

РОЗВІДКА КІБЕРЗАГРОЗ:
ШО ВОНО ТАКЕ? |

ДАВАЙТЕ ЗНАЙОМИТИСЬ!

Іван Гокін



ІТ-аудитор, CISA, 5+ років досвіду в консалтингу та аудиті

У зв'язку з війною рф проти нашої країни мені стало цікаво розібратись, що таке розвідка кіберзагроз, бо наше керівництво має бути забезпечене актуальною та дієвою інформацією про кіберзагрози

ЩО МИ ОБГОВОРИМО

Визначення

Перспективність

Необхідні навички

Інструменти

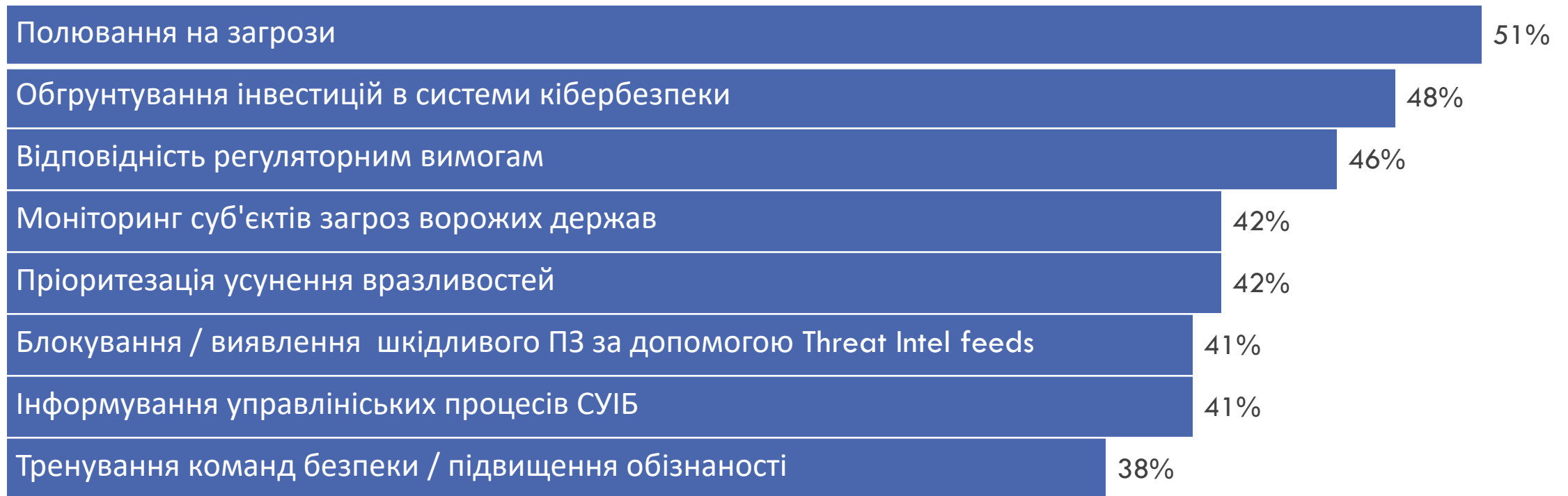
Процес

Кого почитати

ВИЗНАЧЕННЯ



Розвідка загроз – інформація про загрози, яку зібрали, обробили, проаналізували, протлумачили або збагатили для надання необхідного контексту для процесу прийняття рішень. – NIST SP 800-150



ПРИЗНАЧЕННЯ РОЗВІДКИ КІБЕРЗАГРОЗ

Джерело: [The Mind of the CISO by Trellix](#)

ЩО ТРЕБА ВМІТИ?

Сертифікації



[arcX CTI 101](#) - безкоштовна і базова сертифікація



[CREST](#) надає достатньо зрілі сертифікації



Професійний стандарт
«Аналітик загроз безпеки»
(першоджерело: NIST NICE
«[Threat Analysis](#)»)

European Cybersecurity Skills Framework

Вміння



- ☐ Командна робота
- ☐ Збір, аналіз та співвідношення інформації про кіберзагрози, що надходить з різних джерел
- ☐ Ідентифікація суб'єктів загроз, TTP та кампаній
- ☐ Автоматизувати процедури управління розвідданими про загрози
- ☐ Проведення технічного аналізу та звітування
- ☐ Виявлення некібернетичних подій, що впливають на кібернетичну діяльність
- ☐ Моделювання загроз, суб'єктів і ТТП
- ☐ Комунікація, координація та співпраця з внутрішніми та зовнішніми зацікавленими сторонами
- ☐ Комунікація, звітування перед відповідними зацікавленими сторонами

Знання



- ☐ Безпека операційних систем
- ☐ Безпека комп'ютерних мереж
- ☐ Системи кібербезпеки
- ☐ Програмування
- ☐ Відповідальні процедури розкриття інформації
- ☐ Міжгалузеві знання, пов'язані з кібербезпекою
- ☐ Суб'єкти кіберзагроз
- ☐ Процедури кібератак
- ☐ Сучасні та постійні кіберзагрози (APT)
- ☐ Тактики, методи та процедури загроз (TTPs)



ДЕ ОРГАНІЗАЦІЙНО
ЗНАХОДЯТЬСЯ СТІ
АНАЛІТИКИ

Джерело: 11 strategies of a world class cybersecurity operations center - MITRE

ПЕРСПЕКТИВНІСТЬ ПРОФЕСІЇ НА РИНКУ

Зараз представлена в компаніях з розвідки кіберзагроз (напр. Recorded Future)

Адаптація європейських законів [NIS2](#) та [DORA](#) підвищить попит на розвідку кіберзагроз в, в тому числі для проведення пентестів на основі розвідки кіберзагроз (TLPT).

Держспецзв'язку «адаптували» відповідний професійний стандарт, і можливо по ньому почнеться підготовка в університетах протягом наступних трьох-чотирьох років.


Analyst

кібер

Знайти

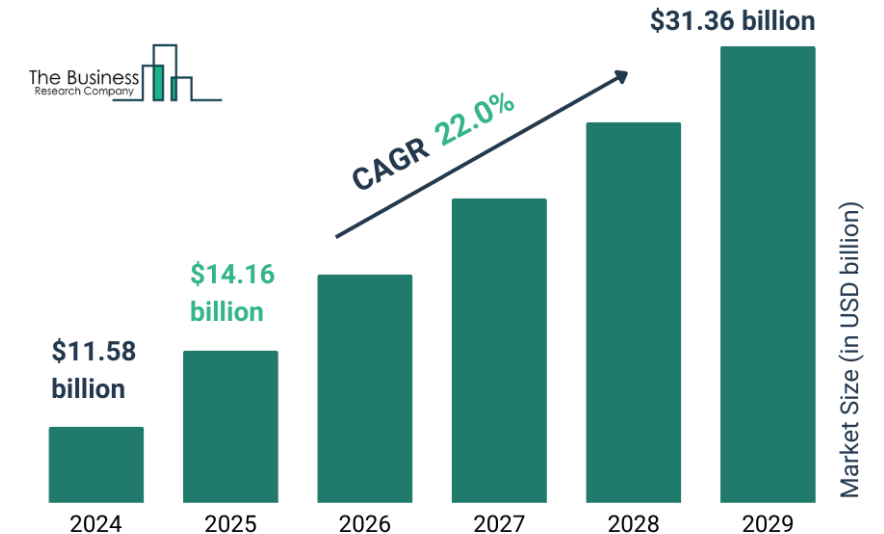
☐ шукати в описах вакансій

Швидкий перехід: [QA](#), [SysAdmin](#), [початківцям](#), [govtech](#), [miltech](#), [сили оборони](#), [бронювання](#).

1 вакансія в категорії Analyst за запитом «кібер»  [RSS](#)

Досвід
Без досвіду
< 1 року

Cyber Threat Intelligence Global Market Report 2025



Найближчим часом ця професія буде актуальнішою в основному в державних органах

ПЛАТФОРМИ РОЗВІДКИ КІБЕРЗАГРОЗ

Основні функції

Збір та аналіз даних

Аналіз та кореляція
загроз

Збагачення розслідувань
інцидентів

Збагачення систем
кібербезпеки



MISP

- В базовому варіанті проста для використання система
- Обираєте самі які модулі до неї потрібні
- Використовується в Україні
- Open-source, підтримується Єврокомісією



OpenCTI

- Зручна з коробки, зріла система з різними інтеграціями
- Розробляється французькою компанією Filigran за підтримки уряду Франції

>>DEMO

СПОЖИВАЧ ІНФОРМАЦІЇ МАЄ ОБМЕЖЕНИЙ ЧАС ТА УВАГУ



Споживач інформації не має споживати сирі дані.

Задача аналітика кіберзагроз – відфільтрувати все, що не цікаво споживачу, та надати споживачу рівно те, що він з користю та мінімальними зусиллями може застосувати під час своєї діяльності.

ЩО ЦІКАВО СПОЖИВАЧАМ ІНФОРМАЦІЇ?

Розвідка кіберзагроз може проводитися на тактичному, оперативному, стратегічному рівнях, які визначаються потребами споживачів інформації.

На тактичному рівні, наприклад, аналітики кіберзагроз часто працюють з індикаторами компрометації (IOC).

Індикатор компрометації — це артефакт, що спостерігається в мережі або ОС, який із високою достовірністю вказує на вторгнення.

Цінність індикаторів гарно ілюструється т.зв. «пірамідою болю» (див. праворуч), і, очевидно, найцінніше, що можна збирати — це техніки, тактики та процедури (ТТП), які ви, ймовірно, знаєте з [MITRE ATT&CK](#).



Піраміда болю



ЦИКЛ РОЗВІДКИ

ПЛАНУВАННЯ ТА СПРЯМУВАННЯ

Вимоги визначаються для того, щоб інформація про кіберзагрози була корисною та дієвою.

Підходи до формування вимог:

Загальні вимоги розвідки (GIR) — постійні, узагальнені вимоги, які походять від моделі загроз, загальної геополітичної ситуації або з інших джерел

- «Всі атаки з боку APT28, APT29, APT44»
- «Всі атаки на українську галузь фінансів»

Пріоритетні вимоги розвідки (PIR) — одноразові, конкретні запити

- «Знайди мені відомі набори вторгнень з в'єтнамським походженням, які діяли протягом останніх пів року»

Детальніше



ЗБІР

На цьому етапі ми визначаємо перелік джерел для збору.

Джерела бувають відкриті і закриті, і кожне джерело оцінюється на надійність за [адміралтейською шкалою](#).

- CERT-UA – зазвичай надійне джерело (B), бо це публічна установа, і вони не попадали неправдиві дані
- Kaspersky – відносно надійне джерело (C), оскільки хоча вони не подавали неправдиві дані, це компанія з країни-агресора, яка може потрапити під урядовий тиск

[Collection Management Framework](#)



ОБРОБКА

На цьому етапі ми проводимо перевірку наданої інформації – ми ж не хочемо раптово забанити легітимний і потрібний нам сервіс, такий як публічний DNS сервер або домен комерційної хмари.

Індикатори компрометації (IOC) доволі зручно перевіряти через AlienVault, але все одно необхідно переглядати список індикаторів, оскільки ніякий інструмент не вирішить за вас чи є в списку false positives.

Не менш важливо розуміти, що і не все, що попадає нам в руки, обов'язково є правдою – в такому випадку нам допомагає оцінка надійності джерела, а також пошук підтвердження такої інформації з іншого незалежного джерела. Ми також можемо оцінювати і інформацію за [адміралтейською шкалою](#), що є хорошим тоном.

[LevelBlue/Labs](#) [Dashboard](#) [Browse](#) [Scan Endpoints](#) [Create Pulse](#) [Submit Sample](#) [API Integrations](#)

Create New Pulse

Use our extraction tool to automatically pull indicators of compromise (IOCs) from sources, including any website, blog post, PDF report, etc.

Enter the file source using one of the methods below, then click "Extract Indicators". OTX will automatically identify the indicators of compromise and return individual indicators. You will also have the ability to modify your existing pulses at any time.

ENTER SOURCE URL OR TEXT

Extract Indicators

REFERENCES

<https://hunt.io/blog/cobaltstrike-powershell-loader-chinese-russian-infrastructure>

[Included IOCs \(58\)](#) [Review IOCs \(0\)](#) [Excluded IOCs \(2\)](#) [Suggested IOCs \(0*\)](#)

This is the list of indicators that will be part of your Pulse

Show entries

<input type="checkbox"/>	TYPE	INDICATOR	ROLE	TITLE
<input type="checkbox"/>	IPv4	167.71.215.63	exploit_source	
<input type="checkbox"/>	IPv4	137.184.103.54	scanning_host	
<input type="checkbox"/>	IPv4	150.158.214.98	scanning_host	
<input type="checkbox"/>	CIDR	111.229.0.0/16		
<input type="checkbox"/>	CIDR	114.116.0.0/17		
<input type="checkbox"/>	CIDR	116.114.0.0/16		
<input type="checkbox"/>	CIDR	121.36.0.0/15		
<input type="checkbox"/>	CIDR	123.206.0.0/15		
<input type="checkbox"/>	CIDR	124.220.0.0/14		

ПИТАННЯ АТРИБУЦІЇ

- Під час роботи ви можете часто стикатись з різними конвеціями для найменування суб'єктів загроз, напр. Gamaredon Group (aka: ACTINIUM, Actinium, Aqua Blizzard, UAC-0010)
- З чим це пов'язано?
- Кожна компанія, яка звітує про активність певного суб'єкта загроз, насправді спостерігає у себе чи у своїх клієнтів відповідно схожі ТТП та набори інструментів для втручань, але надійно їх співставляти на постійній основі з даними інших компаній не може по ряду причин, наприклад із-за обмежень на поширення такої інформації клієнтами.
- Зараз є декілька ініціатив щодо уніфікації найменувань, але ймовірно, що завершаться вони нічим. Наприклад, [Crowdstrike та Microsoft зробили співвідношення своїх найменувань](#).
- Наразі просте рішення для співставлення різних найменувань – це користуватись базами знань такими як [malpedia](#) або іншими подібними ресурсами.

АНАЛІЗ

На цьому етапі ми збагачуємо цю інформацію нашою внутрішньою інформацією.

Ключові питання:

- Чи траплялись вже такі або схожі атаки у нас?
- Чи є у нас вразливі до таких атак пристрої?
- Що можна зробити, щоб уникнути таких атак?
- Чи є готові або легкодоступні рішення?
- Що найважливіше зробити першочергово?

Полювання на загрози

Якщо ми знаємо, що кібератака, про яку ми дізнались, цілком могла трапитись у нас, ми маємо провести полювання на загрози.

Це можна зробити з використанням Yara/Sigma правил через EDR системи.

Правила YARA – це текстові описи шаблонів, які можна використовувати для зіставлення з файлами та процесами. Ці правила можуть виявляти певні рядки, шістнадцяткові послідовності та інші шаблони, характерні для шкідливого програмного забезпечення.

Мережеві ІОК також можна перевіряти на мережевих пристроях.

Компанія з українським корінням [SOC Prime](#) має майданчик для поширення правил для полювання на загрози.

ІНФОРМУВАННЯ

На цьому етапі ми адаптуємо зібрану інформацію у формат, зрозумілий цільовій аудиторії – тим, хто визначив завдання розвідки.

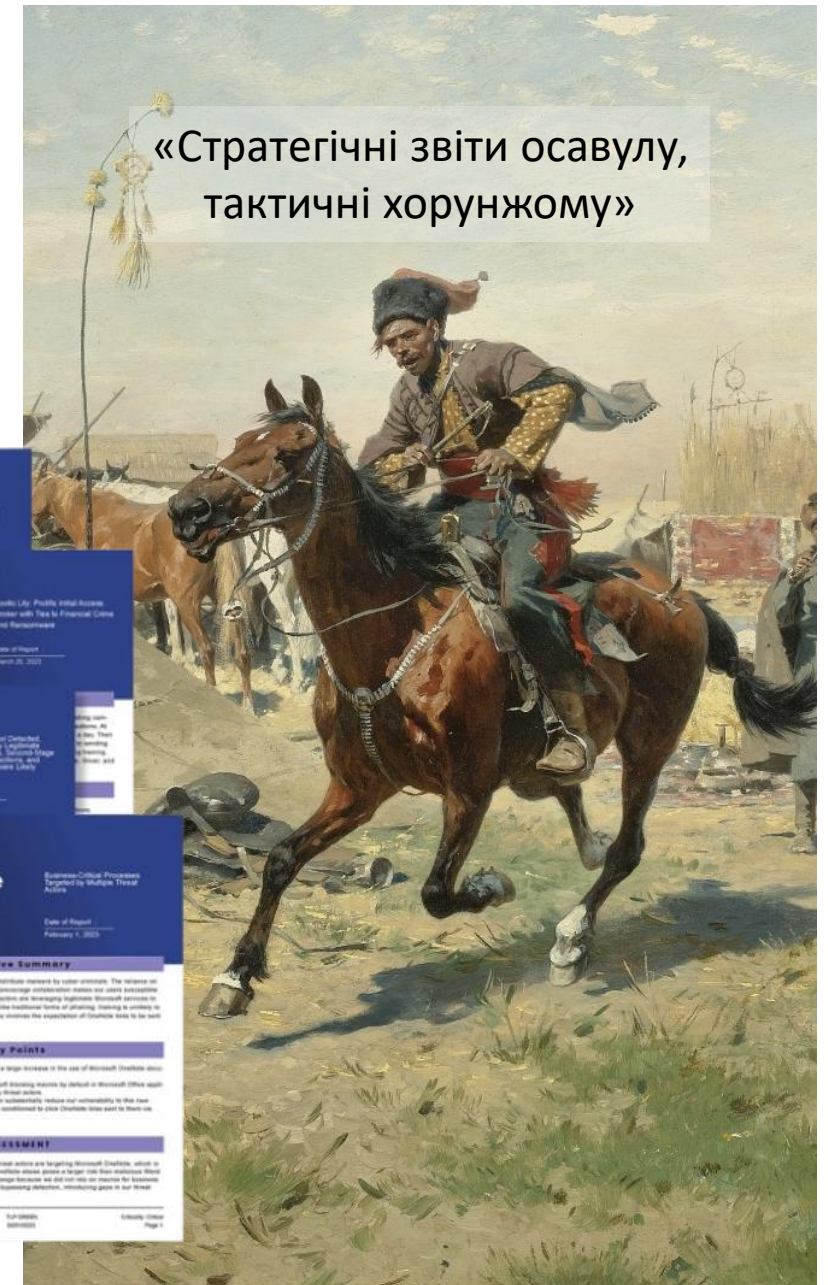
ІОС зазвичай додаються в системи кібербезпеки (системи моніторингу, фаєрволи) з відповідним контекстом.

ТТП цікаві командам з реагування, щоб розуміти яким чином може розвиватись подібна атака, а також для розробки правил виявлення та полювання на загрози.

Керівництву зазвичай цікаво наскільки наша компанія захищена від актуальних атак, тому така інформація для них збирається в регулярні звіти.

CTI Blueprints – шаблони звітів на різні зацікавлені сторони

Один з перших звітів CTI про APT1



ОБМІН ІНФОРМАЦІЄЮ

При інформуванні важливо задати та дотримуватись обмежень на поширення, які задаються [Traffic Light Protocol \(TLP\)](#), щоб уникнути витoku чутливої інформації про інфраструктуру організації.



RED

Не для поширення, тільки для кінцевого одержувача



AMBER

Обмежене поширення, доступне тільки серед представників організації-одержувача



GREEN

Обмежене поширення, доступне тільки для представників спільноти або сектору



CLEAR

Необмежене поширення



ПІДСУМОК

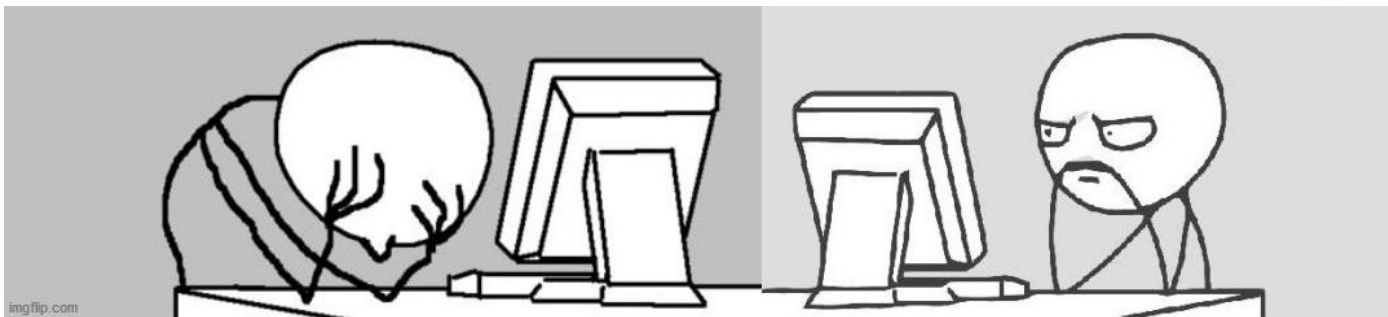
Аналітики кіберзагроз – це радники фахівців з кібербезпеки, їх очі в зовнішній світ і одночасно фільтр від зайвої інформації.

Аналітики кіберзагроз – це перспективна професія, але ймовірно наближчим часом в Україні все ще будуть більше поширені майстри-на-всі-руки, тому такі навички безпечніше засвоювати паралельно з іншими навичками SOC аналітиків.

При цьому, звісно ж, ніщо не заважає вам знайти собі ментора, будувати власний портфель проєктів та проводити власні дослідження, а також шукати віддалену роботу на західні компанії.

Пересічний SOC в Україні be like

- Хто сьогодні виконуватиме роль аналітика кіберзагроз?



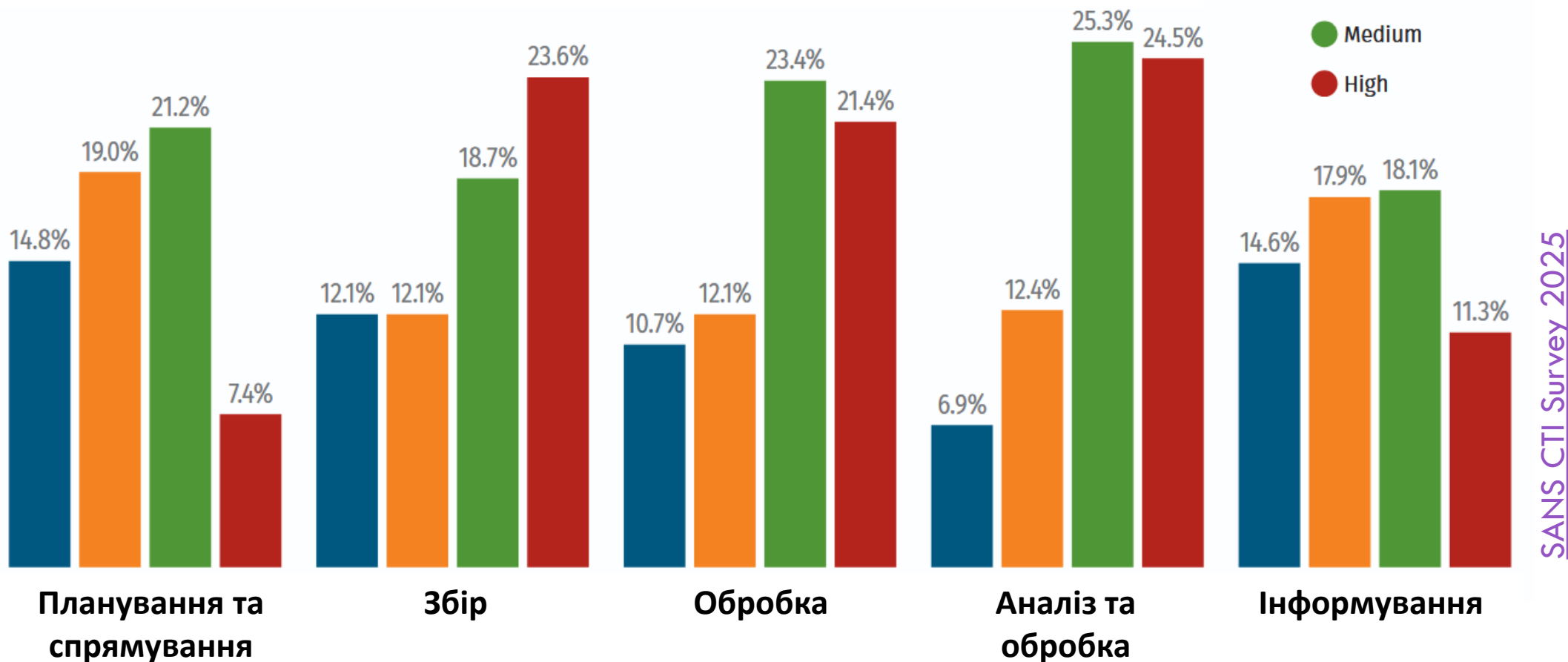
- Ти, я ж вчора заступав



Q&A

Дякую за ці прекрасні картини
польському художнику Юзефу
Брандту

На яких етапах ваших процесів СТІ ви користуєтесь або плануєте використання ШІ, і яка користь такого процесу?



ПОТЕНЦІАЛ ДЛЯ ВИКОРИСТАННЯ ШІ

СТАНДАРТИ

NIST SP 800-150

Cyber Threat Intelligence Capability Maturity Model (CTI-CMM)

КОГО ВАРТО ПОЧИТАТИ

[Gert-Jan Bruggink](#) / [Venation](#) – багато методологічно корисної інформації

[Adam Goss](#) - багато практичних порад, його матеріали частково використовувались в цій презентації

[Flare.io](#) – практичні, корисні курси

[Intel-ops.io – Hunting Adversary Infrastructure](#) – курс, який допоможе вам розмотати одну IPшку в цілісну історію

CTI CHALLENGE

Хочете розібратись та перевірити свої навички?

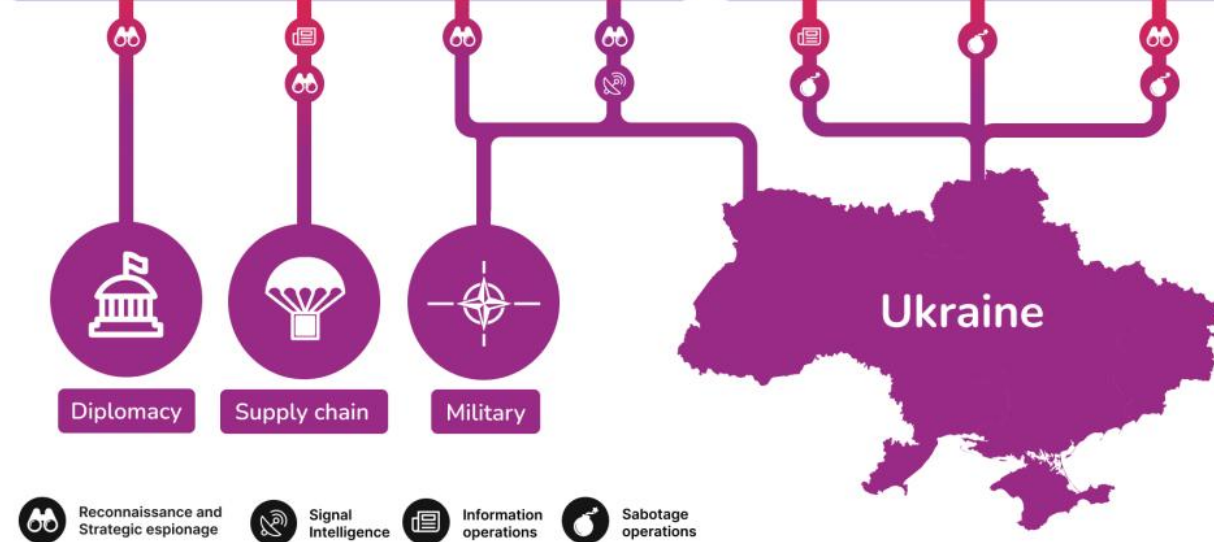
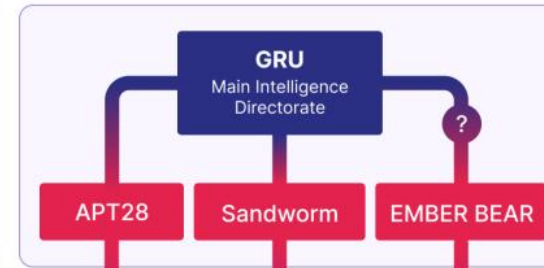
Пройдіть CTI challenge 😊



Espionage & Reconnaissance



Destabilisation & hybrid warfare



ГАРНИЙ ПРИКЛАД
СТРАТЕГІЧНОЇ РОЗВІДКИ
КІБЕРЗАГРОЗ ВІД SEKOIA.IO

