MICRO FOCUS

Автоматизація інформаційної безпеки

Alexander Kulakovskiy

Sales Representative ITOM/ADM and SRG Solution

Трохи цифр

Ці ризики мають вартість

За період Січень- Червень 2020, було виявлено….

2,037 зламів та виставлено в DarkNet

27,000,000,000 записів

Source: Data Breach QuickView 2020 Mid Year Report, Risk Based Security, August 2020

Статистика

80%

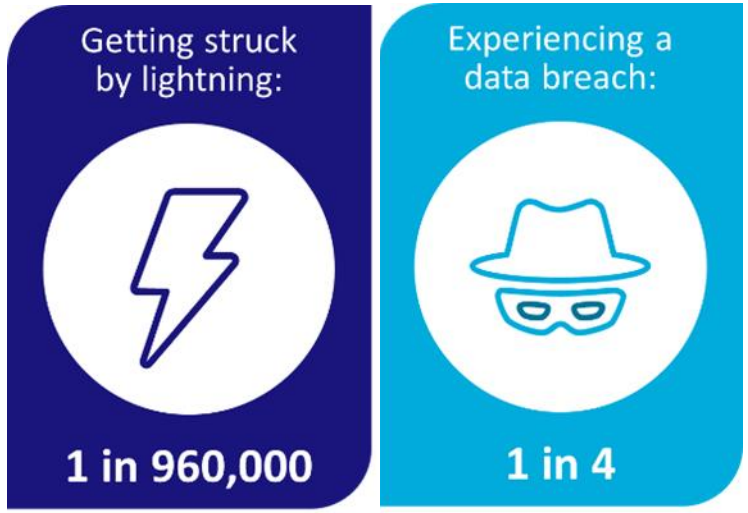
Споживачів змінювали постачальница сервісів у разі витоку їх даних

Source: IDC Research (as reported by Varonis)

93%

Користувачів подавали до суду на постачальника сервісу у випадку витоку їх даних

Source: Gemalto Survey (as reported by Tech Wire Asia)



$3,86 M

Середня вартість наслідків кібер-атак

Source: Ponemon Institute, 2020

280 днів

Середній період виявлення зламу

Source: Ponemon Institute, 2020

Arcsight SIEM

Що таке SIEM?

Комплексна платформа виявлення та аналізу загроз в режимі реального часу, яка значно скорочує час на виявлення та реагування на загрози.

1:

Збір

Технічних даних з усіх активних елементів IT інфраструктури, таких як: Firewall, IPS, Сервери, ПЗ, анти-віруси, тощо.

2:

Стандартизація

Форматів, протоколів та виду даних з пристроїв різних виробників в загальноприйнятий формат подій

3:

Збагачення

Зібраних даних артефактами, таксономією, первинною аналітикою з урахуванням деталей мережі та об’єктів

4:

Зберігання

Зібраних даних у захищенному вигляді з компресією 10:1, яке зменшує витрати, навіть для лог-записів за декілька років

5:

Пошук та аналіз

З використанням текстового інструменту з інтуітивним інтерфейсом та локалізацією

6:

Виявлення та запобігання

В режимі реального часу будь-якій загрозі чи порушенню

Автоматизація за допомогою ArcSight SOAR

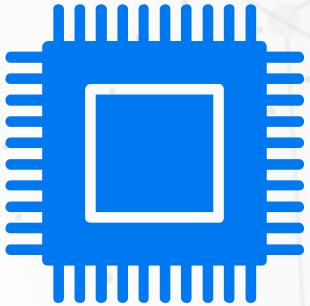
Автоматичне сортування

- Критичність події
- Консолідація подій в інциденти
- Робота з карткою інциденту

Повна автоматизація роботи 1 рівня підтримки

Збір даних

- Кінцеві пристрої, Сервери, Мережа
- HR, СКУД
- SIEM, Логи
- Програмне забезпечення
- Хмари



Обмежувальні дії

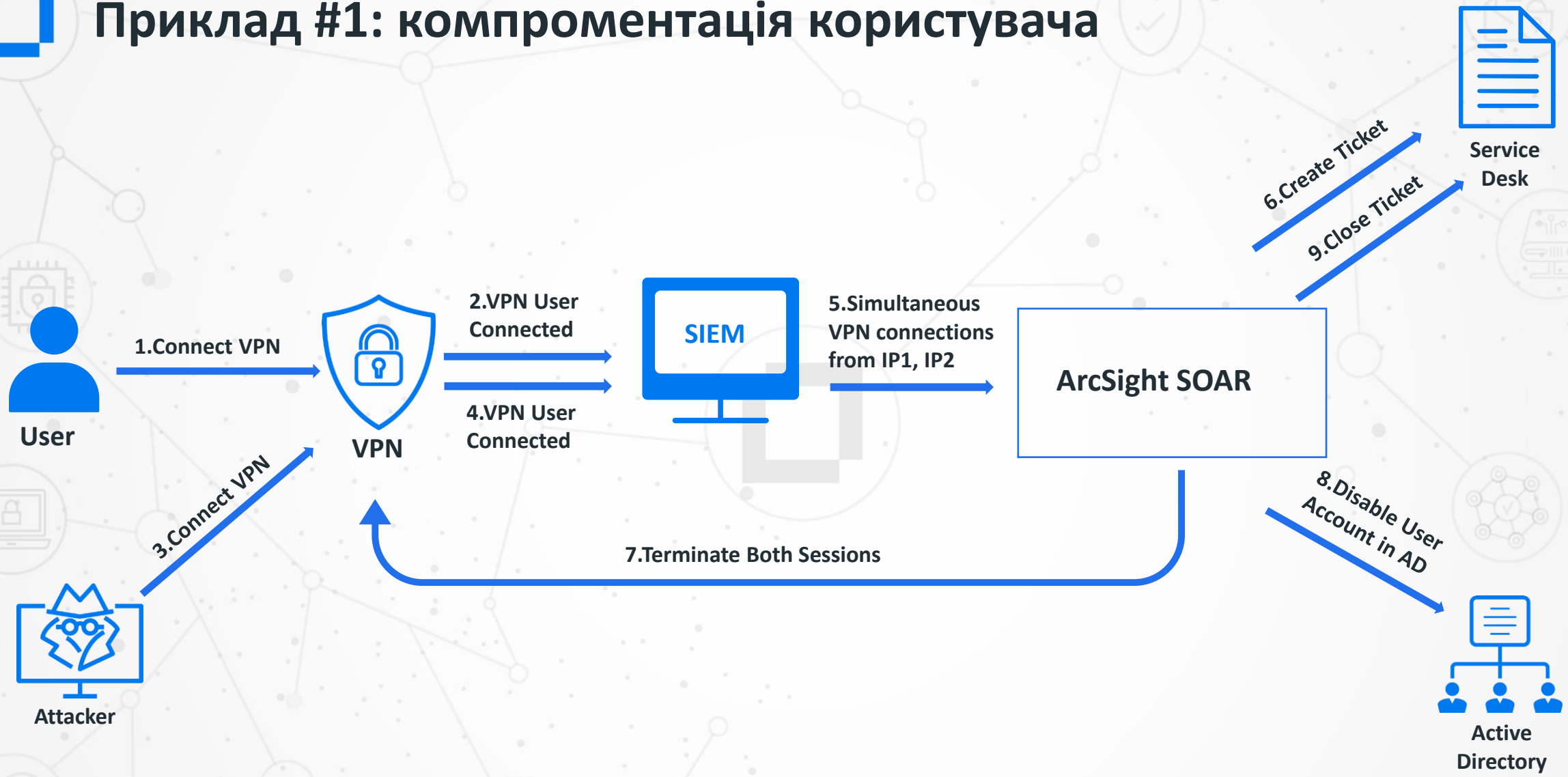
- NAC/Поміщення в карантин
- Блокування на рівні Firewall, Web-шлюзів, тощо
- Блокування або видалення облікових записів
- Фізичне блокування на рівні СКУД
- тощо*

З можливістю узгодження

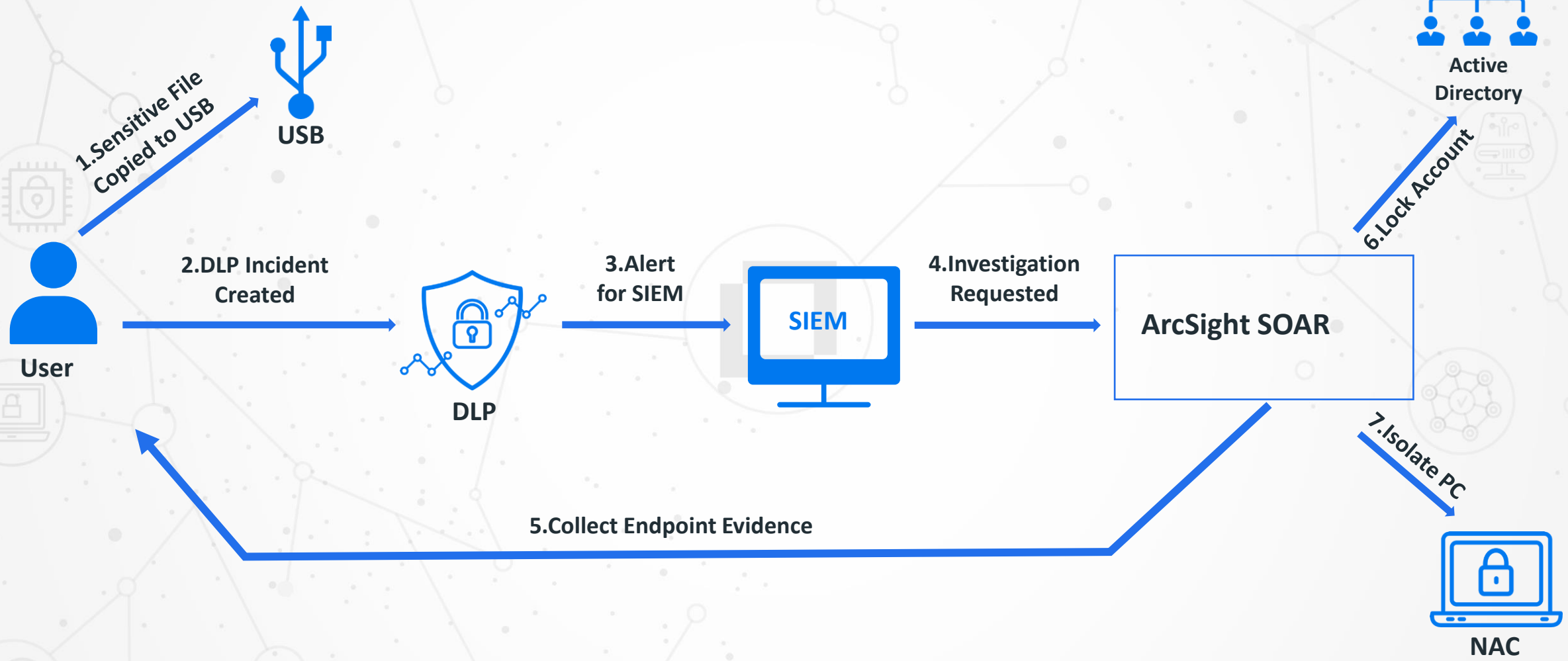
*ініціація або зупинка будь-якого технологічного процесу

MICRO FOCUS

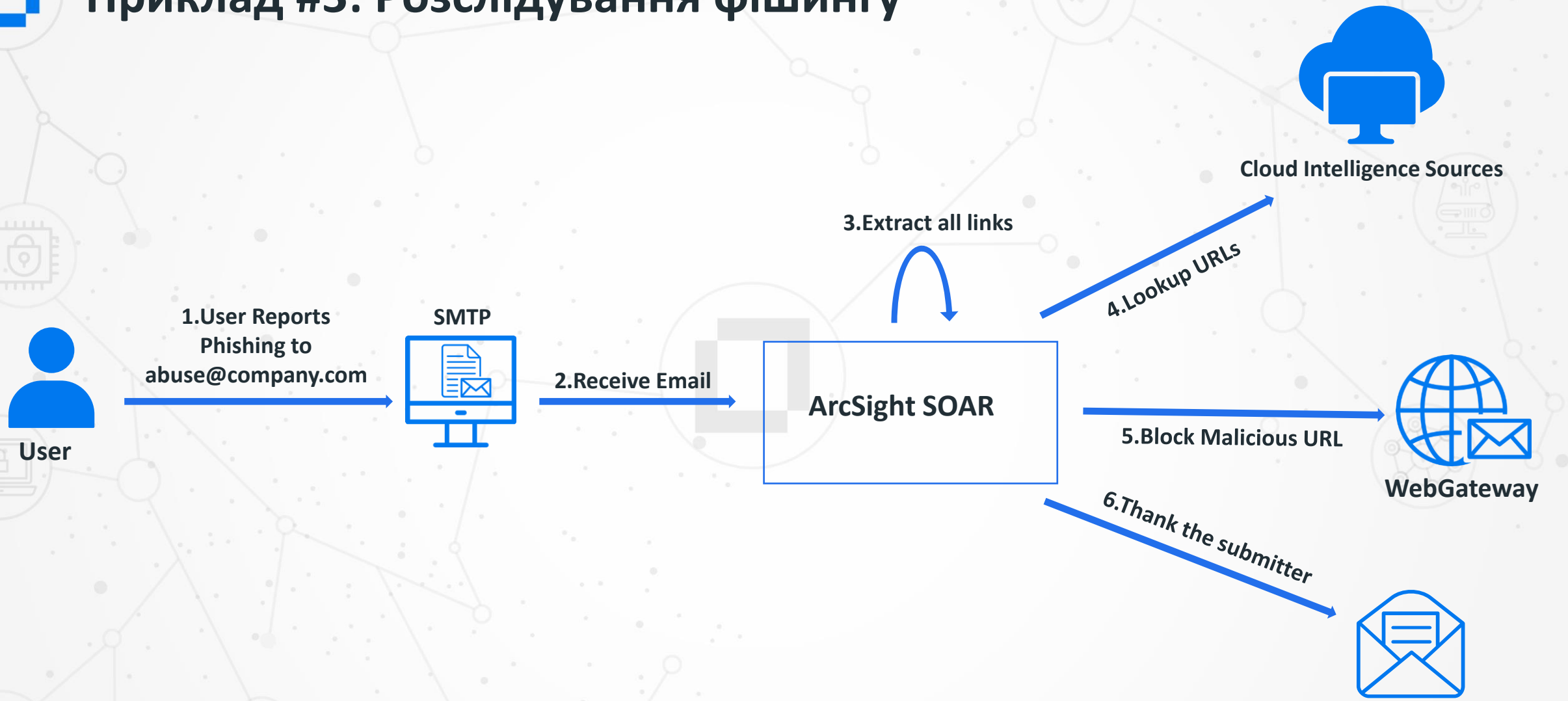
Приклад #1: компроментація користувача



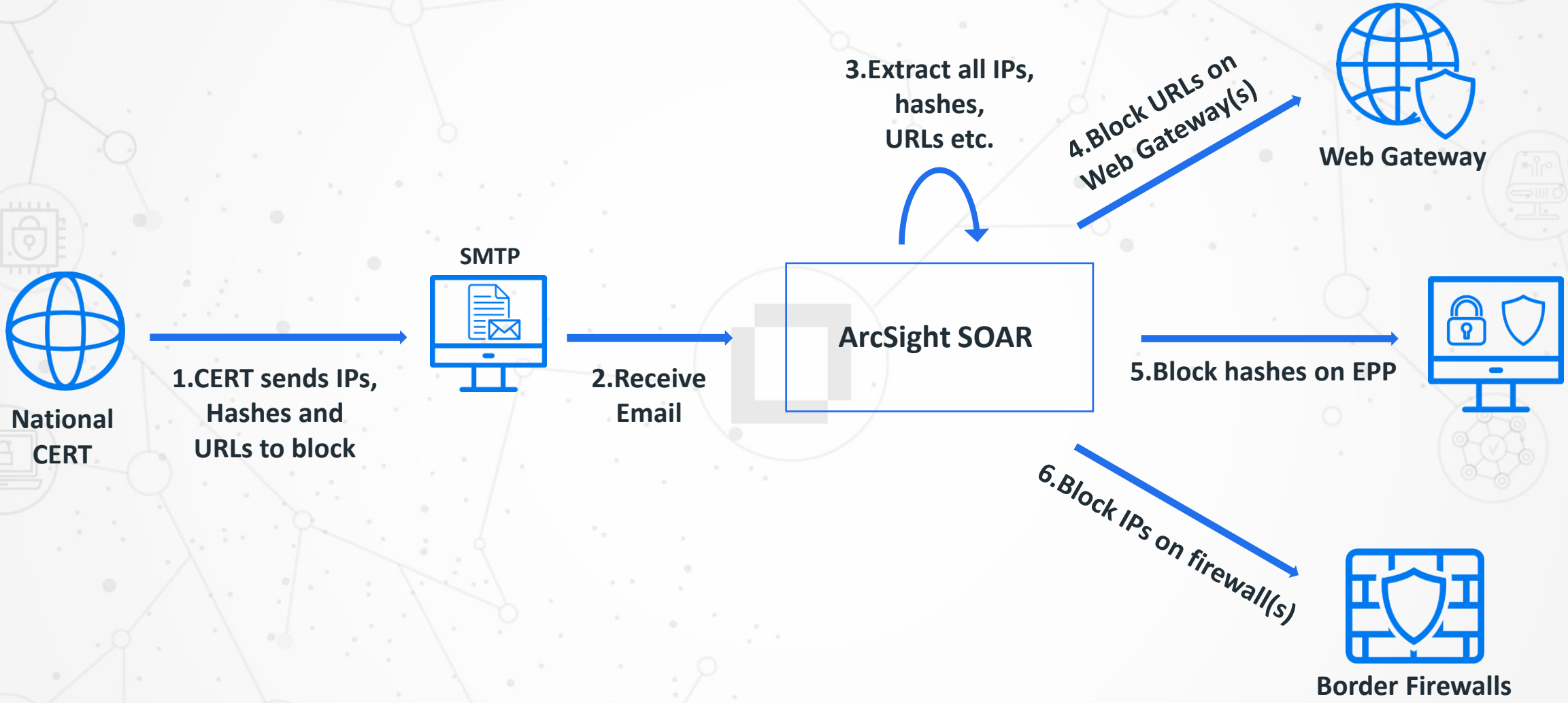
Приклад #2: виток інформації



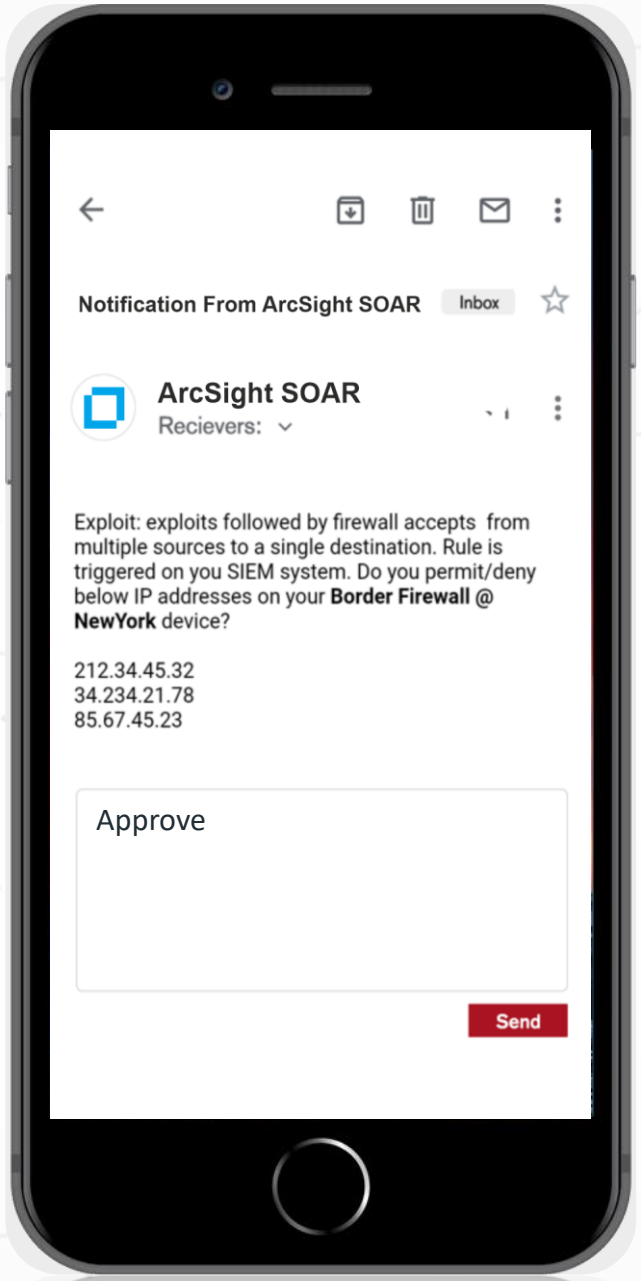
Приклад #3: Розслідування фішингу



Приклад #4: Взаємодія з CERT

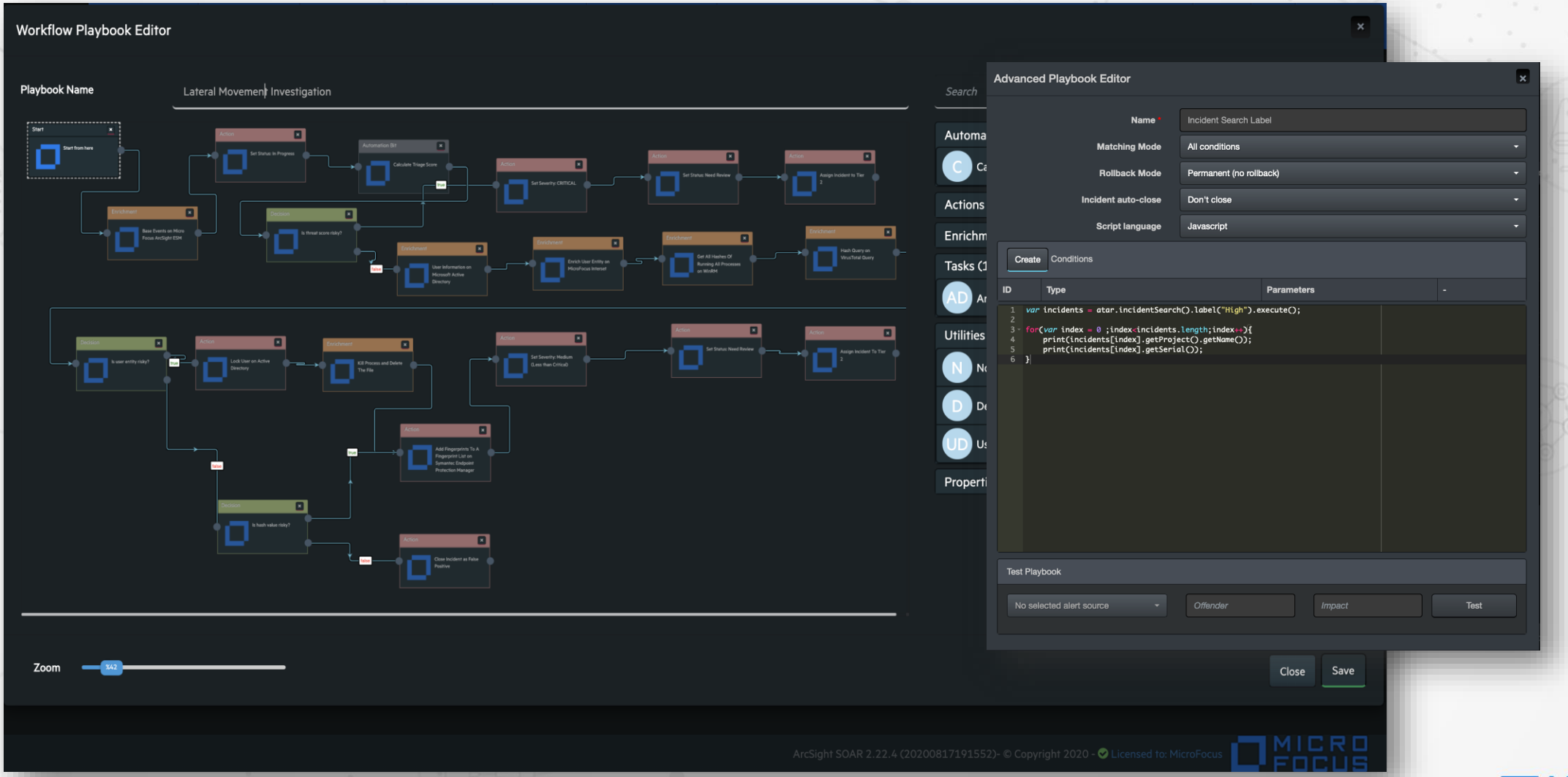


Швидка реакція



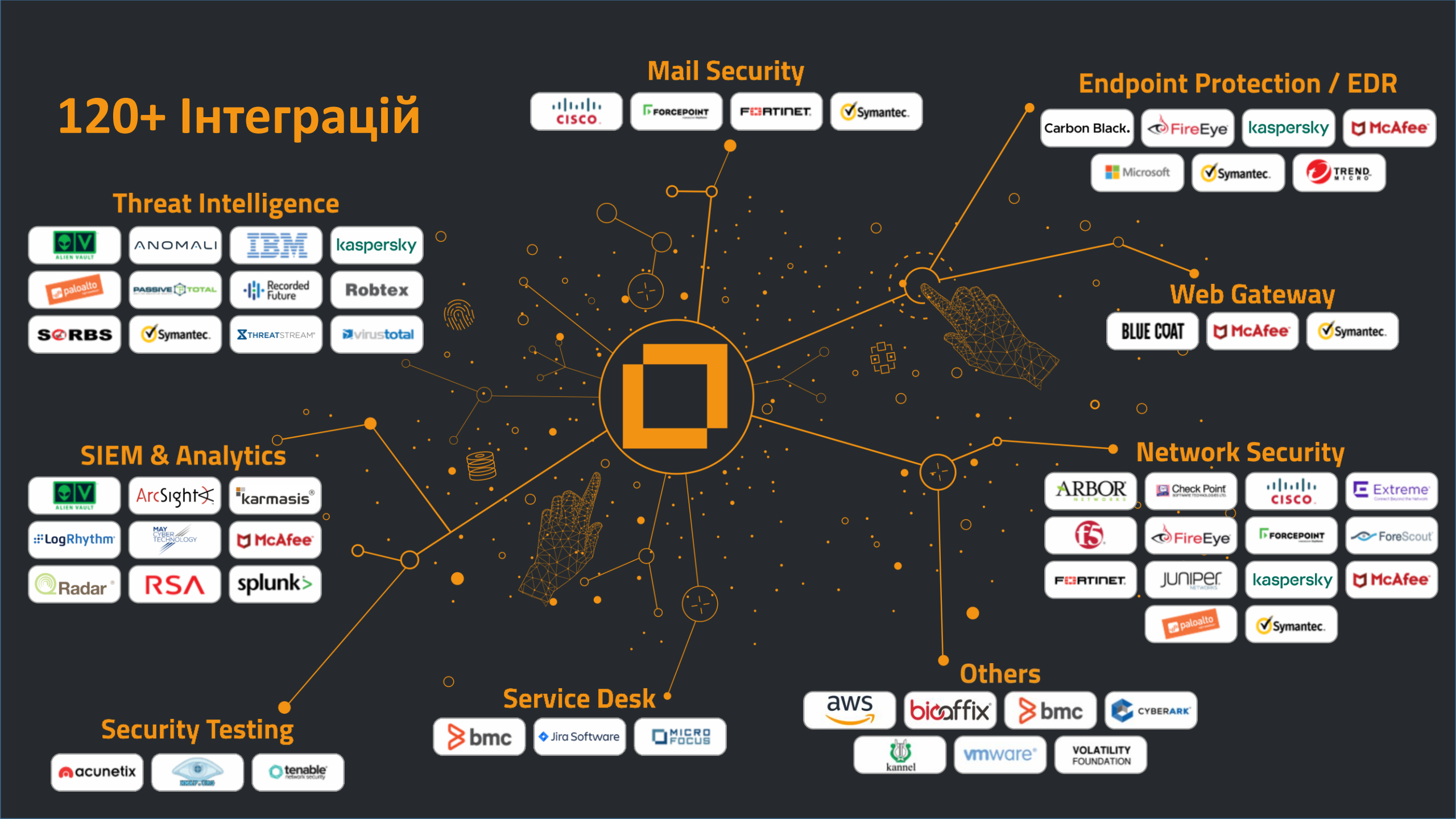
з узгодженням дій

Створення алгоритмів **ArcSight SOAR**

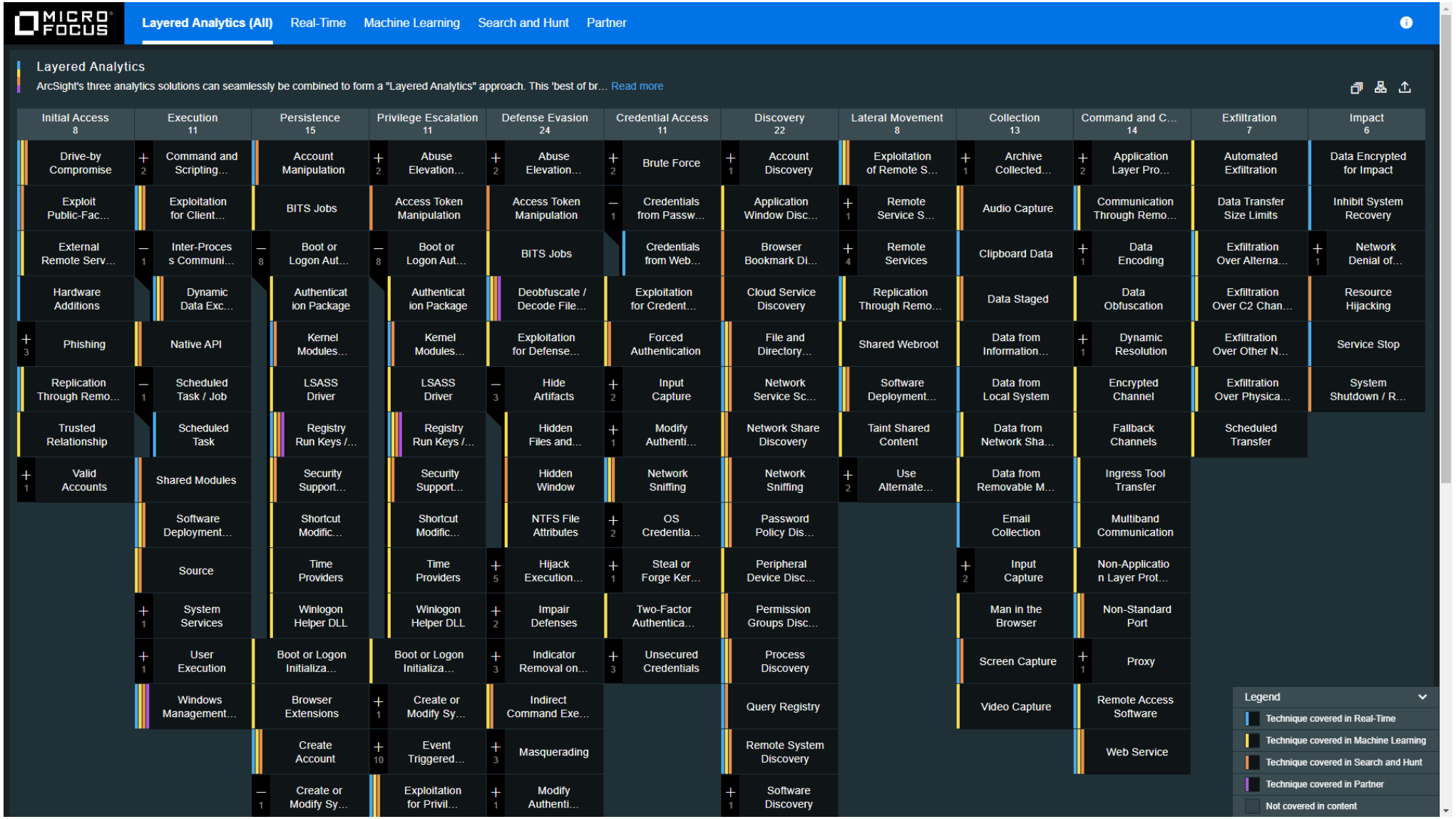


MICRO FOCUS

120+ Інтеграцій



Micro Focus має власний MITRE ATT&CK



Arcsight – лідер ринку Інформаційної Безпеки

$4B
інвестиції компанії Micro Focus в інновації продуктів Інформаційної Безпеки

81
Центрів Кіберзахисту створено «під ключ»

485+
патентів у сфері Інформаційної Безпеки

75PB
найбільша «Приватна Хмара» у світі

65TB
даних для розслідувань у форензиці

450M+
пристроїх та ПЗ

2000+
сертифікованих спеціалістів

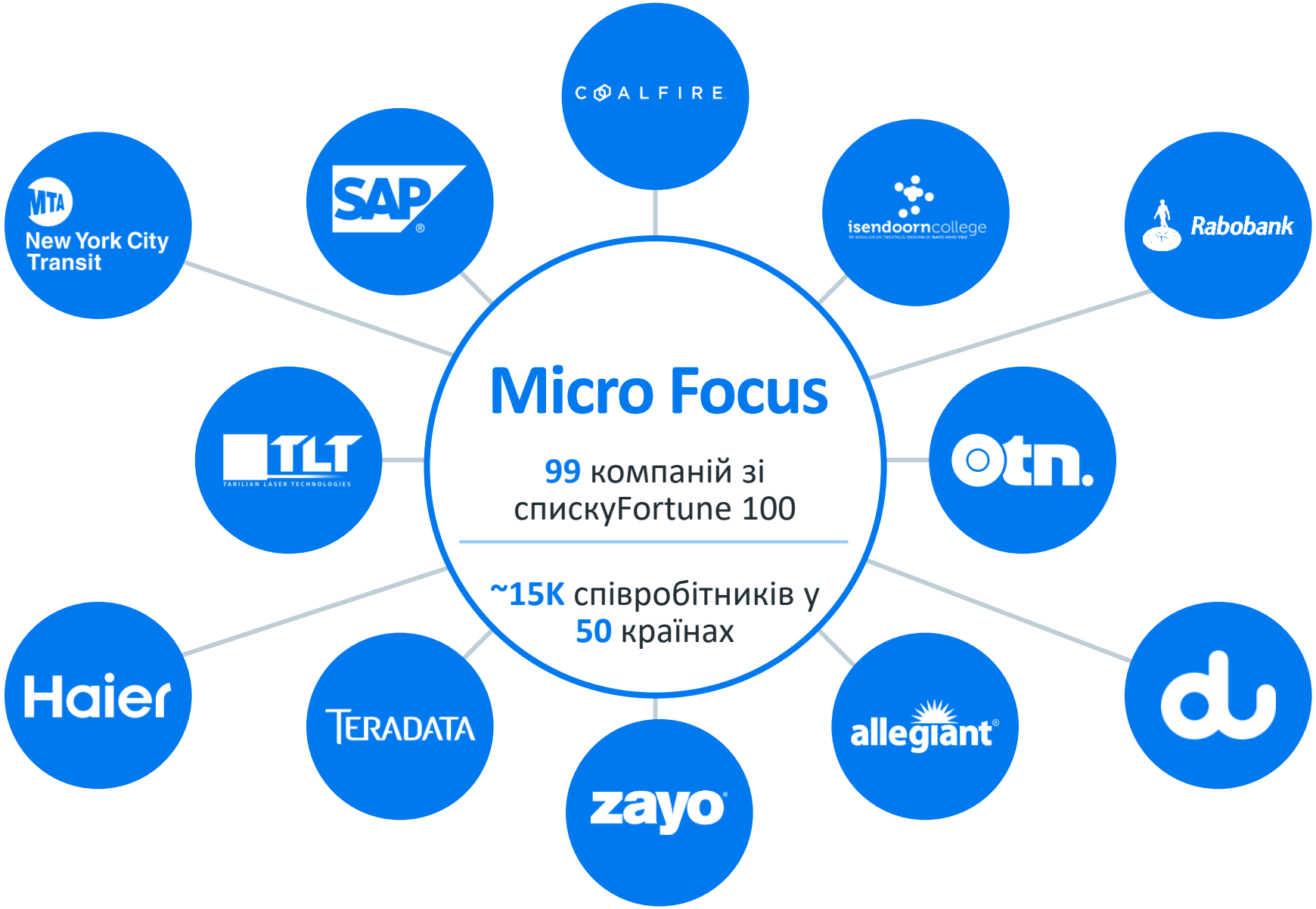
10/10
Найбільших банків світу

9/9
платіжних систем

145M
документів 1100 адвокатів захищено

20+
досвіду в Інформаційній Безпеці

Глобальні Клієнти



MICRO FOCUS®

Дякую!

Alexander.Kulakovskiy@microfocus.com