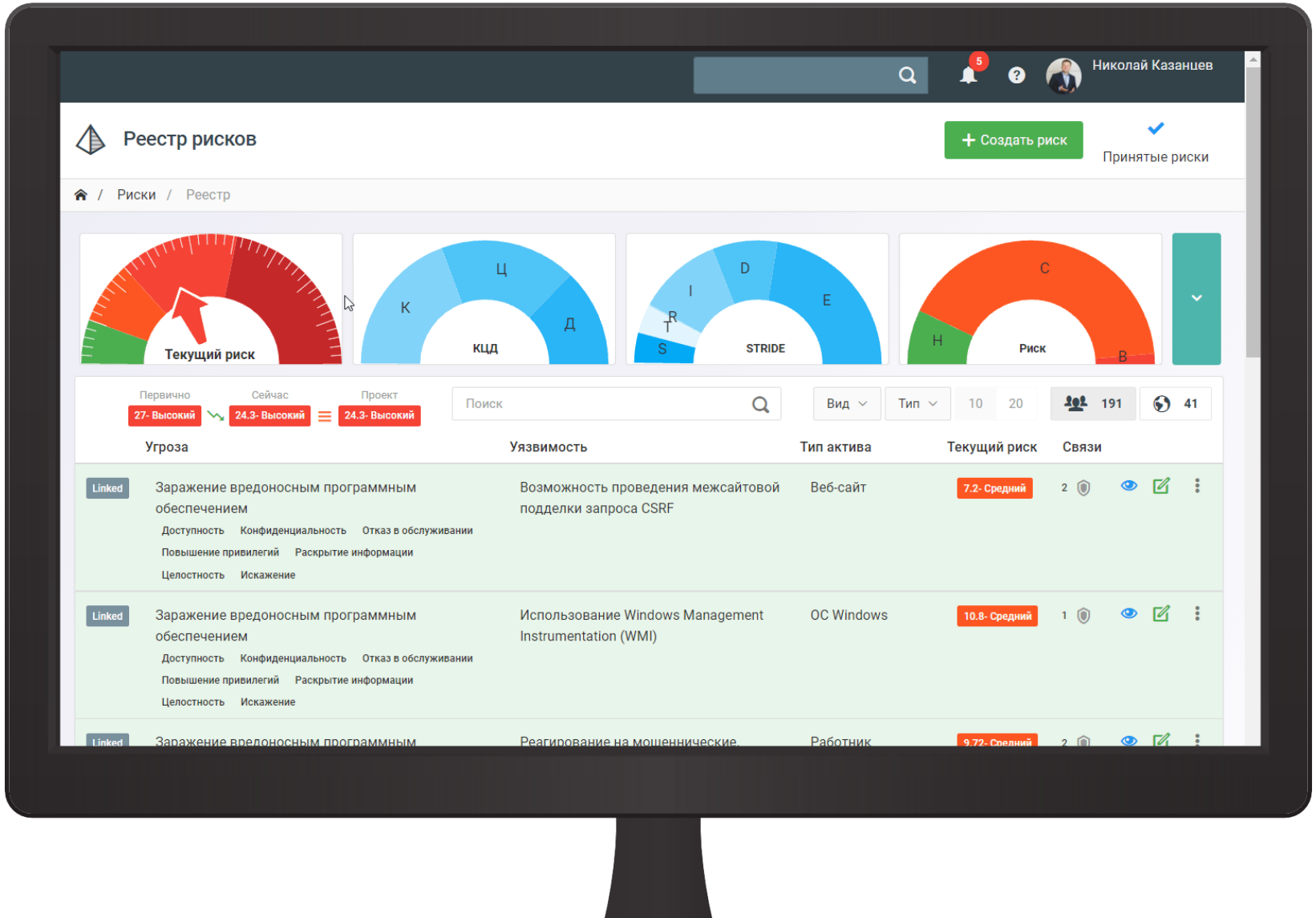
KPI



- Уровень интегральной уязвимости
- Количество уязвимостей:
  - Обнаруженные
  - Устраненные
  - Принятые

Community

securitm.ru



Спасибо за внимание

Николай Казанцев

t.me/NicKazantsev

+7(906)255-2009

spbsecurity.blogspot.com