РОЗВІДКА КІБЕРЗАГРОЗ: ШО ВОНО ТАКЕ?

ДАВАЙТЕ ПОЗНАЙОММИМОСЬ

Іван Гокін 

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

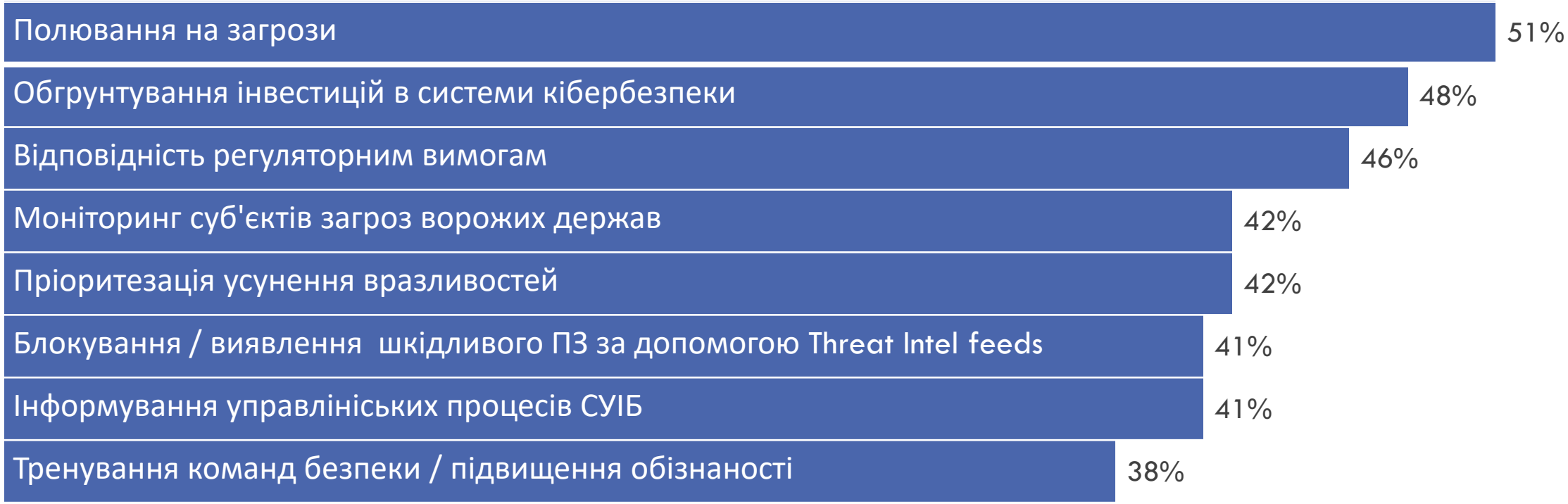
У зв’язку з війною рф проти нашої країни мені стало цікаво розібратись, що таке розвідка кіберзагроз, бо наше керівництво має бути забезпечене актуальною та дієвою інформацією про кіберзагрози

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?

- Англійська – обов’язково
- Знання російської – це конкуретна перевага при роботі на західні компанії
- Решта непогано розписана наприклад в ECSF (див. праворуч->)
- Варіанти по сертифікації таких аналітиків:

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

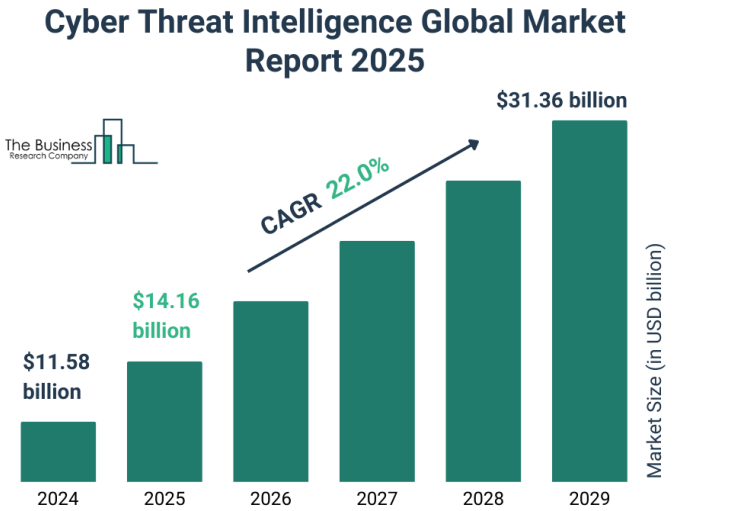
Main task(s)	• Develop, implement and manage the organisation's cyber threat intelligence strategy • Develop plans and procedures to manage threat intelligence • Translate business requirements into Intelligence Requirements • Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders • Identify and assess cyber threat actors targeting the organisation • Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence • Produce actionable reports based on threat intelligence data • Elaborate and advise on mitigation plans at the tactical, operational and strategic level • Coordinate with stakeholders to share and consume intelligence on relevant cyber threats • Leverage intelligence data to support and assist with threat modelling, recommendations for Risk Mitigation and cyber threat hunting • Articulate and communicate intelligence openly and publicly at all levels • Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders
Key skill(s)	• Collaborate with other team members and colleagues • Collect, analyse and correlate cyber threat information originating from multiple sources • Identify threat actors TTPs and campaigns • Automate threat intelligence management procedures • Conduct technical analysis and reporting • Identify non-cyber events with implications on cyber-related activities • Model threats, actors and TTPs • Communicate, coordinate and cooperate with internal and external stakeholders • Communicate, present and report to relevant stakeholders • Use and apply CTI platforms and tools
Key knowledge	• Operating systems security • Computer networks security • Cybersecurity controls and solutions • Computer programming • Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks • Responsible information disclosure procedures • Cross-domain and border-domain knowledge related to cybersecurity • Cyber threats • Cyber threat actors • Cybersecurity attack procedures • Advanced and persistent cyber threats (APT) • Threat actors Tactics, Techniques and Procedures (TTPs) • Cybersecurity-related certifications

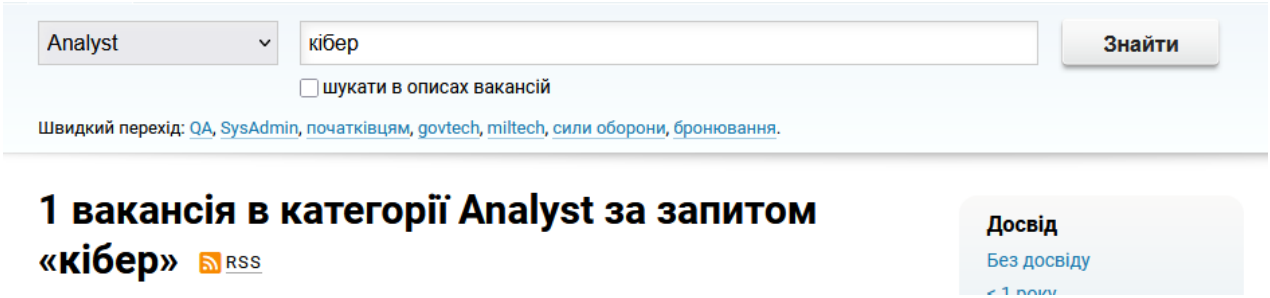
ПЕРСПЕКТИВНІСТЬ ПРОФЕСІЇ НА РИНКУ

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.





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 розлідувань інцидентів
- Збагачення систем кібербезпеки

MISP

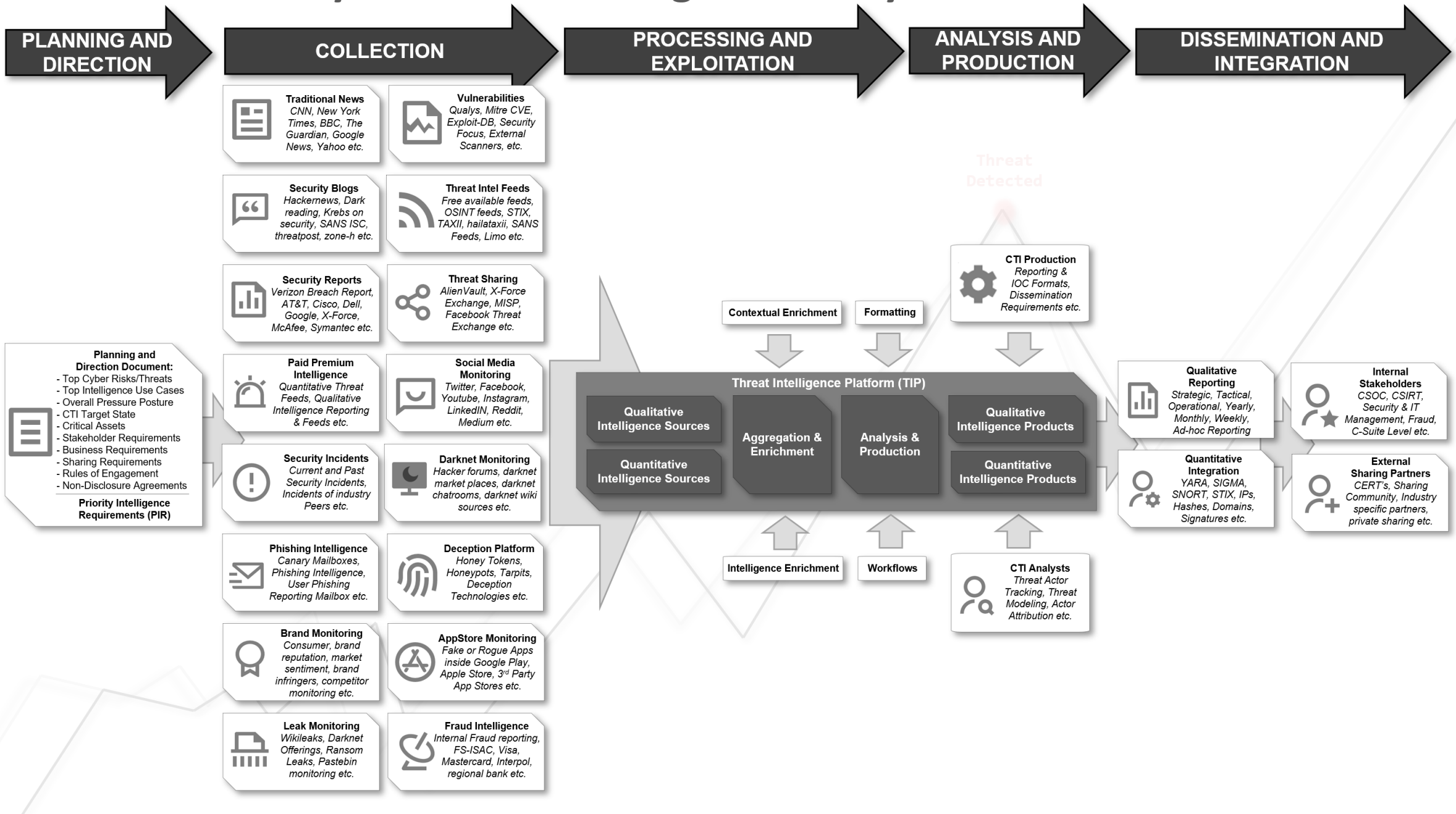
- В базовому варіанті проста для використання система
- Обираєте самі які модулі до неї потрібні
- Використовується в Україні
- Open-source, підтримується Єврокомісією

OpenCTI

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

>>DEMO

Cyber Threat Intelligence Lifecycle Overview



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

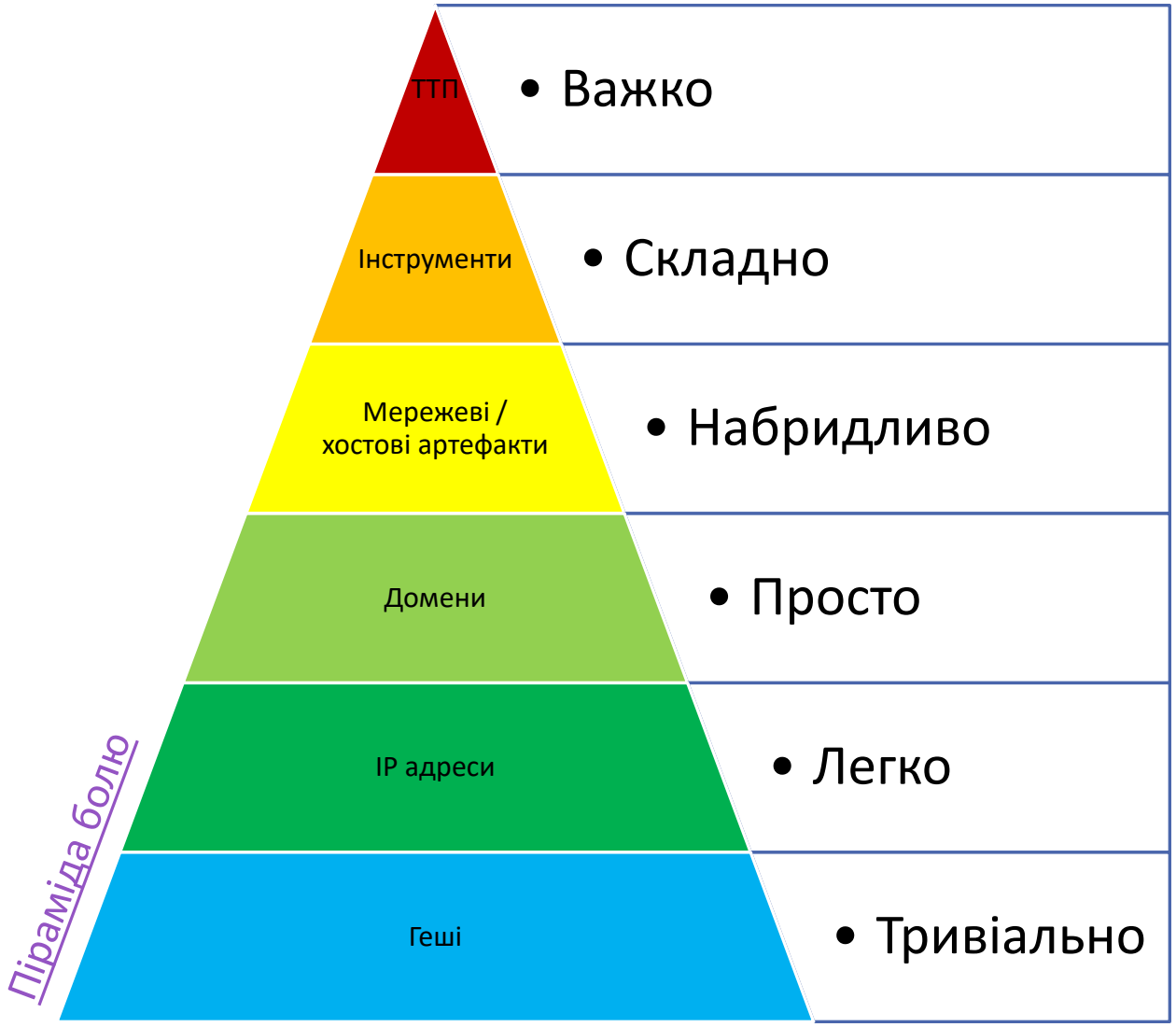
- «Знайди мені відомі набори вторгнень з в'єтнамьским походженням, які діяли протягом останніх пів року»

Детальніше

ЩО ЦІКАВО СПОЖИВАЧАМ ІНФОРМАЦІЇ?

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

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.



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 попасти під урядовий тиск

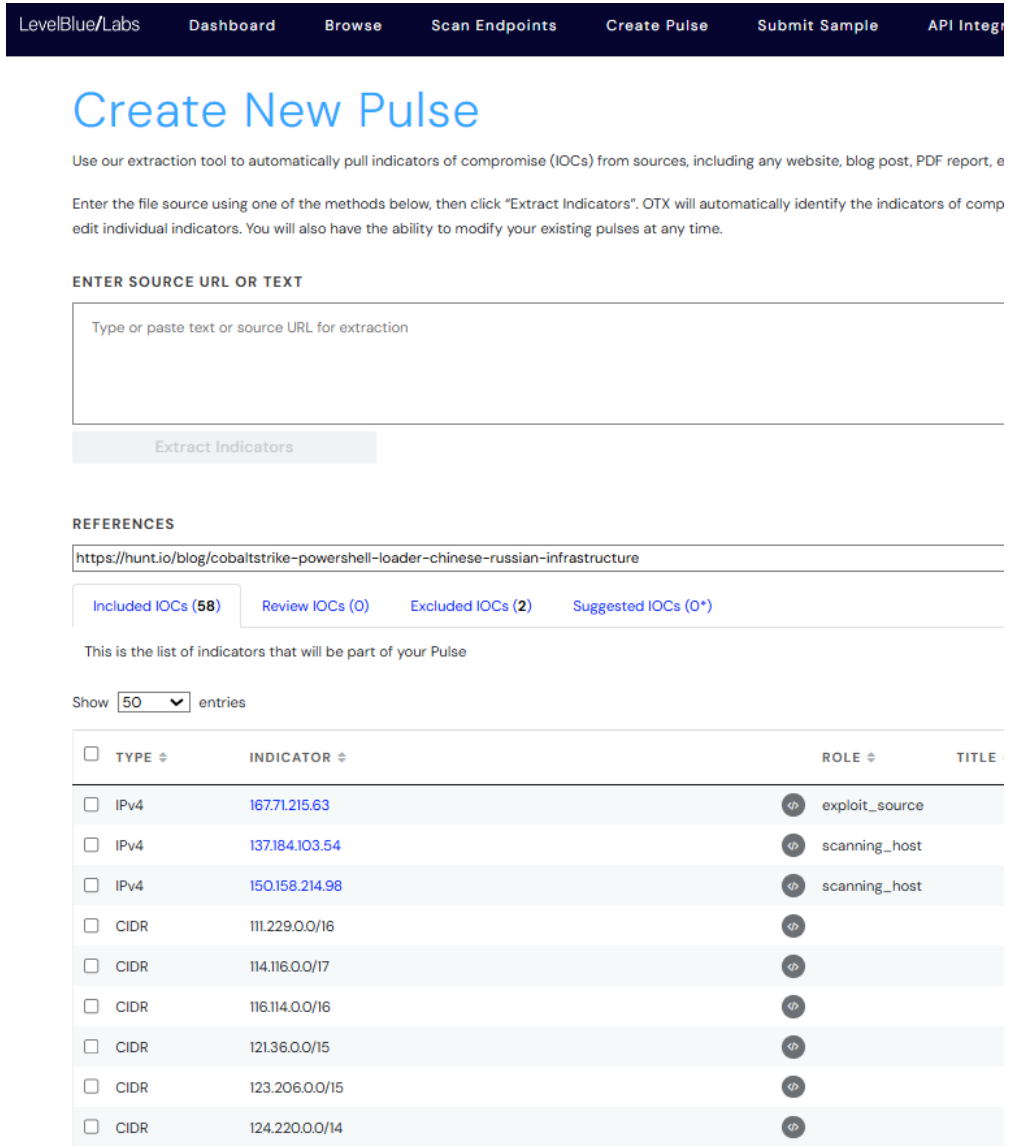
Collection Management Framework

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 окрему інформацію за адміралтейською шкалою, що є хорошим тоном.



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?

Українська компанія SOC Prime надає правила для полювання на загрози, що може допомагати з пошуком рішень для уникнення атак

ІНФОРМУВАННЯ

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

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

TTП 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

ПІДСУМОК

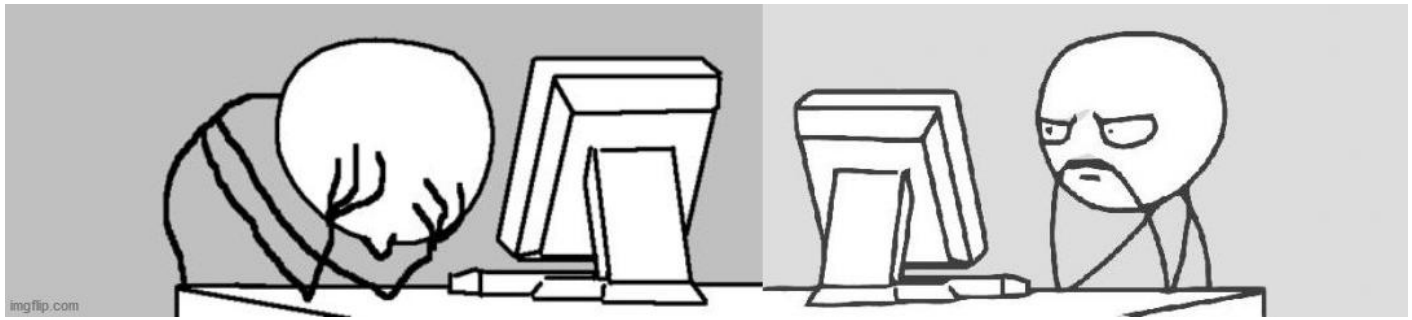
Аналітики кіберзагроз – це радники фахівців з кібербезпеки, їх очі в зовнішній світ і одночасно фільтр від зайвої інформації.

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.

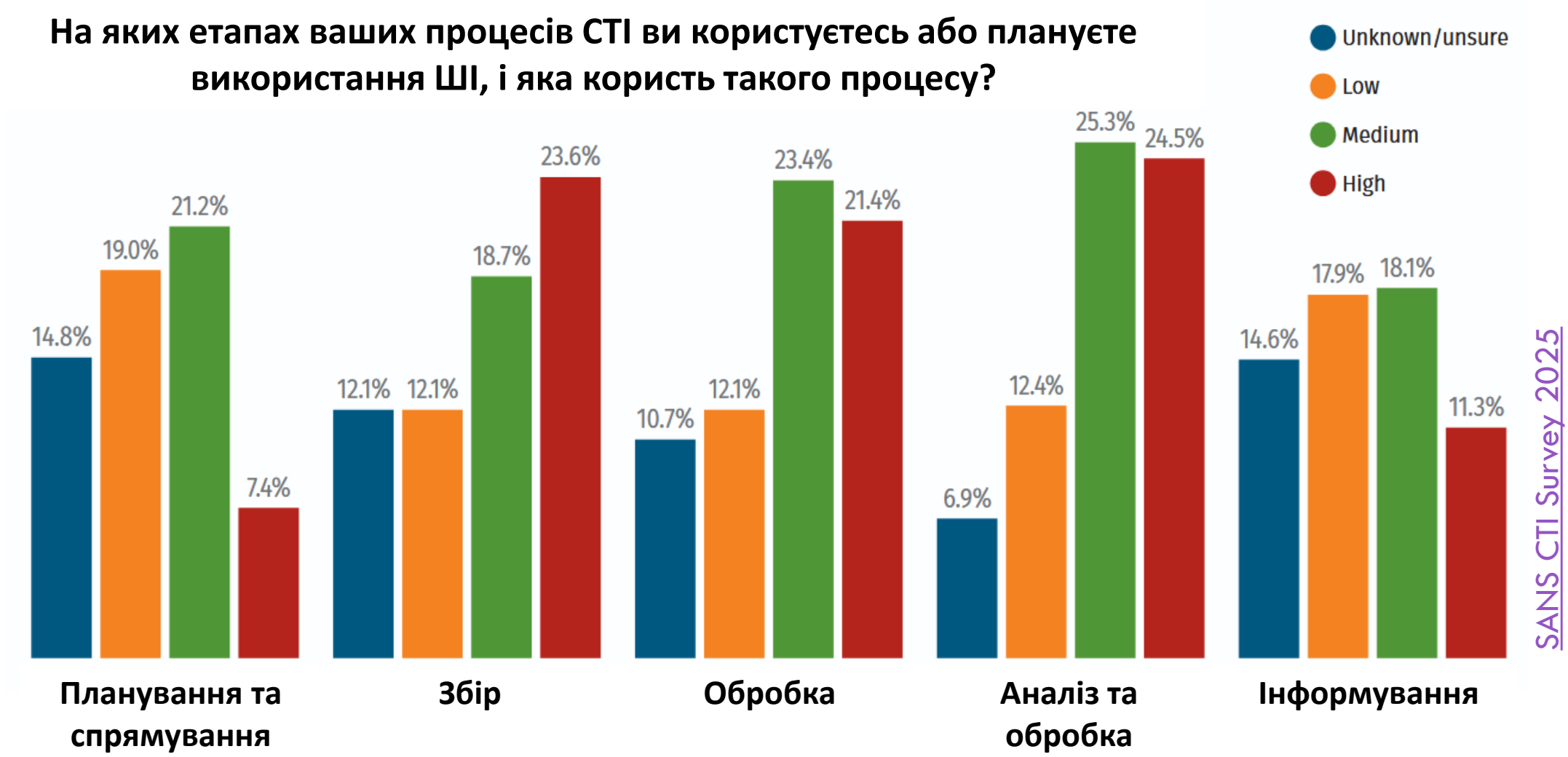
Пересічний SOC в Україні be like

- Хто сьогодні виконує роль аналітика кіберзагроз?



- Ти, я вже вчора заступав

На яких етапах ваших процесів CTI 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

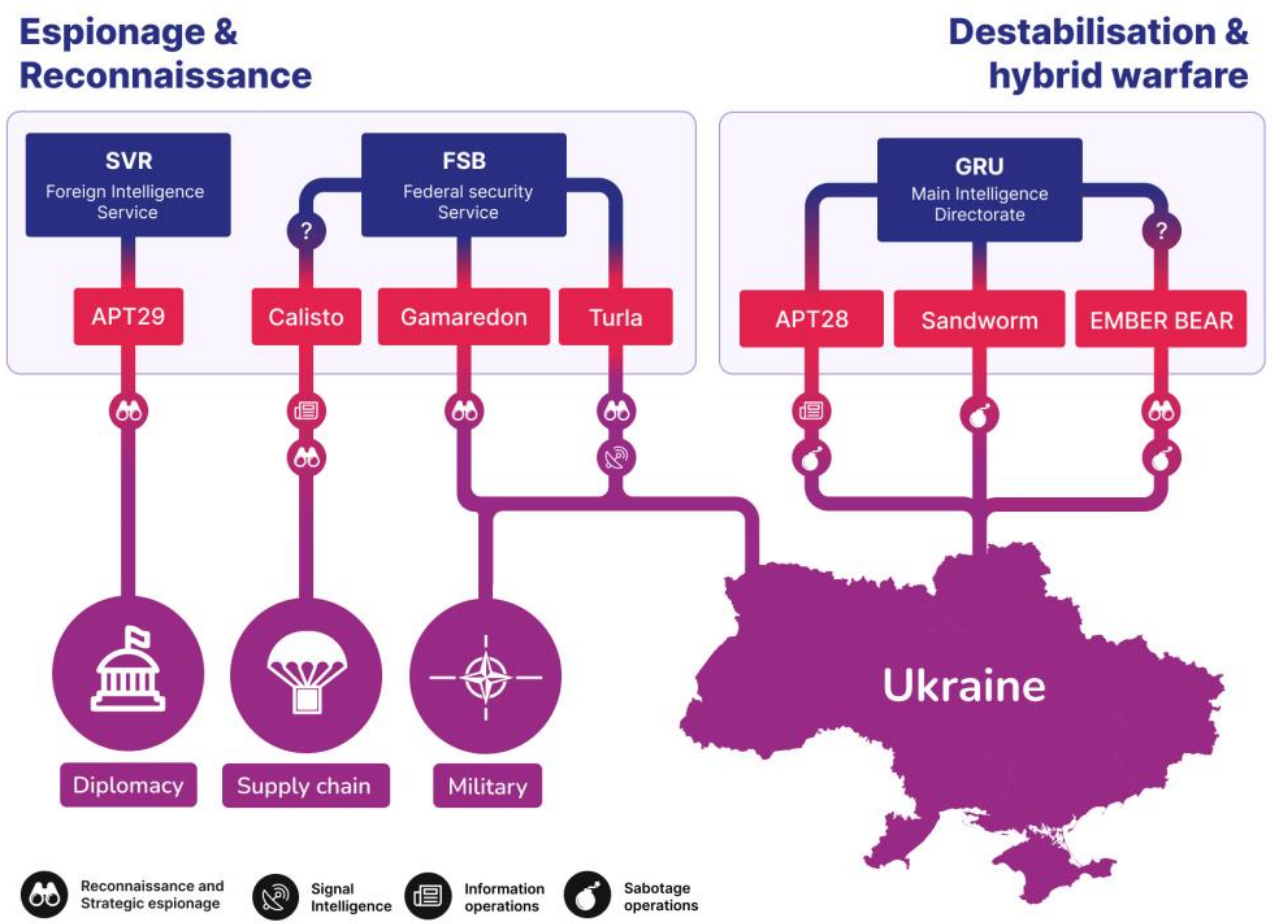
Flare.io – практичні, корисні курси

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 ☺



ГАРНИЙ ПРИКЛАД СТРАТЕГІЧНОЇ РОЗВІДКИ КІБЕРЗАГРОЗ ВІД SEKOIA.IO

- росія
- іран
- кндр
- Китай