



MKD-CIRT

РЕПУБЛИКА МАКЕДОНИЈА
АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР
НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Александар Ацев

Раководител на служба за информатички технологии

Агенција за електронски комуникации

aleksandar.acev@aec.mk

Прв јавен состанок на АЕК за 2016 година, 8 јуни 2016 година

Сајбер безбедност и цели



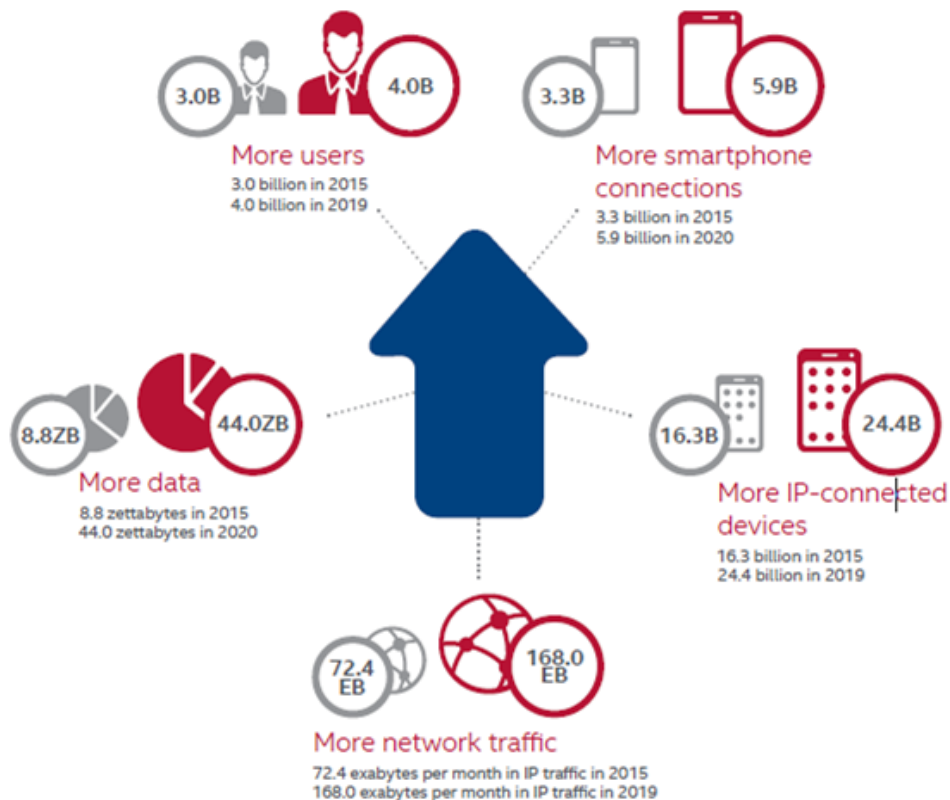
Cyber security – Поврзани технологии, процеси и практики со цел да се заштити мрежи, компјутери , програми и податоци од напади , оштетување или неовластен пристап. Во контекст на компјутери , поимот безбедност подразбира сајбер безбедност.

Основната улога на владата и државата (преку националниот CIRT) во обезбедувањето на инфраструктурата во државата против сајбер заканите е:

- Да се обезбеди континуитет на општеството во услови на криза.
- Заштита на основните услуги и критичната национална инфраструктура.
- Подобрување на отпорност на прекин.
- Сузбивање на ефекти од штетни активности.
- Враќање на способност за ширење на информации за закани, ранливости и напади.
- Брзо враќање во првичната состојба на нормалност за критичните системи.
- Да се идентификуваат трендовите и вектори на сајбер- напад.
- Обука на службите за брза реакција

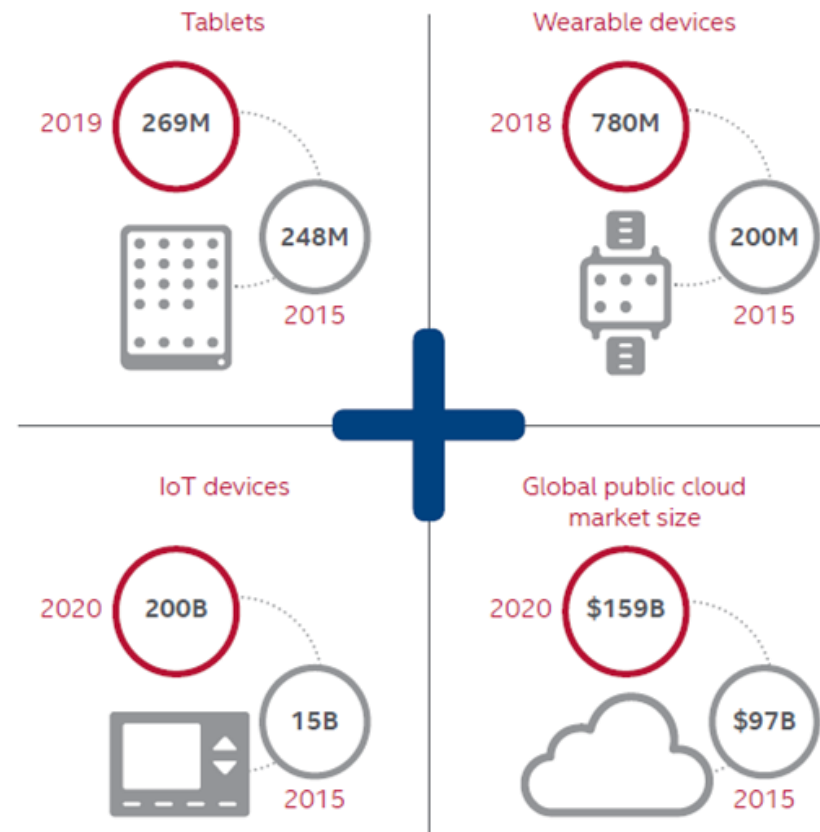
Површина за сајбер напади

The Growing Cyberattack Surface



Source: McAfee Labs, 2015.

New Device Types



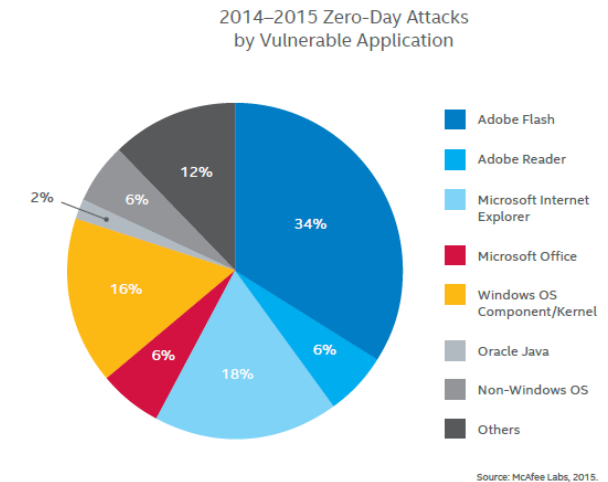
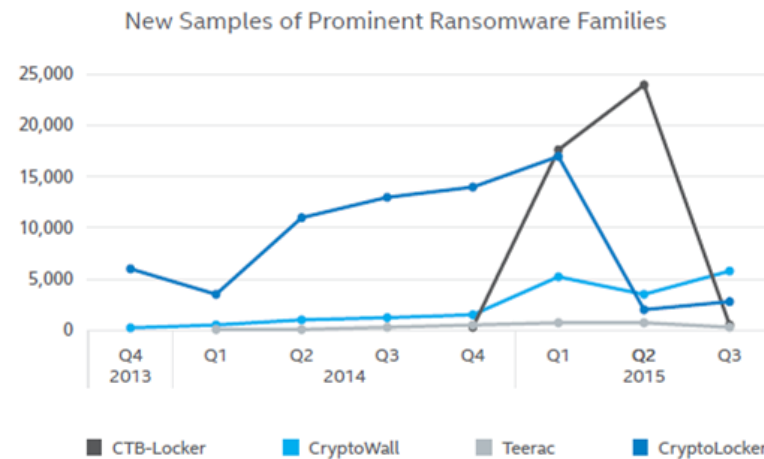
Source: McAfee Labs 2015

Извор: Извештај објавен на веб страницата на ITU: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec_and_trend_micro.aspx

Трендови за сајбер закани во 2016



- ❖ Hardware
- ❖ Ransomware
- ❖ Vulnerabilities
- ❖ Payment systems
- ❖ Attacks through employee systems
- ❖ Cloud services
- ❖ Wearables
- ❖ Automobiles
- ❖ Warehouses of stolen data



Извор: Извештај објавен на веб страницата на ITU: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec_and_trend_micro.aspx

Сајбер безбедноста е заедничка заложба



Историја

на MKD-CIRT



Студија од ITU/ИМРАСТ
2012-2013

Информација со препораки
од ITU/ИМРАСТ
2014

Одлука на Влада на РМ
2014

MKD-CIRT

Измена на Закон за
електронските комуникации
Декември 2014

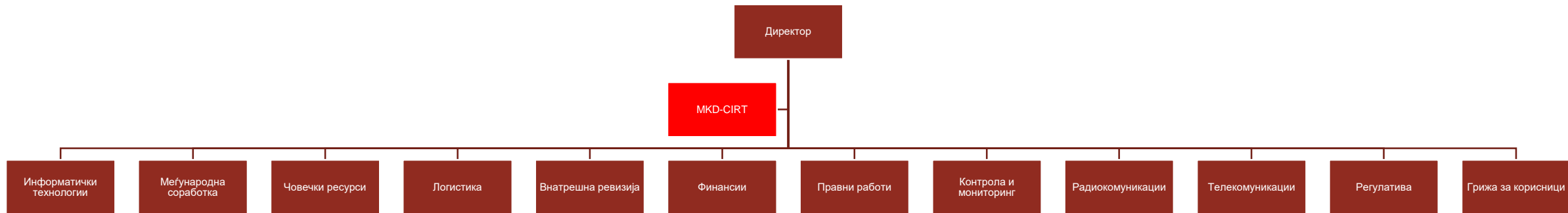
Формирање на MKD-CIRT
како орг.единица во АЕК
2015

ОРГАНИЗАЦИЈА

на MKD-CIRT



НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ MKD-CIRT



МИСИЈА

на MKD-CIRT



Националниот центар за одговор на компутерски инциденти ја има следната мисија:

- ❖ да координира и да помага/асистира на органите и институциите од јавниот сектор во имплементацијата на проактивните услуги за намалување на ризикот од компјутерски безбедносни инциденти, како и при справувањето со инцидентите кога истите ќе настанат ,**
- ❖ да спроведува активности за едуцирање и подигање на свесноста кај граѓаните за негативните ефекти на сајбер заканите и компјутерскиот криминал, и**
- ❖ навремено да обезбедува совети за сите негови конституенти.**

КОНСТИТУЕНТИ

на MKD-CIRT



Конституенти на MKD-CIRT се:

- ❖ Сите министерства, јавната администрација и услугите на Влада на Република Македонија,
- ❖ Операторите на критичната инфраструктура во Република Македонија, и
- ❖ Големи организации во банкарскиот, транспортниот, комуникацискиот, здравствениот, енергетскиот и други стратешки сектори во Република Македонија

ЦЕЛИ

на MKD-CIRT

- **СОРАБОТКА ВО РМ**
разменува информации со институциите за спроведување на законите
- **ЕДУКАЦИЈА**
разменува информации, знаење и искуство со конституентите
- **СЕКТОРСКИ CSIRT-ови**
Помош за воспоставување на интерни CSIRT тимови
- **СВЕШНОСТ**
Кај граѓаните за сајбер заканите



- **КООРДИНАЦИЈА**
при справувањето со инциденти на нац. ниво.
- **МОНИТОРИНГ**
Ризици, закани и инциденти.
- **НАЦИОНАЛНА ТОЧКА**
за контакт и размена на информации
- **ИНФОРМИРАЊЕ**
на конституентите со безбедносни совети и одговор на прашања

УСЛУГИ на MKD-CIRT

Услугите на MKD-CIRT имаат за цел да се обезбеди ефикасно справување со компјутерскиот инцидент од страна на конституентите и корисниците на интернет

- ❖ ИЗВЕСТУВАЊА И ПРЕДУПРЕДУВАЊА
- ❖ ДАЛЕЧИСКИ ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ
- ❖ ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ НА ЛИЦЕ МЕСТО
- ❖ ОДГОВОР НА РАНЛИВОСТИ
- ❖ ОСНОВНА СВЕСТ, ЕДУКАЦИЈА И ОБУКА



Корисници на услугите

на MKD-CIRT



Јавен сектор
во РМ



Граѓани на РМ



Оператори на
критична
инфраструктура

Придобивки од соработката

со MKD-CIRT



Јавен сектор во РМ, и Оператори на критична инфраструктура

- ❖ Навремено информирање за нови закани и ранливости
- ❖ Помош во справување со инцидентите со кои се соочуваат
- ❖ Можност за меѓународна соработка преку членството на MKD-CIRT во меѓународните организации
- ❖ Едукација, Сајбер вежби ...

Граѓани на РМ

- ❖ Навремено информирање за нови потенцијални закани и ранливости.
- ❖ Упатства и совети за безбедност на интернет при користење и електронска трговија

Комуникација и соработка

со MKD-CIRT



E-mail

Испраќање на пријави за инциденти и прашања преку адресите за е-пошта:
info@mkd-cirt.mk
contact@mkd-cirt.mk.

01

02

Соработка

Дисеминација на информации до конституентите и информмирање за нови закани и ранливост

03

Пријави на инциденти

Со посебни обрасци за пријава на инциденти – за конституентите на MKD-CIRT

Анонимна пријава преку веб-страницата <https://mkd-cirt.mk>

Поддршка 24/7

04



Активности на MKD-CIRT согласно програмата за работа за 2016

Р.Бр.	Реализирани активности во 2016 година
1	Инсталација на хардверската опрема и софтверски решенија за поддршка на мониторирање и евиденирање на информации за компјутерски закани и инциденти.
3	Обезбедување безбеден начин на пријавување на инцидентите преку различни канали за комуникација : телефон/мобилен, е-маил со PGP енкрипција, факс, писмен допис, и web формулари .
4	Креирање на официјален веб сајт
5	Припрема на правилници и процедури
10	Пристапување во меѓународните организации како официјална национална точка за контакт за одговор на компјутерски инциденти.
8	Воспоставување на мрежа на доверба со конституентите. Целосно соработува и разменува информации со институциите од државата надлежни за спроведување на законите, а особено со оние од областа на сајбер криминалот

Годишната програма за работа на MKD-CIRT е достапна на <https://mkd-cirt.mk/mk/dokumenti/>

Информации за MKD-CIRT и пријава на инцидент

https://mkd-cirt.mk



The screenshot displays the MKD-CIRT website interface. At the top, the header includes the MKD-CIRT logo, the full name of the agency in Macedonian, and a search bar with a phone icon and the number +389 2 3091 232. Below the header is a dark red navigation bar with links for 'За нас', 'Регистрација', 'Услуги', 'Пријава на инцидент', 'Документи', and 'Контакт'. The main content area features the MKD-CIRT logo and name on the left, and a detailed description of the center's mission and services on the right. A prominent red button labeled 'Пријавете инцидент' is positioned in the lower-left of the main content area. The footer contains the AEC logo, contact details, and a secondary navigation menu.

MKD-CIRT РЕПУБЛИКА МАКЕДОНИЈА
АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ
НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР
НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Search... → +389 2 3091 232

За нас · Регистрација · Услуги · Пријава на инцидент · Документи · Контакт

MKD-CIRT РЕПУБЛИКА МАКЕДОНИЈА
АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ
НАЦИОНАЛЕН ЦЕНТАР ЗА
ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Навигација

- Почина
- ЧП
- Контакт

Пријавете инцидент

За пријава на инцидент преку веб-страницата, Ве молиме пополнете го овај извод.

- Позиви
- Постави информацији

Добро дојдете на веб-страницата на Националниот центар за одговор на компјутерски инциденти на Република Македонија.

Со член 25-а од Законот за електронските комуникации во состав на Агенцијата за електронски комуникации се формира посебна организациона единица – Национален центар за одговор на компјутерски инциденти (MKD-CIRT), која ќе претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај приватите и интернационалните системи и кој ќе идентификува и ќе обезбедува одговор на безбедносните инциденти и разлик.

Завенат клуч и неговите латински ознаки да се наоѓаат на големите мајкударски јавни сервери за клучеват.

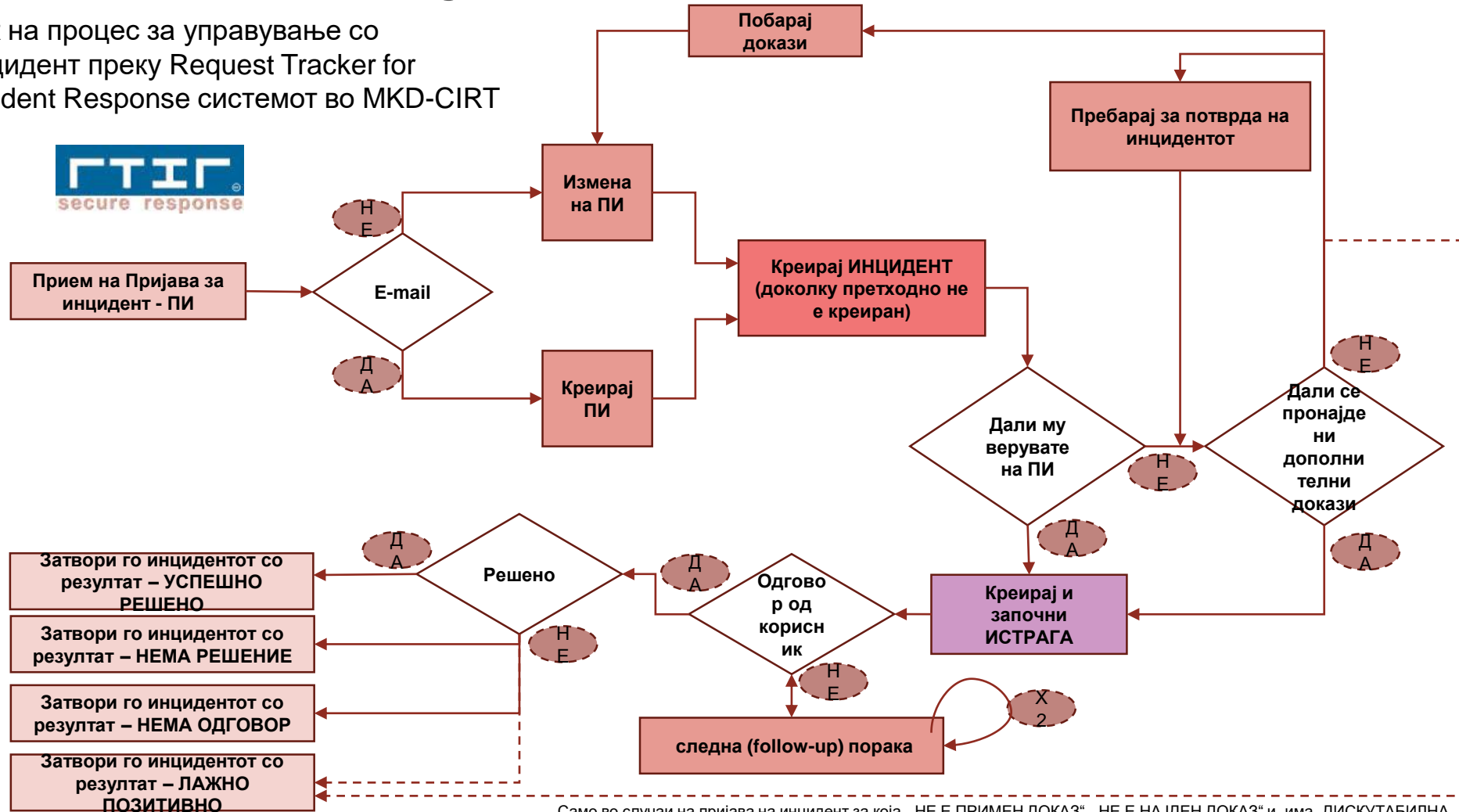
- Клуч ID: 0c33c00000
- Клуч Турк: RSA 4096
- Клуч Федерални: 0F09 30A2 6008 F45B F0BA 9C71 0741 17A1 233C 0000

AEC
Агенција за електронски комуникации
Национален центар за одговор на компјутерски инциденти
Кеј Димитар Блазов 21, 1000 Скопје
Република Македонија
Е-маил: info@mkd-cirt.mk
Телефон: +389 2 3091 232

Н Почина
Н За нас
Н Регистрација
Н Пријава на инцидент
Н Политика за приватност
Н PDF логотип

Систем за пријава и решавање по инциденти

Тек на процес за управување со инцидент преку Request Tracker for Incident Response системот во MKD-CIRT

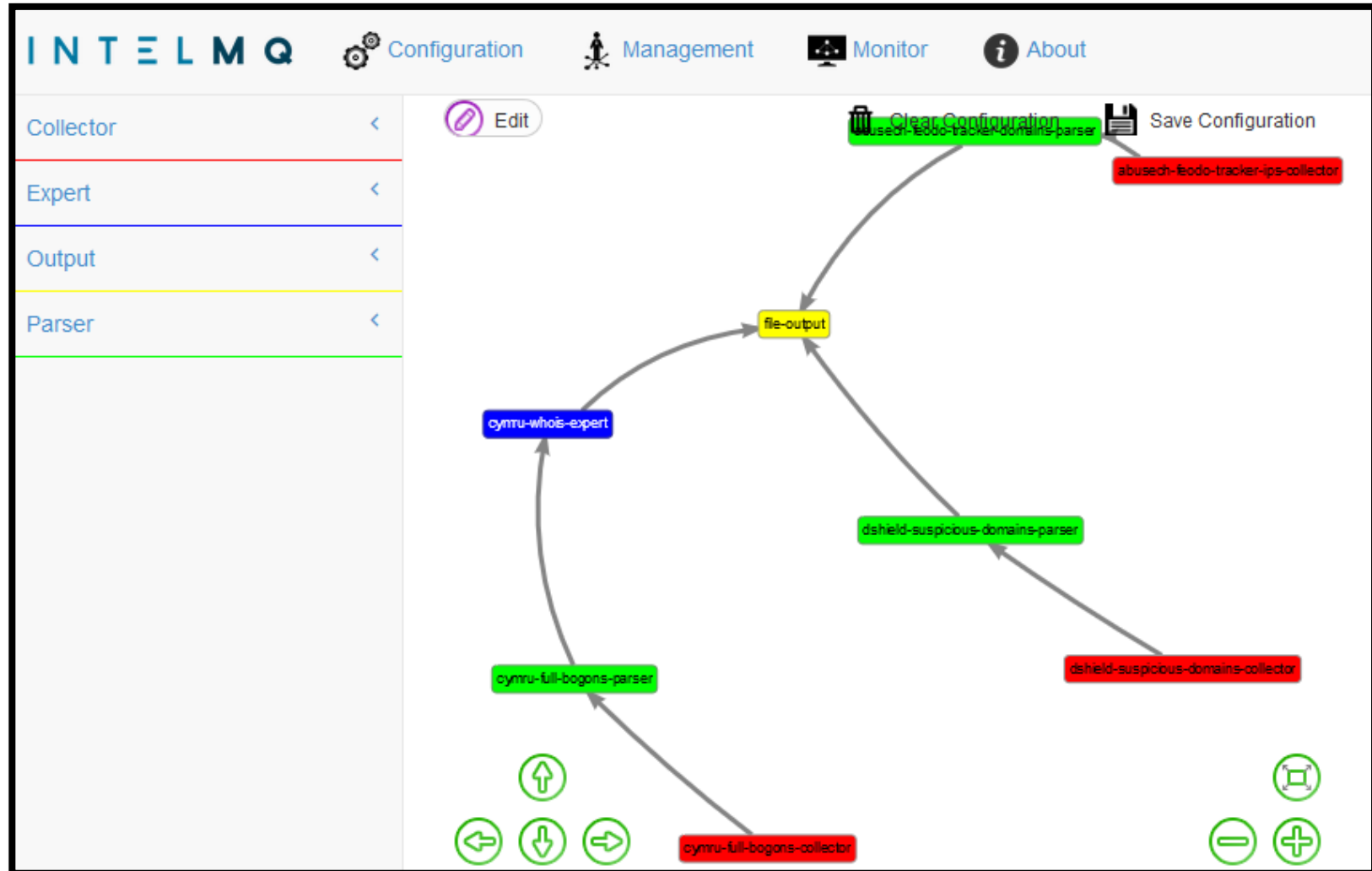


Само во случаи на пријава на инцидент за која „НЕ Е ПРИМЕН ДОКАЗ“, „НЕ Е НАЈДЕН ДОКАЗ“ и има „ДИСКУТАБИЛНА ВЕРОДОСТОЈНОСТ“

Систем за автоматизирано прибирање на информации за инциденти, ранливости и закани

IntelMQ

- Агрегација
- Филтрирање
- Збогатување
- Испраќање



Систем за известување, пребарување и визуелизација

The screenshot shows the Kibana interface with a search for 'malware'. The top navigation bar includes 'Discover', 'Visualize', 'Dashboard', and 'Settings'. The search bar contains 'malware' and shows a count of 30,000 records. The main view is a bar chart titled 'February 28th 2016, 10:48:09.989 - February 28th 2016, 15:05:03.267 — by 5 minutes'. The chart shows the count of records over time, with a significant peak around 13:00. Below the chart is a table of results with columns 'Time' and '_source'. The table shows two records, both classified as 'malware', with details such as 'classification.type', 'raw', 'source', 'feed.url', 'feed.accuracy', 'feed.name', 'time.observation', '@version', '@timestamp', 'beat.hostname', and 'beat.name'.

Selected Fields

- ? _source

Available Fields

- @timestamp
- @version
- _id
- _index
- _score
- _type
- beat.hostname
- beat.name
- classification.type

Quick Count (500 /500 records)

malware

100.0%

Visualize (1 warning ⚠)

- # count
- # feed.accuracy
- # feed.name

Bar Chart Data (Approximate)

Time Interval	Count
11:00 - 11:05	8,000
11:05 - 11:10	0
11:10 - 11:15	0
11:15 - 11:20	0
11:20 - 11:25	0
11:25 - 11:30	0
11:30 - 11:35	0
11:35 - 11:40	0
11:40 - 11:45	0
11:45 - 11:50	0
11:50 - 11:55	0
11:55 - 12:00	0
12:00 - 12:05	4,800
12:05 - 12:10	4,200
12:10 - 12:15	0
12:15 - 12:20	0
12:20 - 12:25	0
12:25 - 12:30	0
12:30 - 12:35	0
12:35 - 12:40	3,500
12:40 - 12:45	0
12:45 - 12:50	0
12:50 - 12:55	0
12:55 - 13:00	0
13:00 - 13:05	800
13:05 - 13:10	7,500
13:10 - 13:15	0
13:15 - 13:20	0
13:20 - 13:25	4,200
13:25 - 13:30	4,200
13:30 - 13:35	0
13:35 - 13:40	1,000
13:40 - 13:45	0
13:45 - 13:50	0
13:50 - 13:55	0
13:55 - 14:00	0
14:00 - 14:05	0
14:05 - 14:10	0
14:10 - 14:15	0
14:15 - 14:20	0
14:20 - 14:25	0
14:25 - 14:30	0
14:30 - 14:35	0
14:35 - 14:40	0
14:40 - 14:45	0
14:45 - 14:50	0
14:50 - 14:55	0
14:55 - 15:00	0

Table Results

Time	_source
February 28th 2016, 13:48:13.723	<code>classification.type: malware raw: MjMuMjQ3LjUuMTQ4IzQjMiNINNYWxpY2lvdXMgSG9zdCNUUyNXYWxudXQjMzQuMDExNTAxMzEyMTE3Ljg1MzUwMDM2NiMz source: /opt/intelmq/var/lib/bots/file-output/events.txt feed.url: https://reputation.alienvault.com/reputation.data feed.accuracy: 100 feed.name: AlienVault time.observation: February 28th 2016, 13:48:01.000 @version: 1 @timestamp: February 28th 2016, 13:48:13.723 beat.hostname: RMBTDB beat.name: RMBTDB count: 1 fields: - input type: log offset: 46,868,491 type: log host: RMBTDB tags: beats_input_codec_j</code>
February 28th 2016, 13:48:13.723	<code>classification.type: malware raw: MjIxLjE5NC40NC4xNzUjNCMyI01hbG1jaW91cy8Ib3N0I0N0I0h1YmVpIz45Ljg4OTcwMTg0MTE1LjI3NTAwMTUyNiMz source: /opt/intelmq/var/lib/bots/file-output/events.txt feed.url: https://reputation.alienvault.com/reputation.data feed.accuracy: 100 feed.name: AlienVault time.observation: February 28th 2016, 13:48:01.000 @version: 1 @timestamp: February 28th 2016, 13:48:13.723 beat.hostname: RMBTDB beat.name: RMBTDB</code>

MKD-CIRT



Целосен назив: НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ
ИНЦИДЕНТИ

Скратен назив: MKD-CIRT

Веб-страница: <https://mkd-cirt.mk>

Е-пошта: info@mkd-cirt.mk

Телефон: 02/3091 232

Јавниот клуч за шифрирање на MKD-CIRT и неговите потписи може да се најдат на големите меѓународни јавни сервери за клучеви.

Key ID: 0x333C00DB

Key Type: RSA 4096

Key Fingerprint: 0FB9 3DA3 E008 FA8B FC6A 9C71 0741 17A1 333C 00DB