CERT.PL
NASK

Operacyjne podejście CERT Polska do OT

Krystian Szefler, Zespół Analiz Bieżących Zagrożeń
Specjalista ds. bezpieczeństwa przemysłowych systemów sterowania

cert.pl

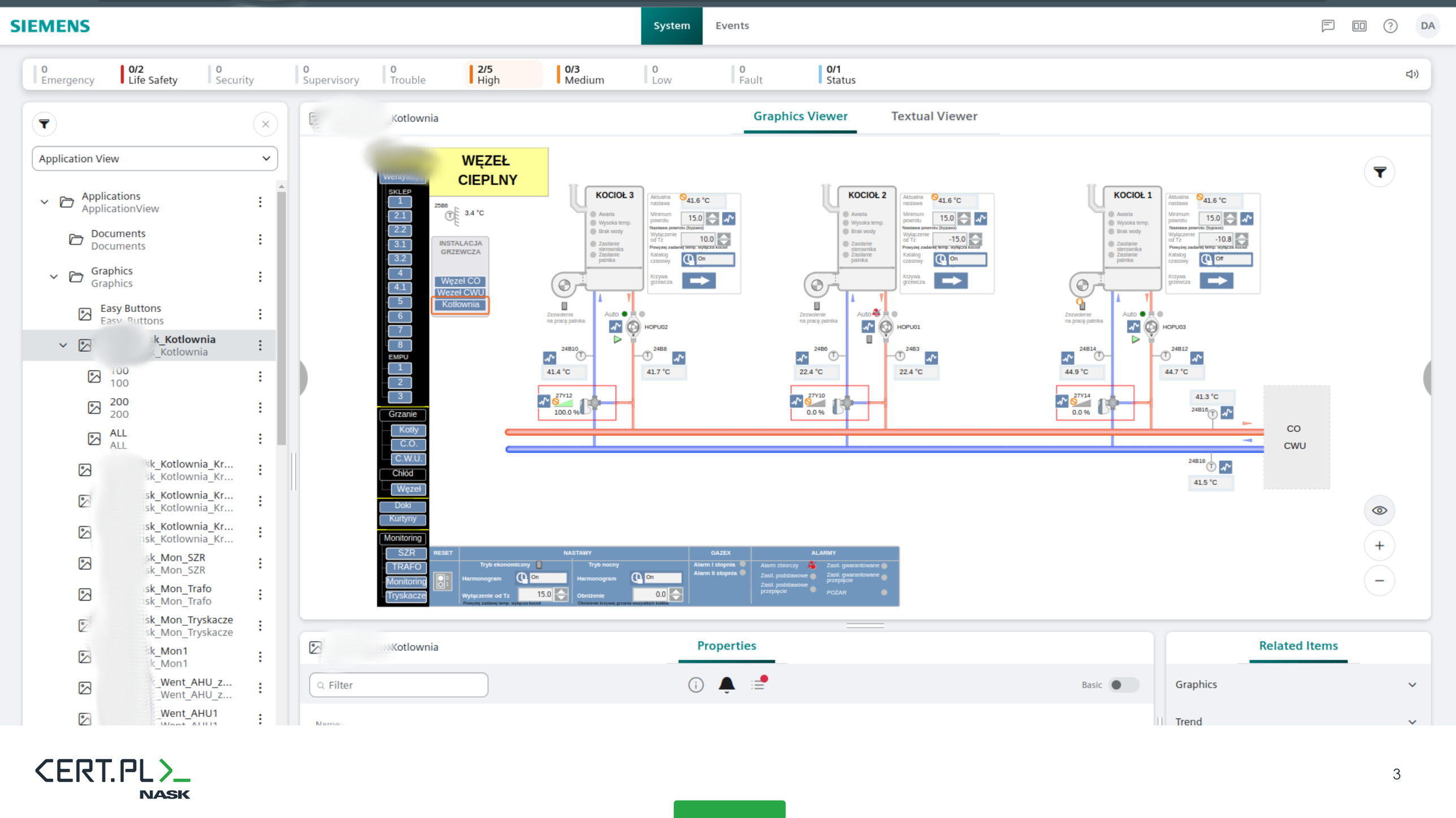
Rola CERTu

- monitorowanie zagrożeń
- klasyfikowanie incydentów
- prowadzenie analiz
- przekazywanie informacji

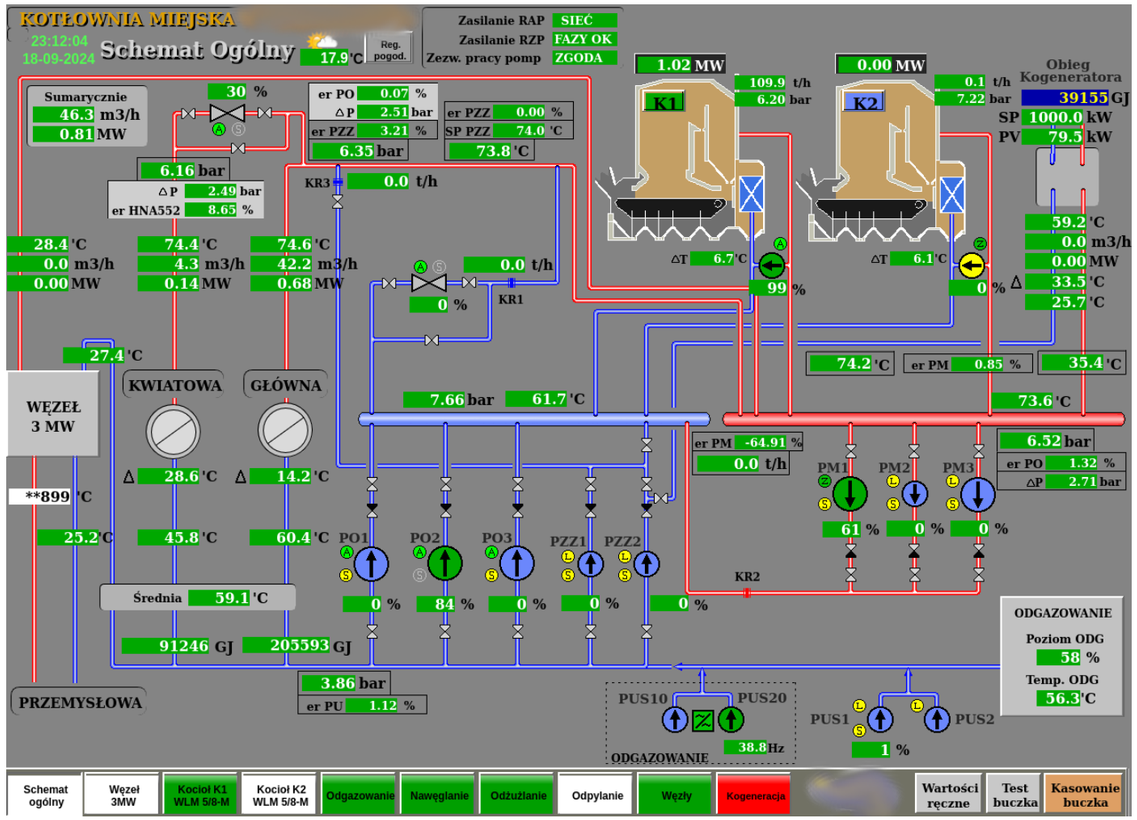
…

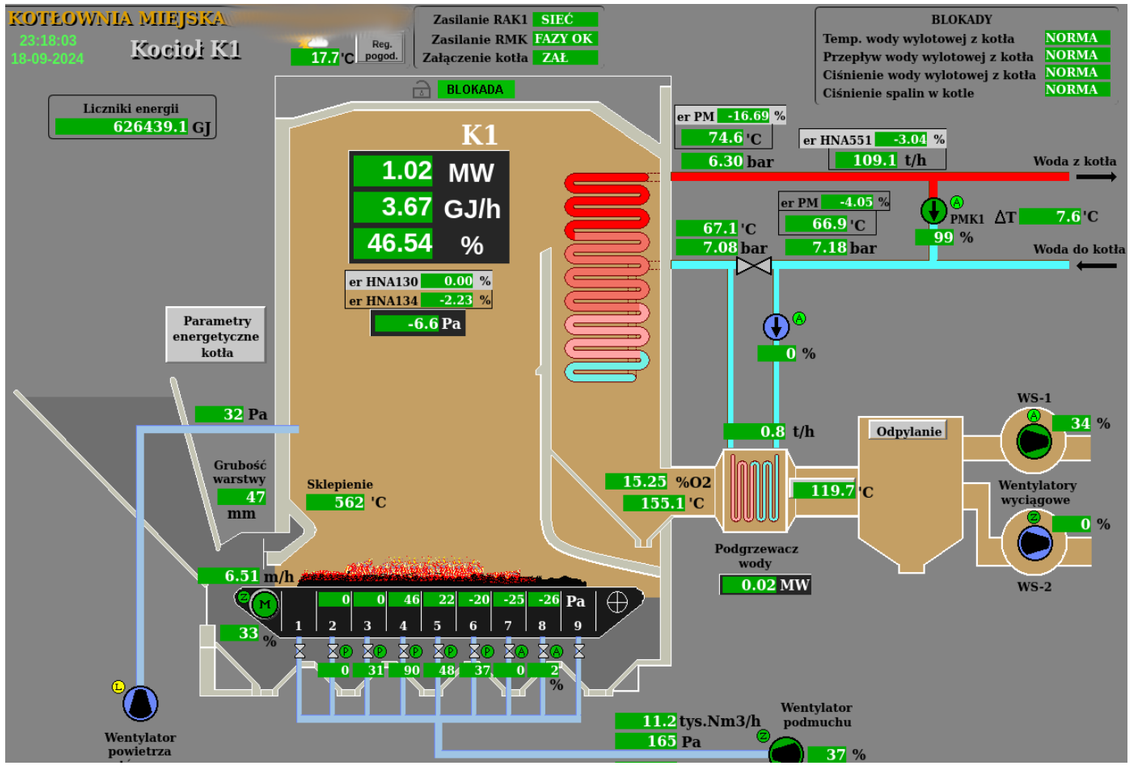
- monitorowanie wskaźników zagrożeń
- rozwijanie narzędzi
- budowania świadomości

CERT.PL NASK


SIEMENS
System
Events
DA
0 Emergency
0/2 Life Safety
0 Security
0 Supervisory
0 Trouble
2/5 High
0/3 Medium
0 Low
0 Fault
0/1 Status
Application View
Applications
ApplicationView
Documents
Documents
Graphics
Graphics
Easy Buttons
Easy Buttons
Kotlownia
Graphics Viewer
Textual Viewer
WĘZEŁ CIEPLNY
SKLEP
INSTALACJA GRZEWCZA
Węzeł CO
Węzeł CWU
Kotlownia
Grzanie
Kotły
C.O.
C.W.U.
Chłód
Węzeł
Drzwi
Kurtyny
Monitoring
SZR
TRAFO
Monitoring
Tryskacze
KOCIOŁ 3
KOCIOŁ 2
KOCIOŁ 1
HOPU02
HOPU01
HOPU03
CO
CWU
RESET
NASTAWY
GAZEX
ALARMY
Properties
Related Items
Graphics
Trend
Filter
Basic

Kotłownia miejska





Fotowoltaika w szpitalu

Zgłoszenie incydentu #noreply

Dziękujemy za przesłanie zgłoszenia. Poniżej znajdują się zarejestrowane przez nas informacje:

E-mail zgłaszającego:

a@b.com

Numer telefonu zgłaszającego:

123456789

Opis incydentu oraz wszelkie dodatkowe informacje:

Chciałbym zgłosić dostępny publicznie panel (prawdopodobnie) falowników fotowoltaicznych Szpitala w Abc. Dostępne są trzy panele pod adresami:

- http://5.x.x.230:1234/

- http://5.x.x.230:1235/

- http://5.x.x.230:1236/

Bez konieczności zalogowania się jest dostęp do statystyk generowania i zużycia prądu, konfiguracji poszczególnych urządzeń podłączonych do falownika a także wgrywanie firmware'u. Oczywiście nie dokonywałem żadnych zmian w panelu. Obawiam się że modyfikacja ustawień może w najgorszym przypadku wyłączyć prąd w danym obiekcie.

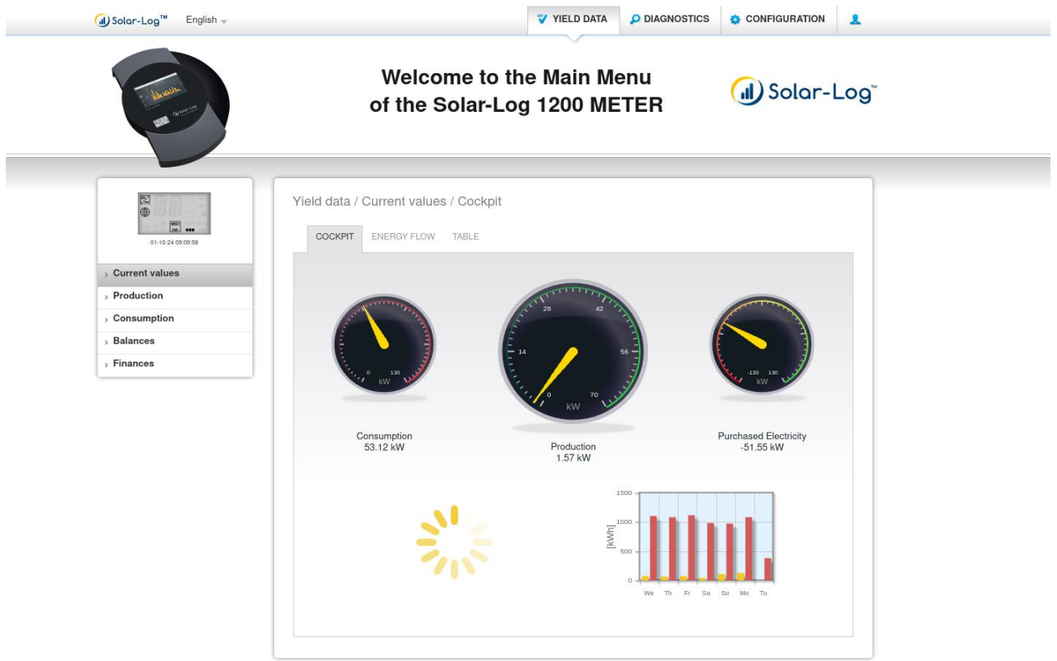
W panelu nie ma nigdzie informacji że urządzenia znajdują się w szpitalu jednak serwer WWW na porcie 443 przedstawia certyfikat dla domeny a.b.pl. W załączniku kilka zdjęć panelu.

Zgoda na przetwarzanie danych osobowych:

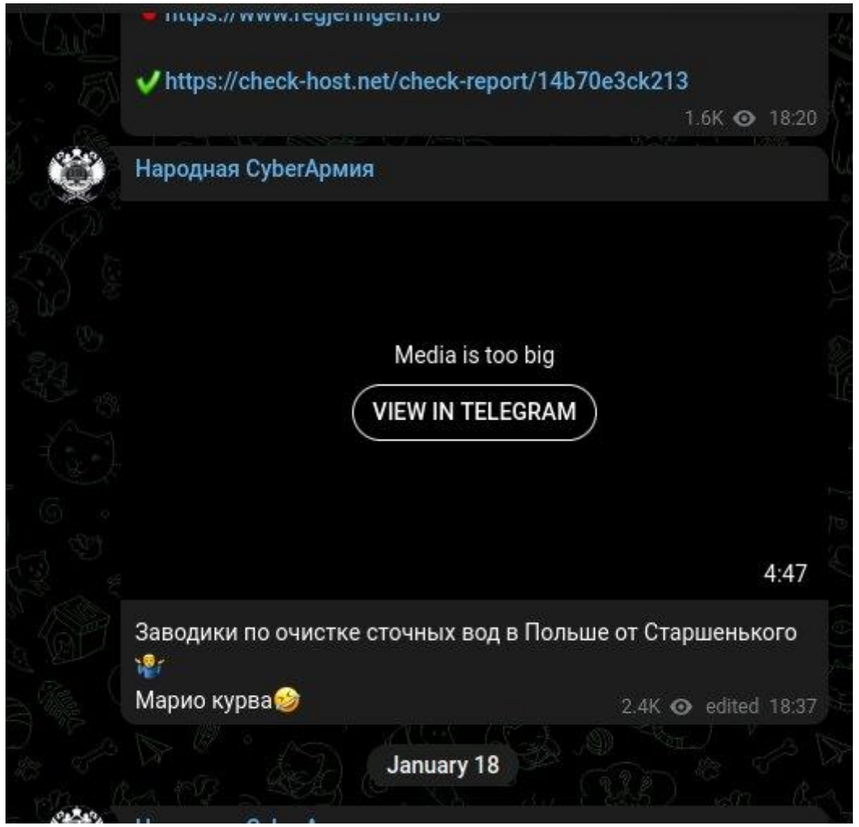
TAK

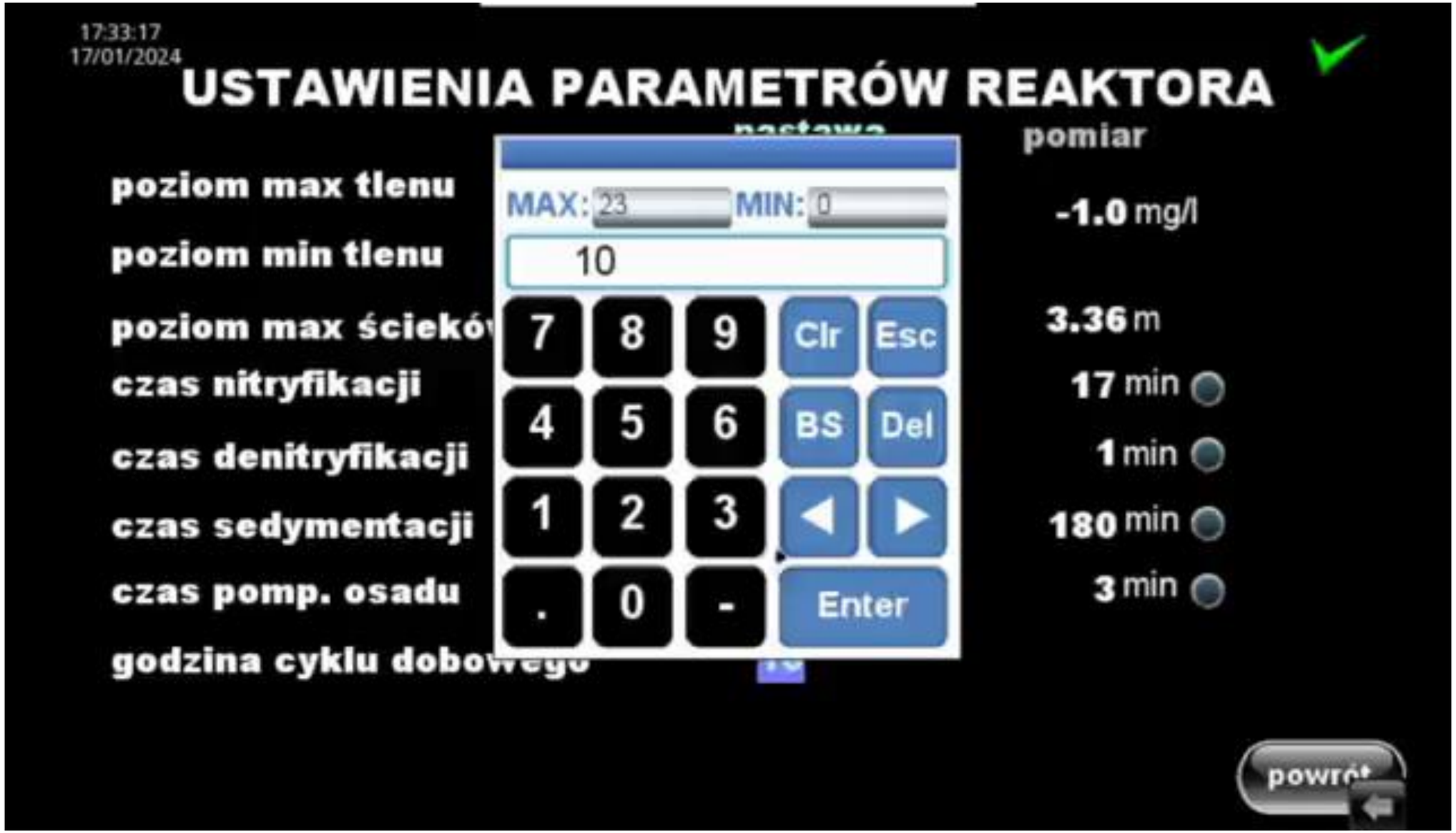
Zgłoszenie wyłącznie informacyjne - nie oczekuję kontaktu zwrotnego:

TAK



4 Oczyszczalnie




17:33:17
17/01/2024
USTAWIENIA PARAMETRÓW REAKTORA
pomiar
poziom max tlenu
poziom min tlenu
poziom max ścieków
czas nitryfikacji
czas denitryfikacji
czas sedymentacji
czas pomp. osadu
godzina cyklu dobowego
-1.0 mg/l
3.36 m
17 min
1 min
180 min
3 min
MAX: 23
MIN: 0
10
7 8 9 Clr Esc
4 5 6 BS Del
1 2 3
. 0 - Enter
powrót


17:43:02
17/01/2024
OCZYSZCZALNIA ŚCIEKÓW
KSD
KOMORA ŚCIEKÓW DOWOŻONYCH
KDF
KOMORA DEFOSFATACJI
KDN1
KOMORA DENITRYFIKACJI 1
KDN2
KOMORA DENITRYFIKACJI 2
KN1
KOMORA NITRYFIKACJI 1
KN2
KOMORA NITRYFIKACJI 2
SD
STACJA DMUCHAW
PP
POMPOWNIA PIANY
PO
POMPOWNIA OSADU
OW
OSADNIK WTÓRNY
MP
MIESZADŁO PRĘTOWE
PIX
DOZOWNIK PIX
ALARMY


OCZYSZCZALNIA ŚCIEKOW W
1
POMPOWNIA
Z RETENCJĄ
2
STACJA MECH.
OCZYSZCZANIA
3
STACJA
ZLEWNA
4
REAKTOR
BIOLOGICZNY
5
ZBIORNIK
OSADU
6
ALARMY
7
POMIAR PRZEPŁYWU

4 Oczyszczalnie

> Jakiś czas temu, mieliśmy informacje z tych obiektów, że **z niewiadomych przyczyn uległy zmianie parametry technologiczne**. Zareagowaliśmy niezwłocznie w celu przywrócenia normalnego układu pracy. Było to zdarzenie jednorazowe. Nie przyszło nam na myśl, że może to być atak hakerów z zewnątrz, ponieważ nigdy wcześniej taki incydent nie miał miejsca.

202.59.167.74

IP-167-74.nap.net.id
PT. NAP Info Lintas Nusa
Added on 2019-11-21 01:19:52 GMT
Indonesia, Jakarta

ics

Moxa Nport Device
Status: Unknown status
Name: **Hacked** by MrMoonz
MAC: 00:90:e8:47:67:d3

81.190.32.209

host-81-190-32-209.dynamic.mm.pl
Multimedia Polska S. A.
Added on 2019-11-17 09:42:28 GMT
Poland, Stargard

ics

Moxa Nport Device
Status: Authentication disabled
Name: **HACKED**
MAC: 00:90:e8:2b:b6:47

212.42.212.140

GNC Alfa Retail
Added on 2019-11-11 17:20:43 GMT
Armenia

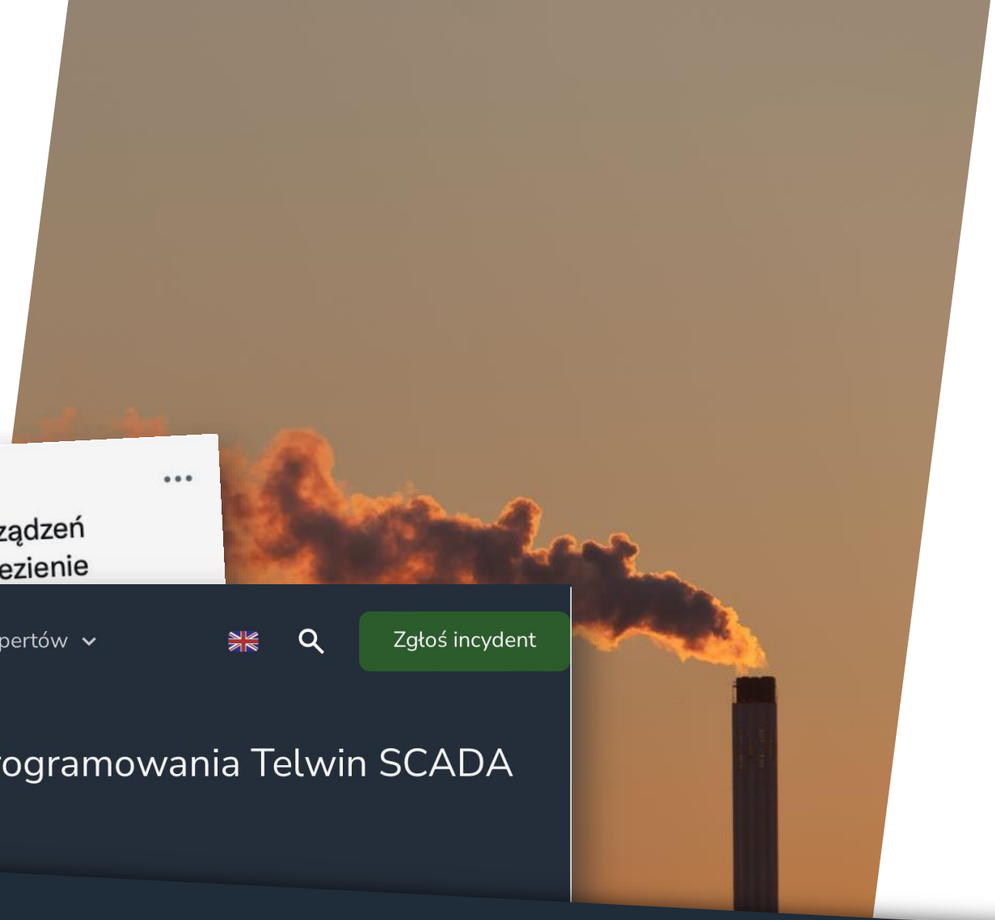
ics

Moxa Nport Device
Status: Unknown status
Name: **Hacked**+Azerbaijan%21%21%21%21%21%21%21%
MAC: 00:90:e8:25:89:63

CERT.PL NASK

Projekt #BezpiecznyPrzemysł

- Ostrzeżenia, artykuły, rekomendacje



NASK
PAŃSTWOWY INSTYTUT BADAWCZY

Warszawa 2020-01-13

Szanowni Państwo,

wypełniając obowiązki CSI
cyberbezpieczeństwa, infor
sterowania informacją pa
Przygotowaliśmy również
urządzeń.

Co wykryliśmy

W toku prowadzonych
firmy **Ente - Awia Rail**
słabym poziomem
serwisowych/testowych

Zagrożenia

Problemy te pozwalają
komunikatów, zarówn
potencjalnie wykorzy

Rekomendacje

Jako CSIRT NASK

CERT Polska @CERT_Polska · Mar 24, 2021

W ramach akcji #BezpiecznyPrzemysł badamy również firmware urządzeń
przemysłow
podatnośc
panelu HM

Marc
My CVE
root – c
Internet

TOT
17
TO

CERT.PL NASK O nas Aktualności Baza wiedzy Dla ekspertów Zgłoś incydent

> Podatność w module WebInterface oprogramowania Telwin SCADA _

03 sierpnia 2023 | CERT Polska | #podatno

CVE ID	
Data publikacji	
Producent podatnego oprogramowania	
Nazwa podatnego oprogramowania	
Podatne wersje	
Typ podatności (CWE)	
Źródło zgłoszenia	

Opis podatności

CERT.PL NASK O nas Aktualności Baza wiedzy Dla ekspertów Zgłoś incydent

> Rekomendacje dla wzmocnienia ochrony systemów OT _

17 maja 2024 | CERT Polska | #rekomendacje, #ICS, #OT, #SCADA, #BezpiecznyPrzemysł

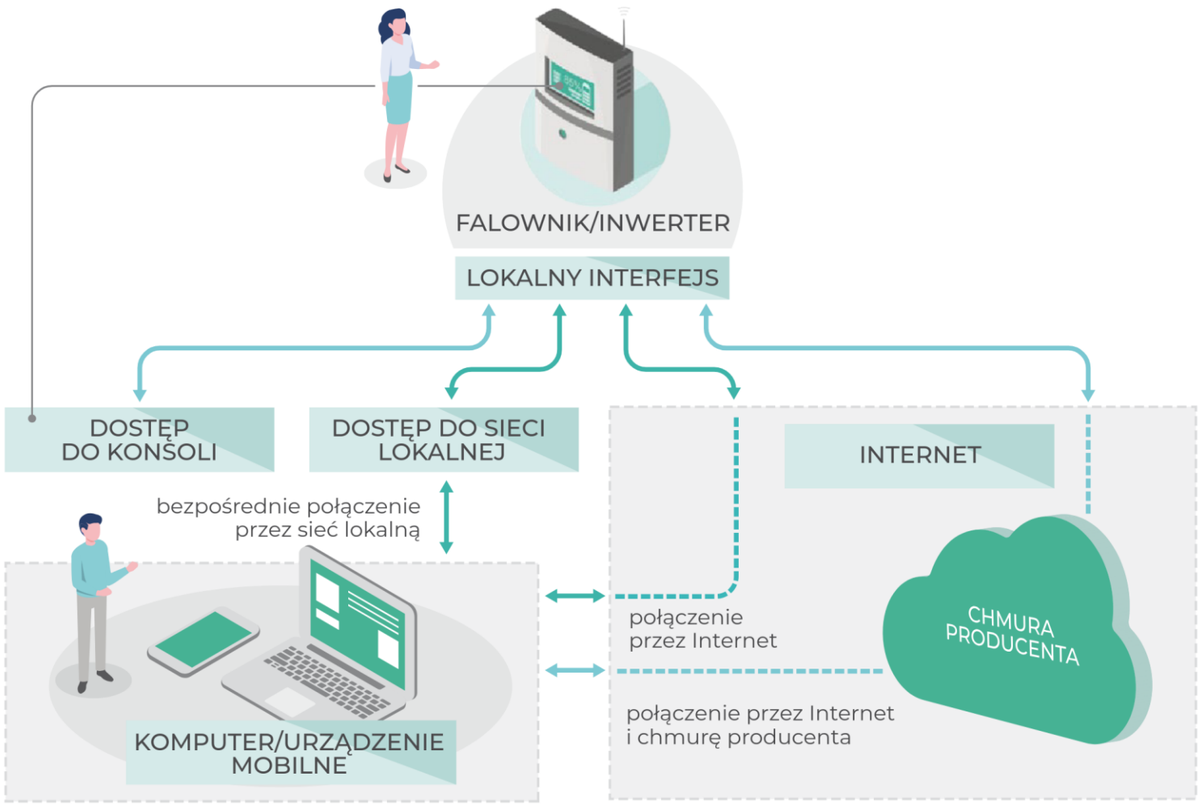
W ostatnim czasie CERT Polska obserwuje zwiększoną liczbę ataków na przemysłowe systemy sterowania (ICS/OT) dostępne bezpośrednio z internetu. Podobne przypadki odnotowali również nasi zagraniczni partnerzy. Ataki te najczęściej są motywowane aktywistycznie lub politycznie i mają na celu medialne wykorzystanie udanego ataku. Warto zaznaczyć, że CERT Polska odnotował również przypadki, w których atak miał realny wpływ na działanie fizycznych systemów.

W związku z obserwowanym zagrożeniem CERT Polska od trzech lat prowadzi działania pod nazwą #BezpiecznyPrzemysł, w ramach których w sposób zautomatyzowany poszukiwane są źle zabezpieczone urządzenia przy

W przypadku wykrycia

CERT.

OZE



CERT.PL NASK

REKOMENDACJE

DOTYCZĄCE CYBERBEZPIECZEŃSTWA DLA PROSUMENTÓW OZE

Ministerstwo Cyfryzacji

Ministerstwo Klimatu i Środowiska

CERT.PL NASK

PSE Polskie Sieci Elektroenergetyczne

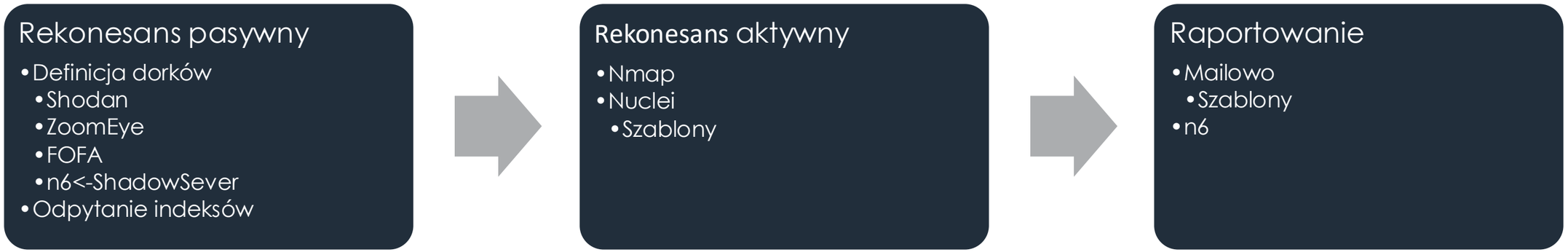
CERT PSE computer emergency response team

Automatyzacja

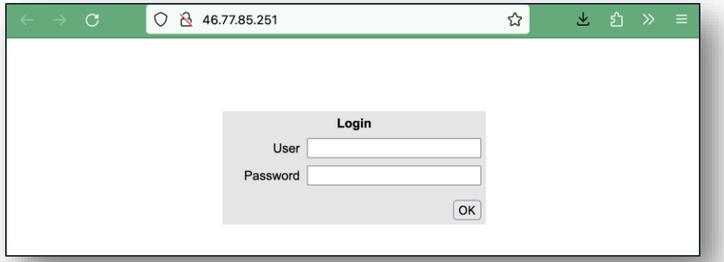
- Jak monitorujemy zagrożenia – systemy n6 i Snitch – i jak z tego skorzystać?

Snitch

Internet-connected devices Monitoring and Reporting System



Rekonesans



Pasywny – Shodan, ZoomEye, FOFA, n6

31.0.202.134 2023-05-23T15:23:35.109883

apn-31-0-202-134.static.gprs.plus.pl
Polkomtel sp. z o.o.
Poland, Kościan

```
HTTP/1.1 200 OK
Content-Length: 01408
Connection: keep-alive
Keep-Alive: timeout=5, max=5
Content-Type: text/html
```

46.77.85.251 2023-05-18T02:33:12.162204

apn-46-77-85-251.static.gprs.plus.pl
Polkomtel sp. z o.o.
Poland, Gdańsk

```
HTTP/1.1 200 OK
Content-Length: 01408
Connection: keep-alive
Keep-Alive: timeout=5, max=5
Content-Type: text/html
```

178.182.254.173 2023-05-22T10:24:46.612306

178.182.254.173.mobile.static.t-mobile.pl
T-Mobile Polska S.A.
Poland, Poznań

```
HTTP/1.1 200 OK
Content-Length: 01408
Connection: keep-alive
Keep-Alive: timeout=5, max=5
Content-Type: text/html
```

Aktywny – nmap, nuclei

```
Starting Nmap 7.90 ( https://nmap.org ) at year-mo-day hh:mm EDT
Nmap scan report for site.domain (xx.xx.xx.xx)
Host is up (0.15s latency).
Not shown: 89 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
```

I (a)dork you

Siemens

- **Siemens Generic by SSL Cert**

  Shodan: `ssl:"[redacted]"` (some FP because of official Siemens pages)
  Censys: `parsed.issuer.organization.raw: "[redacted]"`

- **Siemens web**

  `http.html:"siemens [redacted]"`

- **Siemens S7-1200 PLC by favicon**

  `http.favicon.hash:-105[redacted]`

- **Siemens Scalance by favicon**

  `http.favicon.hash:66[redacted]`

- **Siemens Sm@rtClient (VNC)**

  Zoomeye: `"[redacted]"`
  shodan: `title:"Siemens [redacted]"` `http.html:"Siemens [redacted]"`

- **Siemens Climatix**

  `title:"[redacted]"`

Moxa

Moxa by SSL

`ssl:"[redacted]"`

Moxa by favicon

`http.favicon.hash:-23[redacted]`

Westermo

- **Przemysłowy router 3G**

`Westermo[redacted]`

- **Przemysłowy Switch**

`Westermo[redacted]`

- **Przemyslowy konwerter Ethernet - Serial**

`Westermo[redacted]`

Plum (polski)

- **IK-301 industrial router**

Shodan: `http.html_hash:-84[redacted] "Content-Length: 01[redacted]`

Zoomeye: `plum-settings-[redacted]`

- **IK-401**

zoomeye: `"/pages/scripts[redacted]`

codesys webserver

`"3S[redacted]"`

zoomeye: `3S[redacted] +country:"PL"` `Web[redacted] +country:"PL"` `WAGO[redacted] +country:"PL"`

Shodan: `"web[redacted]" country:"PL"`

Fofa: `country="PL" && "webv[redacted]"`

CERT.PL NASK

Snitch RULES INCIDENTS SCRIPTS REPORTS BACKEND Search by IP address operator52

Rule #56 - WAGO Web-based Management

Brand WebPanel OT

EDIT RULE

HOSTS REPORTS DISCOVERY

Discovery (5)

RUN

Source	Returned	Last execution	Duration	Status
http.favicon.hash:-1405767 country:pl	5 (2)	Yesterday at 11:54	0:00:02.799720	✓
title:"-" country:pl	34 (5)	Yesterday at 11:54	0:00:05.435431	✓
title:"-" country:pl	1 (1)	Yesterday at 11:54	0:00:02.020892	✓
-	51 (23)	Yesterday at 12:45	0:00:13.660927	✓

Details

Reporting
n6

Criticality
Low

Reliability
Excellent

Created
31.12.2023 1:15
(operator66)

Updated
01.08.2024 14:17
(operator52)

Note
Różne systemy Wago.
Domyślne logowanie często

CERT.PL NASK

Snitch RULES INCIDENTS SCRIPTS REPORTS BACKEND Search by IP address operator52

Rule #50 - Lumel ND45

WebPanel Energy OT

EDIT RULE

HOSTS REPORTS DISCOVERY

Hosts 44 / Online 41

EXPORT TO CSV

Online	IP Address	Whitelisted	Ports	serialNo	system_ver
	31.x.x.123			22090066	0.3.15
	5.x.x.119		tcp/9000	22090057	0.3.15
	31.x.x.68		tcp/8081	22080038	0.3.14
	5.x.x.225		tcp/8081	22070132	0.3.14
	94.x.x.138		tcp/50000	22070071	0.3.14
	31.x.x.123		tcp/8081	22020075	0.3.13
	79.x.x.22		tcp/8081	21070125	0.3.07
	5.x.x.95		tcp/8081	21070124	0.3.07
	5.x.x.81		tcp/8081	21070120	0.3.07

Details

Reporting
RT n6

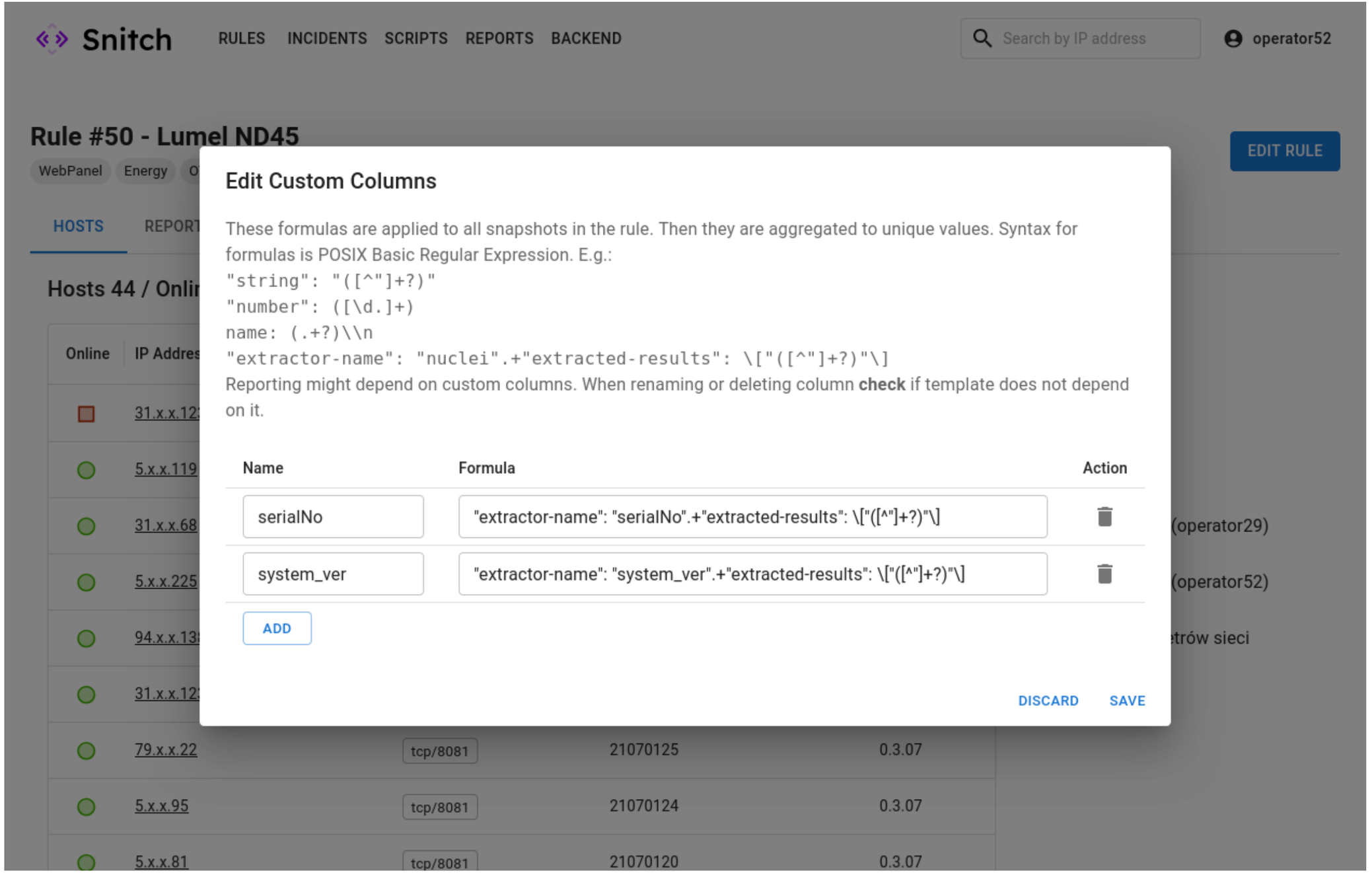
Criticality
Low

Reliability
Excellent

Created
18.08.2023 17:33 (operator29)

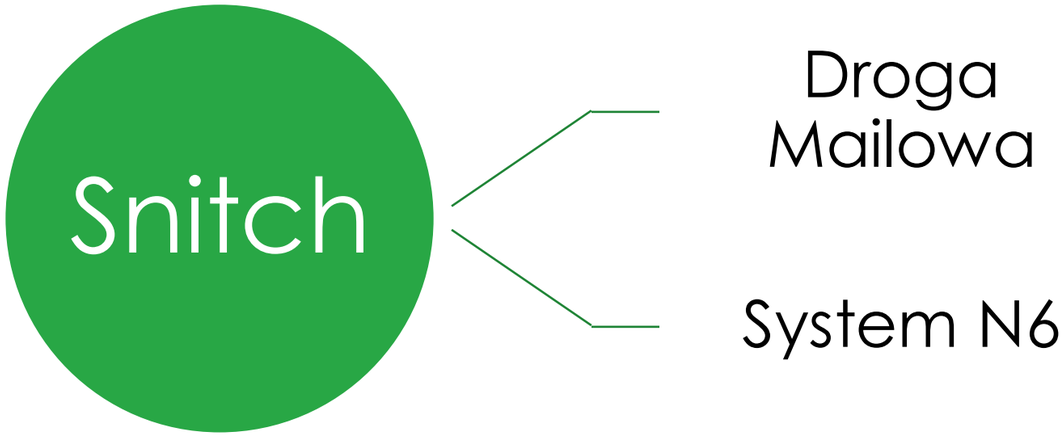
Updated
24.10.2024 12:26 (operator52)

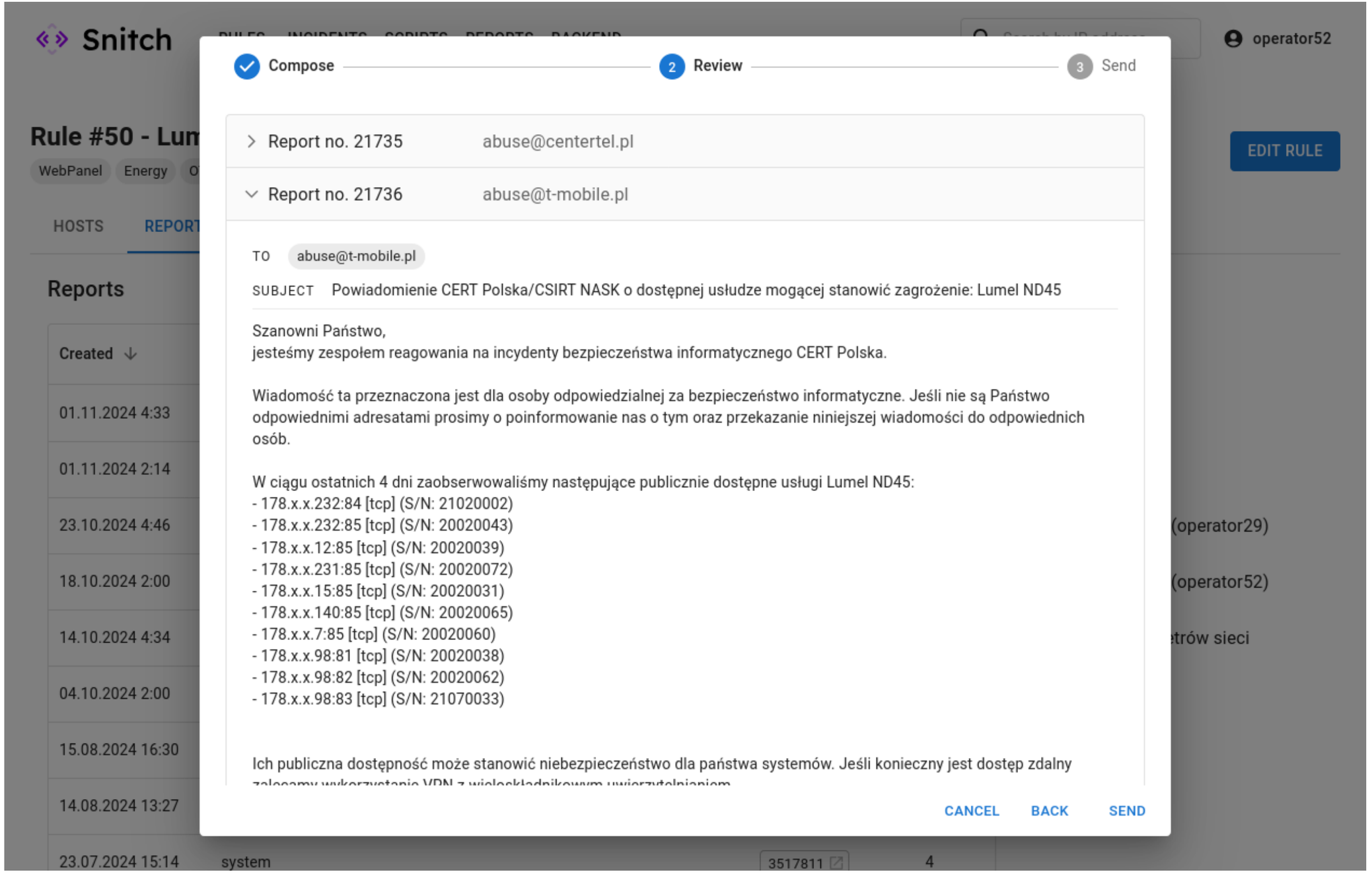
Note
rejestrator parametrów sieci


Snitch
RULES
INCIDENTS
SCRIPTS
REPORTS
BACKEND
Search by IP address
operator52
Rule #50 - Lumel ND45
WebPanel
Energy
EDIT RULE
HOSTS
REPORT
Hosts 44 / Onli
Online
IP Addres
31.x.x.12
5.x.x.119
31.x.x.68
5.x.x.225
94.x.x.13
31.x.x.12
79.x.x.22
5.x.x.95
5.x.x.81
tcp/8081
21070125
0.3.07
tcp/8081
21070124
0.3.07
tcp/8081
21070120
0.3.07
(operator29)
(operator52)
trów sieci
Edit Custom Columns
These formulas are applied to all snapshots in the rule. Then they are aggregated to unique values. Syntax for formulas is POSIX Basic Regular Expression. E.g.:
"string": "([^"]+?)"
"number": ([\d.]+)
name: (.+?)\\n
"extractor-name": "nuclei".+"extracted-results": \["([^"]+?)"\]
Reporting might depend on custom columns. When renaming or deleting column check if template does not depend on it.
Name
Formula
Action
serialNo
"extractor-name": "serialNo".+"extracted-results": \["([^"]+?)"\]
system_ver
"extractor-name": "system_ver".+"extracted-results": \["([^"]+?)"\]
ADD
DISCARD
SAVE

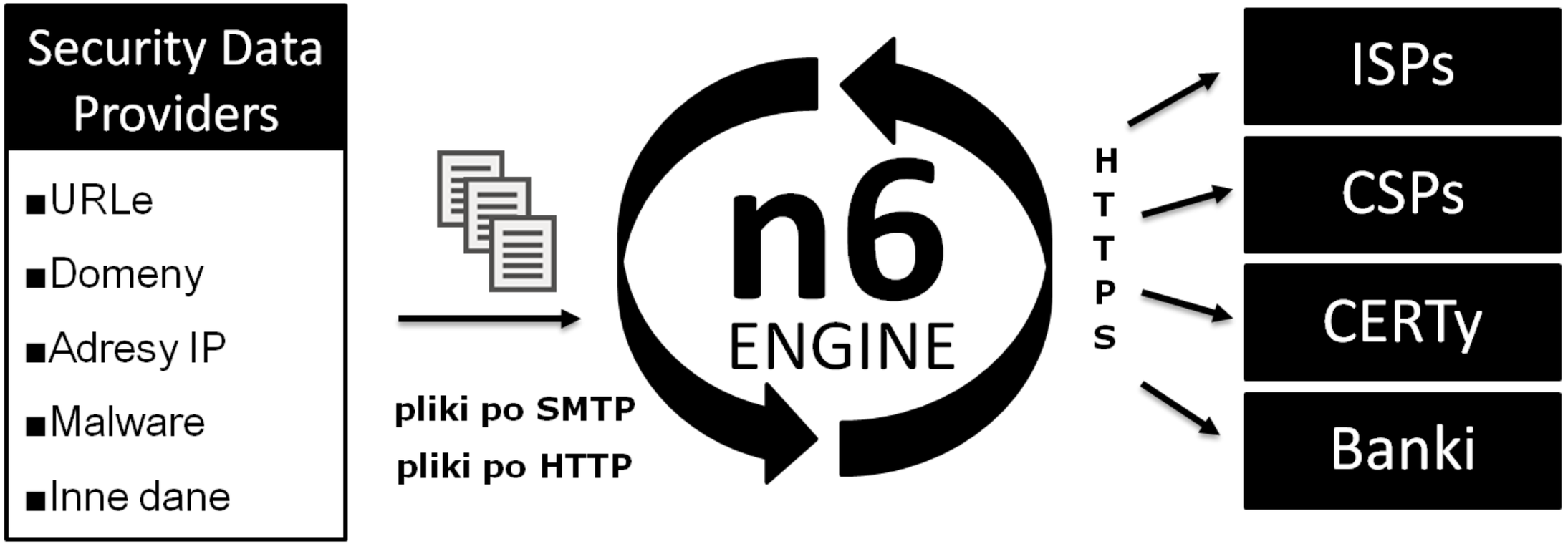
CERT.PL NASK

Raportowanie

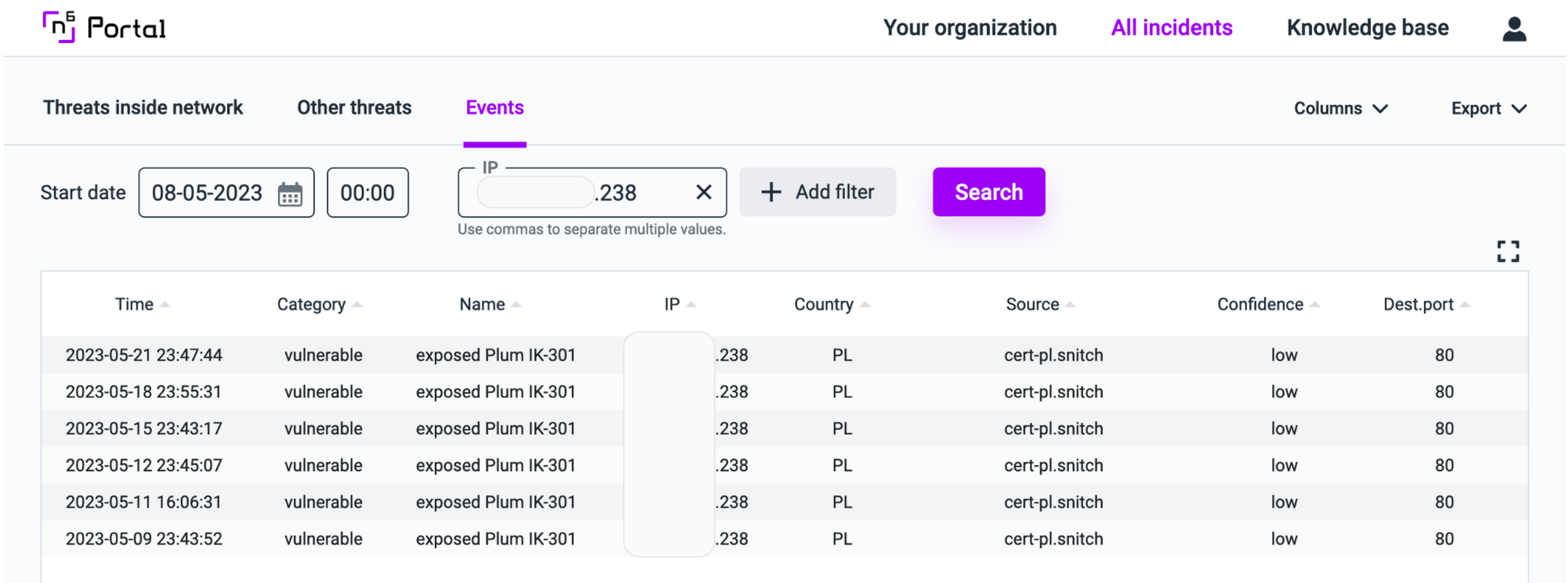



Snitch
operator52
Rule #50 - Lum
WebPanel
Energy
EDIT RULE
HOSTS
REPORT
Reports
Created
01.11.2024 4:33
01.11.2024 2:14
23.10.2024 4:46
18.10.2024 2:00
14.10.2024 4:34
04.10.2024 2:00
15.08.2024 16:30
14.08.2024 13:27
23.07.2024 15:14
system
3517811
4
(operator29)
(operator52)
trów sieci
Compose
2 Review
3 Send
Report no. 21735 abuse@centertel.pl
Report no. 21736 abuse@t-mobile.pl
TO abuse@t-mobile.pl
SUBJECT Powiadomienie CERT Polska/CSIRT NASK o dostępnej usłudze mogącej stanowić zagrożenie: Lumel ND45
Szanowni Państwo,
jesteśmy zespołem reagowania na incydenty bezpieczeństwa informatycznego CERT Polska.
Wiadomość ta przeznaczona jest dla osoby odpowiedzialnej za bezpieczeństwo informatyczne. Jeśli nie są Państwo odpowiednimi adresatami prosimy o poinformowanie nas o tym oraz przekazanie niniejszej wiadomości do odpowiednich osób.
W ciągu ostatnich 4 dni zaobserwowaliśmy następujące publicznie dostępne usługi Lumel ND45:
- 178.x.x.232:84 [tcp] (S/N: 21020002)
- 178.x.x.232:85 [tcp] (S/N: 20020043)
- 178.x.x.12:85 [tcp] (S/N: 20020039)
- 178.x.x.231:85 [tcp] (S/N: 20020072)
- 178.x.x.15:85 [tcp] (S/N: 20020031)
- 178.x.x.140:85 [tcp] (S/N: 20020065)
- 178.x.x.7:85 [tcp] (S/N: 20020060)
- 178.x.x.98:81 [tcp] (S/N: 20020038)
- 178.x.x.98:82 [tcp] (S/N: 20020062)
- 178.x.x.98:83 [tcp] (S/N: 21070033)
Ich publiczna dostępność może stanowić niebezpieczeństwo dla państwa systemów. Jeśli konieczny jest dostęp zdalny
CANCEL
BACK
SEND

CERT.PL NASK


Security Data Providers
URLe
Domeny
Adresy IP
Malware
Inne dane
pliki po SMTP
pliki po HTTP
n6
ENGINE
HTTPS
ISPs
CSPs
CERTy
Banki

Raportowanie do n6



Time	Category	Name	IP	Country	Source	Confidence	Dest.port
2023-05-21 23:47:44	vulnerable	exposed Plum IK-301	.238	PL	cert-pl.snitch	low	80
2023-05-18 23:55:31	vulnerable	exposed Plum IK-301	.238	PL	cert-pl.snitch	low	80
2023-05-15 23:43:17	vulnerable	exposed Plum IK-301	.238	PL	cert-pl.snitch	low	80
2023-05-12 23:45:07	vulnerable	exposed Plum IK-301	.238	PL	cert-pl.snitch	low	80
2023-05-11 16:06:31	vulnerable	exposed Plum IK-301	.238	PL	cert-pl.snitch	low	80
2023-05-09 23:43:52	vulnerable	exposed Plum IK-301	.238	PL	cert-pl.snitch	low	80

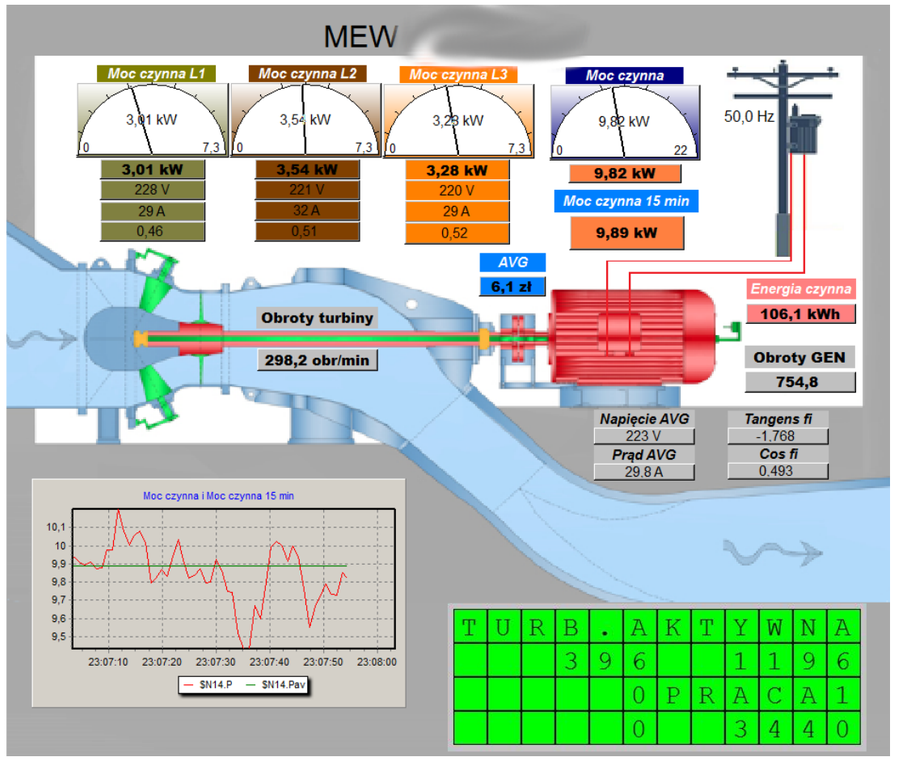
Problemy

Przed nawiązaniem kontaktu

- Ustalenie kontaktu
- WHOIS
- Operatorzy komórkowi

Po nawiązaniu

- Administratorzy
- Kompetencje
- Priorytety

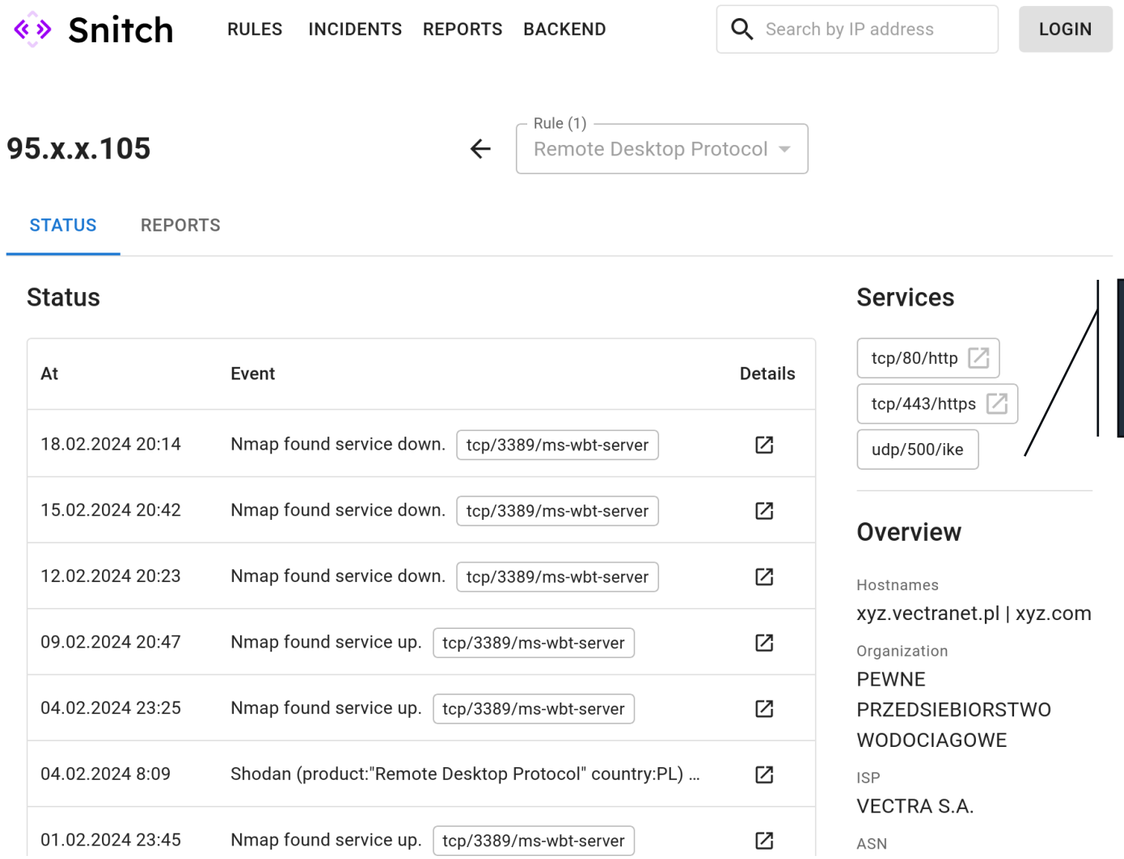


> (…) przedmiotowa usługa jest własnością **prywatnego przedsiębiorcy** działającego na terenie gminy (…). Przedmiotowa działalność polegająca na prowadzeniu małej elektrowni wodnej, nie jest w żaden sposób powiązana z Urzędem Gminy w (…). Właściciel przedstawionego adresu IP posiada wiedzę o jego publicznym udostępnieniu i **ma świadomość z zagrożenia** jakie to stwarza dla jego działalności.

Pewne przedsiębiorstwo wodociągowe

Na adresie ip 95.x.x.105 wykorzystywanym przez PEWNE PRZEDSIEBIORSTWO WODOCIAGOWE **wystawione są usługi**, **które** wg dobrych praktyk **nie powinny być dostępne z Internetu**. Serwisy Shodan, Censys w swoich bazach potwierdzają otwarte porty usług:
80 – api
135 – MSRPPC
139 – Netbios
443 – api
445 – SMB v2 (CVE-2020-0796 score 10.0)
3389 – RDP
5357 – api
5985 - WinRM

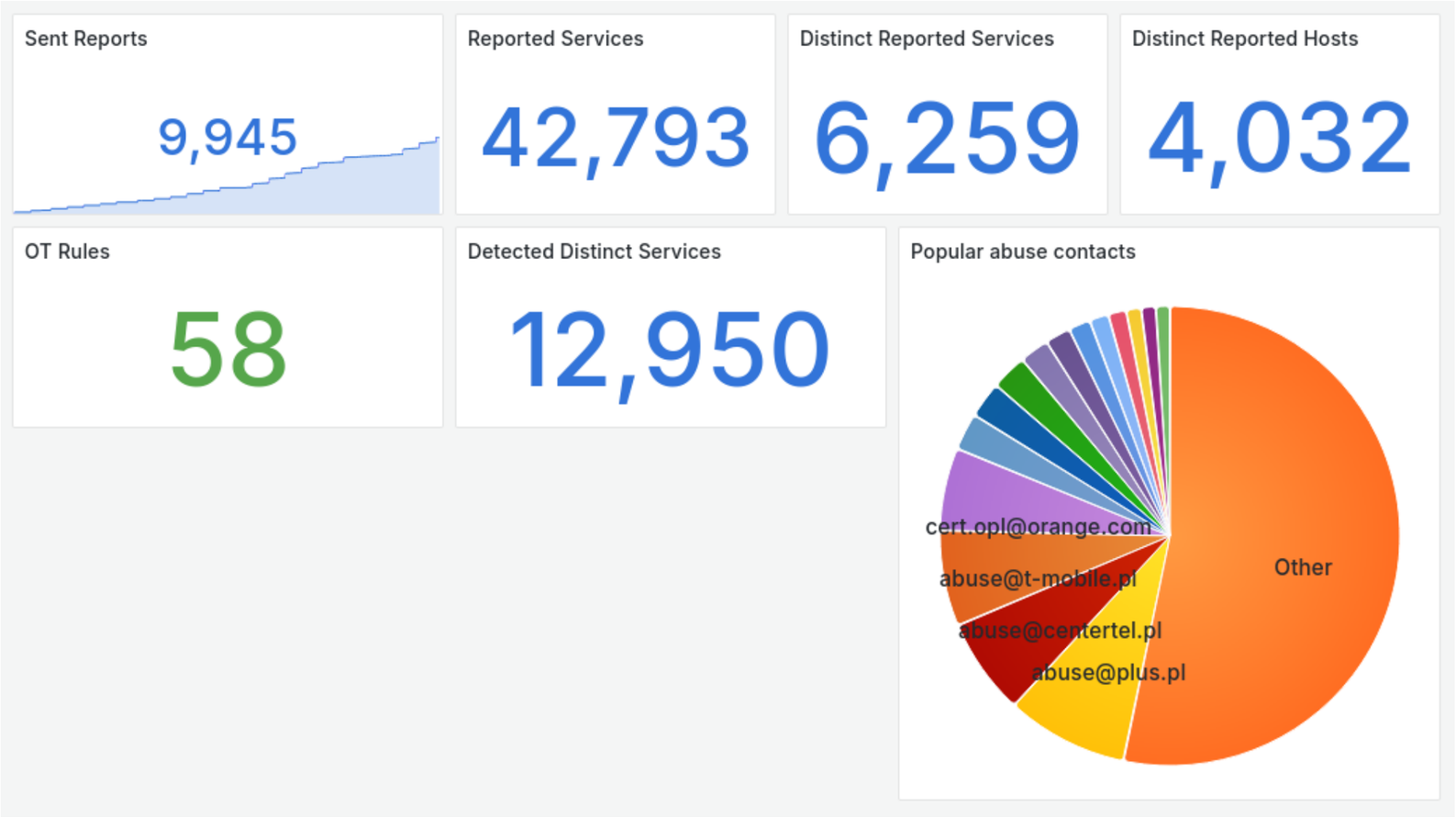
Nazwa domenowa hosta oraz certyfikat RDP wskazuje na „XYZ-SCADA" i jeśli faktycznie bazując na nawie, **urządzenie jest elementem sieci przemysłowej** związanej z procesem dostarczania wody można uznać, że jest krytycznie **ważne aby utwardzić system** i zmniejszyć wektor potencjalnego ataku.



Usługi zastąpione VPNem

Dziękujemy za zgłoszenie. **Zastosowano** odpowiednie **polityki** firewalla na routerze i bezpośrednio w systemie.

Statystyki


Sent Reports
9,945
Reported Services
42,793
Distinct Reported Services
6,259
Distinct Reported Hosts
4,032
OT Rules
58
Detected Distinct Services
12,950
Popular abuse contacts
cert.opl@orange.com
abuse@t-mobile.pl
abuse@centertel.pl
abuse@plus.pl
Other

Jak możemy sobie pomóc?

- WHOIS, adres abuse

- Dostęp jest bezpłatny, Jest OT!
- https://n6.cert.pl

- https://incydent.cert.pl
- https://moje.cert.pl
- cert@cert.pl

Skanowanie

Możesz tu zamówić bezpłatne skanowanie bezpieczeństwa wszystkich Twoich domen.

Dotychczas CERT Polska przeskanował ok. 887 tys. domen i subdomen, na których znaleźliśmy ok. 452 tys. podatności i błędnych konfiguracji. Ok. 28 tys. z nich wiązało się w wysokim ryzykiem dla instytucji, której dotyczyły.

Zdarzenia w Twojej sieci

Infekcje złośliwym oprogramowaniem, a może inne zagrożenia dotyczące Twojej sieci? Jeśli jesteś administratorem sieci, to będziesz otrzymywać od CERT Polska informacje o takich zdarzeniach.


CERT.PL
NASK
2023
RAPORT ROCZNY
z działalności CERT POLSKA
2023

CERT.PL
NASK

CERT.PL>_
NASK

Dziękuje za uwagę

```
<!--
       ._(.)< (MEOW)
        \___)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~-->
```