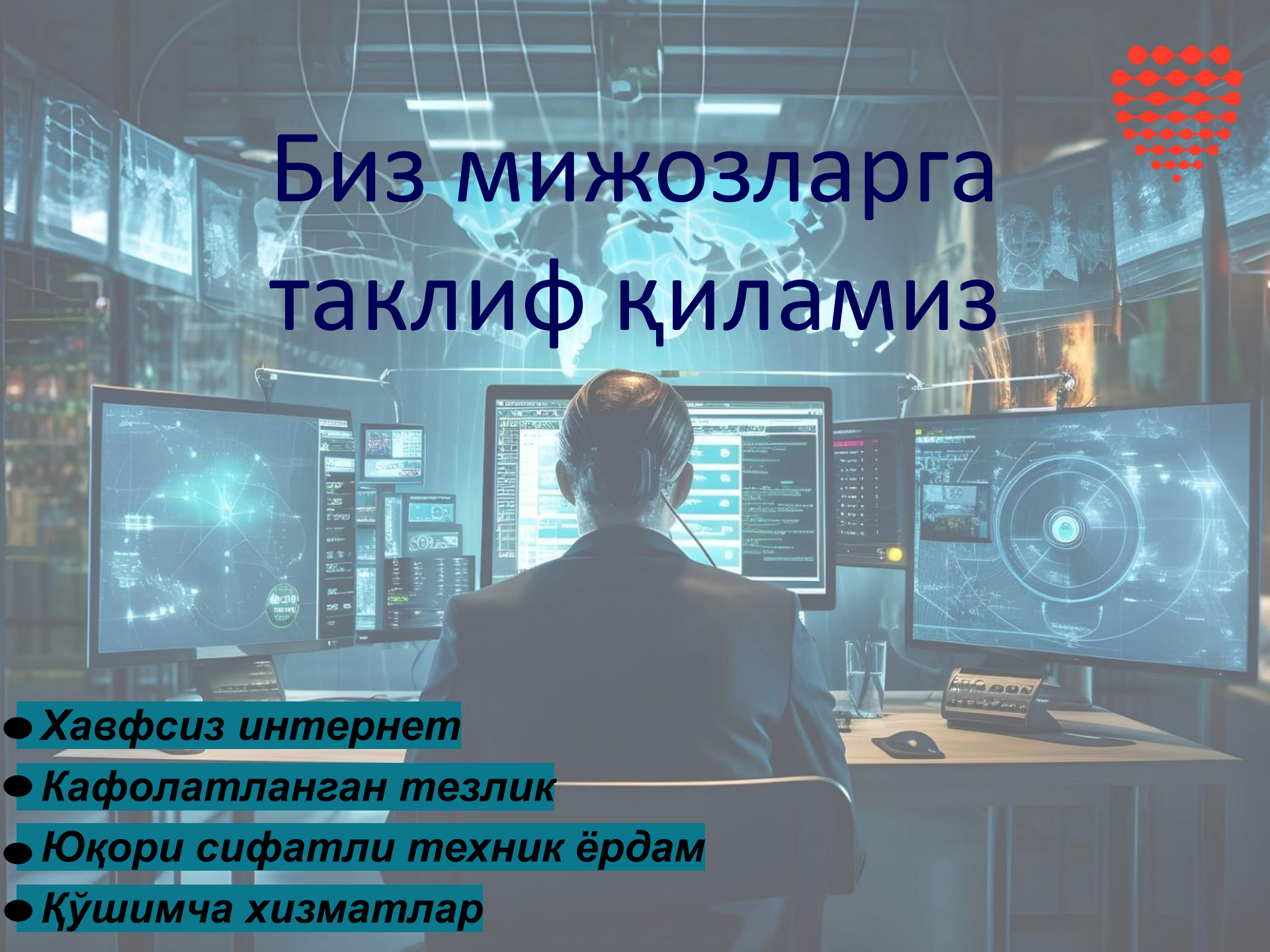

“ONE-NET” МЧЖ
ЯГОНА ОПЕРАТОР
www.one-net.uz



Биз мижозларга таклиф қиламиз

- ***Хавфсиз интернет***
- ***Кафолатланган тезлик***
- ***Юқори сифатли техник ёрдам***
- ***Қўшимча хизматлар***

Кўпроқ бериладиган саволлар

- “ONE-NET” ягона операторига уланиш учун қандай технологиялар ишлатилади?
- ***NETFLOW технологияси бўйича амалга оширилади.***
- Бизга ажратилган IP адреслар Тас-ИХ рўйҳатига қўшилганми?
- ***Ҳа***
- Интернет билан боғлиқ муаммоларни қандай аниқлаш керак?
- ***“ONE-NET” тармоғига уланган мижозлар туну-кун мониторинг назоратида бўлади бундан ташқари қуйидаги рақамга мурожаат қилсангиз бўлади (71)-203-30-05***
- GPON технологияси орқали “ONE-NET” ягона оператори уланса бўладими?
  GPON технологияси “ONE-NET” ягона оператори технологиясига мос келмайди.
- Қанча IP адрес ажаратилади?
- ***IP адреслар мижозлар баёноти ва эҳтиёжига кўра ажратилади.***
- Ягона операторга уланиш учун қандай коммутаторлар ишлатилади?
- ***1 Гбит/с тезликга эга L2 даражали коммутаторлар ишалтилади.***
- “ONE-NET” операторига уланиш учун мижоз ўз коммутаторини ишлатиши мумкинми?
- ***Агарда “ONE-NET” ягона оператори талабларига жавоб берсагина***
- Операторлан Оптик тола алоқа линияси мижозгача қандай ташкиллаштирилган?
- ***Ўзбектелеком компанияси мижозгача энг яқин операторлан оптик тола ташлаб беради.***

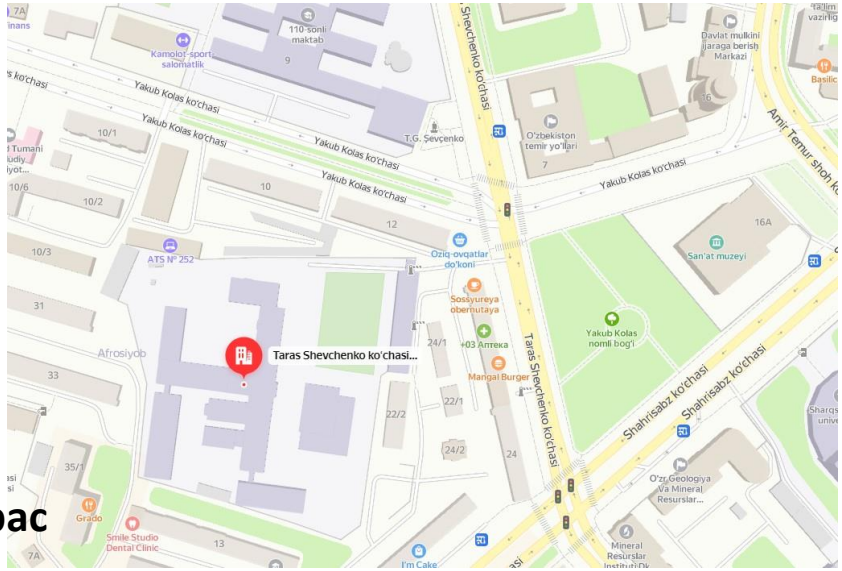
Қўшимча хизматлар

БИЗ БИЛАН БОҒЛАНИНГ

+998 71 203 30 05

info@one-net.uz www.one-net.uz

Тошкент шаҳри, Миробод тумани, Тарас Шевченко кўчаси, 20-уй



- Давлат органлари ва ташкилотларини сифатли, хавфсиз интернет билан таъминлаш, веб сайтларни киберҳужумлардан ҳимоялаш мақсадида “Киберхавфсизлик маркази” ва “ONENET” ягона оператори ўзаро ҳамкорликда “CHECK POINT” , “WAF” қурилма ва веб-иловаларидан фойдаланган ҳолда қуйидаги келтириб ўтилган юқори кўрсаткич ва натижаларга эришиб келинмоқда.

- Мисол қилиб оладиган бўлсак CHECK POINT ҳимоялаш қурилмаси 1 ой давомида турли хил ташкилотларга хужум қилишга бўлган уринишларни аниқлаб бартараф этмоқда. Қуйида хавфсизлик қурилмасини бази бир ҳисоботлари кўрсатилган:

Bu tekishiruv hisobotida tarmoqdagi xavfsizlik natijalari keltirilgan ,hisobotda xavflarni barataraf etish bo`yicha masalahatlar taklif etilgan. Xavfni baholash uchun Check Point kompaniyasi trafiklarda quyidagi xavfsizlik tahdidlarini aniqladi: zararli dastrular bilan kasallangan kompyuterlar, Yuqori xavf darajali veb dasturlar, bostirib kirishga urinish ,konfedensial ma`lumotlarni yo`qotish xavfi va hokazolar.

Zararli dasturlar va xujumlar

317
Botlar bilan kasallangan kompyuterlar

1.4M
C&C saytlari bilan aloqa

* C&C - Buyruq va boshqaruv. Agar proksi server o`rnatigan bo`lsa qo`shimcha zararlangan kompyuter bo`lishi mumkin.

35
Zararli dasturlar tomonidan yuklab olingan

138

42

Yuklab olingan nol kunlar antivirus imzosi nomalum bo`lgan yoki zararli dasturning noyob sonini taqdim etadi.

522
Dasturiy ta`minotni noyob zaifliklarini ishlatishga harakat qilindi

Sizning tarmog`ingizdagi potensial xujumni ko`rsatadi.

Ma`lumotlar yo`qolishi

0
Ma`lumotlarni yo`qotishni taxminiy hodisalari

0
Konfedensial ma`lumotlarni kategoriyasi

Tashkilotdan tashqarida turib ichki lokal tarmoqdagi foydalanuvchilarni malumotlari sizib chiqganiligini bildiradi.

Yuqori havf bilan internetga kirish

79
Yuqori xavfga ega veb dastrular

6.3TB

Potensial xavflar: Tarmog`ingizdagi zaif eshikni ochib malumotlarni sizib chiqishi yoki zararlanishiga olib keladi.

4.1K
Yuqori xavfga ega veb saytlar

211.7K

Potensial xavflar: veb tahdidlarga moyil bo`lgan ,xavflar bularga misol: spamlar zararli fishingli veb saytlar

SaaS dasturlar

73
SAAS Ko`rinadigan dasturlar

183
SAAS dasturlarni ishlatuvchi foydalanuvchilar

Bizning dastur elektron pochtalarni himoya qilish yechimi bilan integratsiya qilingan.

©Check Point Software Technologies Ltd. All rights reserved.

fppt.com

Mitre Att&ck

Check Point SandBlast Network zararli dasturlarni aniqlash va oldini olishda MITER ATT&CK tizimidan turli usullarda foydalanadi. SandBlast Network zararli fayl aniqlanganda ishlatiladigan usullarni ko'rsatadi.

MITER ATT&CK Tactics - Hujumlar soni

24.0K	Initial Access
36.2K	Execution
459	Persistence
2.9K	Privilege Escalation
125.0K	Defence Evasion
591	Credential Access
1.1K	Discovery
17	Lateral Movement
1.2K	Collection
9.6K	Command and Control
481	Exfiltration
785.6K	Impact

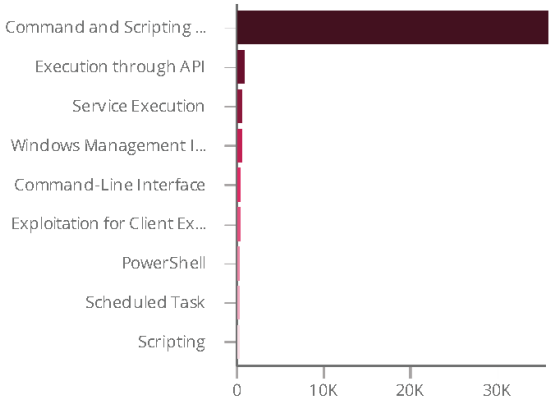
Tahlilchi HOLY GRAIL

Tizim jurnallarini tahlil qilish va tadqiq qilish va bartaraf etish uchun asosiy tahdidlarni samarali aniqlash xavfsizlik tahlilchisining eng katta muammosidir. Aksariyat tashkilotlar har kuni zararli fayllarni oladi. Ilg'or himoya texnologiyasi va tahlilisiz zararli dastur tashkilot tizimlarini buzishi va korporativ tarmoqlar orqali tarqalishi mumkin..

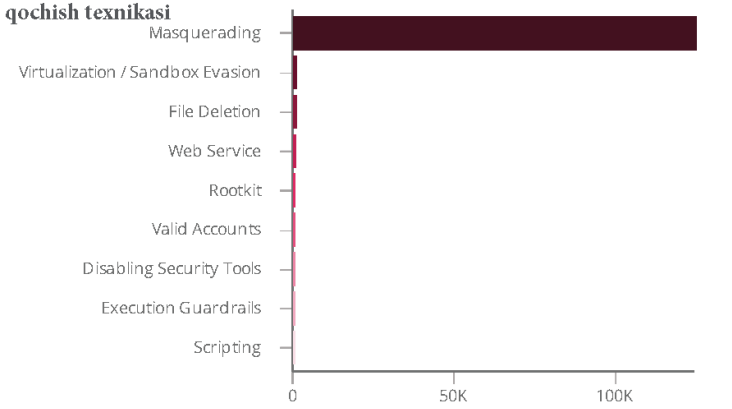
Yechim

Check Point SandBlast Network zararli dasturlarni aniqlash va oldini olishda MITER ATT&CK tizimidan turli usullarda foydalanadi. SandBlast Network zararli fayl aniqlanganda ishlatiladigan usullarni ko'rsatadi..

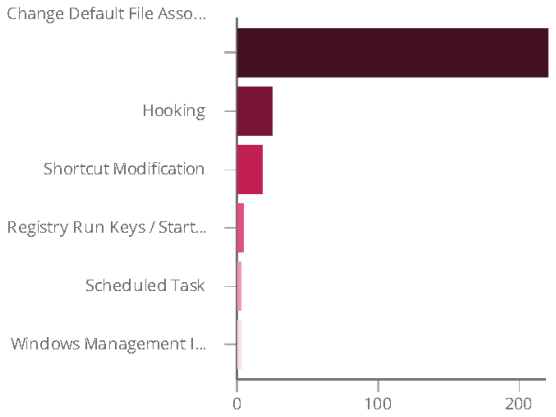
Hujumchilar tomonidan qo'llaniladigan 10 ta eng yaxshi ijro texnikasi



Hujumchilar tomonidan qo'llaniladigan 10 ta eng yaxshi mudofaadan qochish texnikasi



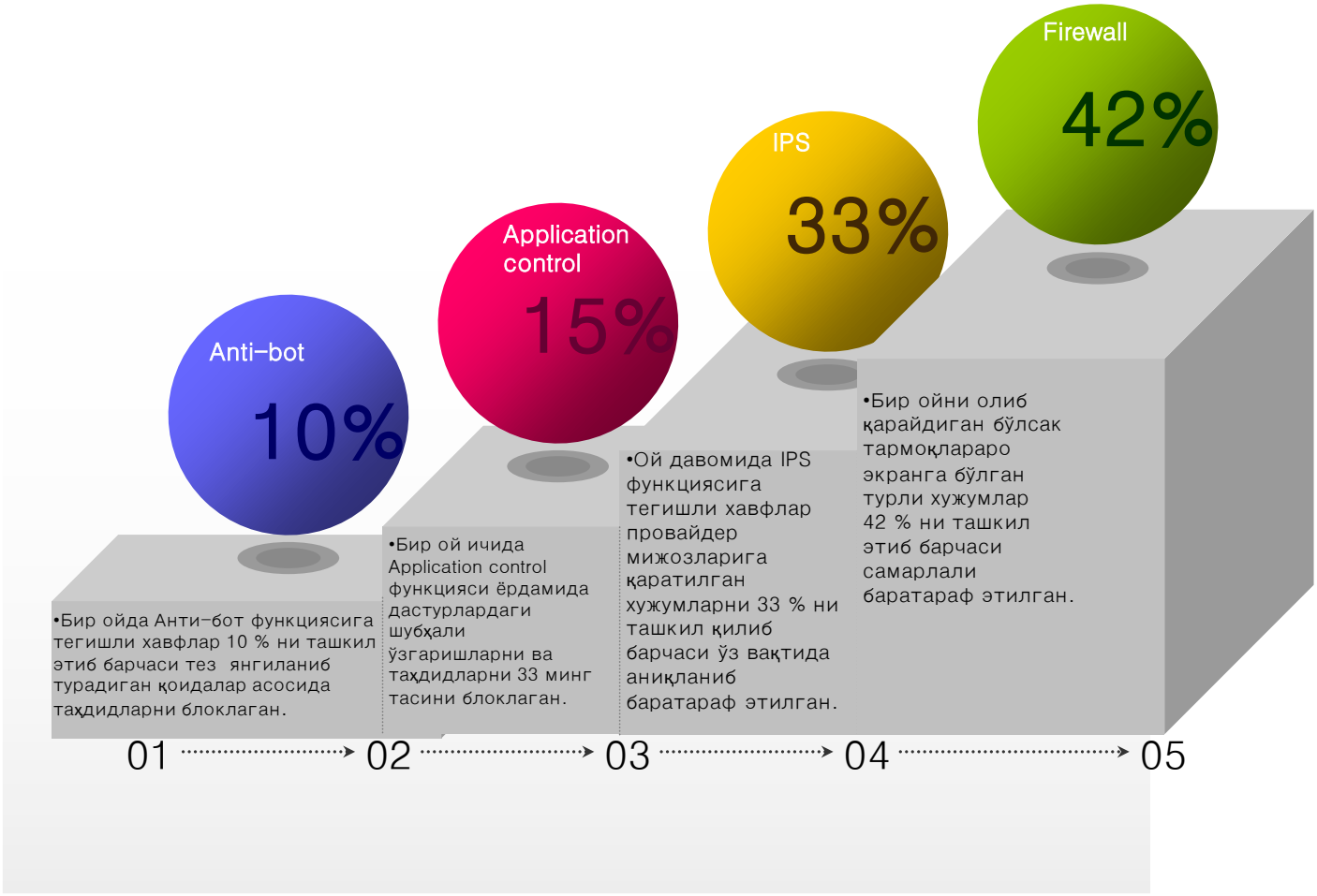
Foydalanadigan 10 ta eng yaxshi qat'iyatlilik texnikasi



©Check Point Software Technologies Ltd. All rights reserved.

fppt.com

- Маълумот учун ҳозирда CHECK POINT қурилмасига уланган мижозларга бўлаётган асосий ҳужум қилишга уриниш турлари DOS , DDos , Phishing , spam , ботлар,вируслар ,Brute force ,sql injection ва ҳоказолар, қуйида кўрсатилган диаграммалардан хужум қилишга урунишни бартараф этилганини фоизларда кўрсак бўлади:


Anti-bot
10%
Application control
15%
IPS
33%
Firewall
42%
•Бир ойда Анти-бот функциясига тегишли хавфлар 10 % ни ташкил этиб барчаси тез янгиланиб турадиган қоидалар асосида таҳдидларни блоклаган.
•Бир ой ичида Application control функцияси ёрдамида дастурлардаги шубҳали ўзгаришларни ва таҳдидларни 33 минг тасини блоклаган.
•Ой давомида IPS функциясига тегишли хавфлар провайдер мижозларига қаратилган хужумларни 33 % ни ташкил қилиб барчаси ўз вақтида аниқланиб баратараф этилган.
•Бир ойни олиб қарайдиган бўлсак тармоқлараро экранга бўлган турли хужумлар 42 % ни ташкил этиб барчаси самарлали баратараф этилган.
01
02
03
04
05

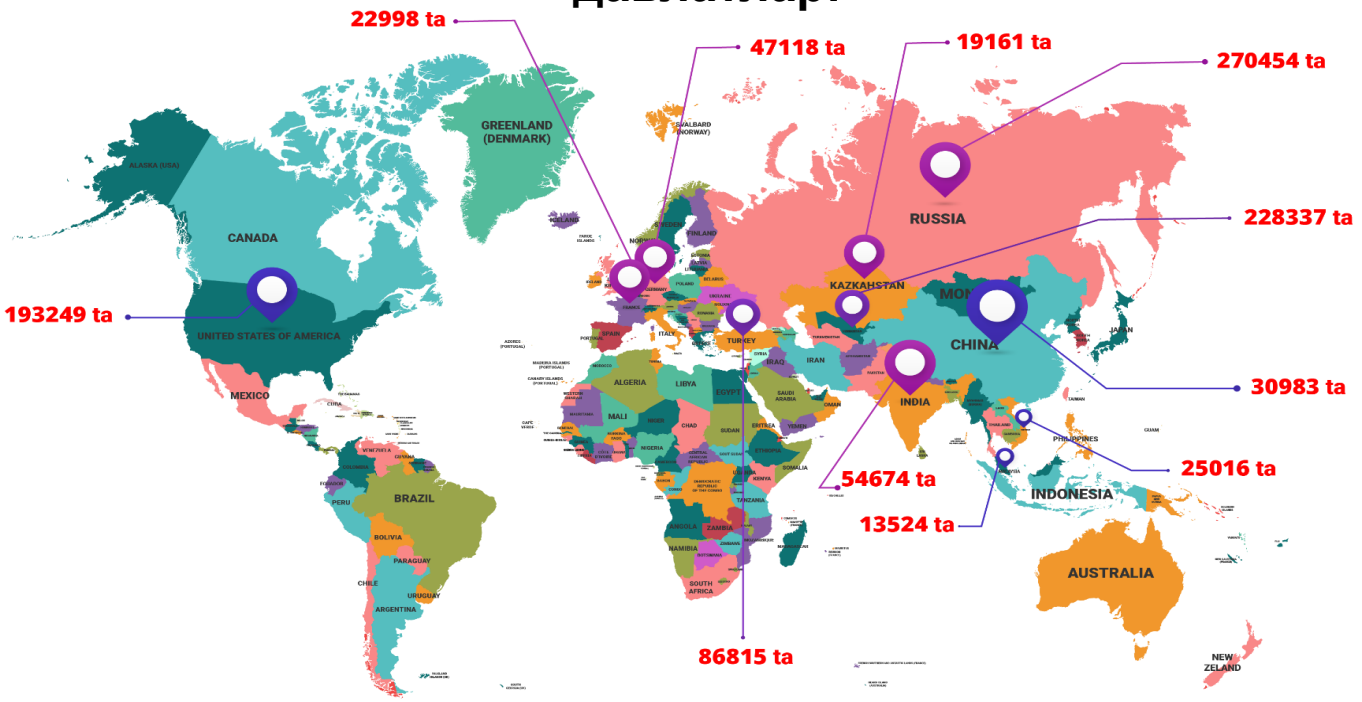
fppt.com

“ONE-NET” ягона оператори ва “Киберхавфсизлик маркази” билан ҳамкорликда қуйидаги хужум ва хавфлар ўз вақтида бартараф этилиб сифатли интернет етказиб берилмоқда:

- Тармоқлараро экран орқали 719 минг хавф ва таҳдидлар қайтарилган.
- IPS функцияси орқали жами 468 минг турли хужумларни олди олинди.
- Application control функцияси ёрдамида дастурлардаги шубҳали ўзгаришларни ва таҳдидларни 33 минг тасини блоклаган.
- Антибот функцияси орқали жами 25 минг ботлар аниқланиб блокланди.
- Антивирус функцияси орқали 818 та вируслар аниқланиб йўқ қилинган.

- Бир неча ойни олиб қарайдиган бўлса “WAF” тизими веб ресурсларига нисбатан амалга оширилган жами 839 мингдан ортиқ киберҳужумлар аниқланиб бартараф этилган. Киберҳужумларнинг асосий турлари қуйидагилардан иборат:
- Киберҳужумлар уюштирилган асосий давлатлар:

Киберҳужумлар уюштирилган асосий давлатлар:



Шу жумладан, шубхали сўровларни блоклаш – 22,3 %; PHP маълумотлари

Тарқалиши-25,4 %; протоколларга ҳужум -10%; СҚЛ-инъекция-11,5 %; чекланган файлларга рухсатсиз киришга уруниш -12,4 % ва бошқалар-18,4%

fppt.com

хавфлар ўз вақтида бартараф этилиб сифатли интернет етказиб берилмоқда:	Бўлган таҳдид ва хужумлар сони	Қайтарилган ёки блокланган таҳдид ва хужумлар сони	Хавфсизлик қурилмаси томонидан химоя қилинмаган таҳдидлар ва хужумлар сони
Тармоқлараро экран	719 минг	719 минг	0
IPS	468 минг	468 минг	0
Application control	33 минг	33 минг	0
Anti bot	25 минг	25 минг	0
Anti-virus	818 та	818 та	0

fppt.com

SIEM тизими (Security Information and Event Management)

SIEM ташкилотлардаги тизимларга хавф солаётган тахдидларни аниқлаш,тахлил қилиш,бартараф этишда хизмат қилади.

SIEM тизимини асосий вазифалари:

Ахборот хавфсизлиги сохасида маълумотларни тўплайди,тахлил қилади ва сақлайди.

Ахборот ресурсларини назорат ва химоя қилади.

Ахборот хавфсизлиги сохасида кибер хужумларни аниқлайди ва текширади.

Барча инфратузилмани ишлашини мониторинг қилади.

Хисоботларни тўплаб беради.

Тармоқ топологиясини чизиб беради.

Тахлил қилиш учун маълумотлар қуйидаги манбалардан йиғилади.

Антивируслар

Тармоқ қурилмаларини журналларидан

Тармоқлар аро экранлардан

Серверлар ва Компютерлардан

Хужумларни аниқлаш ва бартараф этиш дастуридан (IPS/IDS)

Маълумотларни чиқиб кетишини олдини олиш дастуридан (DLP)

Почта Серверларидан