УКРЕНЕРГО
Національна енергетична компанія

КІБЕРБЕЗПЕКА

Прогрес за напрямком

ДИНАМІКА ЗМЕНШЕННЯ РИЗИКІВ

89%

Динаміка за напрямком *документи/процеси* в період 2017-2019

80%

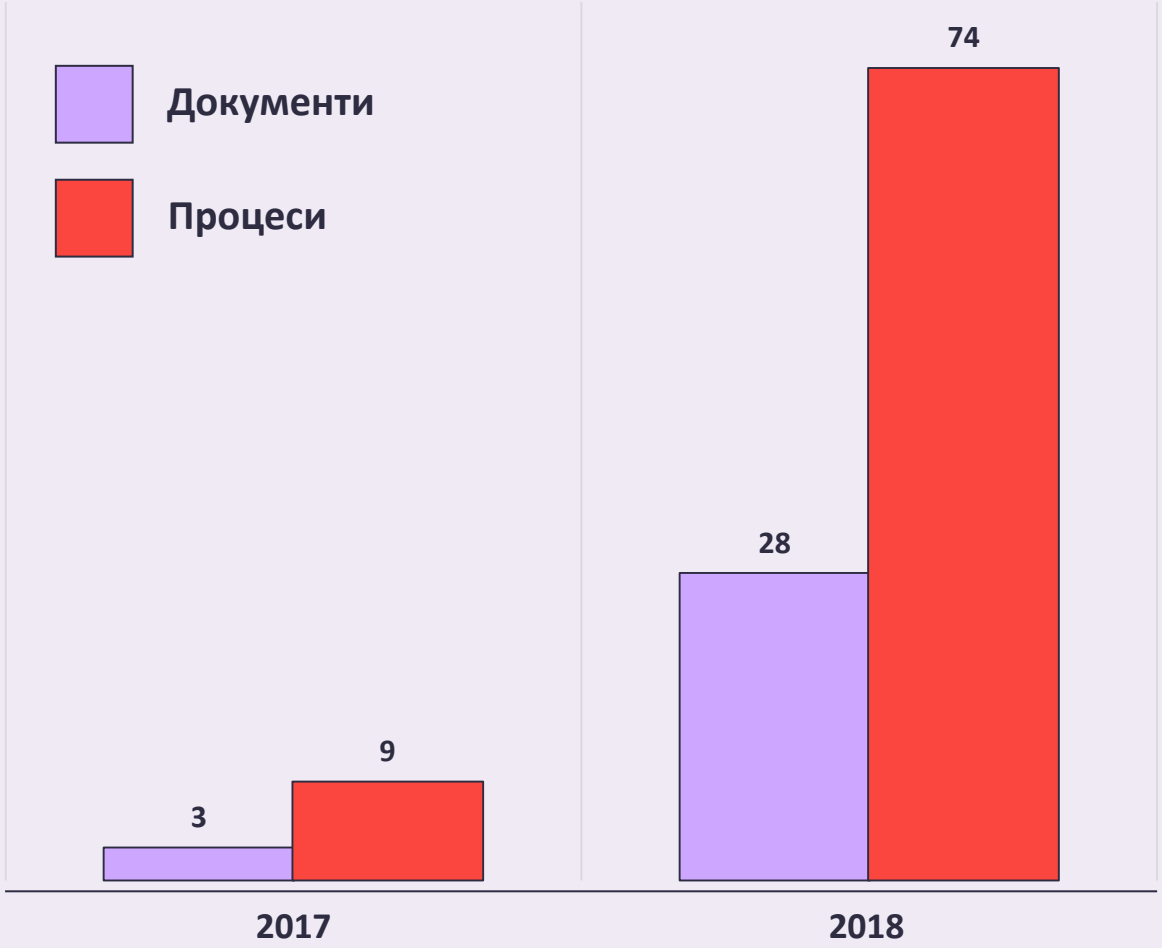
Динаміка за напрямком *технічні рішення* в період 2017-2019

Динаміка зменшення ризиків

Все почалося з впровадження процесу оцінки ризиків інформаційної безпеки який враховує результати виїзної перевірки виконання вимог з інформаційної безпеки по всій країні

ДОКУМЕНТИ ТА ПРОЦЕСИ НАПРАВЛЕНІ НА ЗМЕНШЕННЯ РИЗИКІВ

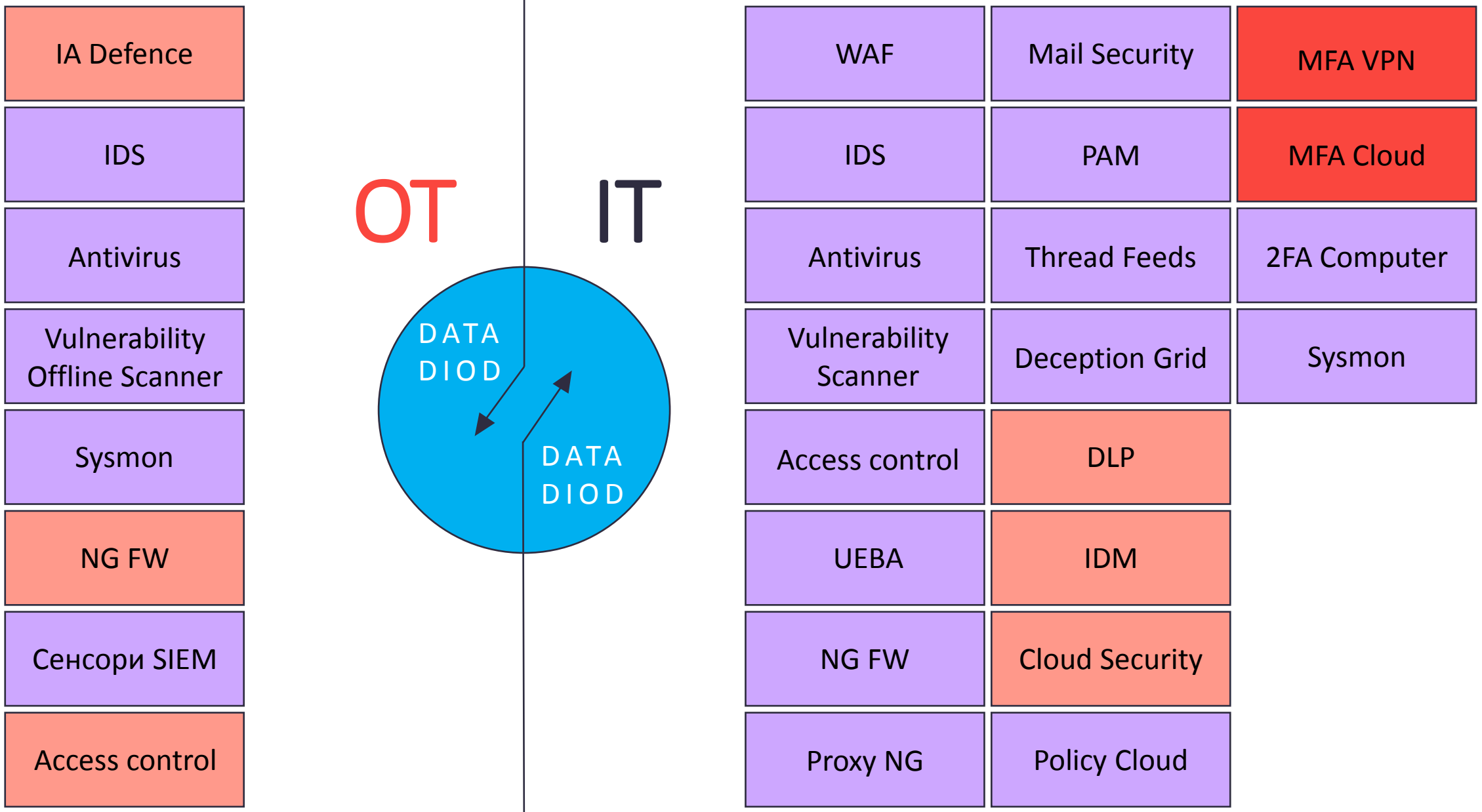
- Впроваджено весь перелік процесів управління та регламентуючі їх внутрішні нормативні документи які вимагає від нас ISO 27001;
- Проведено 3 цикли оцінки ризиків інформаційної безпеки;
- Проведено 2 цикли внутрішніх аудитів;
- В листопаді/грудні заплановано проведення сертифікаційного аудиту за стандартом ISO 27001



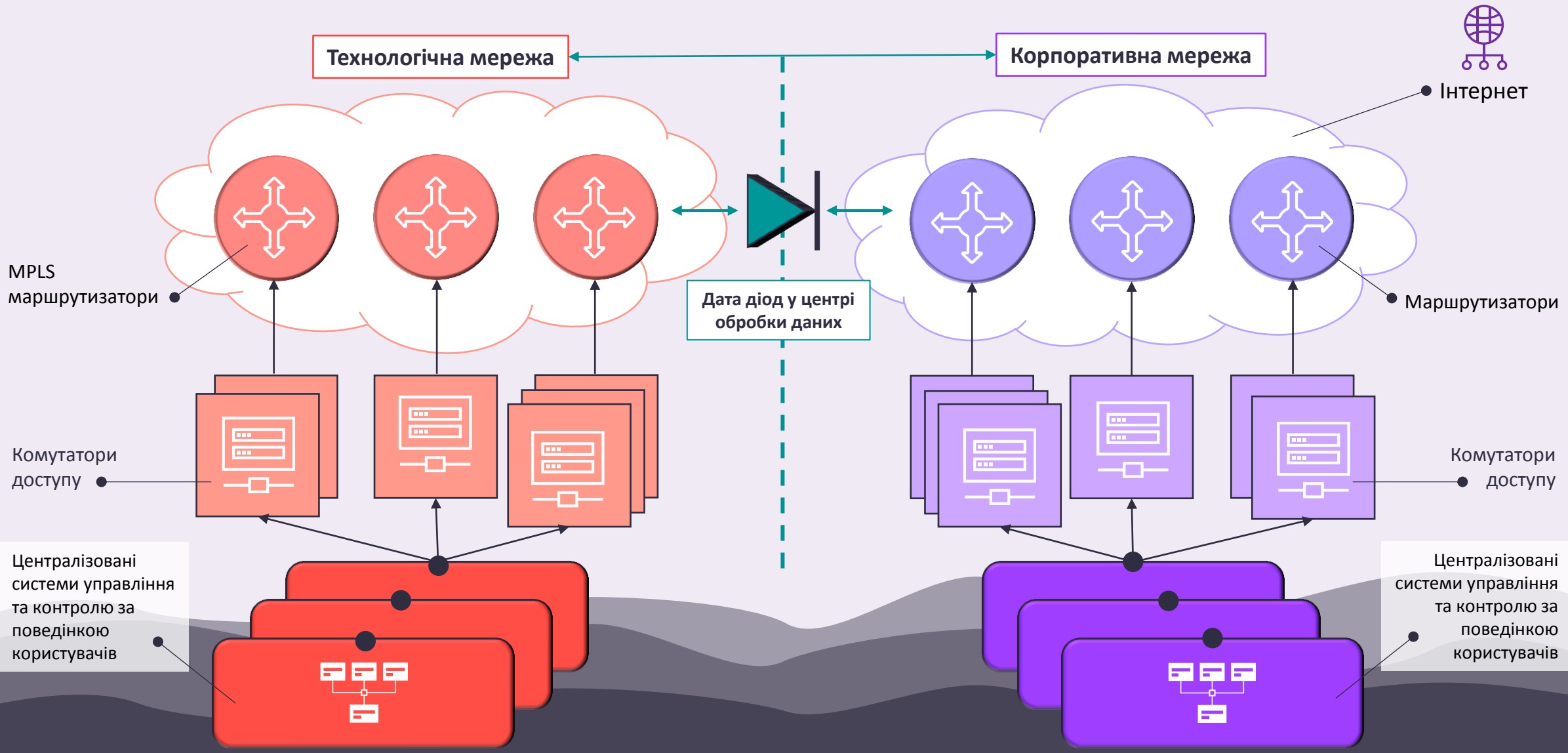
Динаміка збільшення процесів / документів
(2019 рік – актуалізація та підтримка вже створеного)

ТЕХНІЧНІ ЗАСОБИ ЗМЕНШЕННЯ РИЗИКІВ

- SIEM ArcSight
- Сканер вразливостей Qualys
- Захист веб ресурсів BigIP F5
- Антивірус McAfee
- Індикатори компрометації IntelMQ, STIX/TAXII, MISP
- Firewall Firepower
- Аналіз аномальної поведінки UEBA Introspect
- Контроль пристроїв Windows Intune
- Мережеві пастки Deception Greed Illusive
- Контроль підрядників FUDO PAM

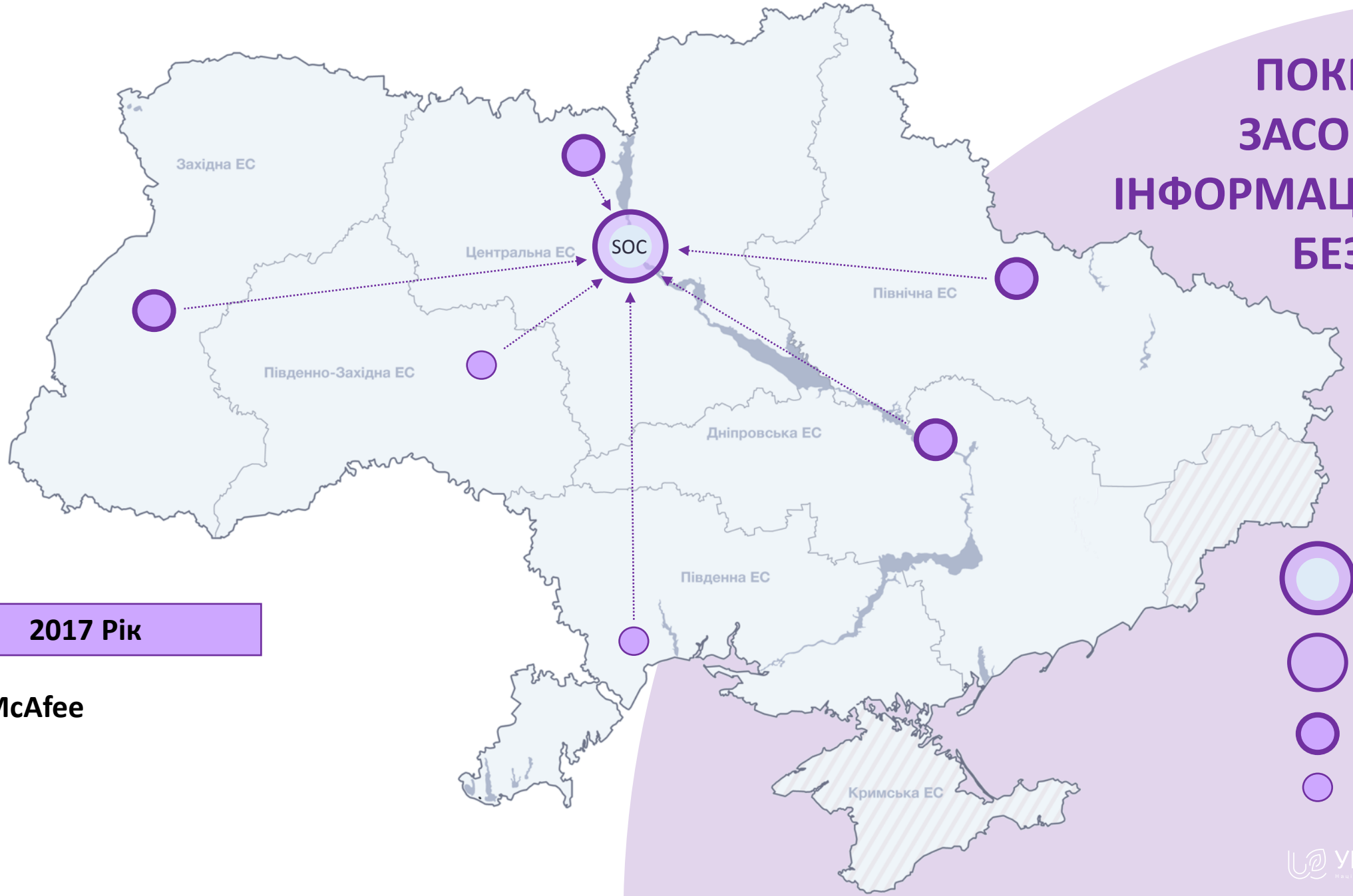

IA Defence
IDS
Antivirus
Vulnerability Offline Scanner
Sysmon
NG FW
Сенсори SIEM
Access control
OT
IT
DATA DIOD
DATA DIOD
WAF
Mail Security
MFA VPN
IDS
PAM
MFA Cloud
Antivirus
Thread Feeds
2FA Computer
Vulnerability Scanner
Deception Grid
Sysmon
Access control
DLP
UEBA
IDM
NG FW
Cloud Security
Proxy NG
Policy Cloud

БУДУЄМО ДВІ РОЗПОДІЛЕНІ МЕРЕЖІ



УКРЕНЕРГО
Національна енергетична компанія

ПОКРИТТЯ ЗАСОБАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

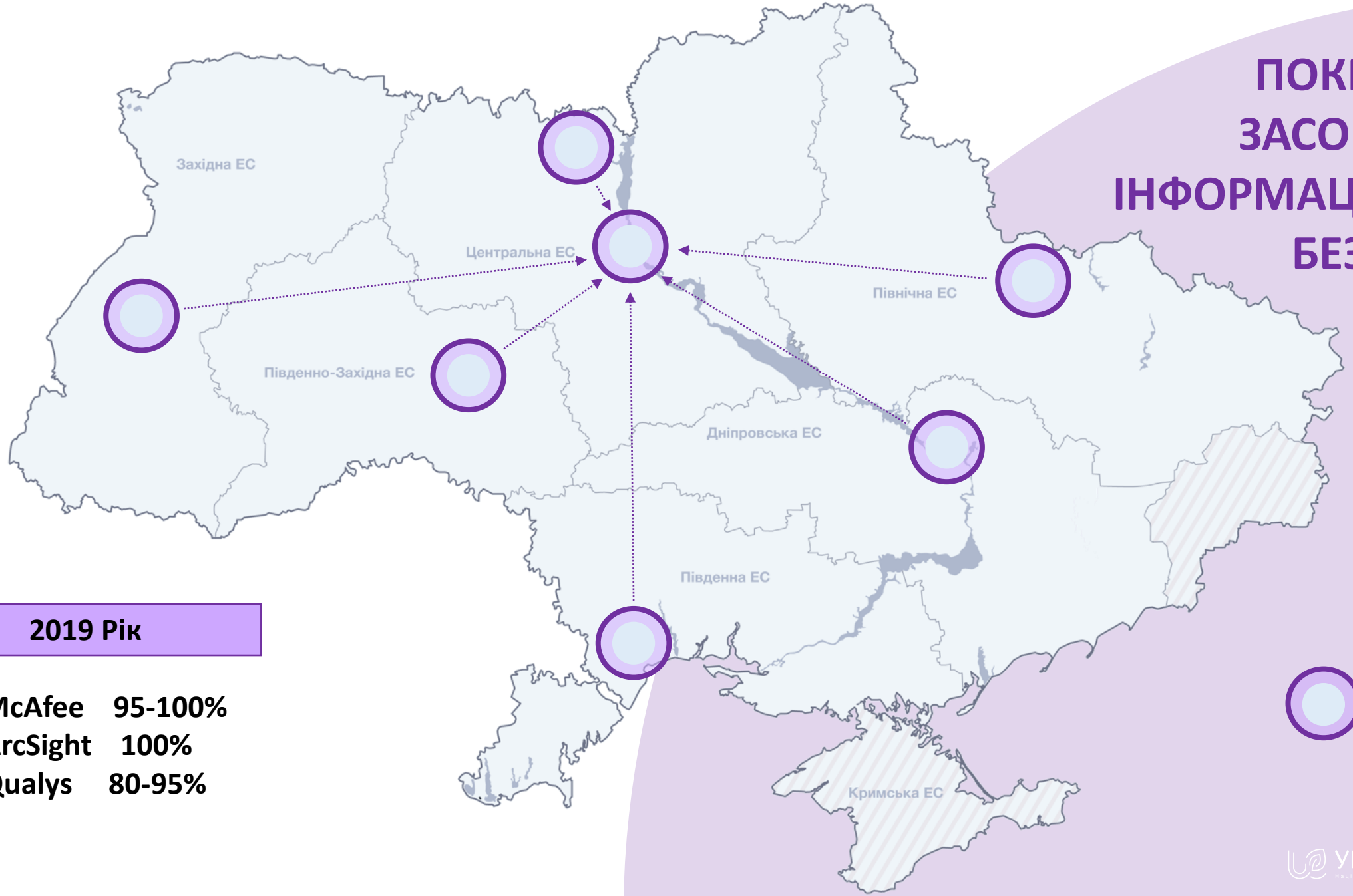


2017 Рік

- **McAfee**

УКРЕНЕРГО
Національна енергетична компанія

ПОКРИТТЯ ЗАСОБАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



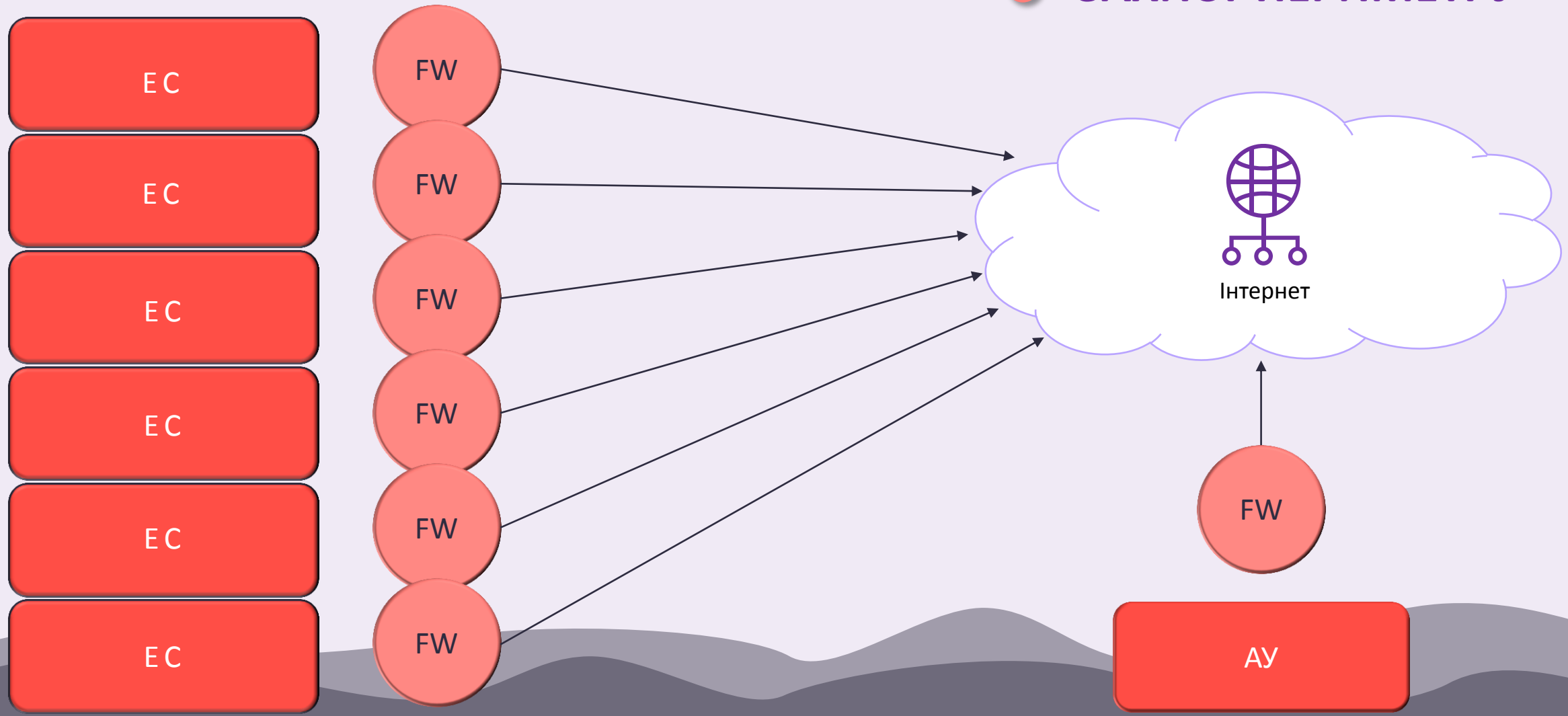
2019 Рік

- **McAfee 95-100%**
- **ArcSight 100%**
- **Qualys 80-95%**

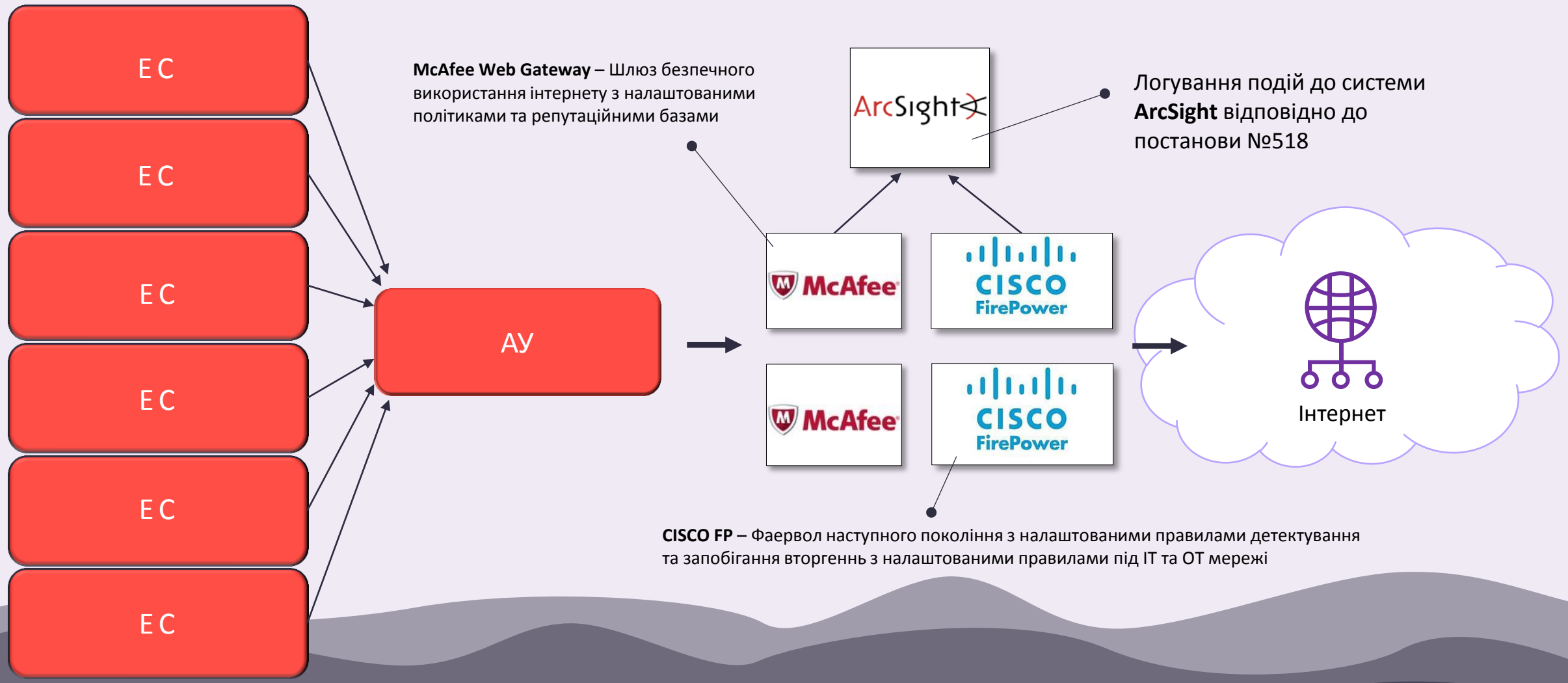
90-100%

УКРЕНЕРГО

ЗАХИСТ ПЕРИМЕТРУ



ЗАХИСТ ПЕРИМЕТРУ

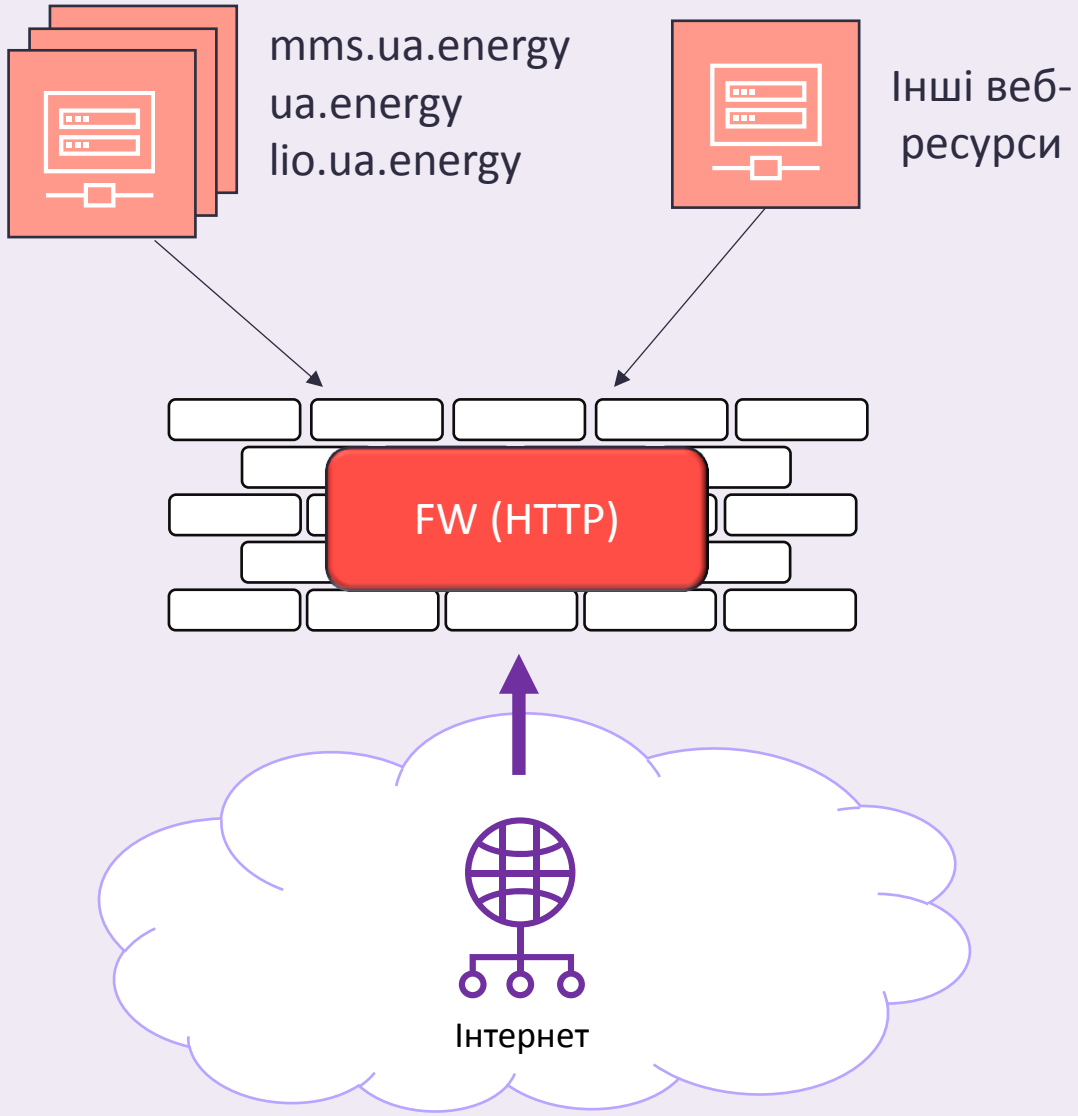


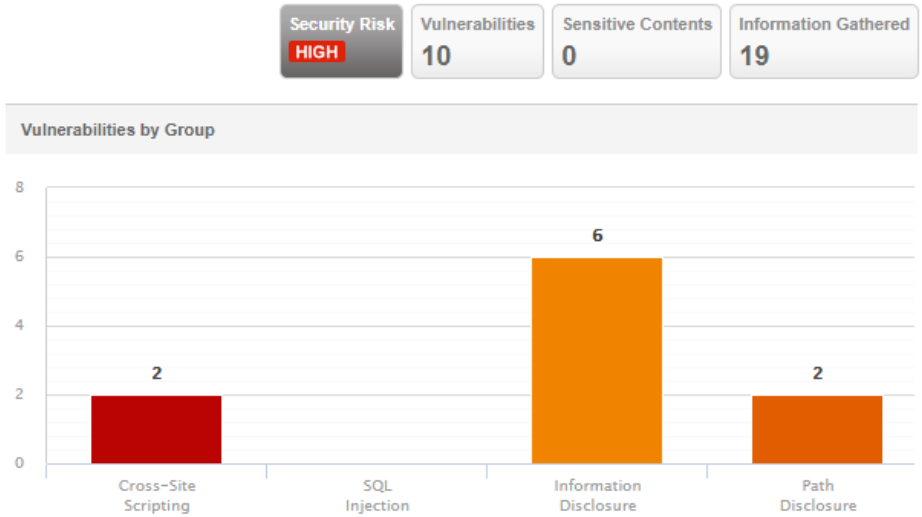
McAfee Web Gateway – Шлюз безпечного використання інтернету з налаштованими політиками та репутаційними базами

Логування подій до системи **ArcSight** відповідно до постанови №518

CISCO FP – Фаервол наступного покоління з налаштованими правилами детектування та запобігання вторгненнь з налаштованими правилами під IT та OT мережі

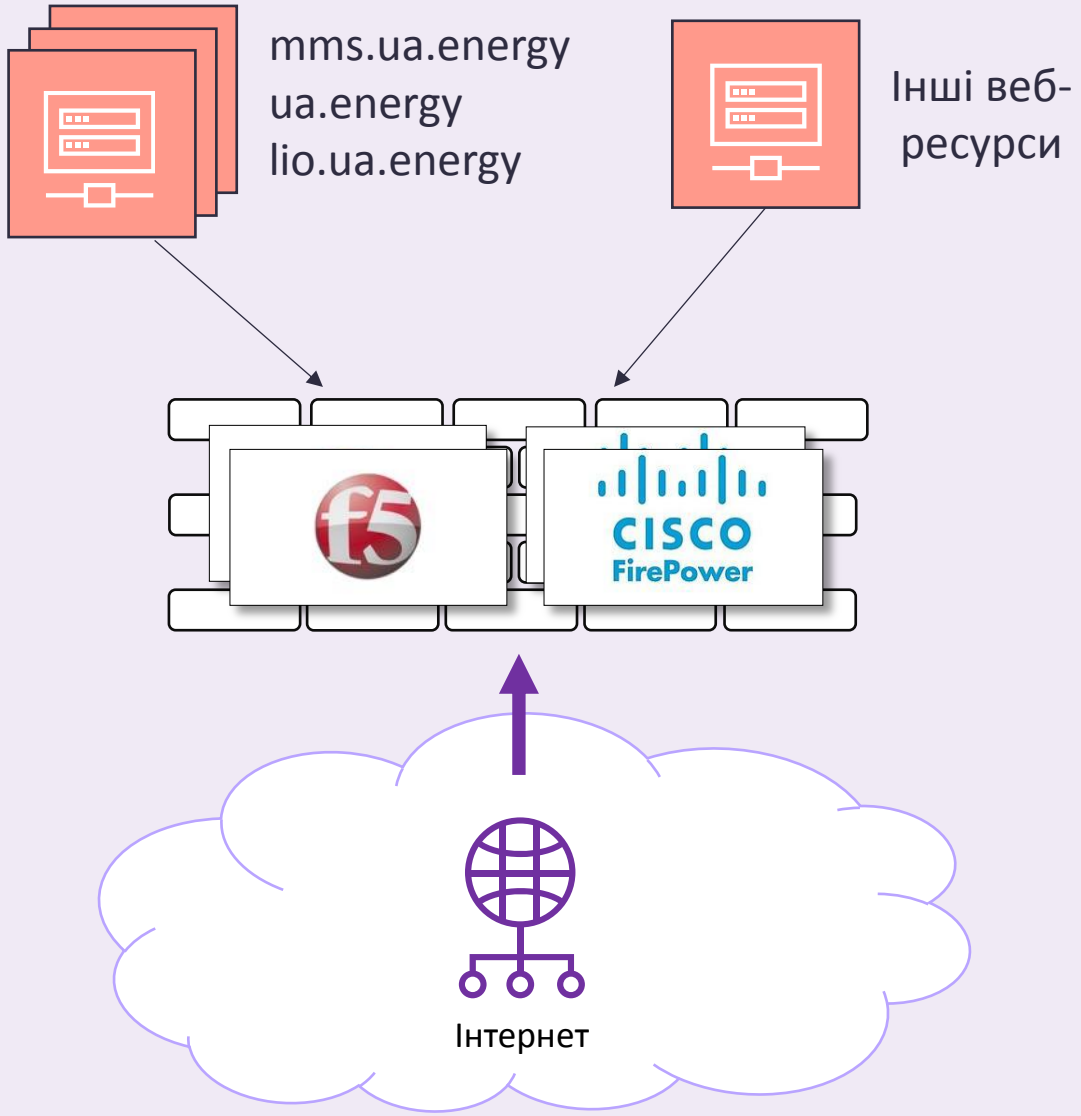
ЗАХИСТ ВЕБ РЕСУРСІВ



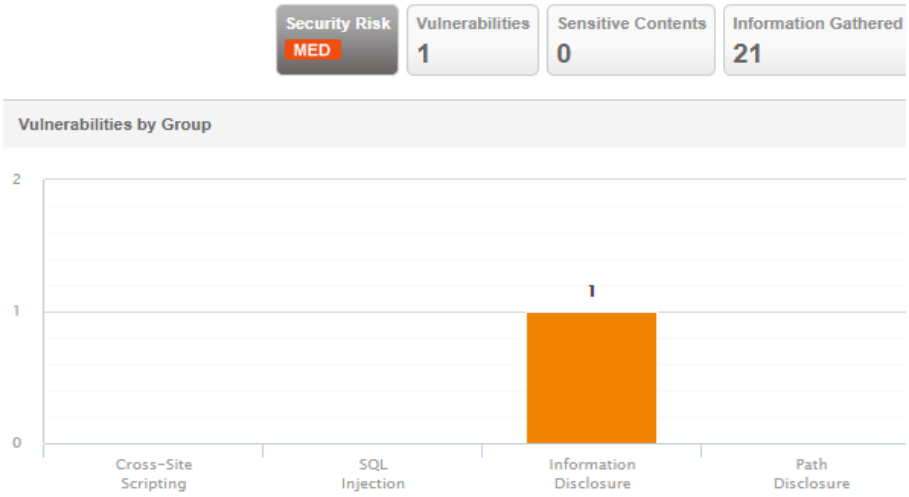


Вразливостей до використання WAF

ЗАХИСТ ВЕБ РЕСУРСІВ

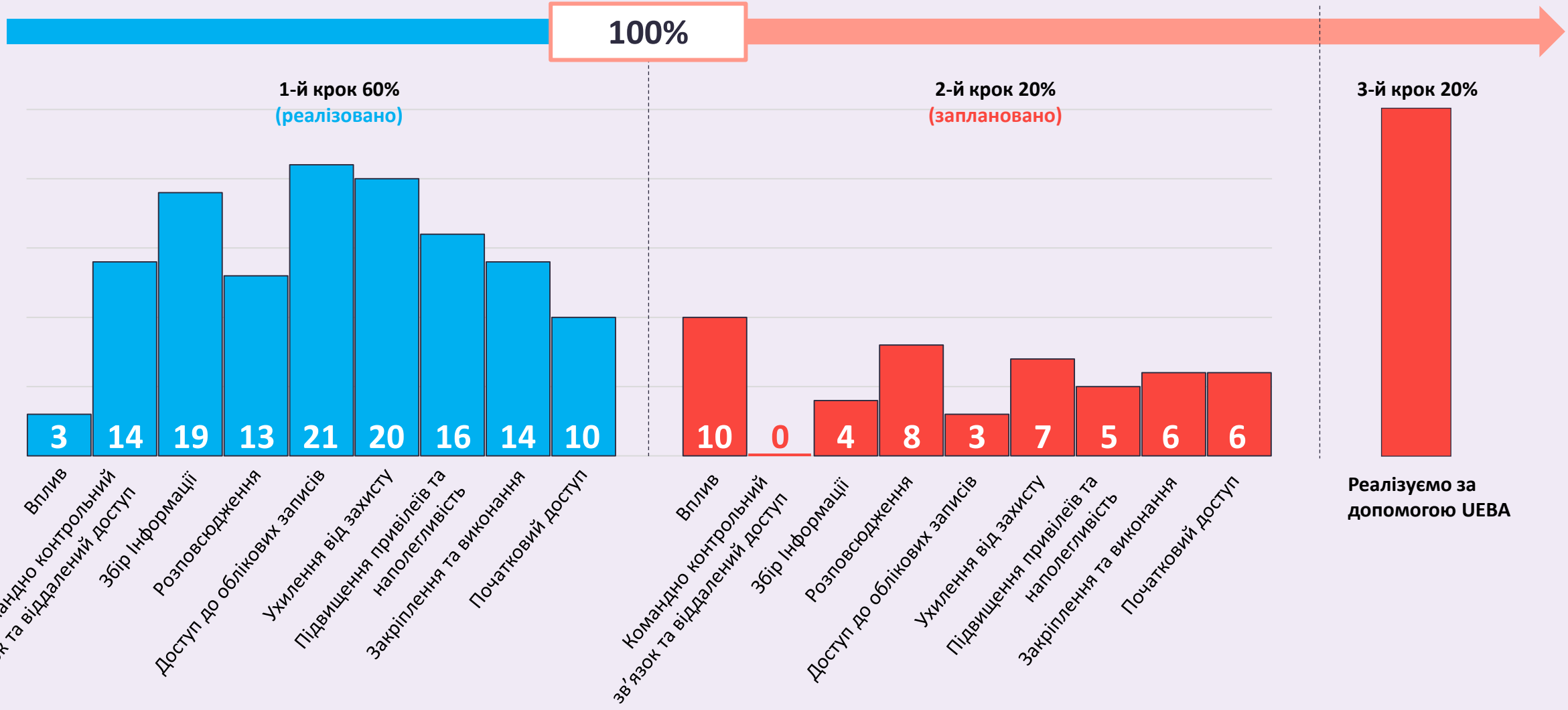


F5 Big-IP – система захисту веб додатків за допомогою фільтрації трафіку та аналізу запитів до веб рессурсу

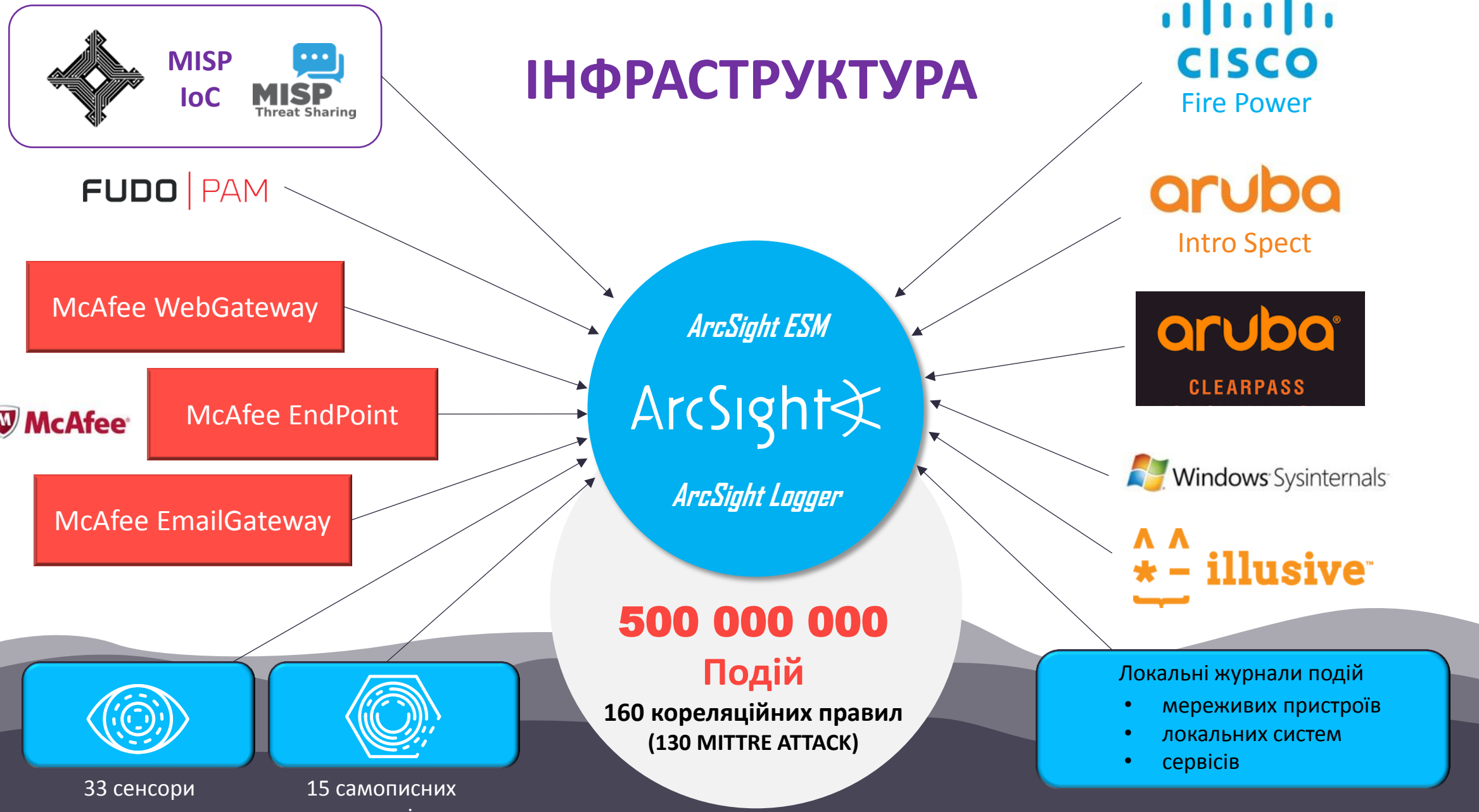


Вразливостей після використання WAF

РЕАЛІЗОВАНІ ТИПИ ТЕХНІК MITTRE ATTACK ТА КІЛЬКІСТЬ ПРАВИЛ ДО КОЖНОЇ З ТЕХНІК



ІНФРАСТРУКТУРА



ПРОГРЕСС ТЕХНІЧНИХ СПЕЦІАЛІСТІВ

Власна підтримка 70%
технічних рішень

VIP клієнт компанії
Microfocus ArcSight

Найкраща інсталяція
Qualys в Україні

Найкраща інсталяція
Aruba UEBA в Україні

Тісна співпраця з ДКІБ
СБУ, ДСЗІ

Найактивніший учасник
MISP.GOV.UA

УКРЕНЕРГО
Національна енергетична компанія

ДЯКУЮ ЗА УВАГУ!