



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 **evaluating 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.

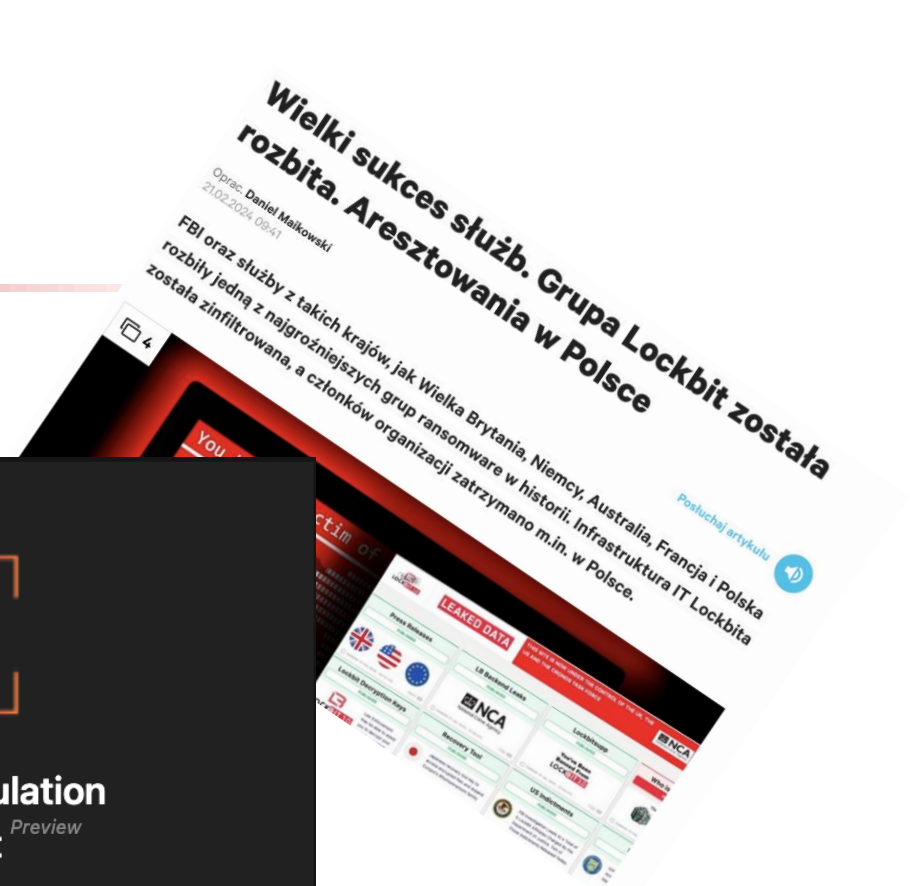
Źródło: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

1. Świadomość i edukacja

- Informacja Zarządcza
- Edukacja pracowników
- Dystrybucja informacji o zagrożeniach



The image displays a "Phishing Simulation Assessment" interface. At the top, there is an icon of a mail envelope with a hook, symbolizing phishing. Below the icon, the text reads "Phishing Simulation Assessment" with "Preview" in smaller text. A paragraph describes the purpose: "Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats." Below this, the status is "Assessment status: Ready". At the bottom, there is a large button labeled "Start Assessment".



2. Ustanowienie w organizacji ról i obowiązków

- Odpowiedzialność
- Zakres obowiązków
- Komunikacja

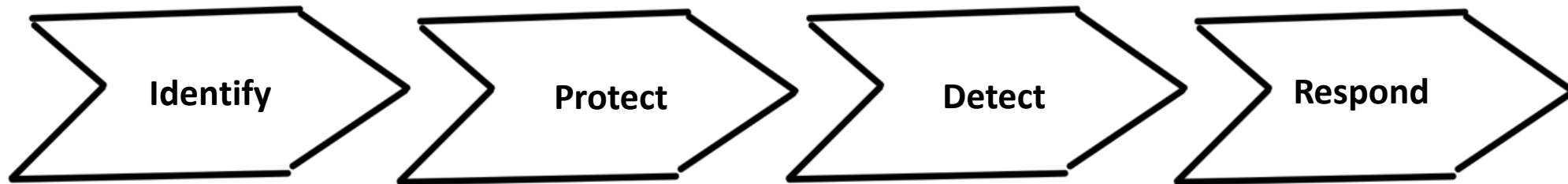


Zarządzanie Ryzykiem a odpowiedzialność

“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

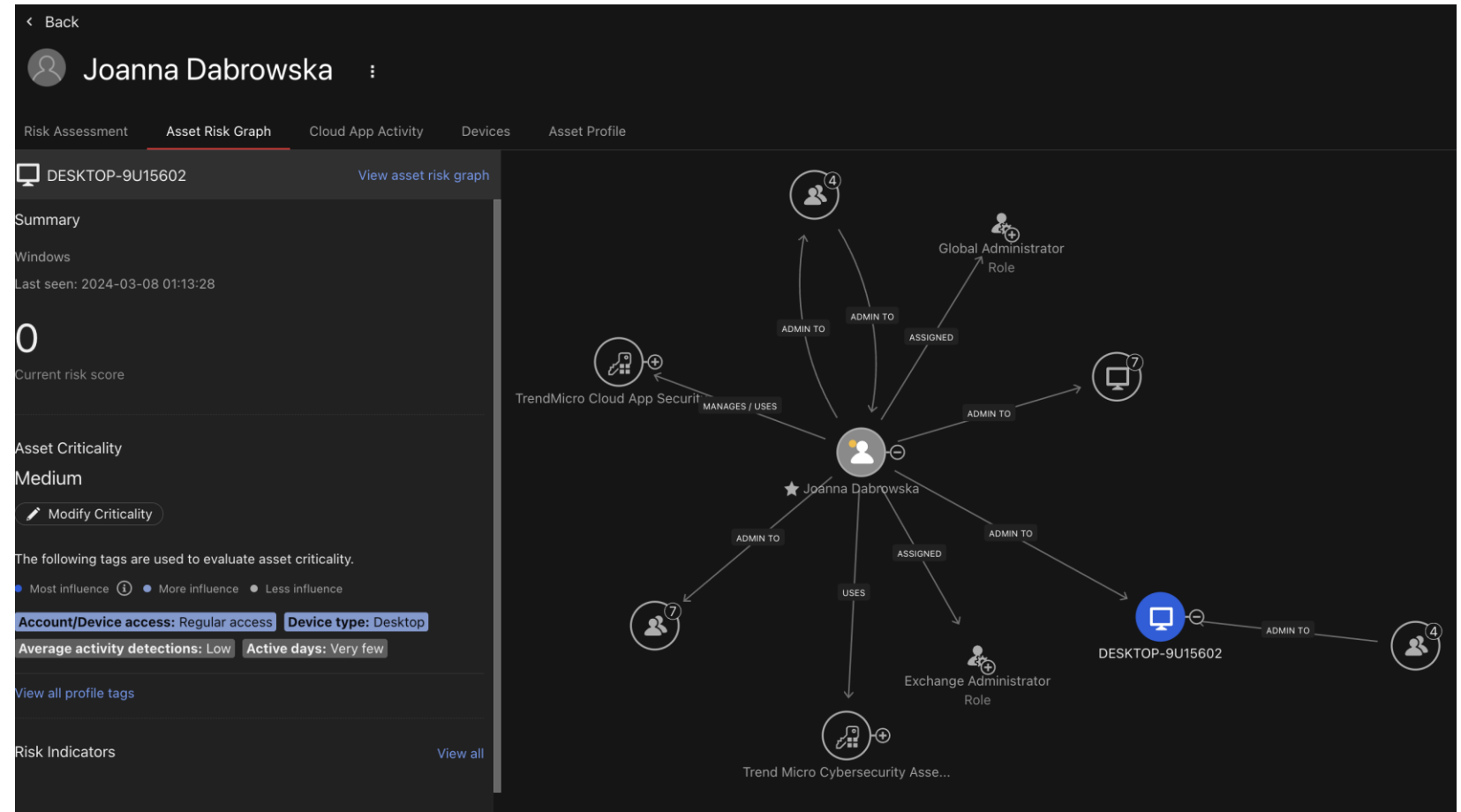
The image shows a screenshot of the Trend Vision One Campaign Intelligence interface. The main content is a report for 'Earth Preta', an APT group. The report includes details such as AKA (BRONZE PRESIDENT, HoneyMyte, Mustang Panda, Red Lich, RedDelta, TA416, TEMP.HEX), targeted countries (Australia, Bangladesh, Belgium, Bulgaria, Ethiopia, Ghana, Hong Kong, India, Japan, Korea), and targeted industries (Construction, Defence, Education, Energy, Financial Services, Government/Public Services, Healthcare). It also lists motivation (Information theft and espionage) and the last update date (2024-02-22 20:26:41). Below the report details is a table of intelligence data reports.

Report name	Source	Last updated ↓
IOC Update for Earth Preta - 2024-03-11	Trend Micro	2024-03-12 04:27:55
Earth Preta Campaign Uses DOPLUGS to Target Asia	Security vendors	2024-02-25 09:25:53
Earth Preta Campaign Uses DOPLUGS to Target Asia	Security vendors	2024-02-20 20:25:26
Cyberespionage Attacks Against Southeast Asian Government Link...	Trend Micro	2023-10-17 04:26:27
Cyberespionage Attacks Against Southeast Asian Government Link...	Security vendors	2023-09-27 21:26:45

Overlaid on the screenshot is a white box containing text from a consultation notice: 'CONSULTATION | Publication 13 February 2024', 'Evaluation of the Cybersecurity Act', 'Opening: 13 February 2024', 'Closing: 05 March 2024', and 'The Commission has started the evaluation of the Cybersecurity Act(CSA), Regulation (EU) 2019/881), according to art. 67 of this regulation.'

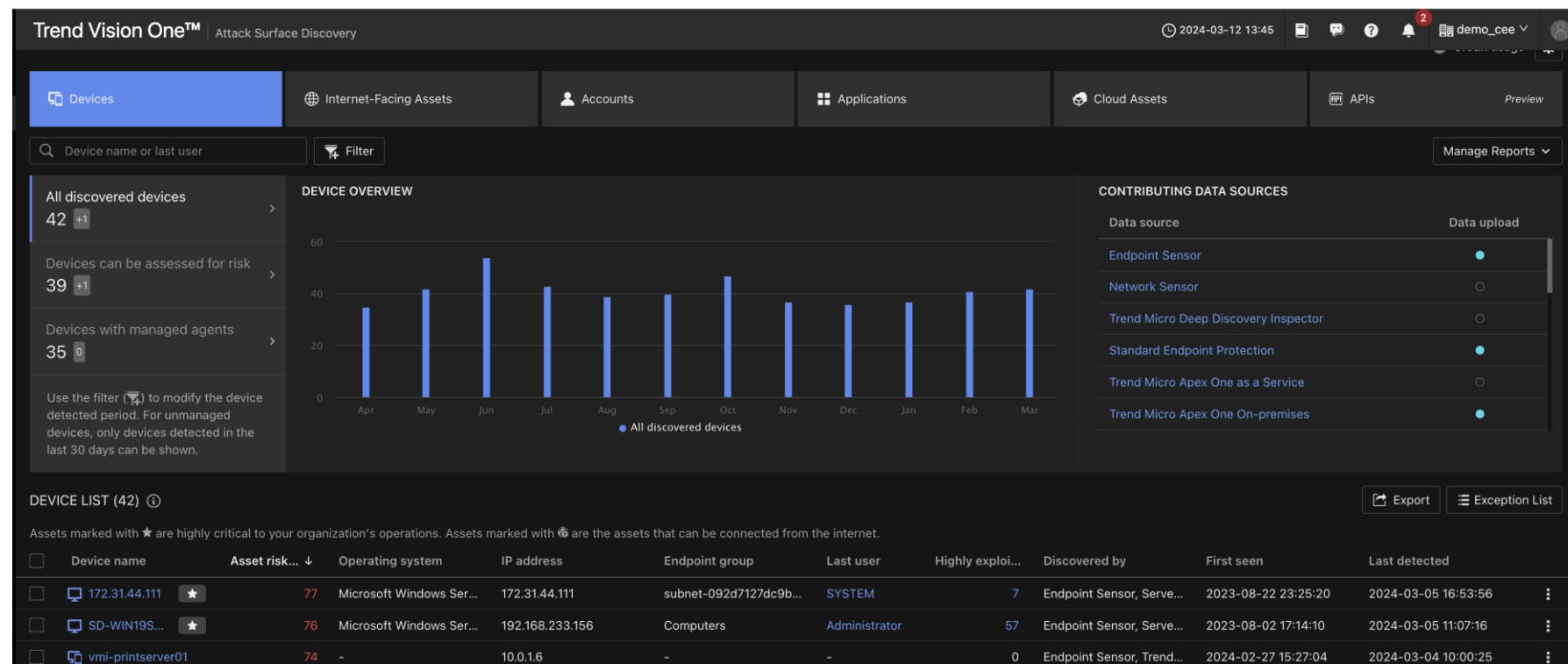
5. Inwentaryzacja zasobów

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



6. Zmapowanie usług teleinformatycznych

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

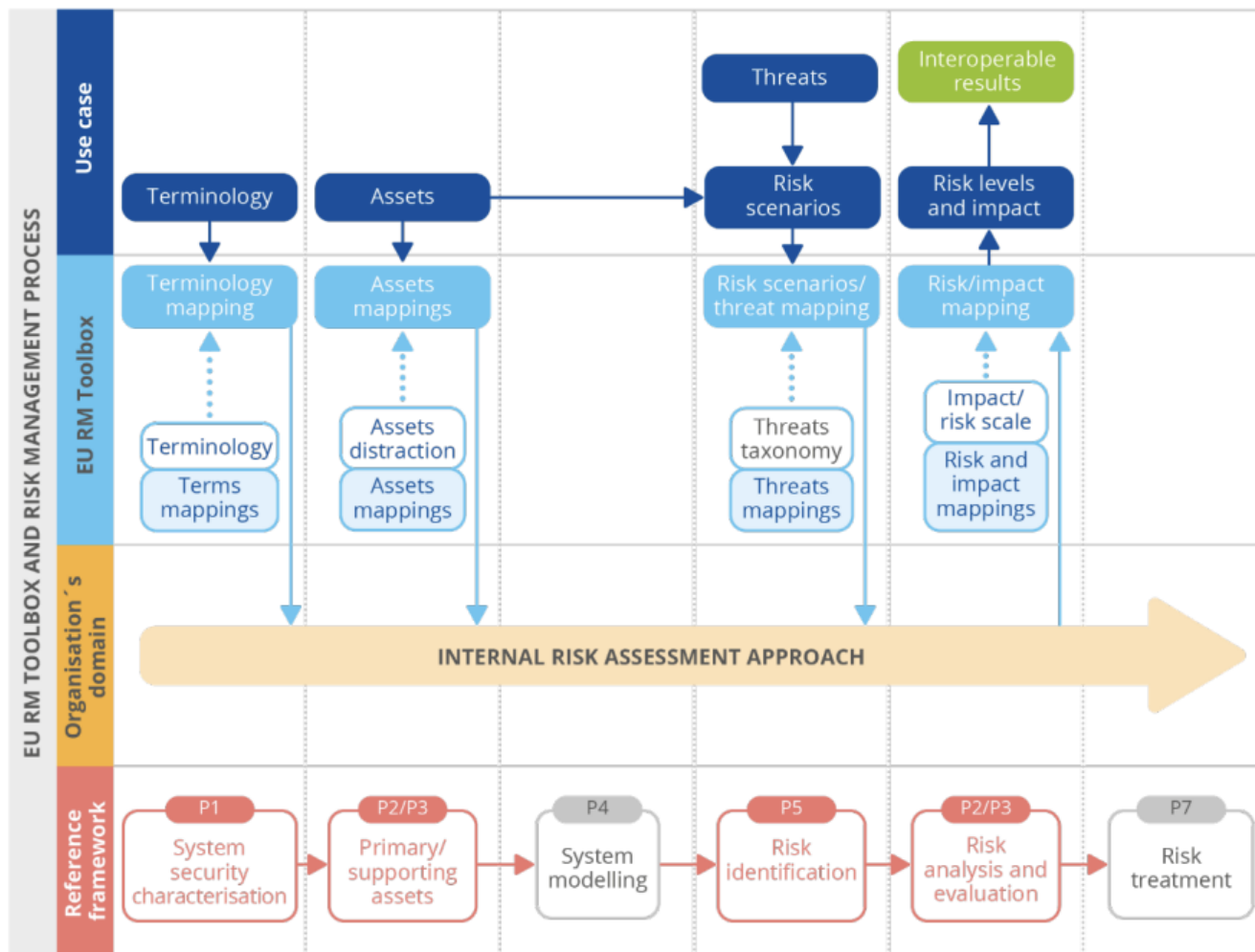


7. Zmapowanie dostawców usług

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



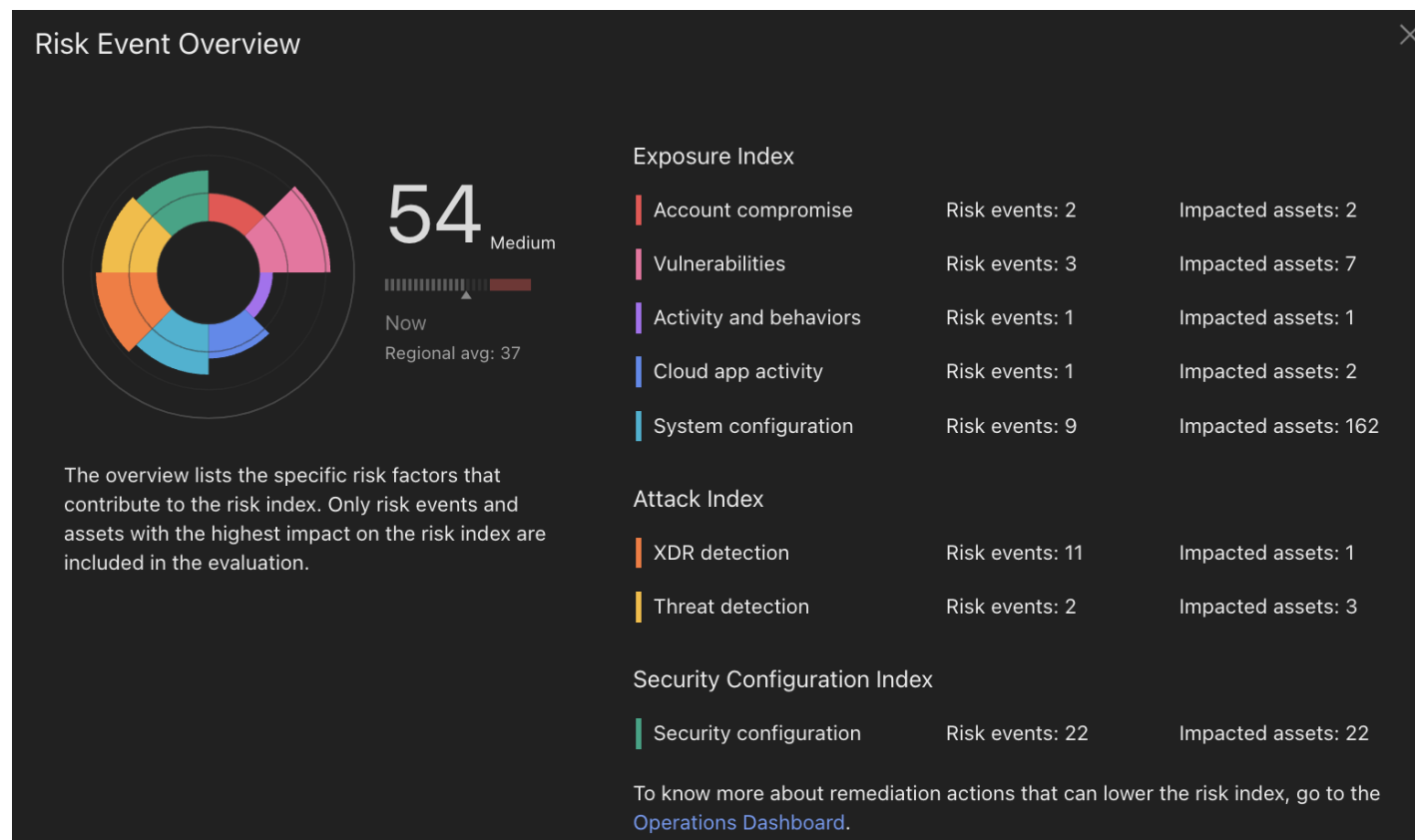
ENISA toolbox



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

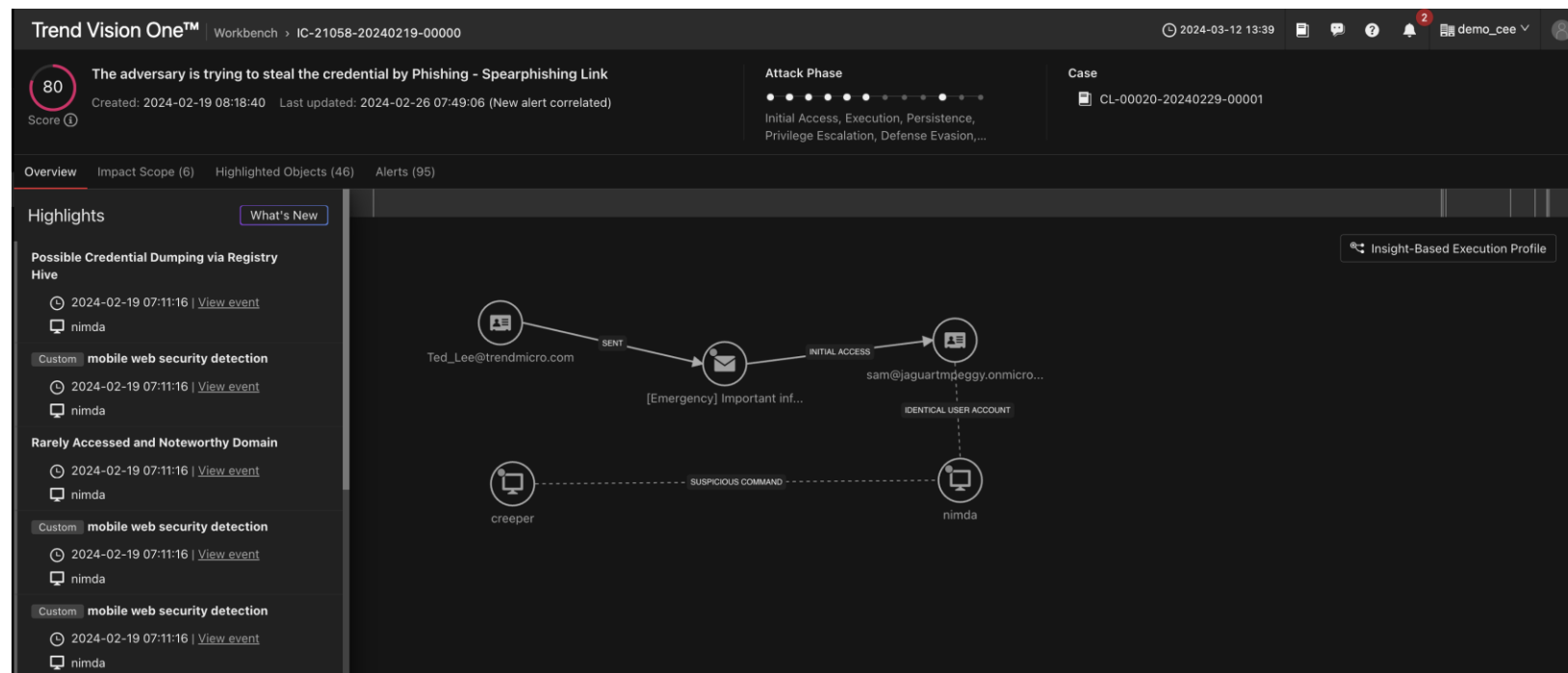
8. Analiza i modyfikacja procesu zarządzania ryzykiem

- Policzalny
- Pozwalający na śledzenie trendów
- Ciągły
- Pokrywający możliwie całą organizację
- Raportowany
- Komunikowany



9. Przegląd i modyfikacja procesu zarządzania incydentami

- Automatykacja
- 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

The screenshot displays a workflow automation interface. The main workspace shows a sequence of steps: 'Start' (with a right arrow), 'Trigger' (with a lightning bolt icon), and 'Target' (with a target icon). The 'Trigger' step is configured with 'Automatic or manual (executed from Workbench)'. The 'Target' step is configured with 'Workbench alert' and 'Severity: High'. To the right, the 'Action Settings' panel is open, showing a dropdown menu for 'Action:' set to 'Workbench alert'. Below this, there are several sections of settings, each with a list of options and checkboxes:

- General actions:** Add objects to block list [①](#)
- Emails:** Take no action, Delete emails, Quarantine emails
- Files:** Collect files, Submit file objects for Sandbox Analysis [①](#)
- URLs:** Submit URL objects for Sandbox Analysis [①](#)
- Processes:** Terminate processes *Preview*
- User accounts:** Take no action, Disable user account, Force sign out, Force password reset
- Endpoints:** Isolate endpoints, Run custom scripts
- Require manual approval for actions [①](#)

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



Devices



Cloud Apps

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