Гадәти алдакчылык гамәлләрен ачыклау

Secure Bank белән

Ни өчен Group-IB

Group-IB — югары технологияләрне кулланып, киберҗинаятьләрне һәм алдакчылык очракларын булдырмый калу һәм эзәрлекләү буенча әйдәп баручы халыкара компанияләренең берсе

1000+

бөтен дөнья буйлап уңышлы эзәрлекләү эше, 150 аеруча катлаулы җинаять эшләре

$300 млн

безнең хезмәт нәтиҗәсендә Group-IB клиентларына кайтарып бирелде

EUROPOL ҺӘМ INTERPOL рәсми партнеры

Европада куркынычсызлык һәм хезмәттәшлек буенча оешма (ОБСЕ) тарафыннан тәкъдим ителде

Бөтендөнья икътисад форумының даими әгъзасы

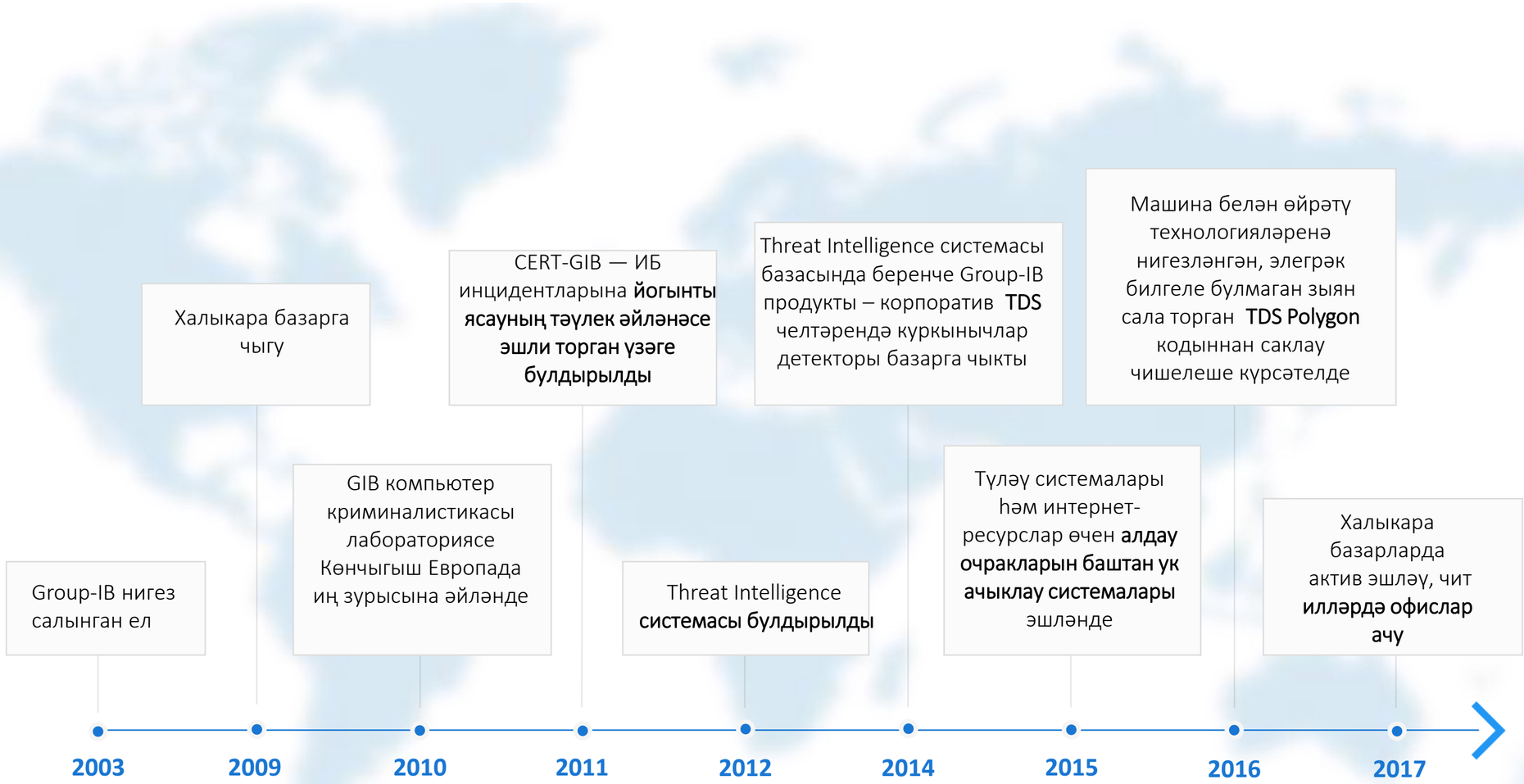
Group-IB тарафыннан Threat Intelligence – Forrester һәм Gartner бәяләмәсе буенча иң яхшы дөнья системалары исәбендә

Business Insider версиясе буенча киберкуркынычсызлык өлкәсендә иң йогынтылы 7 компаниянең берсе

Киберкуркынычларны тикшерү буенча Россия базарында лидер

Безнең хакта сөйлиләр: theguardian Bloomberg Forbes REUTERS Esquire ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ

Компаниянең тарихы



Group-IB күп еллык эш тәҗрибәсе киберкуркынычларны алдан ук ачыклау системасында – иң актуаль белешмәләргә һәм чынбарлыктагы хакерлык һөҗүмнәренә ясалган тирәнтен анализга нигезләнгән югары технологик продуктлар линейкасында гамәлгә ашырылды.

260+
хезмәткәр

40%
эшләп чыгаручы

27
уртача яше

45 000
йогынты ясау сәгатьләре

Уникаль ресурслар базасы

15 ел эшләү дәвамында тупланган уникаль ресурслар базасы

Без хакерлык активлыгын мониторинглау, бот-челтәрләрне күзәтү һәм инцидентларны чикләү өчен кирәкле белешмәләрне алу өчен югары технологияле инфраструктура ясадык. **Белешмәләрнең 90%ы системага ябык чыганаклардан килә**, аларның абсолют күпчелеге – уникаль. Без ябык мәйданчыкларны мониторинглыйбыз, зыян сала торган программаларның конфигурация файлларын һәм урланган идентификаторлар турында мәгълүматларны алып, бот-челтәрләрдәге үзгәрешләрне күзәтеп торабыз.

1 ЧЕЛТӘРЛЕ ИНФРАСТРУКТУРА

- Мониторингның һәм HoneyNet-тозакларның бүлгәләнгән челтәре
- Бот-челтәрләр аналитикасы
- Челтәрләрдәге һөҗүмнәрнең трекерлары
- Хакер форумнарын һәм ябык челтәр бергәлекләрен мониторинглау
- TDS сенсорларындагы белешмәләр

2 HUMAN INTELLIGENCE

- Group-IB лабораториясендә криминалистик экспертизаларның нәтиҗәләре
- Тикшерү материаллары
- Зыянлы ПТ мониторинглау һәм анализлау
- CERT-GIB мөрәҗәгатьләр базасы һәм инцидентларга йогынты ясау тәҗрибәсе
- Аудит нәтиҗәләре
- Group-IB максатчан аналитикасы

3 БЕЛЕШМӘЛӘР БЕЛӘН АЛМАШУ

- CERT йогынты ясау командалары
- Теркәгечләр һәм хостинг-провайдерлар
- Яклагыч чараларны җитештерүчеләр
- Киберкуркынычларга каршы көрәш оешмалары һәм берләшмәләре
- Europol, Interpol һәм хокук саклау органнары

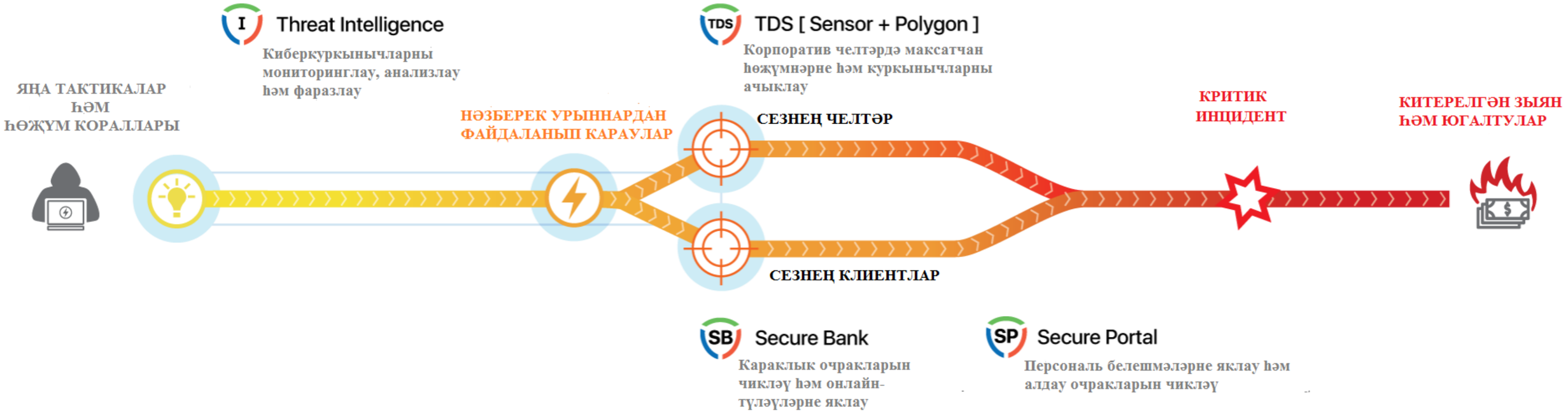
Киберкуркынычларны алдан кисәтү системасы

Без иң мөһимен бирәбез – инцидентларга әзерлек өчен вакыт.

Group-IB киберкуркынычларны алдан кисәтү системасы сезнең оборона чикләрендә барлыкка килгән яңа куркынычлар турында оператив рәвештә белергә һәм аларның барлыкка килүен туктатырга булыша. Ул безнең командаңның 15 еллык эш тәҗрибәсенә, хакер кампанияләренә ясалган тирәнтен анализга һәм дөнья буйлап эзәрлекләнгән актуаль киберҗинаятьчелеккә нигезләнгән.

15 ел

компьютер криминалистикасы, мәгълүмат куркынычсызлыгы буенча консалтинг һәм аудит өлкәсендәге эш тәҗрибәсе



Компаниянең төзелеше

АЛДАН КИСӘТҮ СИСТЕМАСЫ

- Threat Intelligence
- TDS
- Secure Bank
- Secure Portal

ЧИКЛӘҮ КУРКЫНЫЧЛАРНЫ

- Куркынычсызлык аудиты
- Compromise Assessment
- Red Teaming
- Brand Protection
- Anti-Piracy

ЙОГЫНТЫ ЯСАУ 24/7/365

- CERT-GIB мәгълүмат куркынычсызлыгы инцидентларына йогынты ясау үзәге

ИНЦИДЕНТЛАРНЫ ЭЗЛӘТҮ

- Компьютер криминалистикасы һәм зыян китерүче кодны тикшерү
- МК инцидентларын тикшерү
- Бәйсез финанс һәм корпоратив тикшерүләр

Group-IB продуктлар һәм сервислар юнәлеше бер-берсен тулыландырып тора, төрле типтагы куркынычларга каршы көрәштә синергетик нәтиҗәгә ирешү мөмкинлеген бирә.

Group-IB & AIG CyberEdge

Киберҗинаятьләрдән яклау һәм иминиятләштерү буенча Россиядә беренче комбинацияле продукт

Аерым очракларда киберҗинаятьчеләр зыянлы ПТ кулланып калмыйча, социаль инженерия, хезмәткәрләрне алдау, сатып алу белән дә шөгыльләнә. Безнең AIG белән хезмәттәшлегебез нәтиҗәсендә Group-IB клиентлары шундый катлаулы һөҗүм очракларыннан якланган.

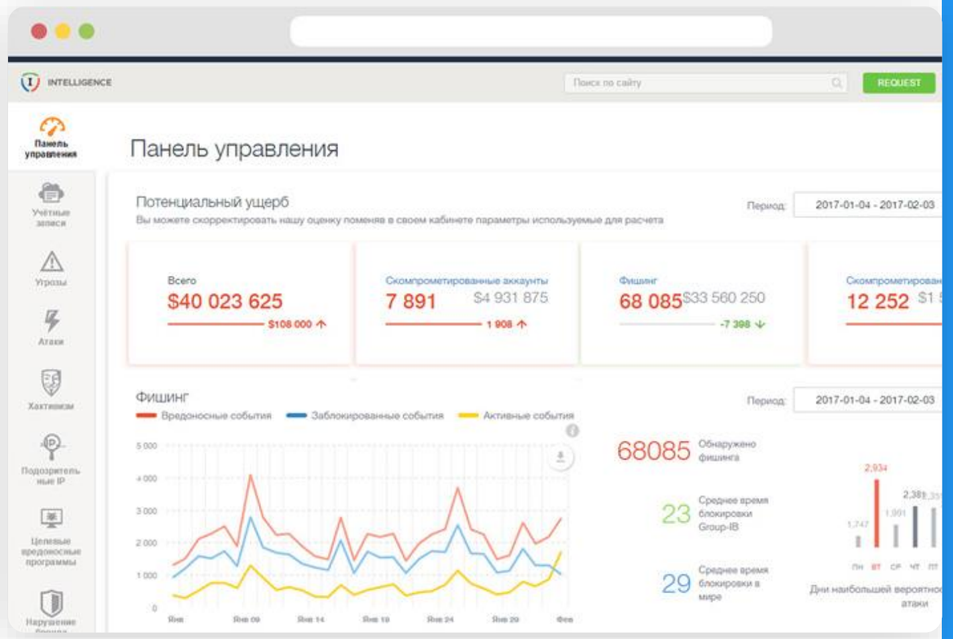
ИМИНИЯТ ЯКЛАВЫНА НӘРСӘ КЕРӘ

- Белешмәләр бозылуга бәйле югалтулар
- Белешмәләргә карата административ эзләтү
- Белешмәләр бозылганда йогынты ясауга киткән чыгымнар

Threat Intelligence

Компания, клиентлар һәм партнерлар өчен куркынычларны мониторинглау, анализлау һәм фаразлау

- Куркынычларны үлчәнгән рәвештә бәяләү һәм өстенрәк куркынычларны ачыклау өчен стратегик мәгълүмат
- Һөҗүмнәргә әзерләнү һәм яклагыч системаларны көйләү өчен оператив белешмәләр
- Инцидентка йогынты ясау вакытын минимальләштерә торган тактик индикаторлар



Үзебезнең илдәге ПТ реестрына кертелгән

Forrester Gartner IDC

Group-IB — Gartner (2015) һәм Forrester (2017) аналитик агентлыклары бәяләмәсе буенча дөньяда иң яхшы Threat Intelligence тәэминатчыларының берсе. 2017 елда IDC агентлыгы Group-IB киберкуркынычларны тикшерү буенча базар лидеры булып таныды.

- Һөҗүмнәр һәм куркынычлар турында оператив хәбәр итү
- Күрсәтмәле веб-интерфейс
- Сезгә кызыклы булган тармакларда хакерлык активлыгын күзәтеп тору, таркату, фаразлау
- Куркынычлар турында белешмәләр тапшырылганда STIX/TAXII тәэминаты
- Фаш ителгән белешмәләрдән һәм идентификаторлардан турыдан-туры файдалану
- Тәүлек әйләнәсе тәэмин итеп тору

Threat Intelligence файдалану нәтиҗәләре

Аналитиклар һәм Incident Response командалар

- Threat Intelligence белешмәләре нигезендә өстен инцидентларны сыйфатлы билгеләү
- Incident Response процессларын тизләтү
- Тәгаенләштерелгән куркынычлар контекстына керү, компания белән потенциаль кызыксынучы җинаятьчел төркемнәрнең тактикаларын һәм коралларын белү

CISO

- Киберкуркынычлар эволюциясен тирәнтен аңлау һәм сезнең сектордагы чын һөҗүмнәрне анализлау нәтиҗәсендә МК стратегиясен төзү
- Актуаль куркынычлардан яклау өчен технологик чишелешләрне үлчәнгән рәвештә сайлау
- Аналитикларның һәм Incident Response командаларының нәтиҗәлелеген һәм мөмкинлекләрен арттыру

CEO һәм топ-менеджмент

- Куркынычсызлык, Incident Response командалары һәм аналитиклар системасына булган инвестицияләрдән ROI максимальләштерү
- Идарәи карарларны кабул итүгә йогынты ясый торган куркынычлар турында мәгълүмат алу
- Җинаять максатларында компания брендыннан файдалануны чикләү, абруй җую куркынычларын киметү

MSSP

- Клиентларга куркынычлар контекстын тирәнтен аңлауга нигезләнгән сервис күрсәтү
- Үзләре өчен актуаль куркынычлар турындагы мәгълүматлардан чыгып, клиентлар өчен тәкъдимнәрне тагын да сыйфатлырак сайлап алу
- Куркынычлар барлыкка килүне һәм threat intelligence глобаль белешмәләре нигезендә аларга каршы тору чараларын фаразлау

Group-IB тарафыннан Threat Intelligence сезгә түбәндәге мөмкинлекләрне бирер:

- Инцидентларга булган йогынты вакытын минимумга кадәр киметү
- Һөҗүмнәргә каршы яңа кораллар һәм методлар барлыкка килүен күзәтеп тору
- Ябык хакер мәйданчыкларыннан персональләштерелгән белешмәләр алу
- Компаниянең мәгълүмат куркынычсызлыгы өчен сайлап алынган инвестицияләр стратегиясенең нәтиҗәлелеген бәяләү

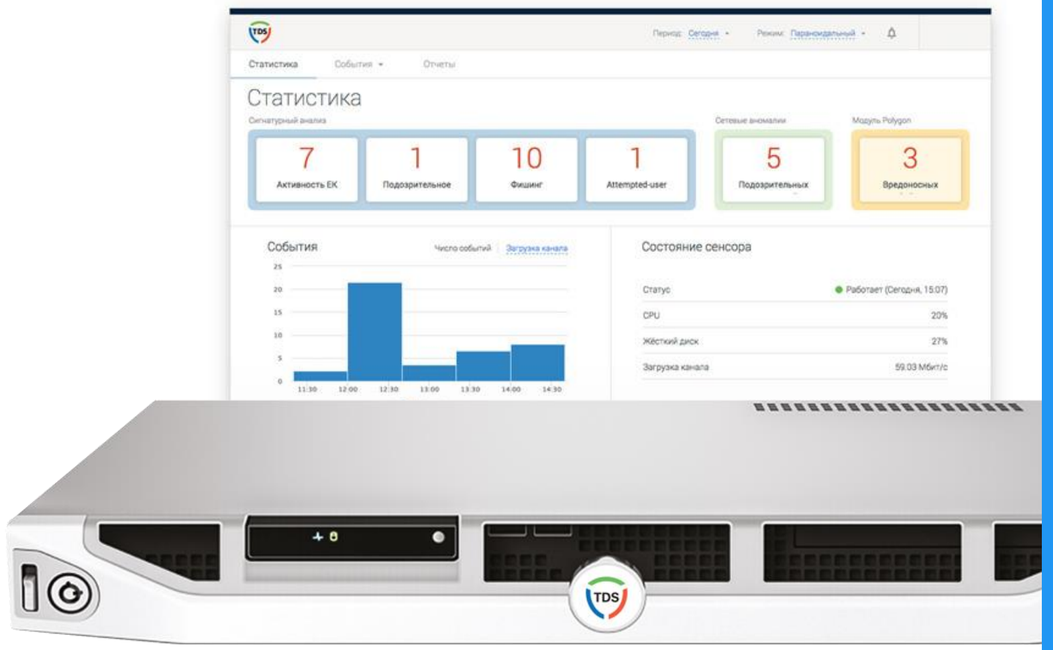
TDS Sensor

TDS — максатчан һөҗүмнәрне абайлау

Зарарланган төеннәрне ачыклый, үтеп керү, мәгълүмат урлау очракларын, максатчан һөҗүмнәрне һәм сәнәгый шпионлыкны чикли

Дөньянең төрле төбәкләрендә максатчан һөҗүмнәрнең үзгәлеген һәм җинаятьчел төркемнәрнең активлыгын тирәнтен аңлау нәтиҗәсендә без башкаларга шәйләнмәгән куркынычларны ачыклыйбыз, шул исәптән:

- ниятләнмәгән һәм куркынычлы челтәр багланышы
- күчә торган куркынычлы объектлар
- шпионлык ПТ
- читтән торып эшләү чаралары
- нәзбереклектән файдалану очраклары



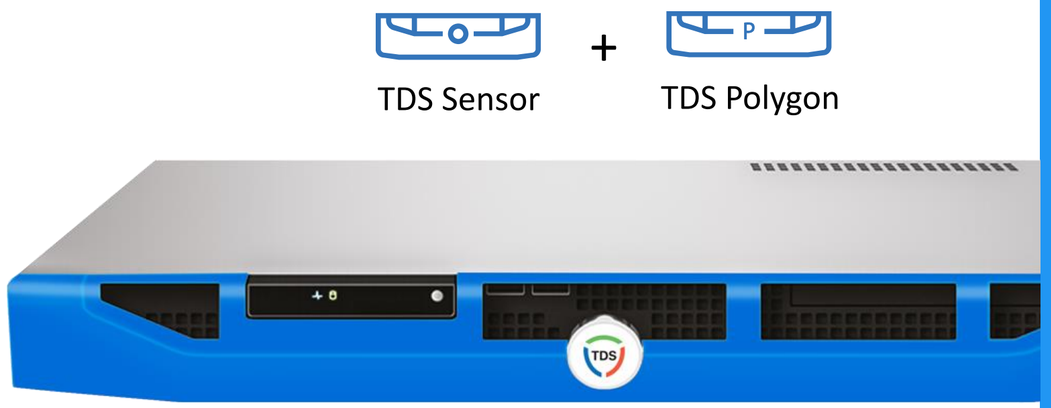
Куркынычларны югары төгәллек белән ачыклау өчен уникаль чыганаклар һәм автор эшләнмәләре:

1. Үз-үзен тоту ын анализлау алгоритмнары + машина белән укыту
2. Компьютер криминалистикасы лабораториясеннән һөҗүмнәр турында белешмәләр
3. Group-IB тарафыннан Threat Intelligence системасы белешмәләре

- Зыян салучы барлык актуаль һәм элегрәк билгеле булмаган программа төркемнәре турында шунда ук хәбәр итү
- Wi-Fi челтәрләрендә зарарланган мобиль җайланмаларны ачыклау
- Тәүлек әйләнәсе тәэмин итү һәм консультацияләү
- Уңайлы веб-интерфейс һәм күрсәтмә хисаплар
- Group-IB белгечләре ярдәмендә логларны кулдан анализлау һәм критик әһәмиятле инцидентларны ачыклау
- Объектларның куркынычлылык дәрәҗәсен ачыклау өчен даими яңартылып тора торган классификатор

Polygon корпоратив челтәрендә куркынычлар детекторы

Polygon сезнең эчке куркыныч-сызлык контурының изоляция-ләнгән тирәлегендә TDS алынган файлларны җибәрә, аларның үз-үзен тотышын анализлый һәм объектның куркынычлылыгы турында объектив бәяләмә чыгара



Виртуаль машиналар фермасы

Шик тудыра торган файллар сезнең бизнес һәм төбәк үзлегенә карап көйләнә торган тест тирәлегендә җибәрелә

Түбән дәрәҗәле система мониторы

Үзенең барлыгын белгертмичә, куркынычсыз тирәлектә эшләтеп җибәргәндә полигон иң түбән дәрәҗәдә объектларның үз-үзен тотышын күзәтеп тора

Даими рәвештә яңартыла торган классификатор

Объектның куркыныч булуы Machine Mind һәм билгеләнгән ешлыгы белән яңа мәгълүмат алучы классификатор ярдәмендә билгеләнә.

Почта юлламалары
Социаль инженериядән файдалану нәтиҗәсендә алына торган зарар салучы файллар

Күчереп алына торган файллар
Файдаланучылар тарафыннан һәм/яки аларның компьютерларына фонлы режимда күчереп алына торган файллар

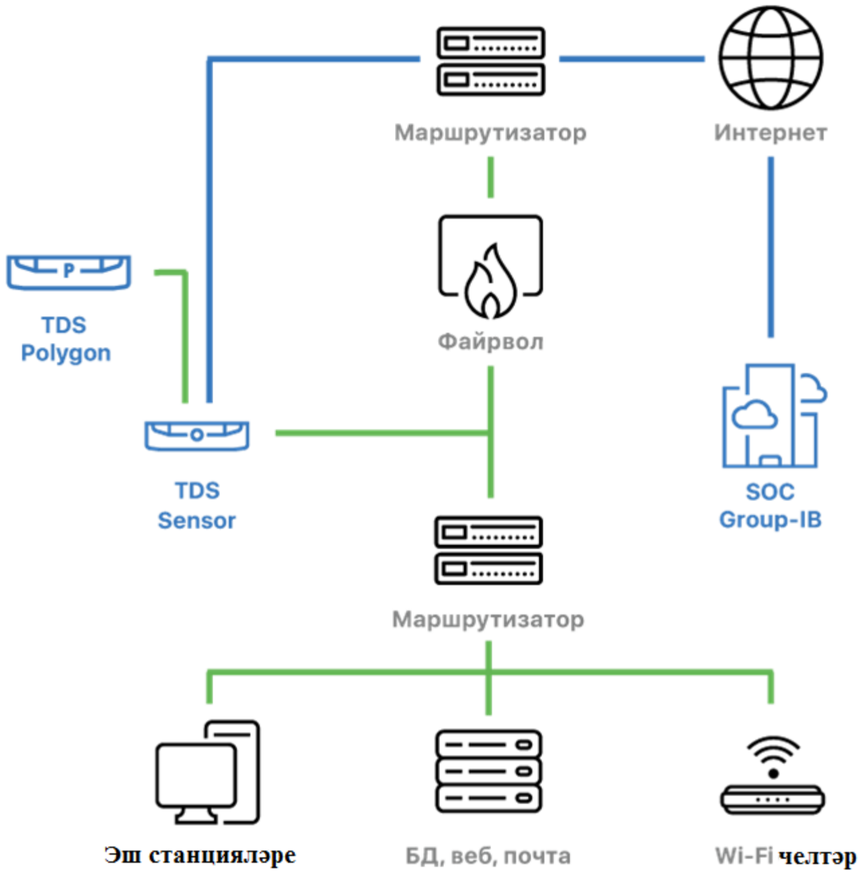
Максатчан һөҗүмнәр
Тәгаен сезнең инфраструктурага максат тоткан, зарар салучы ПТ

һәм башкасы,
элегрәк билгеле булмаган, антивируслар һәм сигнатур алымнар белән ачыкланмый торган зыян салучы объектлар

TDS ничек эшли

ТРАФИКНЫ АНАЛИЗЛАУ СЕНСОРЫ

- Зарарланган төеннәрне ачыклый, аларның уникаль чыганаклардан алынган белешмәләр нигезендә эшләп чыгарыла торган зарар салу активлыгы билгеләре буенча команда үзәкләре белән үзара бәйләнешен билгели.
- Зарар салучы программалар белән кертелә торган челтәр аномалияләрен машинадан өйрәнү алгоритмнары ярдәмендә тикшерә.
- Элегрәк билгеле булмаган зарар салучы кодны ачыклау өчен TDS Polygon торышны анализлау системасы белән интеграцияләнә.
- Ачыкланган инцидентлар турында мәгълүматны ышанычлы канал аша SOC Group-IB яки МК вакыйгаларын исәпкә алу буенча теләсә нинди эчке корпоратив системага тапшыра.



SOC GROUP-IB

- Сенсордан алынган инцидентлар турында белешмәләр. Белешмәләрне эшкәртү үзәгендә классификацияләнә һәм үзара бәйләнеше буенча бүленә.
- Вакыйгалар квалификацияле Group-IB белгечләре тарафыннан кулдан анализлана.
- SOC экспертлары сезнең белгечләргә телефон яки e-mail аша критик куркынычлар турында хәбәр итәчәк, ә анализның барлык нәтиҗәләре уңайлы web-интерфейста булачак.

Тәҗрибәле Group-IB белгечләре критик инцидентларны ачыклау эшен үз өстенә ала, сезнең МК хезмәтенә йогынты салуга игътибар итү мөмкинлеген калдыра.

Secure Bank

Түләү системалары өчен фродны алдан ачыклау системасы

Чынбарлык вакыт тәртибендә клиентның барлык җайланмаларында һәм платформаларында банкка бәйле алдау очракларын актив ачыклау.

Безнең чишелеш:

- Караклыкларны алдан ук тикшереп тору хисабына урлау очракларын чикли.
- Ялган эшләрне һәм клиентларга шалтыратуларны эшкәртүгә сарыфларны киметә.
- Сезнең онлайн- һәм мобиль банкинг системаларының яклангалык һәм кызыксындыргыч булу дәрәҗәсен арттыра.
- Зарарланулар һәм һөҗүмнәр турында клиентларны кисәтү мөмкинлеген бирәп, банкка булган ышанычны ныгыта.

Secure Bank үзебезнең илдәге ПТ реестрына кертелгән

Secure Bank
"Сбербанк Онлайн"ны
саклый

GROUP-IB

- Караклыкка бәйле түләүләрне һәм аларны эшләүгә әзерлекне ачыклый
- Яңа һөҗүмнәрне һәм караклык схемаларын тикшереп тора
- Кагыйдәләр һәм сигнатурлар көн саен яңарып тора
- Аналитик тәэминат һәм консультация
- Интернет-банкны яклау өчен JavaScript-модуль
- Android һәм iOS өчен Mobile SDK
- Клиент җайланмасына урнаштыруны таләп итми

Secure Bank ничек эшли

Secure Bank банкның веб-сәхифәләре яки мобиль банк кушымтасы белән бергә кертелә һәм клиентка зарарлану яки аның җайланмасын компрометацияләү турында үз вакытында хәбәр итү мөмкинлеген бирә.

Система зарар сала торган веб-инъекцияләрне, социаль инженерияне, фишингны, бот-челтәрләрне, исәпкә алу язуларына һөҗүм итүне, законсыз рәвештә акчага әйләндерү челтәрләрен һәм банкка бәйле караклыкның башка төрләрен ачыклый.

Secure Bank антифрод-технологияләре

- Җайланманың санлы эзе
- Файдаланучының глобаль профиле
- Кагыйдәләрнең алга киткән конструкторы
- Үз-үзен тотышына анализ
- Зарар салучы программаларны агенттан башка ачыклау
- Кросс-каналлы аналитика
- Group-IB Threat Intelligence белешмәләре

Secure Bank зыян китерә торган программаларны ачыклау һәм караклык очрагы барлыкка килер алдыннан ук аның үз-үзен ни рәвешле тотуына анализ ясау буенча кинәйтелгән чаралардан файдалана

Караклык очракларына каршы көрәштә классик системалар транзакцияләрне анализлый, алар клиент җайланмасына программа тәэминатыннан зыян салыну-салынмавын, транзакциягә кадәр анда нинди дә булса шикле күренешләрнең булу-булмавын ачыкламый

1. КАРАКЛЫКНЫ КЫЛЫП КАРАУ
(зыян китерә торган программаларны җибәрү, социаль инженерия, читтән торып эш итү)

2. АЛДАВЫЧ ТҮЛӘҮНЕ УЗДЫРУ

3. АКЧАНЫ ЧЫГАРУ

МОШЕННИКЛЫК ЭШЕ БЕРНИЧӘ СЕКУНДТАН БАШЛАП БЕРНИЧӘ АЙ ДӘВАМЫНДА ГАМӘЛГӘ АШЫРЫЛЫРГА МӨМКИН

Банк инфраструктурасы белән әзер интеграция

Гадәти антифрод-системалар өчен күренми торган куркынычларны ачыклау

Түләүле алдау

- *Кредитлы алдау*
- *CNP-операцияләре белән алдау*
- *Зарарлы веб-инъекцияләр*

Secure Bank клиентның электрон түләүләрен һәм кредит картасындагы белешмәләрен якларга булыша.

Персональ мәгълүматларны урлау

- *Исәпкә алу язуына һөҗүм итү*
- *Счет ачуга бәйле алдаучылык*
- *Бот гамәлләре*

Үз-үзен тотуны анализлау системасы һәм җайланманың санлы "эзе" технологиясе урланган исәпкә алу белешмәләреннән файдалануны күзәтү мөмкинлеген бирә.

Социаль инженерия

- *Алдый торган хәбәрләрне тарату*
- *Максатчан һөҗүмнәр*
- *Фишинг*

Клиентның бердәм профилен ясау һәм Group-IB Threat Intelligence белешмәләреннән файдалану белешмәләрнең читкә китүен һәм челтәрдәге алдауларны чикли.

Акча үзләштерү

- *Законсыз акчага әйләндерү челтәрләре*
- *Салымнардан качу схемалары*

Счетлар һәм башка төрле банк структуралары арасындагы бәйләнешләргә ясалган анализ шикле транзакцияләрне ачыкларга булыша.

Зарар салучы программалар

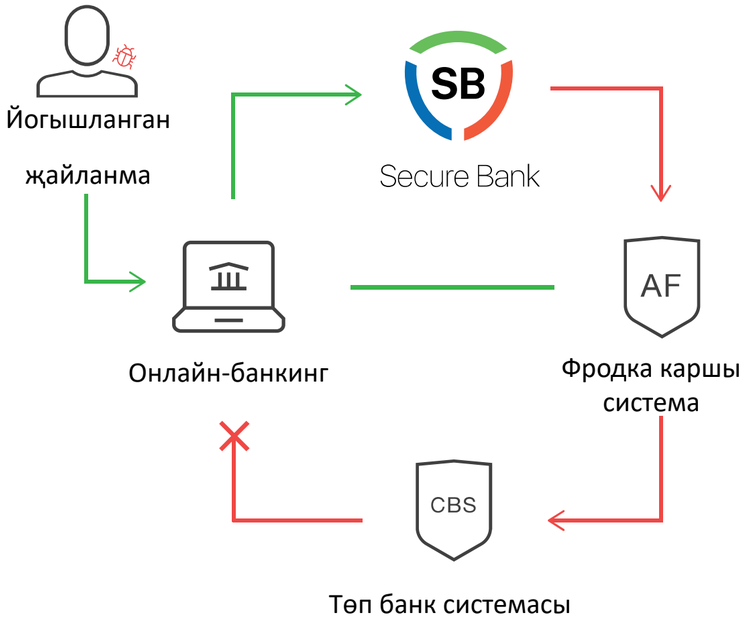
- *Трояннар*
- *Фарминг*
- *Бот-челтәрләр*

Патентланган Secure Bank алгоритмнары клиент ягына өстәмә программаларны урнаштырмыйча банк трояннарын ачыкларга булыша.

Кросс-каналлы һәм кросс-клиент һөҗүмнәре

- *E-commerce*
- *Мобиль җайланмалар*
- *Веб-интерфейс*

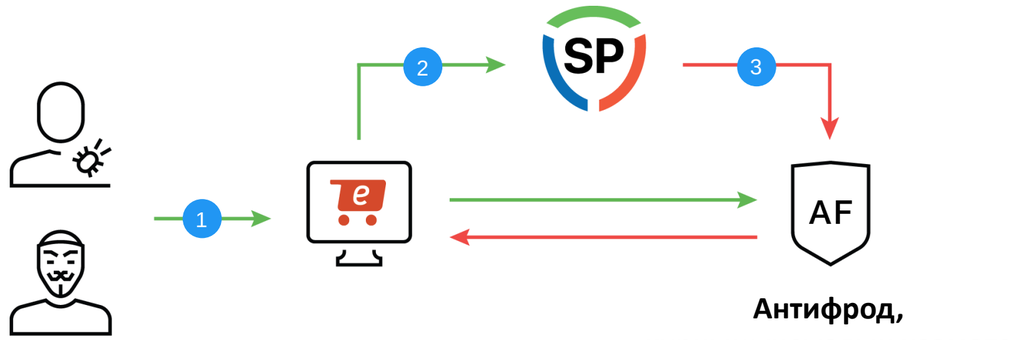
Secure Bank клиентны, интернет-кибетләрне һәм корпоратив порталларны да кертеп, барча мобиль һәм веб-платформаларда саклый.



Secure Portal

Файдаланучылар – интернет-порталларның куркынычсызлыгын тәэмин итү чылбырындагы иң нәзберек буын ягында алдакчылыкны алдан ачыклау системасы

Үзебезнең илдәге ПТ реестрына кертелгән



Антифрод, куркынычсызлык хезмәте

1. Портал сәхифәсендәге JavaScript-модуль клиент җайланмасындагы уникаль "эз"не билгели һәм алдакчылык активлыгы индикаторларын туплый
2. Иясезләндерелгән белешмәләр якланган канал аша SP тапшырыла, биредә Threat Intelligence системасы белешмәләрен кулланып эшкәртелә
3. Заказчыга чынбарлык вакыт режимында алдау очрагы турында хәбәр ителә, API инцидентларга йогынтыны автоматлаштыру мөмкинлеген бирә

Чишелеш түбәндәгеләрне чикли:

- Бонус балларын урлау өчен ябык корпоратив порталларга өченче затларның үтеп керүен
- Парольләр сайлауны, тавыш бирүчеләр санын арттыруны, фейк-кайтавазлар урнаштыруны
- Түләүле язылулардан уртак файдалануны
- Портал сәхифәләрендә көндәшләрнең реклама игъланнарын күрсәтеп, сатып алучыларны үз ягына аударуны

GROUP-IB

- Персональ белешмәләр һәм банк карталары турында мәгълүмат урлауны чикли
- Урланган карталар буенча сатып алуларны ачыклый
- Ботлардан файдалануны чикли
- Порталның ИТ-инфраструктурасына инвестицияләр таләп итми
- Фродка каршы системалар, SIEM, Firewall, EPS белән интеграллаштыру өчен API
- Аналитик тәэминат һәм консультация

Мәгълүмат куркынычсызлыгына аудит

Иң зур банклар һәм перспективалы стартаплар, энергетика гигантлары һәм зур булмаган адвокат бюролары белән эшлибез, теләсә нинди зурлыктагы һәм билгеләнештәге IT-инфраструктураларның нәзберек урыннарын аңлыйбыз.

- ДБО һәм мобиль банкинг кушымталары системалары
- DoS / DDoS-һөҗүмнәрне кисәтү, басымлы тест уздыру
- Элемтә операторларының сигнал челтәрләрен коммутацияләү төгәллеге
- Веб-ресурслар, шул исәптән корп./дәүләт порталлары, e-commerce мәйданчыклары
- Социотехник тестлар (социаль инженерия)
- Челтәр инфраструктураларының нәзберек урыннарны эзләү
- Программа тәэминаты, шул исәптән iOS, Android, Windows Phone
- POS, mPOS-терминалларның якланганлыгын тикшерү
- Коммерция серен һәм персональ белешмәләрне саклау системалары
- АСУ ТП һәм SCADA программа белән тәэмин итү

Group-IB тарафыннан мәгълүмат куркынычсызлыгына аудит:

- 10 елдан артык нәзберек урыннарны анализлыйбыз
- Сезнең системалар эшендә эчке мантыйкка тирән үтеп керәбез.
- Башкалар күрми торган куркынычларны күрәбез
- Һәр хисапта кабул итүчеләр өчен кыскача резюме, шулай ук белгечләр өчен тулы тасвирлама һәм конкрет киңәшләр дә бар

Compromise Assessment

Читләрнең үтеп керү һәм хакерлык һөҗүмнәренең әзерләнү билгеләрен ачыклау.

Compromise Assessment хакерлык һөҗүменә әзерлек, белешмәләрдән читләрнең файдалану билгеләрен ачыклый, килгән зыян күләмен бәяләргә һәм кайсы системаларга һөҗүм ясалуын һәм моның ни рәвешле башкарылуын билгеләргә булыша.

Group-IB экспертлары сезгә чын зыян килергә өлгергәнче үк яшерен куркынычларны ачыклар

Compromise Assessment кысаларында Group-IB белгечләре TDS программа-аппарат комплексын урнаштырыр, ә йөзләрчә тикшерү тәҗрибәсенә ия булган экспертлар инфраструктурага һәм читләр үтеп керүнең ачыкланган билгеләренә анализ уздырыр.

Compromise Assessment нәтиҗәләре буенча:

1. **Читләрнең үтеп керүе турында хисап**

   Инфраструктурага читләрнең үтеп керү эзлеклелегенә тасвирлама, җинаятьчеләрнең гамәлләрен җентекле ачыклау

2. **Башкарылган эшләр турында хисап**

   Эшләрнең составын һәм йомгакларын Compromise Assessment уздыруның һәр этабында җентекләп тасвирлау

3. **Киңәшләр**

   Киләчәктә һөҗүмнәрне булдырмас өчен инфраструктураны модернизацияләү буенча киңәшләр

4. **Җитәкчелек өчен хисап**

   Инфраструктураны тикшерүнең төп йомгакларын тасвирлый торган кыска хисап

Компьютер криминалистикасы буенча экспертлар читләр үтеп керүе предметына инфраструктураның әһәмиятле элементларын тикшерер

- Хосусый эшләр махсуслаштырылган форензик-кораллардан һәм уникаль Threat Intelligence белешмәләреннән файдалана
- Инфраструктураның әһәмиятле төеннәрен: домен контроллеры, процессинг, түләү шлюзлары һ.б. тикшерер.
- Инцидентларның кабатлаунын булдырмас өчен инфраструктурага читләр үтеп керү хронологиясен торгыза

TDS комплексы элегрәк билгеле булмаган максатчан кибер-һөҗүм билгеләрен ачыкларга булышыр

- TDS Sensor челтәр аномалияләрен, йогышлануларны һәм җайланмаларның гадәти булмаган торышын ачыклый
- TDS Polygon изоляцияләнгән тирәлектә потенциаль куркынычлы булган объектларны эшләтеп җибәрә, объектның торышын анализлый һәм аның куркынычлылык дәрәҗәсен билгели
- Ачыкланган барлык вакыйгалар белгечләр тарафыннан 24/7 режимында анализлана

Яшерен куркыныч-ларны сез айлар буе күрмәскә мөмкин

Максатчан һөҗүмгә әзерлек

Хакерлар һөҗүм ясау өчен инфраструктураны берничә ай дәвамында сезгә белгертмичә эшкәртә

Берләштерүләр һәм "йотулар"

Башка бизнес белән интеграллаштырулар яңа инфраструктурада яшерен булган куркынычларга ия: билгеләр, бэкдорлар, CVE

Намуссыз конкурентлар

Коммерция сереннән файдалану мөмкинлеген алып, конкурентлар базарда үзләре өчен өстенлек тудыра

Инсайдерлар яки эштән куылган хезмәткәрләр

Компания инфраструктурасының ничек төзелгәнен белеп, алар белешмәләрне сиздермичә генә "шудыралар" һәм озак вакыт билгесез кала

Red Teaming

Сезнең куркынычсызлык хезмәтен көчәйтү өчен максатчан һөҗүмнәрне даими рәвештә имитацияләү. Сезнең куркынычсызлык хезмәте катнашында зур күләмле өйрәнүләр, алар түбәндәге сорауларга җавап бирәчәк:

- Сезнең системалар инцидентларны нәтиҗәле чикләргә, ачыкларга һәм аларга йогынты ясарга әзерме?
- Куркынычсызлык хезмәте хезмәткәрләре максатчан һөҗүмнәр вакытында ничек гамәл кыла?
- Куркынычсызлыкны тәэмин итү алымнарында компаниянең һөҗүмнәргә каршы тору сәләтен арттыру өчен сезгә нәрсәләрне үзгәртергә кирәк?

Һөҗүм итүләрне даими рәвештә имитацияләү нәтиҗәсендә Red Teaming максатчан һөҗүмнәргә әзерлек дәрәҗәсен арттырырга, яңа зәгыйфьләнгән урыннарны ачыкларга һәм бетерергә, командагызга күнекмәләр бирергә һәм чын уркынычларга каршы тору процессларын яхшыртырга булыша.

Red Teaming нәтиҗәләре буенча:

- Җитәкчелек өчен кыскача докладлар
- Нәтиҗәләр турында җентекле хисаплар һәм сезнең куркынычсызлык системасын яхшырту буенча эксперт киңәшләре
- Критик зәгыйфьләнүләрне ачыклаган очракта, экстрен хәбәр итүләр

Red Teaming Methodology:

Максатларны килештерү, коралларны сайлау → Берничә ай дәвамында: максатчан һөҗүмнәрне даими рәвештә имита-цияләү, болар хакында бары тик МК җитәкчесе генә белә → Сезнең инфраструктурада һөҗүм өчен яңа өслек ачучы үзгәрешләргә даими мониторинг

Red Teaming вакыт белән берничек тә чикләнмәгән. Әлеге чиксезлек Red Teaming айлар буе һөҗүмгә әзерләнүче чын җинаятьченең үз-үзен тоту моделенә төрле коралларны һәм һөҗүм веторларын кулланып карап, максималь якынайта

Red Teaming төшенчәсе хәрби эштән килеп чыккан: өйрәнүләр вакытында кызыл команда һөҗүм ясый, зәңгәресе – үз-үзен яклый

Brand Protection

Интернетта брендка каршы юнәлдерелгән куркынычларны ачыклау һәм бетерү буенча технологик сервис.

Компаниянең актуаль онлайн-куркынычлардан акчага һәм абруйга бәйле сарыфларын чиклибез:

- Брендтан хокуксыз файдалану һәм интернет-алдау
- Контрафакт таралышы һәм партнерлык сәясәтен үтәмәү
- Мәгълүмати һөҗүмнәр һәм тискәре кайтавазлар

Бозуларны эзләү буенча алдынгы технологияләр:

Machine learning
Система алдагы тәҗрибәгә нигезләнеп, бозуларны мөстәкыйль квалификацияли

Big data
Зур белешмәләрне анализлау технологиясе сайтлар арасында һәм соцчелтәрләрдәге төркемнәр арасында бәйләнешне автомат ачыклый

Intelligence driven
Киберҗинаятьләрне ачыклауда кулланыла торган Group-IB технологияләре хокук бозучылар белән турыдан-туры элемтә булдырырга ярдәм итә

3 млн ресурс
24/7 режимында автомат күзәтелә

10 мең
көн саен шуның кадәр җитешсезлек бетерелә

85% бозу
судка кадәр тәртиптә бетерелә

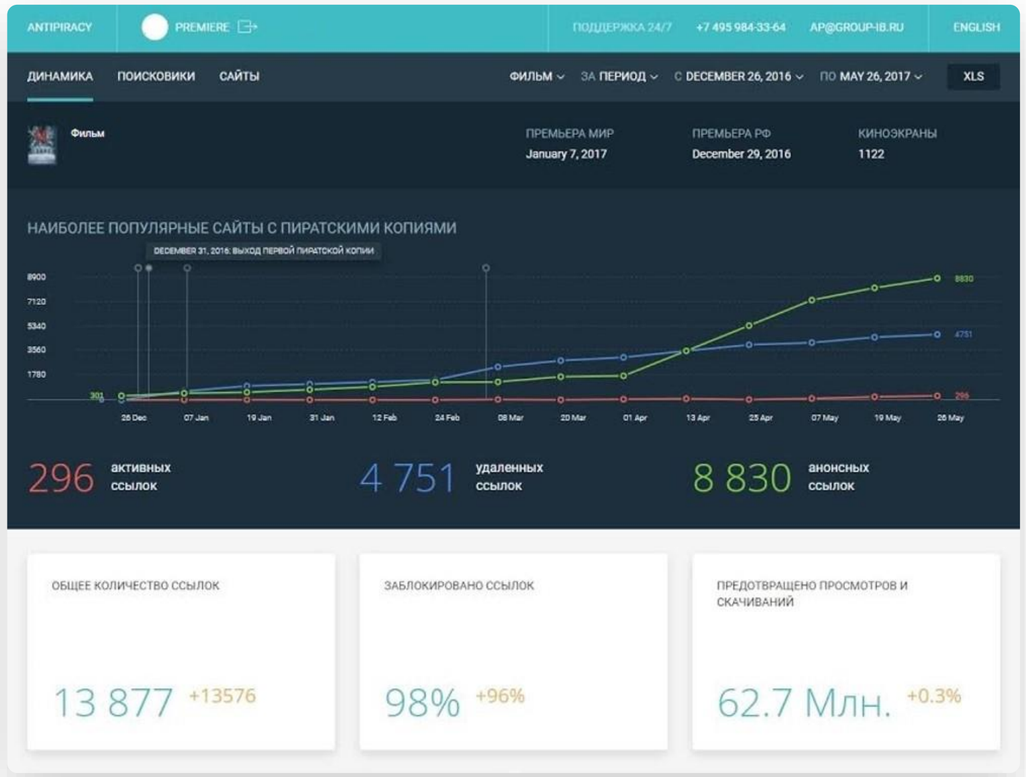
GROUP-IB

- Куркыныч сайтларны тиз арада туктату
- Рунеттан читтә йогынты ясау мөмкинлеге
- Тәүлек әйләнәсе мониторинг
- Санлы дәлилләр туплау
- Алдаучы сайтлар арасындагы бәйләнешләрне ачыклау
- Рецидивларны чикләү

Anti-Piracy

Санлы контентны акыллы яклау базарында лидер

- 120 000+ ресурсны, vk.ru, veterok.tv, kinostock.tv кертеп, мониторинглау
- Пират мәйданчыкларын суд нигезендә туктатуның уңышлы кейслары
- Зур пират мәйданчыкларында контентны оператив рәвештә ябу
- Файдаланучыларны сезнең рәсми ресурсларга юнәлтү



30 минут

теләсә нинди пират контентын ачыкларбыз, хәтта шактый үзгәрешләргә дучар ителгәнен дә

24 сәгать

рунетның иң зур пират мәйданнарыннан контент таралышына чик куярбыз

7 көн

сезнең контентка булган сылтамаларның 99%ына кадәр ябабыз һәм ачык булмаган мәйданчыклар буенча чишелешләр тәкъдим итәрбез

- Блокка кую эшен корректлы рәсмиләштерү
- Хәбәрләрдән югары дәрәҗәле кайтаваз
- Интуитив аңлаешлы интерфейс
- Тәүлек әйләнәсе мониторинг
- Судка кадәр башкарыла торган чараларның киң спектры
- "Бер төймә"гә басып, пират контентын юкка чыгару

CERT-GIB йогынты үзәге

CERT-GIB (Computer Emergency Response Team) — мәгълүмат куркынычсызлыгы инцидентларына тәүлек әйләнәсе йогынты ясау үзәге

- Фишинг ресурслары барлыкка килүен, зарар салучы ПТ таралышын, контрафакт белән сәүдә итүне мониторинглыйбыз
- Йогынты ясау һәм ачыклау буенча барлык этапларда тулы юридик ярдәм күрсәтәбез
- .RU, .РФ доменнарында һәм тагын 1000 артык домен зоналарында куркынычлы сайтларны оператив ябабыз
- Бөтен дөнья буйлап эшлибез: партнерлар челтәре аша, хостинг-провайдерлар һәм доменлы исемнәрне теркәүчеләр белән элемтә

Ростех

Россиядәге иң зур дәүләт корпорацияләренең берсе булган Ростех үзенең CERT RT-Inform ясау өчен партнер сыйфатында Group-IB сайлады

Интернет челтәрендә Илкүләм доменның координация үзәгенең һәм Интернетны үстерү фондының компетентлы оешмасы

Халыкара FIRST һәм Trusted Introducer бергәлекләренең аккредитацияләнгән әгъзасы

IMPACT партнеры – киберкуркынычларга каршы тору буенча халыкара партнерлыклар

Карнегия Университеты тарафыннан авторлаштырылган, рәсми рәвештә CERT сәүдә маркасыннан файдалана

Компьютер криминалистикасы лабораториясе һәм тикшерүләр бүлеге

Көнчыгыш Европадагы иң зур Компьютер криминалистикасы һәм зыян салучы кодка анализ лабораториясе

Иң заманча җайланма һәм алдынгы вирус аналитикасы

Иң яхшы эшләнмәләр, эз югалтуларны әйләнеп узу мөмкинлеген бирүче дөньяви технологияләр

Хокук саклау органнары белән хезмәттәшлек итү

Шул исәптән оператив-эзләтү чараларында рәсми катнашу

Теләсә нинди мәгълүмат саклагычлардан белешмәләр эзләү

Белешмәләр юкка чыгарылган, яшерелгән яки шифр белән бикләнгән булса да, без аларны табарбыз

Мобиль йогынты ясау командасы

Урында санлы дәлилләр туплау һәм тикшерү, нәтиҗәләрне бетерү буенча киңәшләр

80% Россиядә резонанслы югары технологик җинаятьләрнең шул кадәр өлеше безнең белгечләр катнашында ачыклана

Һәркемгә аерым якын килү алымын табарбыз

Белгечләр командасы: E-Discovery һәм Forensic башлап финанс аудиты һәм корпоратив хокук

Чыгарылган активларны кайтару тәҗрибәбез бар

тикшерүләрнең берсе нәтиҗәсендә зыян күрүче компаниягә 3,3 млрд. сум акчасы кайтарып бирелде

Киберҗинаятьләр икътисадын аңлыйбыз

Эксклюзив эзәрлекләнгән Threat Intelligence ярдәмендә акчаның хәрәкәт итү чылбырын торгызабыз

Адвокатларга, тикшерүчеләргә, прокурорларга консультацияләр бирәбез

Тикшерүнең барлык этапларында консультацияләр уздыру мөмкин

- Компьютер-техник экспертиза
- Судта санлы дәлилләр җиткерүдә бай эш тәрибәсе
- Санлы дәлилләр туплау
- Зарар салучы программаларны тикшерү
- Аутсорсинг һәм бәйсез экспертиза
- Криминалистик тикшерүләр

PRE-IR ASSESSMENT

Мәгълүмат куркынычсызлыгы инцидентларына нәтиҗәле йогынты ясау өчен әзерләнү.

Pre-IR Assessment сезнең системаларның, командаларның һәм процессларның йогынты ясауга әзерлеген тикшерү һәм инцидент очрагына төгәл план төзү мөмкинлеген бирер.

Гадәттә күзәтелгән проблемалар

- Белешмәләрнең күпчелеге югала һәм аларны журналга теркәү дөрес алып барылмый
- Инцидент шөбһәгә сала һәм контрольсез гамәл кылуга китерә
- Йогынты ясау процесслары көйләнмәгән, рольләр бүленмәгән

Pre-IR Assessment нәтиҗәләре

- Системаларны инцидентка нәтиҗәле йогынты ясау өчен көйләү буенча киңәшләр
- Ышанычлы һәм төгәл эшләнгән гамәлләр планы
- Департаментлар белән җайга салынган коммуникацияләр

Төп компонентларга комплексы бәяләмә

1 Технологияләр

Челтәр һәм система инфраструктурасын тикшерү – санлы дәлилләрне тулы һәм төгәл туплау мөмкинлекләре, читләрнең тыкшыну индикаторларын ачыклау сәләте, инцидентны оператив туктату һәм йогынты ясау барышында челтәргә идарә итү әзерлеге.

Нәтиҗә – реаль системаларда процессларны эшкәртү: скриптларны эшләтеп җибәрү, төрле инцидент типларында кирәкле белешмәләрне эзләтү һәм туплау.

2 Кешеләр

IT һәм мәгълүмат куркынычсызлыгы хезмәтләре хезмәткәрләренең компетенциясен **тикшерү**.

Нәтиҗә – Group-IB экспертларыннан инцидентларга йогынты ясау буенча ике көнлек укыту, ышанычлы һәм әзерлекле команда.

3 Регламентлар

Регламентларның һәм документацияның тулы, актуаль һәм гамәлдә максатка ярашлы булуын **тикшерү**.

Нәтиҗә – инцидент барлыкка килгән очракта чыннан да файдалы булачак регламентлар һәм документлар.

4 Структура

Команда җаваплылыгының һәм аның оешу структурасының бүленешен **тикшерү**.

Нәтиҗә – инцидентка йогынты ясау барышында төрле департаментларның көйләнгән һәм командада эшләве.

GROUP-IB

Pre-IR Assessment ничек уза

Әзерлек

- Мәгълүмат туплау
- Программаны конкрет клиент һәм тармак өчен яраклаштыру
- Тикшерү кагыйдәләрен раслау
- Срокларны килештерү

Процесс

- Group-IB экспертларының клиент компаниясенә баруы
- Төрле инцидентлар өчен типик булган белешмәләрне сорату
- Белешмәләр алуның тулы, үтемле һәм тиз булуын анализлау
- Инцидентларга йогынты ясау буенча тренинг үздыру

Йомгак

- Системаларны нәтиҗәле йогынты ясау өчен көйләү буенча киңәшләр
- Структураны һәм процессларны оптимальләштерү
- Йогынты ясау планы
- Әзер регламентлар
- Өйрәтелгән команда

2003 елдан башлап киберҗинаятьләрне чиклибез һәм ачыклыйбыз.

www.group-ib.ru
info@group-ib.ru
twitter.com/groupib
t.me/group_ib
group-ib.ru/blog
+7 495 984 33 64
facebook.com/group-ib
instagram.com/group_ib