10 rzeczy, które należy zrobić, zanim nadejdzie NIS2

Joanna Dąbrowska
CEE Cybersecurity Platform Leader, Trend Micro

10 != 10

10 Minimum Measures

In addition to the four overarching areas of requirement, NIS2 mandates that essential and important entities implement baseline security measures to address specific forms of likely cyberthreats. These include:

- **Risk assessments** and security policies for information systems
- Policies and **procedures for the use of cryptography** and, when relevant, encryption.
- **Security around the procurement of systems** and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.
- **Security procedures for employees with access to sensitive or important data**, including policies for data access. Affected organizations must also have an overview of all relevant assets and ensure that they are properly utilized and handled.
- **The use of multi-factor authentication**, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.
- Policies and procedures for e**valuating the effectiveness of security measures.**
- A plan for handling **security incidents**
- **Cybersecurity training** and a practice for basic computer hygiene.
- **A plan for managing business operations during and after a security incident.** This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
- **Security around supply chains** and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.

Źródło: https://nis2directive.eu/nis2-requirements/

EU Cyber Security Strategy Plan

The new strategy aims to ensure a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe. Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments. These three instruments are regulatory, investment and policy initiatives. They will address three areas of EU action:

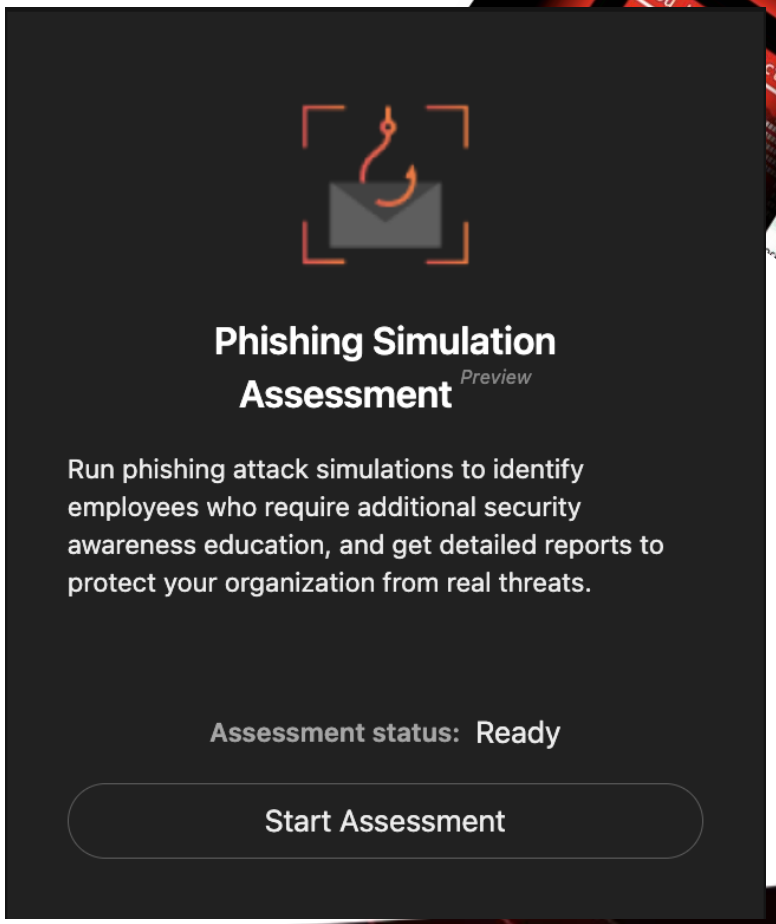
1. resilience, technological sovereignty and leadership;
2. operational capacity to prevent, deter and respond;
3. cooperation to advance a global and open cyberspace.

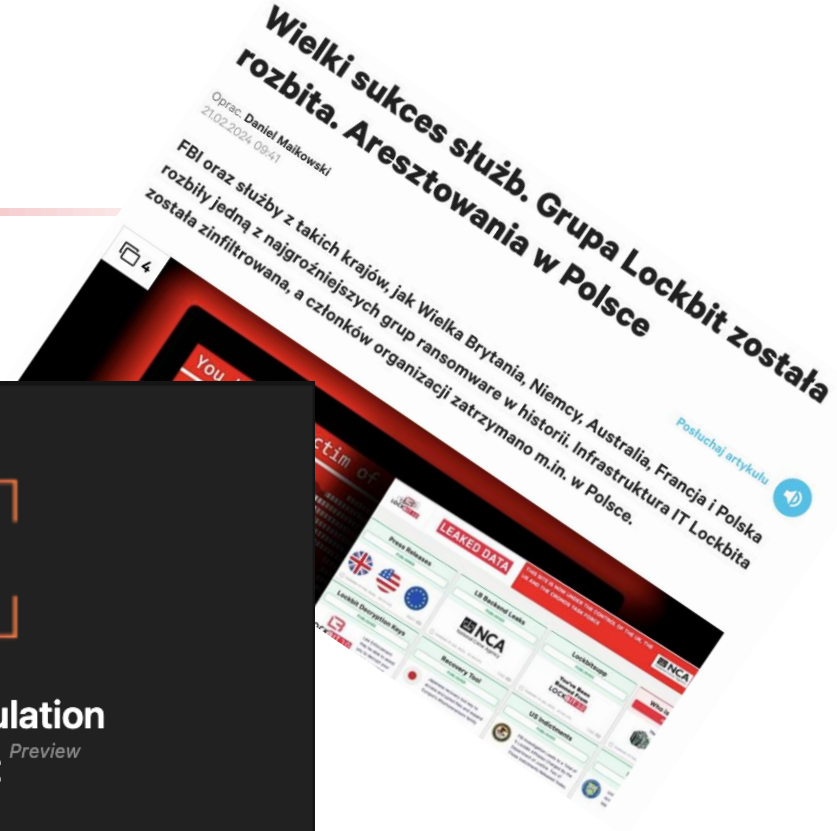
The EU is committed to supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years. This would quadruple previous levels of investment. It demonstrates the EU's commitment to its new technological and industrial policy and the recovery agenda.

Źródło: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

1. Świadomość i edukacja

- Informacja Zarządcza
- Edukacja pracowników
- Dystrybucja informacji o zagrożeniach





2. Ustanowienie w organizacji ról i obowiązków

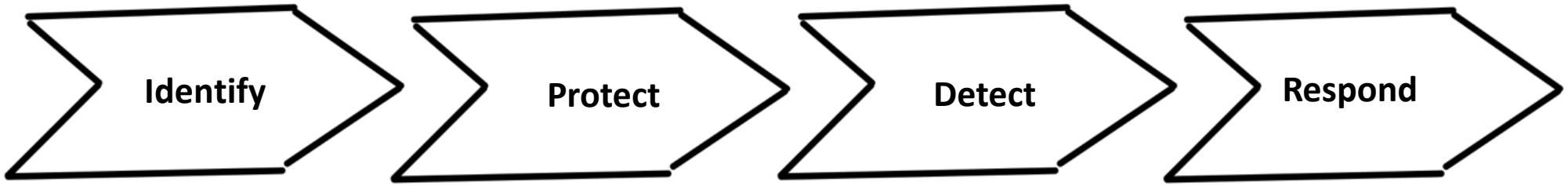
- Odpowiedzialność
- Zakres obowiązków
- Komunikacja

Zarządzanie Ryzykiem a odpowiedzialność

“Senior management is responsible for cybersecurity risk management in essential and important entities. Failure to comply with NIS2 requirements by the management can result in severe consequences such as temporary bans, administrative fines, and liability as per the national legislation.”

3. Przeprowadzenie analizy dojrzałości

- Ankieta
- Audyt zewnętrzny
- Przegląd procedur i dokumentacji



- Asset Management
- Vulnerability management
- Red - Blue Teaming & Penetration Testing

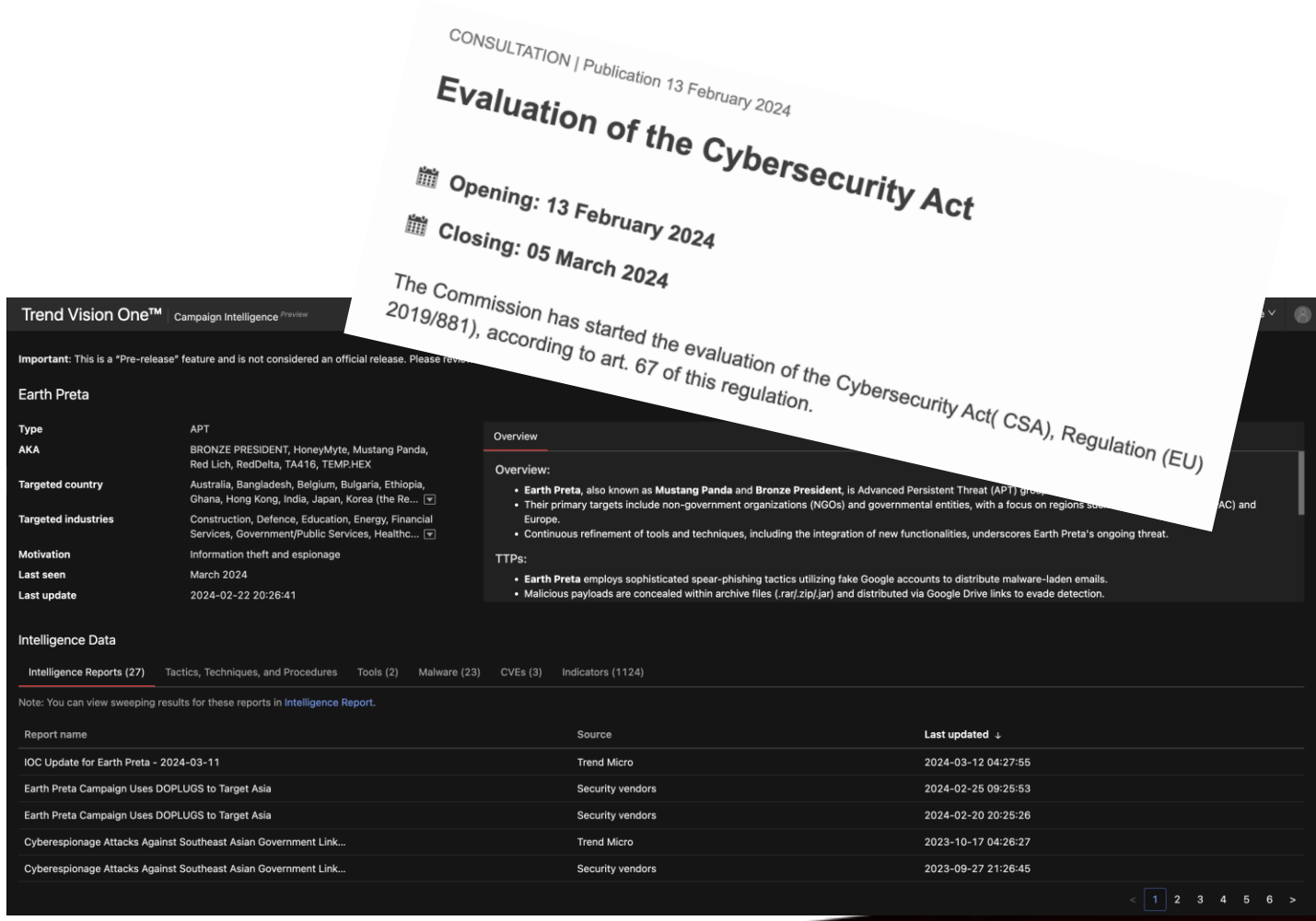
- Endpoint Protection
- Network Protection
- Identity
- E-Mail Protection

- Telemetry
- Data correlation
- Analysis

- Incident Response

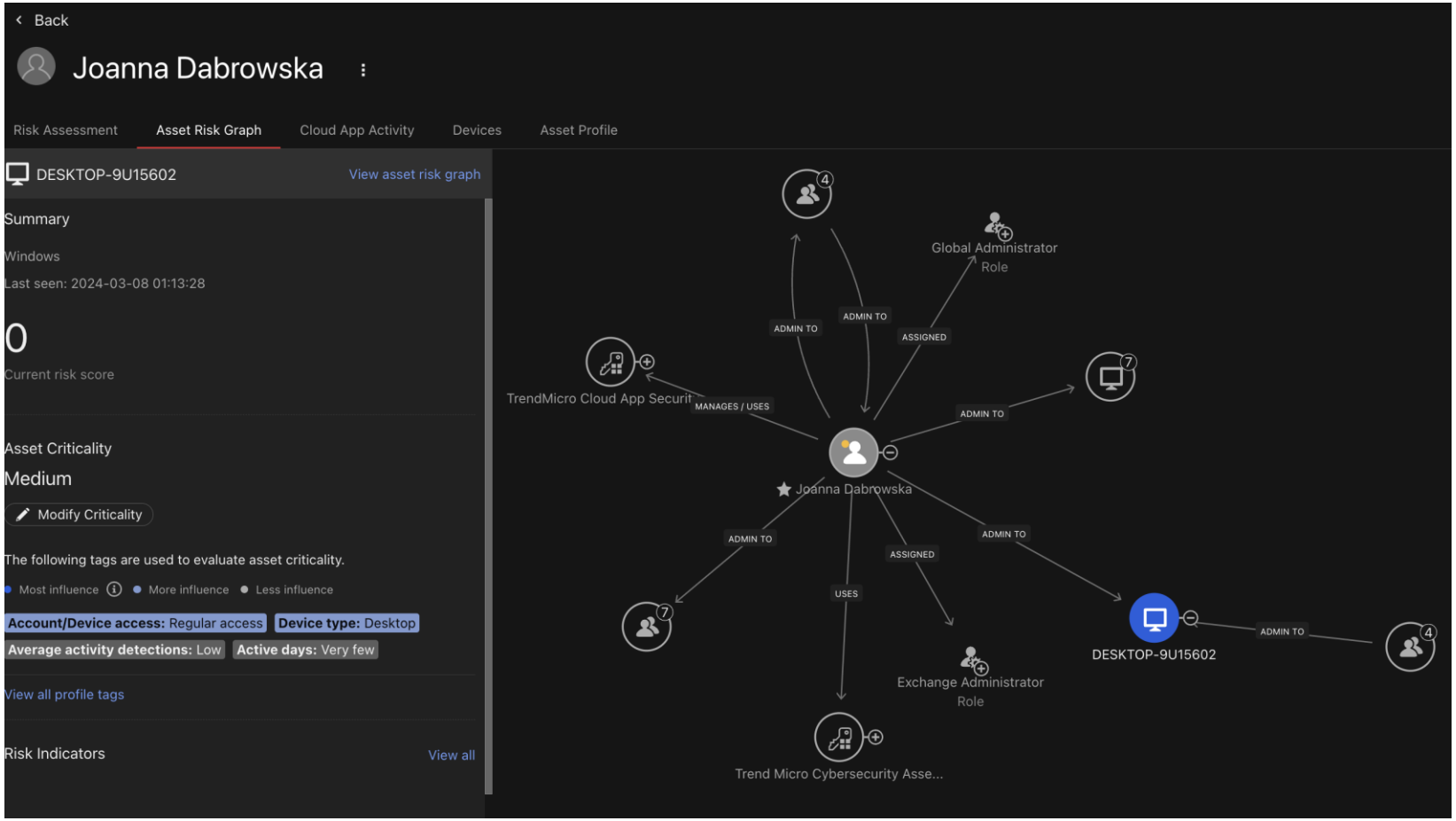
4. Zbieranie i wymiana informacji o zagrożeniach

- Zagrożenia
  - TTP
  - IoC
- Podatności
- Konfiguracja systemów i aplikacji
- Konfiguracja mechanizmów bezpieczeństwa
- Proces ciągły
- Automatyczny
- Wymiana informacji pomiędzy podmiotami



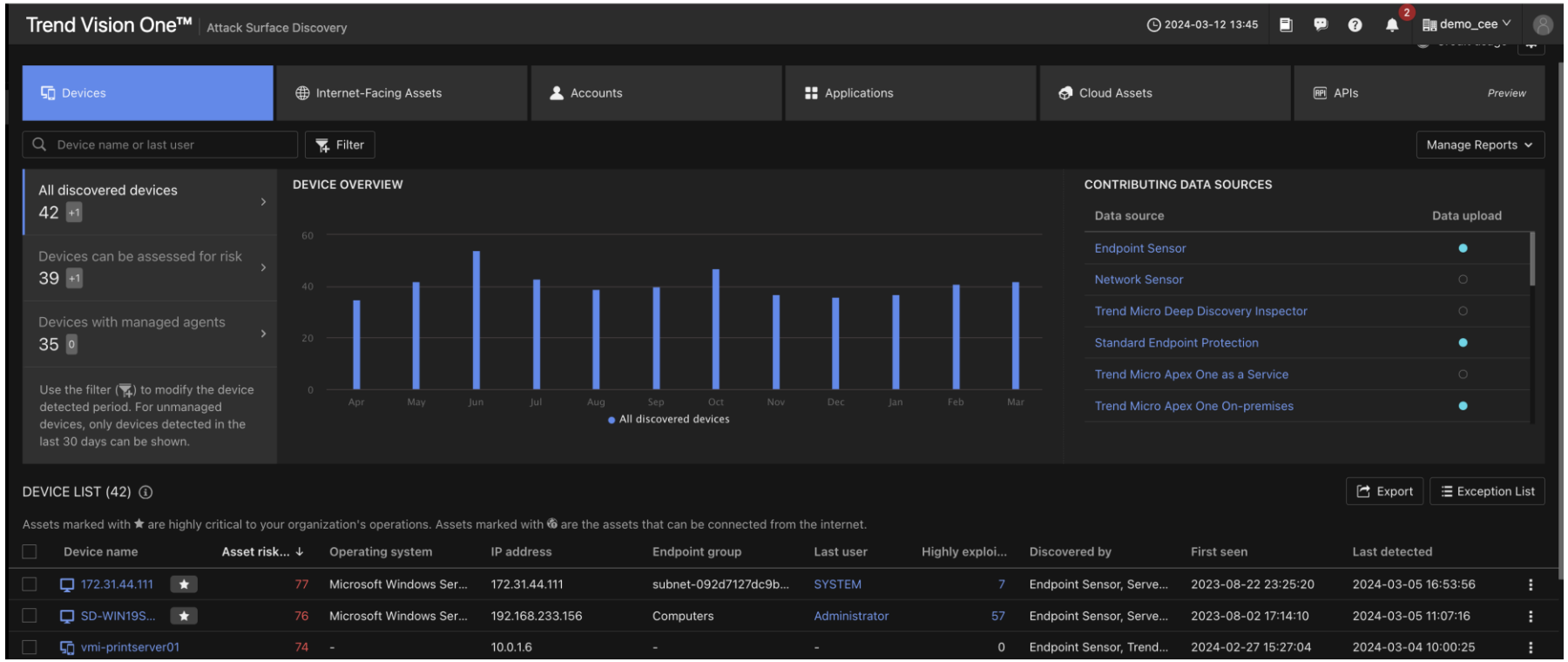
5. Inwentaryzacja zasobów

- Ciągła identyfikacja
- Krytyczność
- Dozwolone operacje
- Relacje i przepływ danych



6. Zmapowanie usług teleinformatycznych

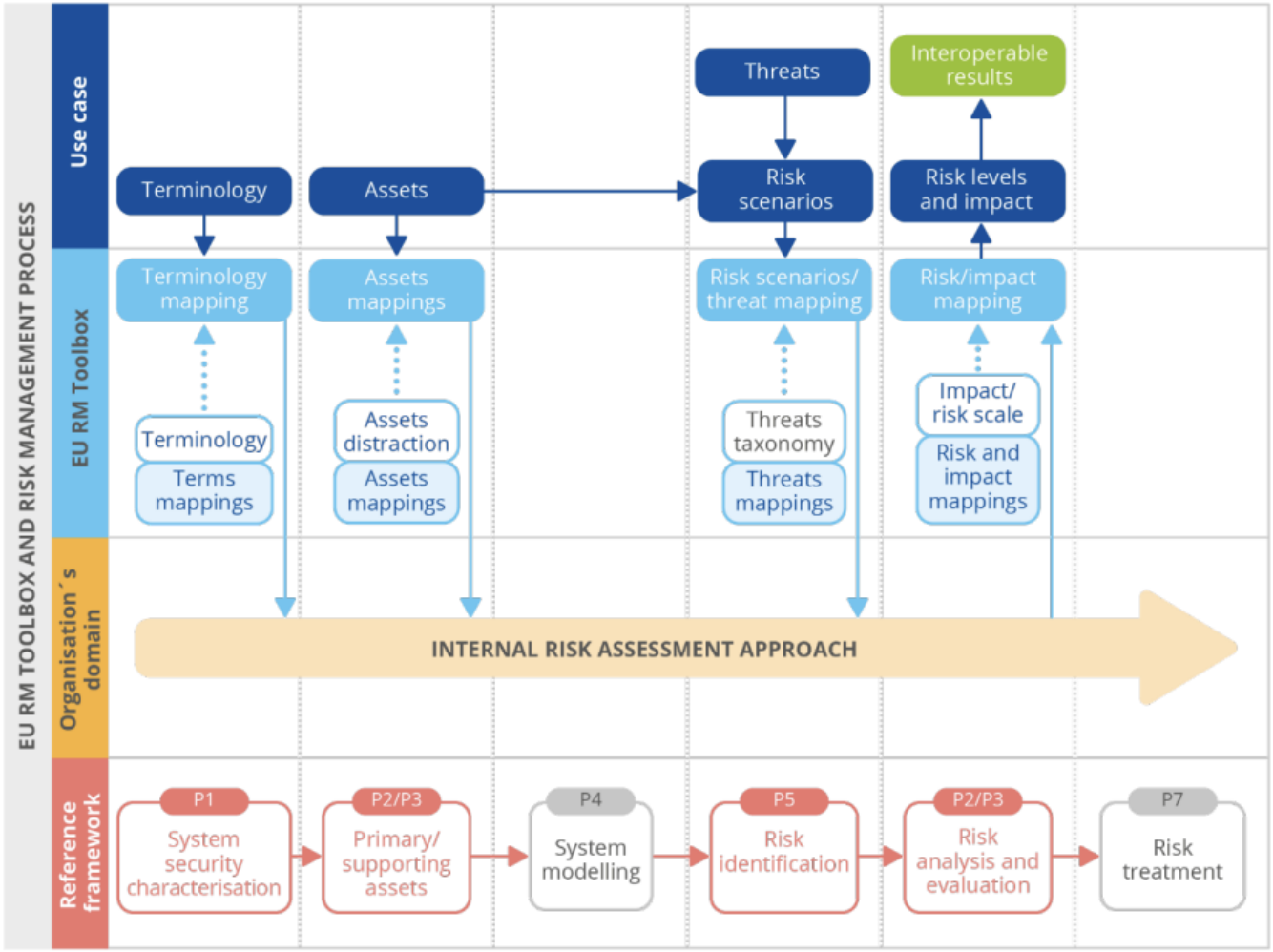
- Na zasoby
- Na procesy biznesowe
- Na dostawców
- Na RYZYKO



7. Zmapowanie dostawców usług

- Typ relacji
- Zakres realicji na poziomie systemów IT
- Komunikacja
- Analiza ryzyka
- Wpływ na organizację

ENISA toolbox



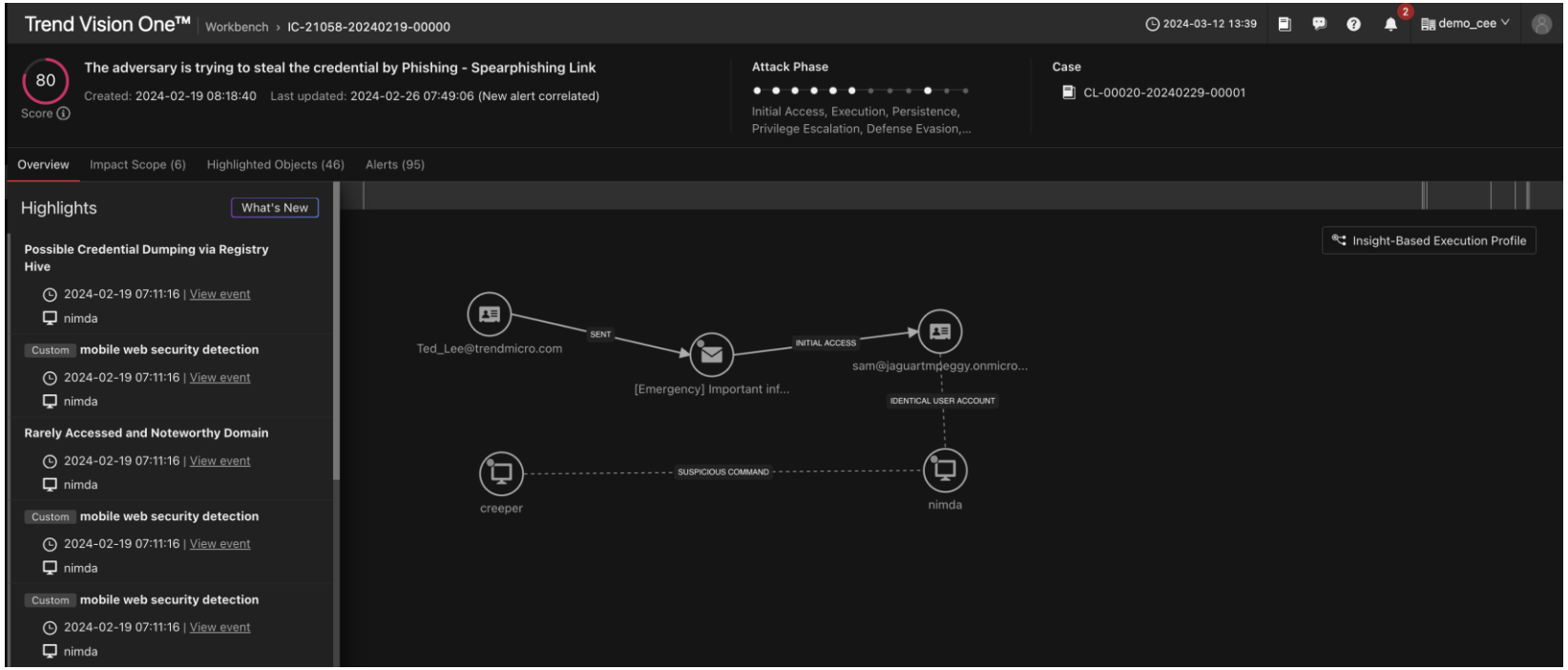
Source: "Interoperable EU Risk Management Toolbox", Luty 2023

8. Analiza i modyfikacja procesu zarządzania ryzykiem

- Policzalny
- Pozwalający na śledzenie trendów
- Ciągły
- Pokrywający możliwie całąorganizację
- Raportowany
- Komunikowany

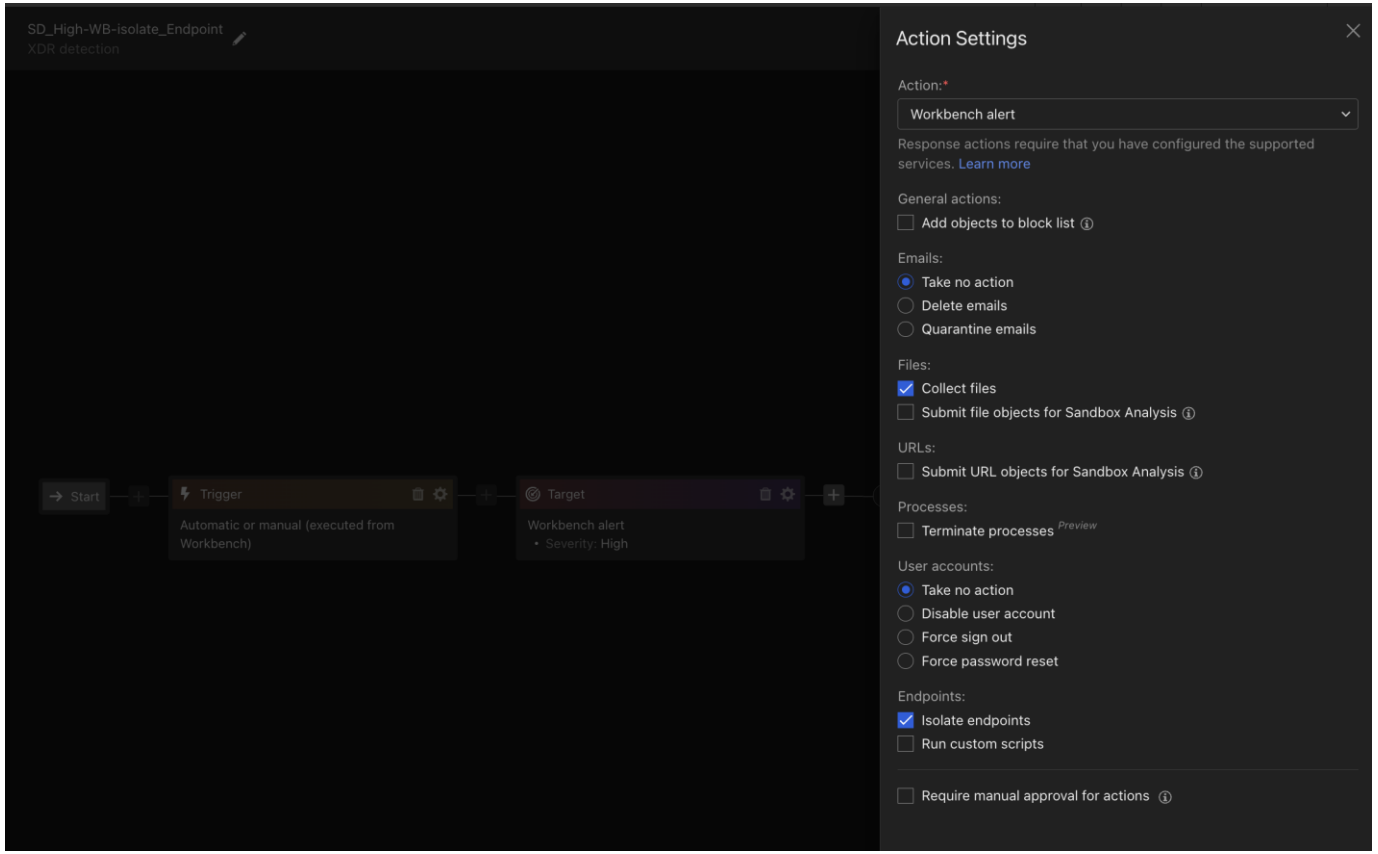
9. Przegląd i modyfikacja procesu zarzadzania incydentami

- Automatyzacja
- Konsolidacja
  - narzędzi
  - danych
- Ryzyko, kontekst i powiązania
- Eskalacja
- Raportowanie
  - 24h/72h/30 dni
  - Analiza przyczyn, skutku, przebiegu
  - Działania zaradcze/redukcja ryzyka
- Kompetencje/wiedza po stronie personelu
- Gotowość na wymianę informacji



10. Automatyzacja

- Raportowania
- Wymiany informacji o zagrożeniach
- Dystrybucji IoC
- Obsługi incydentów
- …
- Tam gdzie jest to możliwe



A na koniec….

Działania efektywne i zdroworozsądkowe

Zdefiniuj realne cele i priorytety

1. Quick Win
   - Telemetria
   - Managed Detection and Response
   - Procedury i scenariusze awaryjne
   - Zarządzanie Ryzykiem w oparciu o realne dane
2. Long-term projects
   - Zarządzanie zasobami
   - Cyber Defense Core Team
   - Centralna korelacja

Native Sensors

Identities | Devices | Email | Cloud Infra | Network | Cloud Apps

Threat Intelligence

Third Party Integrations
Asset Information | Detection Data

Third Party Intelligence
Curated Feeds | STIX/TAXII | MISP

Continuous Assessments

Policy Management

Risk Scoring

Identities 88 | Devices 15 | Cloud Apps 52

Zero Trust Secure Access

Zero Trust Network Access | Secure Web Gateway

Native Enforcement Points

Network | Devices | Cloud Apps | Email

Third Party Integrations
PEP | SOAR | Web Hook | API