KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Анализ и исследование инцидентов информационной безопасности

Жанат Жакупов
Улыкбек Шамбулов
KZ-CERT «ГТС» КНБ РК

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Статистика

Отработано:
В 2017**г**. - 25 958 инцидентов ИБ, из них ГО – 748 инцидентов ИБ;
В I **квартале** 2018**г**. - 5 479 инцидентов ИБ, из них ГО – 202 инцидентов ИБ.

Проверено:
В 2017**г**. – 130 **тысяч** доменных имен выявлено 456 инцидентов ИБ, из них ГО – 12 инцидентов ИБ;
В I **квартале** 2018 **г**. – 133 **тысяч** доменных имен выявлено 136, из них ГО – 3 инцидентов ИБ.

Google
YAHOO!
facebook

Отработано:
В 2017 **г**. - 131 фишинг-инцидента ИБ, из них ГО 1;
В I **квартале** 2018 **г**. - 114 фишинг-инцидента ИБ

Отработано:
В 2017 **г**. - 660 инцидентов ИБ website defacement, из них ГО - 86 инцидентов ИБ;
В I **квартале** 2018 **г**. – 695 инцидентов website defacement, из них ГО - 4 инцидента ИБ.

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Краткий обзор:

Инструментарии по информационной безопасности необходимый для CERTs/SOCs

“Arsenal”

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

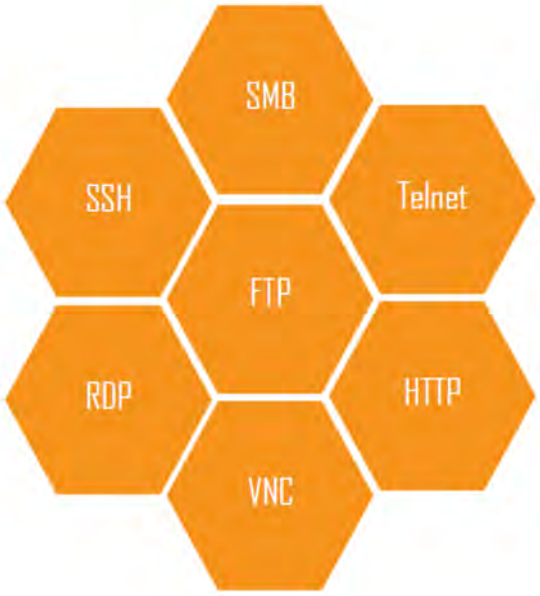
Категория инструментов

- Для обнаружения (Detection Tools)
  - Фиды (Information Feeds)
- Для анализа (Analysis Tools)
- Платформы для автоматизация процессов реагирования (Threat intelligence platform)

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Detection Tools

glastopf



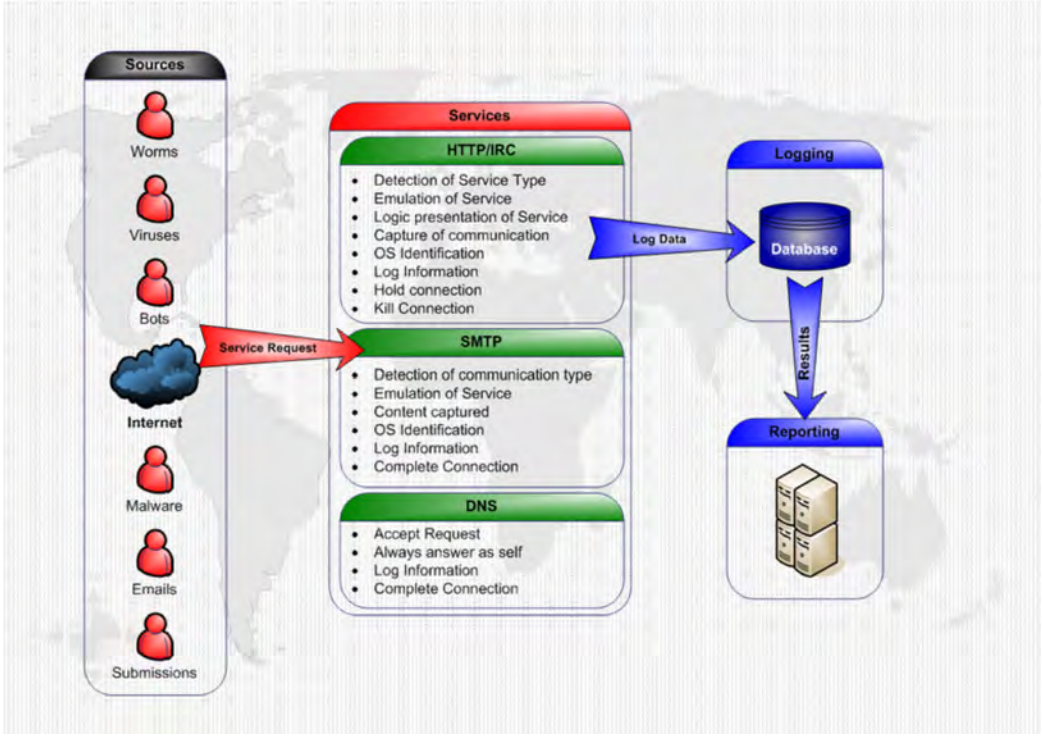
ALIEN VAULT

Passive DNS (STS)
Fast-flux

Система мониторинга (STS)

Web Crawler(STS)
~130,000 доменов .kz

Detection Tools (Sinkhole)



shadowserver

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Information Feeds

shadowserver

bots C&C URLs IPs

TEAM CYMRU

bots C&C URLs IPs

SPAMHAUS

THE SPAMHAUS PROJECT

bots C&C URLs IPs

CERT.PL

bots C&C URLs IPs

zone-h
unrestricted information

URLs

OpenPhish

URLs

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Information Feeds

CIRCL
Computer Incident Response Center Luxembourg

Symantec.

APWG

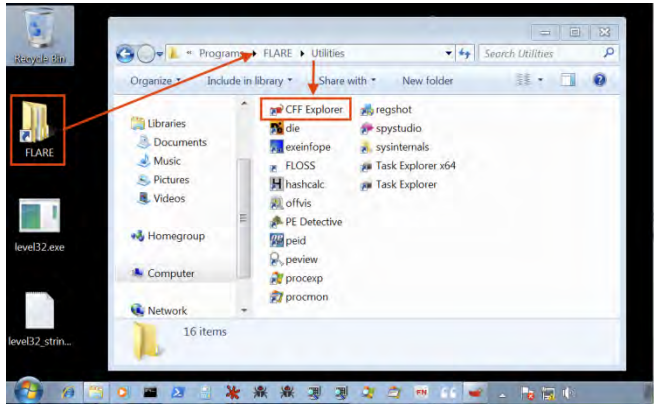
PhishTank®

KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Analysis Tools (Desktops)

Kali-Linux (Debian)

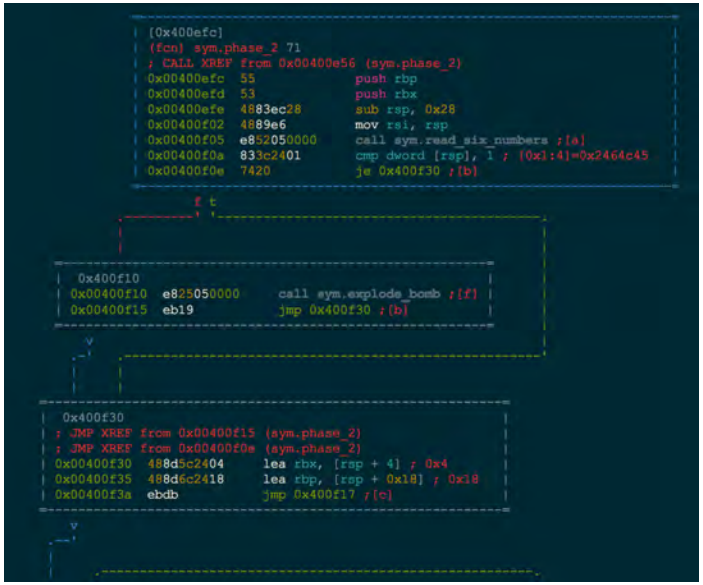
Flare VM (Windows)



KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Analysis Tools (Revese)

IDA Pro (Windows)

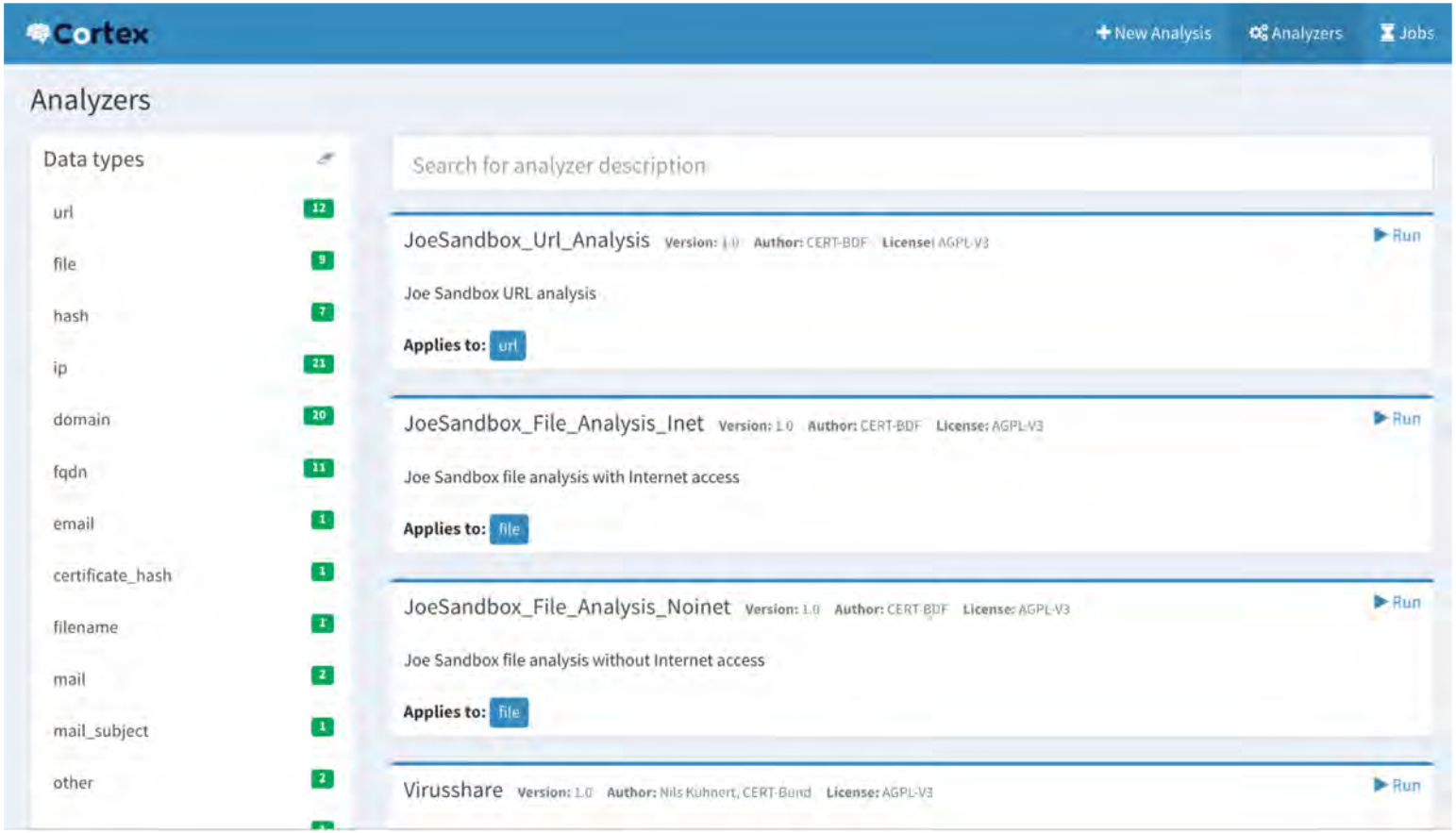


Radare 2 (Linux)

Hopperapp (Mac OS)

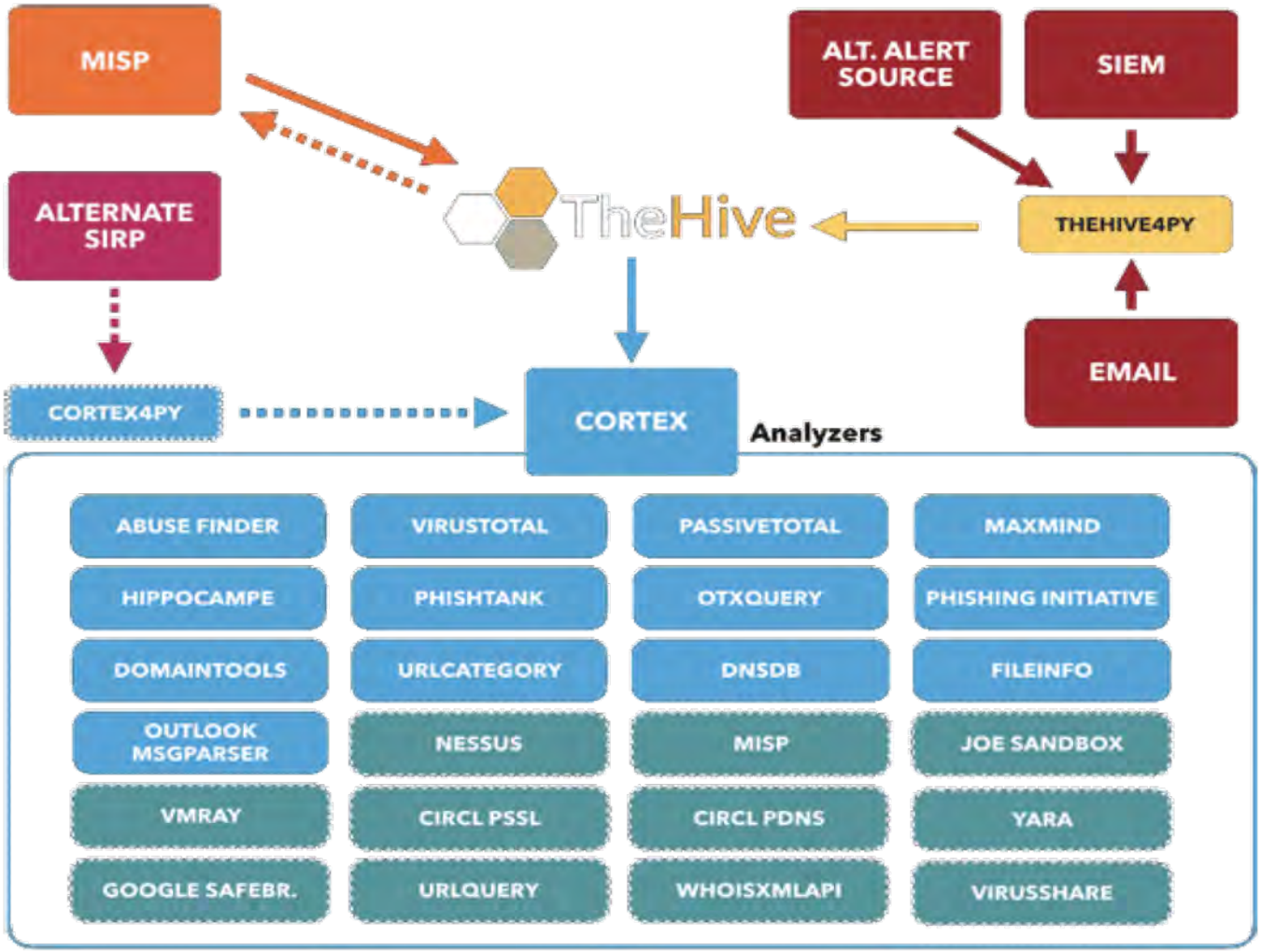
KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Одно окно для всех инструментов



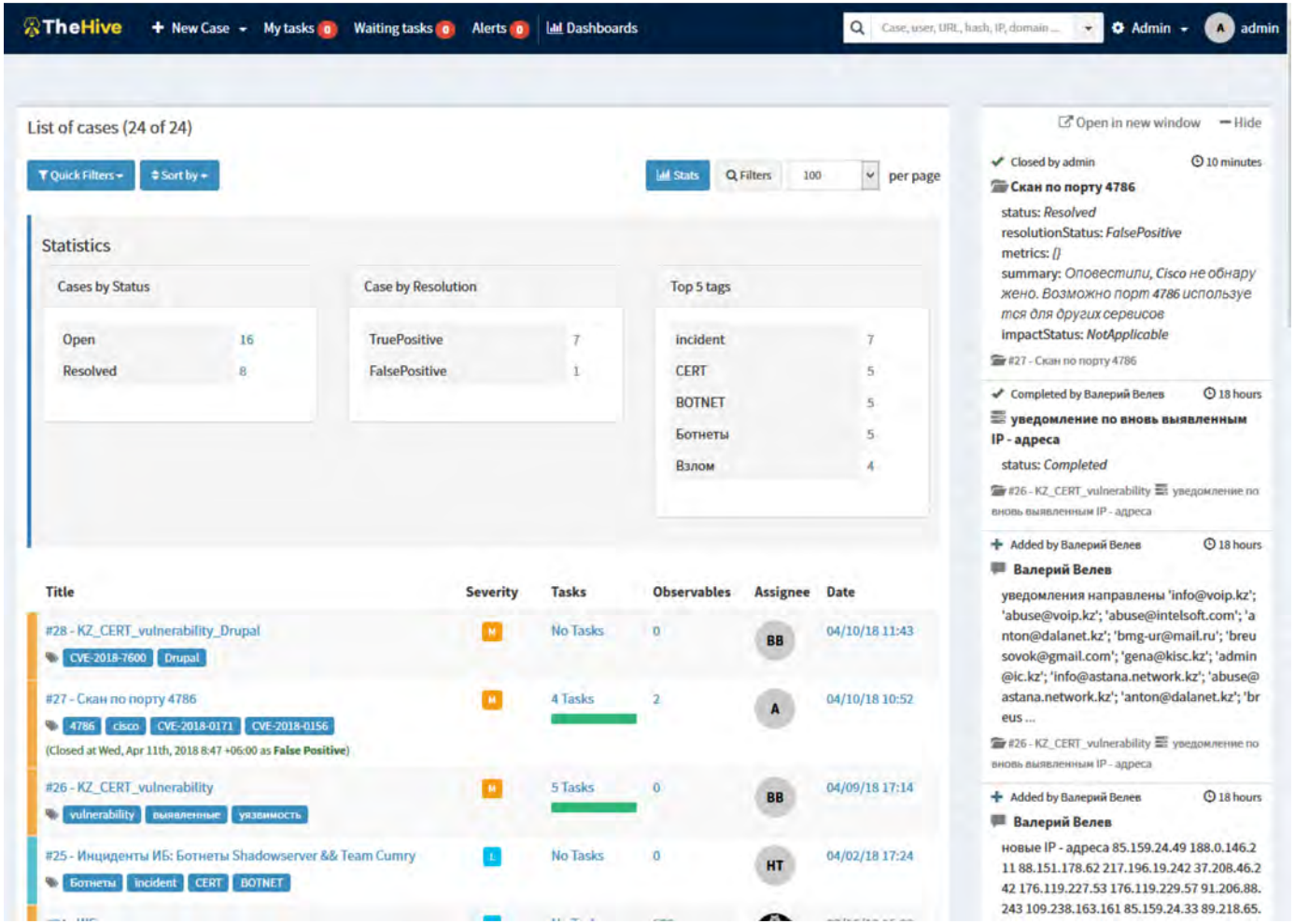
KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Журнал отработки инцидентов + Инструменты



KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Журнал отработки инцидентов + Инструменты



KZ-CERT
Служба реагирования на компьютерные инциденты Республики Казахстан

Обмена данными об угрозах и инцидентах

MISP
Threat Sharing

KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан

Спасибо за внимание!

incident @ kz-cert.kz

Call-center: 1400

www.kz-cert.kz