

Ideco ISG

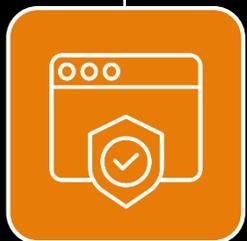
Проектируем решение
для защиты АСУ ТП

Руслан Никифоров

Заместитель директора по развитию



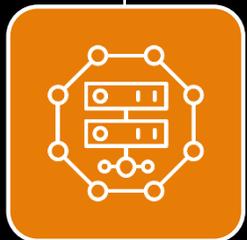
Айдеко – российский разработчик решений для сетевой безопасности



фильтрация
трафика



защита
сети



развитие сетевых
инфраструктур

Защищаем сети компаний межсетевым экраном Ideco UTM

2005

мы стартовали
на рынке ИБ

4 000

компаний используют
Ideco UTM

40 000

человек используют
VPN-подключения

2 000

бесплатных лицензий
для некоммерческого
использования

2020

начали сами
работать удаленно



UTM/NGFW

Модули Ideco UTM:



DPI Фильтрация на 7 уровне модели OSI

15 млн доменов и IP-адресов C&C в нашем BlockList

500 млн URL в обновляемой базе данных

Соответствие требованиям регулятора

Сертификат ФСТЭК №4503
от 28.12.2021 г.

Решение входит в реестр
российского ПО Минцифры РФ

- ✓ Требования доверия (4)
- ✓ Требования к МЭ
- ✓ Требования к СОВ
- ✓ Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ)
- ✓ Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ)
- ✓ Профиль защиты СОВ (четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

Customer success

Гибкая разработка

Моментальная реакция на новые вызовы и угрозы
Road-map по задачам пользователей

Защита сети «из коробки»

Преднастроенные правила фильтрации, IPS, FW

Шай-тек (Shy-tech)

Умные технологии для интуитивно понятных решений



Многоканальная техподдержка

- портал поддержки help.ideco.ru
- электронная почта
- телефон
- Telegram
- чат в продукте

Customer success

Выделенный менеджер для каждого
Фокус на долгосрочное партнерство
CustDev и проблемные интервью
Близко к community

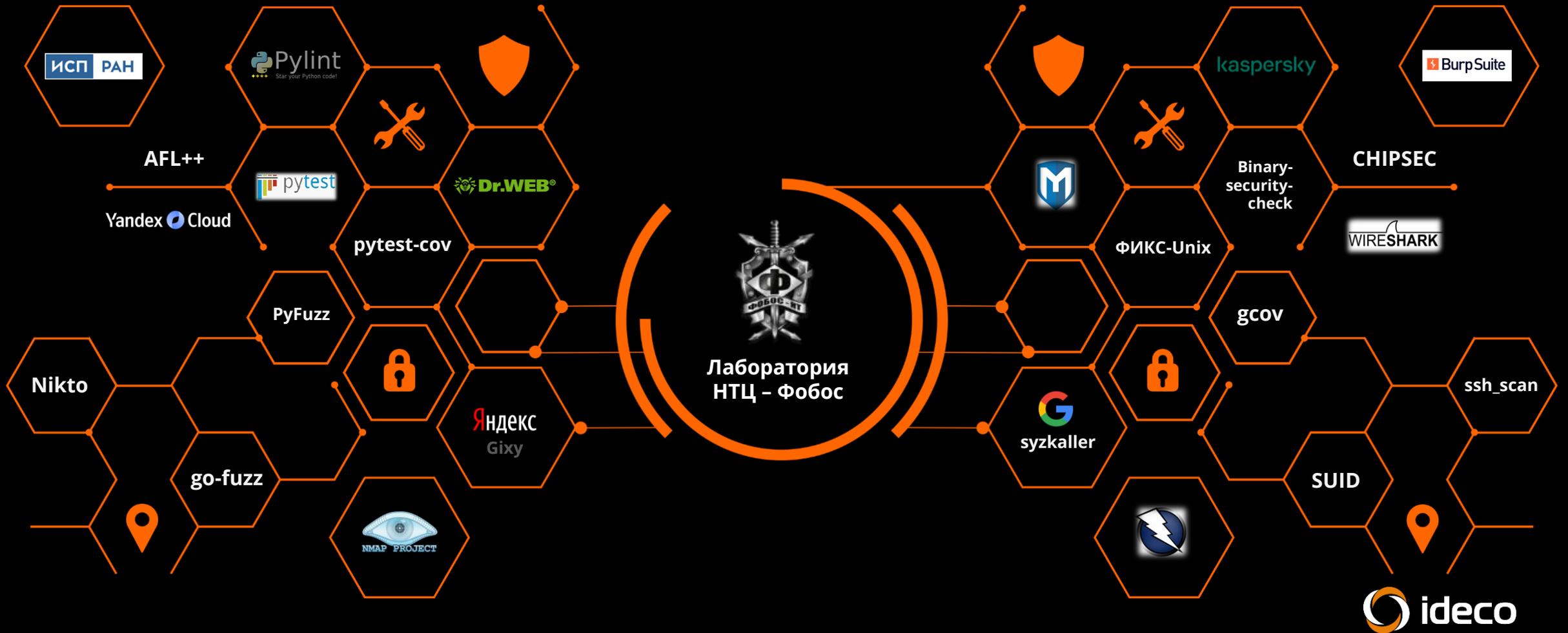
Presale

Поддержка и консультации на этапе тестирования и внедрения
Решения для нестандартных кейсов

SDL



Инструменты безопасной разработки



Svace

The screenshot displays the Svace web interface for a project named 'suricata'. The top navigation bar includes 'Project: suricata', 'Branch: master', and buttons for 'Review', 'Browse code', 'Reports', 'Settings', and 'Agents'. Below this, a 'Snapshot' section shows 'Snapshot 2021-04-21 08:55:33 +0000' and a 'Compare with:' dropdown.

The main content area is a table of detected issues, categorized by severity on the left:

- CRITICAL (checkers: 9, markers: 55)
- MAJOR (checkers: 22, markers: 159)
- NORMAL (checkers: 7, markers: 139)
- MINOR (checkers: 11, markers: 35)
- UNDEFINED (checkers: 0, markers: 0)

The table columns are: Checker, File, Line, and Description. The following table represents the visible data from the screenshot:

Checker	File	Line	Description
DOUBLE_FREE.EX	htp_hooks.c	52	Pointer 'copy' is passed to a function free at htp_hooks.c:82 by passing as 1st parameter to function 'htp_hook_destroy' at htp_hooks.c:52 after the reference...
DOUBLE_FREE.EX	app-layer-dnp3.c	1374	Pointer '(**objects->tqh_first).points' is passed to a function free at app-layer-dnp3.c:653 by calling function 'DNP3ObjectFree' at app-layer-dnp3.c:1374 after...
DOUBLE_FREE.EX	app-layer-dnp3.c	1463	Pointer '(**state->tx_list->tqh_first).de_state' is passed to a function free at app-layer-dnp3.c:1396 by calling function 'DNP3TxFree' at app-layer-dnp3.c:1463 a...
DOUBLE_FREE.EX	app-layer-ftp.c	340	Pointer '(**tx->response_list->tqh_first).str' is passed to a function free at app-layer-ftp.c:261 by calling function 'FTPStringFree' at app-layer-ftp.c:340 after th...
DOUBLE_FREE.EX	app-layer-smtp.c	1536	Pointer '(**tx->rcpt_to_list->tqh_first).str' is passed to a function free at app-layer-smtp.c:1469 by calling function 'SMTPStringFree' at app-layer-smtp.c:1536 a...
DOUBLE_FREE.EX	app-layer-ftp.c	875	Pointer '(**s->tx_list->tqh_first).de_state' is passed to a function free at app-layer-ftp.c:330 by calling function 'FTPTransactionFree' at app-layer-ftp.c:875 afte...
DOUBLE_FREE.EX	app-layer-enip.c	237	Pointer '(**s->tx_list->tqh_first).de_state' is passed to a function free at app-layer-enip.c:210 by calling function 'ENIPTransactionFree' at app-layer-enip.c:237 a...
DOUBLE_FREE.EX	app-layer-template.c	126	Pointer '(**state->tx_list->tqh_first).response_buffer' is passed to a function free at app-layer-template.c:100 by calling function 'TemplateTxFree' at app-layer...
DEREF_AFTER_FREE	detect-engine-loader.c	590	Pointer '&task->Func' is dereferenced at detect-engine-loader.c:590 after the referenced memory was deallocated at detect-engine-loader.c:594 by calling fun...
DEREF_AFTER_NULL	util-decode-mime.c	513	After having been compared to NULL value at util-decode-mime.c:508, pointer 'stack->top' is dereferenced at util-decode-mime.c:513.
UNINIT.LOCAL_VAR	app-layer-detect-pro...	631	Uninitialized data is read from local variable 'rdir' at app-layer-detect-proto.c:631.
OP_PRECEDENCE_ASSIGN_CMP	tm-threads.c	177	Logic operator precedence in assignment can produce an unexpected result
UNREACHABLE_CODE.ENUM	runmode-unix-socket.c	630	This statement in the source code might be unreachable during program execution.
UNREACHABLE_CODE.ENUM	util-storage.c	64	This statement in the source code might be unreachable during program execution.
UNREACHABLE_CODE.ENUM	flow-worker.c	612	This statement in the source code might be unreachable during program execution.
UNREACHABLE_CODE.ENUM	tm-modules.c	245	This statement in the source code might be unreachable during program execution.
UNREACHABLE_CODE.ENUM	detect-engine.c	4275	This statement in the source code might be unreachable during program execution.
UNREACHABLE_CODE.ENUM	util-error.c	384	This statement in the source code might be unreachable during program execution.
INT_OVERFLOW.BIG	detect-content.c	567	Integer value 'offset' may be overflow at detect-content.c:567, see detect-content.c:556 for comparison.
NO_UNLOCK.STRICT	log-pcap.c	449	No unlock for mutex 'pl->plog_lock' at log-pcap.c:449 after lock at log-pcap.c:448 by calling function 'pthread_mutex_lock'.
DEREF_AFTER_NULL.EX	suricata.c	1421	After having been compared to NULL value at suricata.c:1317, pointer 'optarg' is passed as 1st parameter in call to function 'SCStrdupFunc' at suricata.c:1421,...
PASSED_TO_PROC_AFTER_RELEASE	log-pcap.c	579	Value 'comp->file' passed to procedure at log-pcap.c:579 after release at log-pcap.c:329 by calling function 'PcapLogRotateFile' at log-pcap.c:541.
BUFFER_UNDERFLOW	detect-engine-mpm.c	182	Array 'xforms' is accessed by -1 at detect-engine-mpm.c:182. This may lead to buffer underflow. Negative index at detect-engine-mpm.c:182.



Фаззинг

```
dictionary : n/a, n/a, n/a | imported : 460
american fuzzy lop ++3.12c (mmopt_http2) [mmopt] {-1} 96.97%

process timing | overall results
run time : 5 days, 6 hrs, 44 min, 4 sec | cycles done : 42
last new path : 0 days, 3 hrs, 28 min, 51 sec | total paths : 1171
last uniq crash : none seen yet | uniq crashes : 0
last uniq hang : none seen yet | uniq hangs : 0

cycle progress | map coverage
now processing : 273.139 (23.3%) | map density : 3.49% / 5.06%
paths timed out : 0 (0.00%) | count coverage : 2.17 bits/tuple

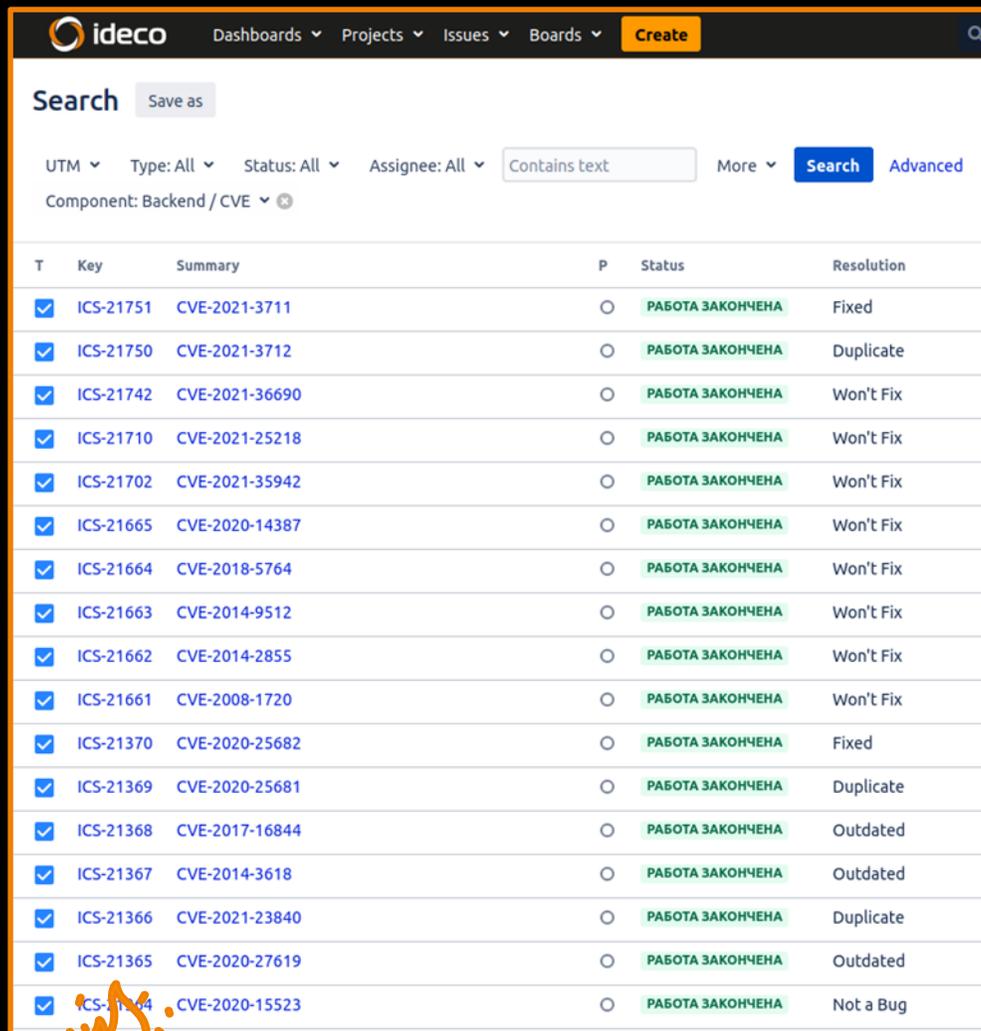
stage progress | findings in depth
now trying : splice 14 | favored paths : 188 (16.05%)
stage execs : 2/12 (16.67%) | new edges on : 299 (25.53%)
total execs : 7.48M | total crashes : 0 (0 unique)
exec speed : 18.44/sec (zzzz...) | total tmouts : 3 (3 unique)

fuzzing strategy yields | path geometry
bit flips : n/a, n/a, n/a | levels : 15
byte flips : n/a, n/a, n/a | pending : 591
arithmetics : n/a, n/a, n/a | pend fav : 0
known ints : n/a, n/a, n/a | own finds : 701
dictionary : n/a, n/a, n/a | imported : 460
havoc/splice : 7/364k, 7/1.12M | stability : 96.97%
py/custom : 0/0, 0/0 |
trim : 0.00%/202k, n/a | [cpu: 25%]
```

```
ivendil@localhost:~/fuzzing_reports/app-control/app-control/out/coe_engine/cia
00000000 d4 c3 b2 a1 02 00 04 00 00 00 00 00 00 00 00 00 |.....|
00000010 00 00 04 00 01 ff 7f 00 2c b4 1b 60 68 93 05 00 |.....h...|
00000020 4a 00 00 00 4a 00 00 00 10 8c cf 33 58 c7 5c 87 |J...J...3X.V...|
00000030 9c 1c ce 51 08 00 45 00 40 3c fb 14 40 00 40 06 |...Q...E.e<...e.e|
00000040 00 00 00 00 00 00 00 00 00 00 e9 f0 00 4d 3c b2 |.....M<...|
00000050 00 1a e8 ff 00 00 00 42 38 b0 18 13 00 0c 00 cc |.....BB.....|
00000060 e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000080 e5 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000090 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000000a0 00 00 02 00 00 00 00 00 00 00 00 00 00 00 21 |.....!|
000000b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000000c0 00 cc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000000d0 00 ff e4 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
000000e0 00 00 00 00 00 80 00 00 00 00 00 00 00 00 1c |.....|
000000f0 00 00 00 00 00 00 00 00 8e 00 4a 00 00 00 4a 00 |.....J...|
00000100 00 00 10 8c cf 33 58 c7 5c 87 9c 1c ce 51 08 00 |...3X.V...Q...|
00000110 45 00 00 3c fb 14 40 00 40 06 00 00 00 00 00 00 |E.<...e.e...|
00000120 00 00 00 00 e9 f0 00 4d 3c b2 00 19 00 00 00 00 |.....M<...|
00000130 00 34 38 b0 18 13 00 00 00 cc 00 00 00 00 00 00 |...48.....|
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000150 00 00 00 00 00 00 00 00 00 00 e5 ff 00 00 80 00 |.....|
00000160 00 00 00 00 00 00 00 00 00 21 00 00 00 00 00 00 |.....!|
00000170 00 00 00 00 00 00 00 00 00 00 00 cc 00 00 00 00 |.....|
00000180 00 00 00 00 00 00 00 00 00 00 ff e4 00 00 00 00 |.....|
00000190 00 00 00 00 00 00 00 00 00 1c 00 00 00 00 00 00 |.....|
000001a0 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 00 |.....!|
000001b0 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 |.....|
000001c0 00 00 8a 00 00 00 00 00 00 00 00 dd 00 00 00 00 |.....|
000001d0 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 |.....e...|
000001e0 00 00 00 00 00 00 00 00 00 00 f7 00 00 00 00 00 |.....|
000001f0 00 00 00 00 00 00 00 00 00 00 e5 ff 00 00 00 00 |.....|
00000200 00 00 00 00 00 00 00 00 00 00 ff ff 00 00 00 00 |.....|
00000210 00 00 00 00 00 00 00 00 00 21 00 00 00 00 10 00 |.....!|
00000220 00 00 00 00 00 00 00 00 00 00 cc 00 00 00 00 00 |.....|
00000230 00 00 00 00 00 00 00 00 00 00 ff e4 00 00 00 00 |.....|
00000240 00 00 00 00 00 00 00 00 00 00 21 00 00 00 00 00 |.....!|
00000250 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 |.....|
00000260 00 00 00 00 00 00 00 00 00 ff ff ff de 00 00 00 00 |.....|
00000270 00 00 8a 00 00 00 00 00 00 00 dd 00 00 00 00 00 |.....|
00000280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000290 00 00 00 00 00 00 00 00 00 00 00 fc 00 00 00 00 |.....|
000002a0 00 00 00 00 00 00 00 00 00 00 e5 ff 00 00 00 00 |.....|
000002b0 00 00 00 00 00 00 00 00 00 1c 00 00 00 b4 1b 60 |.....|
000002c0 68 93 05 00 4a 00 00 00 4a 00 00 10 8c cf 33 |h...J...J...3|
000002d0 58 c7 5c 87 9c 1c ce 51 08 00 45 00 40 3c fb 14 |X.V...Q...E.e<...|
000002e0 40 00 40 06 00 00 00 00 00 00 00 00 00 00 e9 f0 |e.e...|
000002f0 00 4d 3c b2 00 1a e8 ff 00 00 00 34 38 b0 18 13 |.M<...48...|
00000300 00 0c 00 cc e4 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000320 00 00 00 e5 ff 00 00 00 00 00 00 00 00 00 00 00 |.....|
```



CVE. УЯЗВИМОСТИ



The screenshot shows the Ideco Jira interface with a search filter for 'Backend / CVE'. The table below lists the search results:

T	Key	Summary	P	Status	Resolution
<input checked="" type="checkbox"/>	ICS-21751	CVE-2021-3711	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Fixed
<input checked="" type="checkbox"/>	ICS-21750	CVE-2021-3712	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Duplicate
<input checked="" type="checkbox"/>	ICS-21742	CVE-2021-36690	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21710	CVE-2021-25218	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21702	CVE-2021-35942	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21665	CVE-2020-14387	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21664	CVE-2018-5764	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21663	CVE-2014-9512	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21662	CVE-2014-2855	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21661	CVE-2008-1720	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Won't Fix
<input checked="" type="checkbox"/>	ICS-21370	CVE-2020-25682	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Fixed
<input checked="" type="checkbox"/>	ICS-21369	CVE-2020-25681	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Duplicate
<input checked="" type="checkbox"/>	ICS-21368	CVE-2017-16844	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Outdated
<input checked="" type="checkbox"/>	ICS-21367	CVE-2014-3618	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Outdated
<input checked="" type="checkbox"/>	ICS-21366	CVE-2021-23840	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Duplicate
<input checked="" type="checkbox"/>	ICS-21365	CVE-2020-27619	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Outdated
<input checked="" type="checkbox"/>	ICS-21364	CVE-2020-15523	<input type="radio"/>	РАБОТА ЗАКОНЧЕНА	Not a Bug

Таблица 5.4.2.1 – Результаты автоматического поиска в базе данных уязвимостей CVE

Идентификатор уязвимости	Принятые меры по устранению уязвимости
CVE-2020-25682	Данные уязвимости исправлены путем обновления пакета dnsmasq до версии 2.8.4.
CVE-2020-25681	
CVE-2020-27619	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6

Испытательная лаборатория ООО НТЦ «Фобос-НТ»

41

Протокол № 21/3/6605-ПР2

Идентификатор уязвимости	Принятые меры по устранению уязвимости
CVE-2021-3711	Данные уязвимости исправлены путем обновления пакета OpenSSL до версии 1.1.1i
CVE-2021-3450	
CVE-2021-3712	

Выводы по результатам автоматизированного анализа известных уязвимостей в сторонних компонентах, входящих в состав ОО:

- Подтвержденные потенциальные уязвимости в составе ОО устранены разработчиком в ходе испытаний.
- Повторный анализ не выявил в составе ОО известных уязвимостей.

5.4.3 Ручное сканирование пакетов C, Python на наличие известных уязвимостей

Эксперт выполнил автоматизированный поиск сведений об известных уязвимостях ОО, модулей ОО и среды функционирования ОО с использованием следующих инструментов:

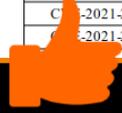
- ossaudit для Python;
- srrcheck для кода на C.

Результаты сканирования в виде логов работы сканера зафиксированы в электронных приложениях («Электронные приложения/КАО.2/Сканеры пакетов C, Python»).

Результаты работы сканера ossaudit приведены в таблице 5.4.3.1.

Таблица 5.4.3.1 - Результаты работы сканера ossaudit

Идентификатор уязвимости	Принятые меры по устранению уязвимости
CVE-2020-36242	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2020-26137	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2021-3350	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2021-27291	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2021-20270	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6



Баг-трекер

<input type="checkbox"/> ICS-20761 [svace] squid: src/acl/Random.cc:76: PROC_USE.VULNERABLE.SSCANF	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20762 [svace] squid: src/auth/basic/RADIUS/basic_radius_auth.cc:592: UNREACHABLE_CODE.RET	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20763 [svace] squid: src/ipc/mem/Pages.cc:67,76: OVERFLOW_UNDER_CHECK	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20764 [svace] squid: src/ip/QosConfig.cc:322: SIMILAR_BRANCHES	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20766 [svace] squid: lib/snmp/lib/parse.c:787: UNCHECKED_FUNC_RES.STAT	<input type="radio"/> ОЖИДАЕТ П... ✕
<input type="checkbox"/> ICS-20767 [svace] squid: lib/ltl/ltl.c:776: UNCHECKED_FUNC_RES.STAT	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20768 [svace] squid: src/neighbors.cc:789: DEREf_OF_NULL.EX	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20769 [svace] squid: NO_CAST.INTEGER_OVERFLOW: The value of an arithmetic expression 2*skew is subject to overflow	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20770 [svace] squid: src/cf_gen.cc:381,390: NO_EFFECT	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20771 [svace] squid: src/clients/FtpClient.cc:164: UNINIT.CTOR	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20772 [svace] squid: src/auth/negotiate/kerberos/negotiate_kerberos_pac.cc:124,136: WRONG_ARGUMENTS_ORDER	<input type="radio"/> ОЖИДАЕТ П...
<input type="checkbox"/> ICS-20707 [svace] squid: lib/rfcnb/rfcnb-io.c:402: DEREf_AFTER_NULL.EX	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20709 [svace] squid: src/ssl/support.cc:72: DEREf_OF_NULL.RET.LIB.PROC	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20715 [svace] squid: src/urn.cc:388: MEMORY_LEAK	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20754 [svace] squid: src/ssl/ErrorDetailManager.cc:212: BUFFER_OVERFLOW.EX	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20754 [svace] squid: src/peer_digest.cc:728: NULL_AFTER_DEREF	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20755 [svace] squid: src/store.cc:1463: NULL_AFTER_DEREF	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20756 [svace] squid: src/store/Controller.cc:210: NULL_AFTER_DEREF	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20757 [svace] squid: src/store_client.cc:316: NULL_AFTER_DEREF	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20758 [svace] squid: tools/cachemgr.cc:819: DEREf_OF_NULL.RET.STAT	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20759 [svace] squid: src/http.cc:1809: DEREf_OF_NULL.RET.STAT	<input type="radio"/> РАБОТА ЗАКО...
<input type="checkbox"/> ICS-20765 [svace] squid: src/any/Uri.cc:705: SIMILAR_BRANCHES	<input type="radio"/> РАБОТА ЗАКО...



Ideco Industrial Security Gateway (Ideco ISG)

Инспекция АСУ-ТП протоколов:
IEC-61850 MMS, IEC-61850 GOOSE,
IEC-60870-5-104, МЭК-104,
MODBUS (TCP), S7-COM, OPC UA

Потоковый антивирус
SMB, FTP, SSH, HTTP

Firewall

Реализация
сетевых интерфейсов без
разделения LAN/WAN

Оффлайн обновления
системы, сигнатур.
Работа шлюза без связи
с сервером лицензирования

Резервирование
каналов

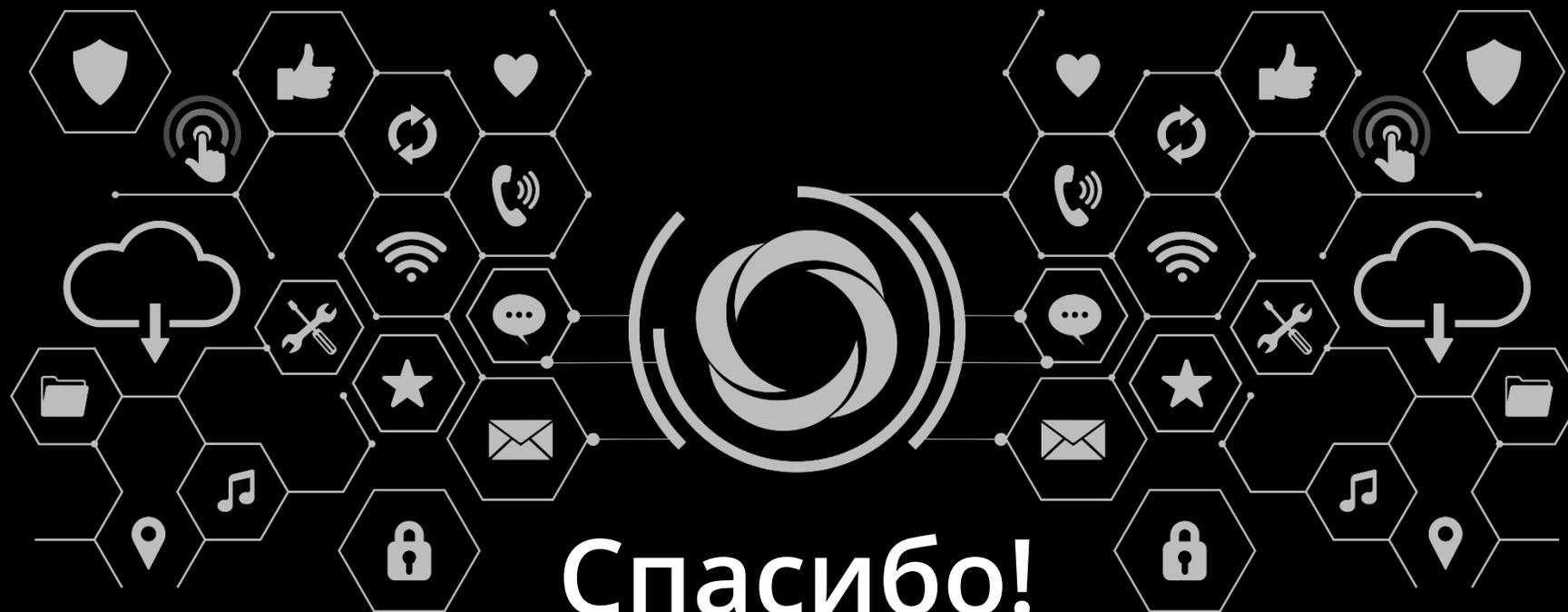
VPN (OpenVPN)

Конфигурирование через JSON,
без веб-интерфейса

Работа с протоколом OPCDA
на базе DCERPC

Сбор событий безопасности и
отправка их во внешние
системы (clickhouse? syslog?)

Кластеризация



 @RuslanNikiforov

 r.nikiforov@ideco.ru



 t.me/idecoutm

 @ideco