

Опыт реализации SOC и MSSP в PK





Членство в международной организации в области реагирования на компьютерные инциденты



Оперативный центр информационной безопасности



TTC-CSIRT

Более 20 000

рабочих станций

Более 4 000 000

выявлено потенциально опасных событий и угроз Более 800 000

вирусных событий обнаружено и вылечено Более 60 000

заражённых писем очищено

2 000 000

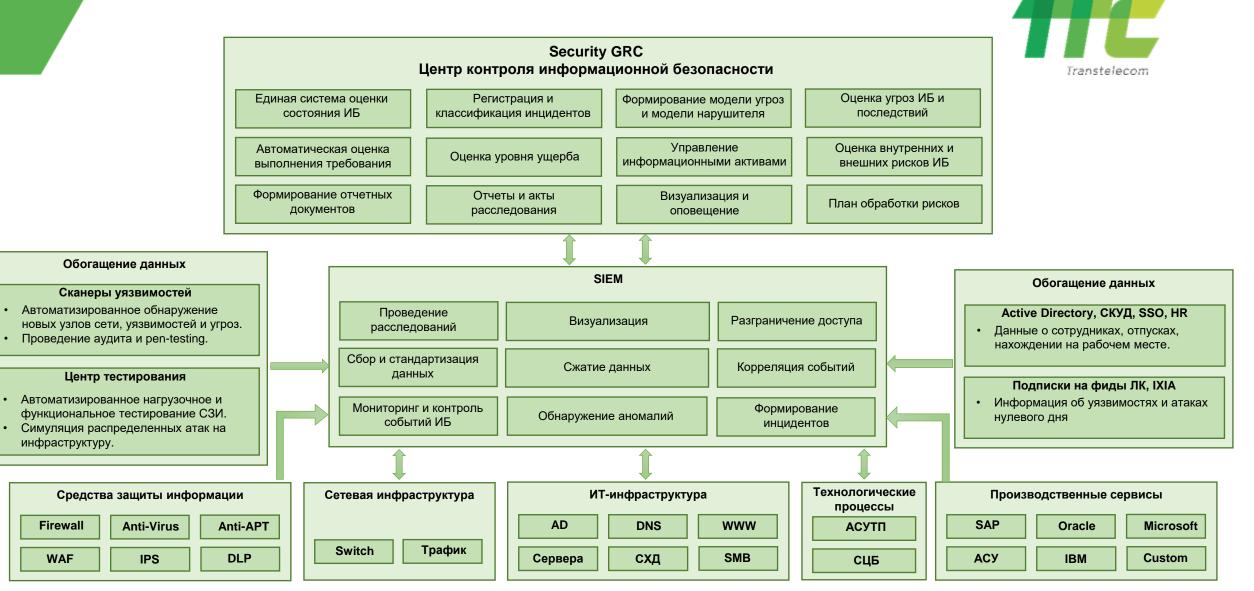
СПАМ сообщении заблокировано

5 000

факта срабатывания модуля таргетированных атак и нежелательного ПО

3 000 000

обнаружено попыток обращений к фишинговым и вредоносным ссылкам



инфраструктуру.

Firewall

WAF



Закрытый код

Партнеры Поставщики информации Платные каналы Платное обогащение

Открытый код

Открытые каналы Поисковые службы Новости

Внутренние

Журналы Средства безопасности SIEM

Потребители

Партнеры Управление ИТ-операции SOC CIRT

- Автоматизированный фбмен
- АРІ интерфейс
- Проверка и обогощение данных

- Интеграция средств защиты иформации через API или файловый обмен с платформой
- Интеграция данных об угрозах в SIEM
- Обогощение инцидента данными из платформы
- Выгрузка подозрительных индикаторов

ПЛАТФОРМА ОБМЕНА ДАННЫМИ ОБ УГРОЗАХ

- Данные о текущих и потенциальных атаках
- Индикаторы компроментации систем (IOC)
- Процедуры реагирования на различные типы инцидентов
- Объединение всех участников отрасли на борьбу с киберпреступностью





Министерство цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан



РГП «Государственная Техническая Служба"





••••••••





















Мировое сообщество



WØRLD ECONOMIC

FORUM















Мировые производители













НАЗАРЛАРЫҢЫЗҒА PAXMET! THANK YOU FOR ATTENTION! СПАСИБО ЗА ВНИМАНИЕ!