IX FORUM KIEROWNIKÓW IT W ADMINISTRACJI

22–24.04.2024

ZAKOPANE
BACHLEDA HOTEL KASPROWY

forum.itwadministracji.pl

Narzędzia w skutecznym zarządzaniu cyberbezpieczeństwem

Prowadzący: Artur Cieślik
MBA, IRCA lead auditor ISO/IEC 27001 ISO 22301,CISA
Ekspert ACSEC Sp. z o.o.
redaktor naczelny „IT Professional”
artur.cieslik@politykabezpieczenstwa.com.pl

Artur Cieślik
politykabezpieczenstwa.com.pl

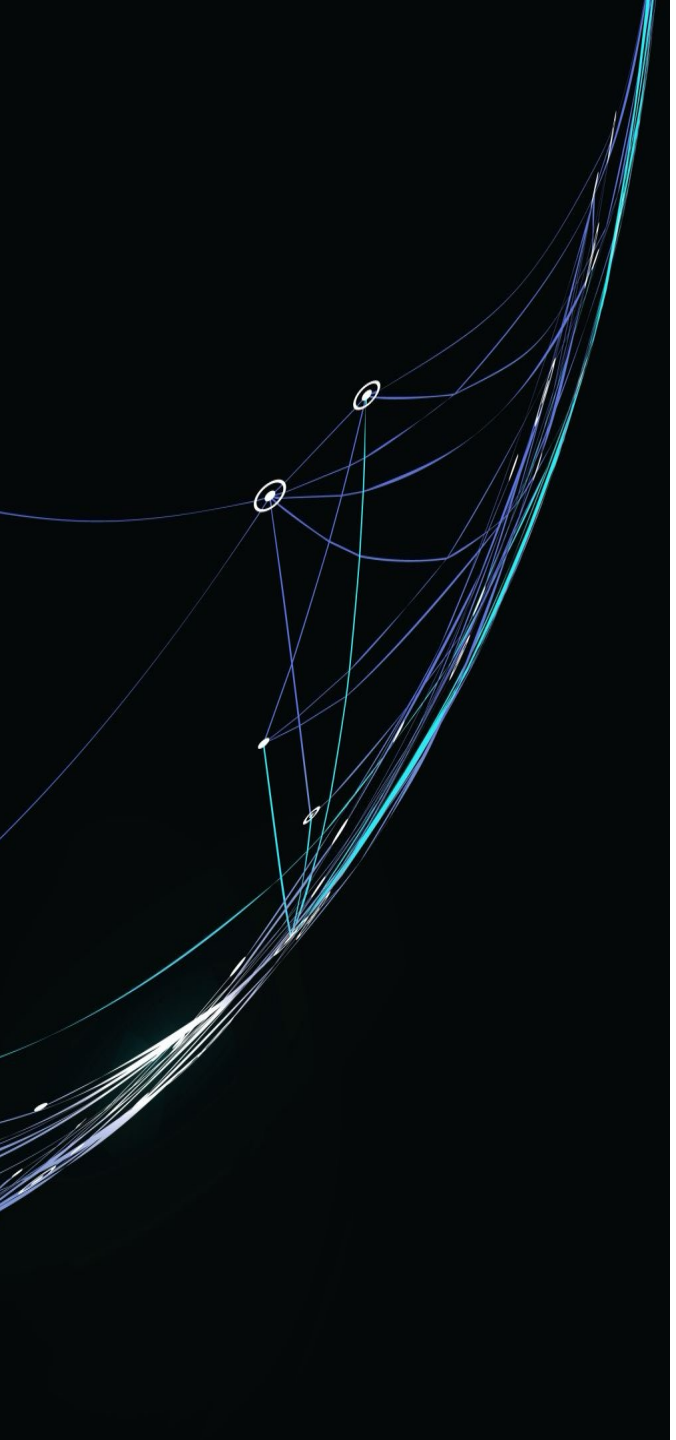
- **Założyciel i główny ekspert ACSEC Sp. z o.o.:**
- Audytor wiodący normy ISO/IEC 27001 IRCA Certified Lead Auditor (nr w rejestrze: 6035034).
- Audytor wiodący normy ISO/IEC 22301 uzyskany zgodnie z IRCA.
- Certified Information Systems Auditor (CISA)
- Członek SABI – Stowarzyszenia Inspektorów Ochrony Danych.
- Członek IIA – Instytutu Audytorów Wewnętrznych IIA Polska
- Redaktor naczelny miesięcznika „IT Professional”.
- Członek rady programowej „ABI Expert”.
- Szkolenia i wykłady: Akademia Leona Koźmińskiego, Politechnika Wrocławska, Uniwersytet Ekonomiczny we Wrocławiu, Uniwersytet im. Kardynała Wyszyńskiego „IT Professional Academy” „Informacja Publiczna”, „Forbes Academy”, „IT w Administracji”.

Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Przy uwzględnieniu najnowszego **stanu wiedzy** oraz, w stosownych przypadkach, odpowiednich **norm europejskich i międzynarodowych**, a także **kosztów** wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych **odpowiedni do istniejącego ryzyka**.
- Oceniając proporcjonalność tych środków, należycie uwzględnia się **stopień narażenia** podmiotu na ryzyko, **wielkość podmiotu** i **prawdopodobieństwo** wystąpienia incydentów oraz ich dotkliwość, w tym ich **skutki** społeczne i gospodarcze

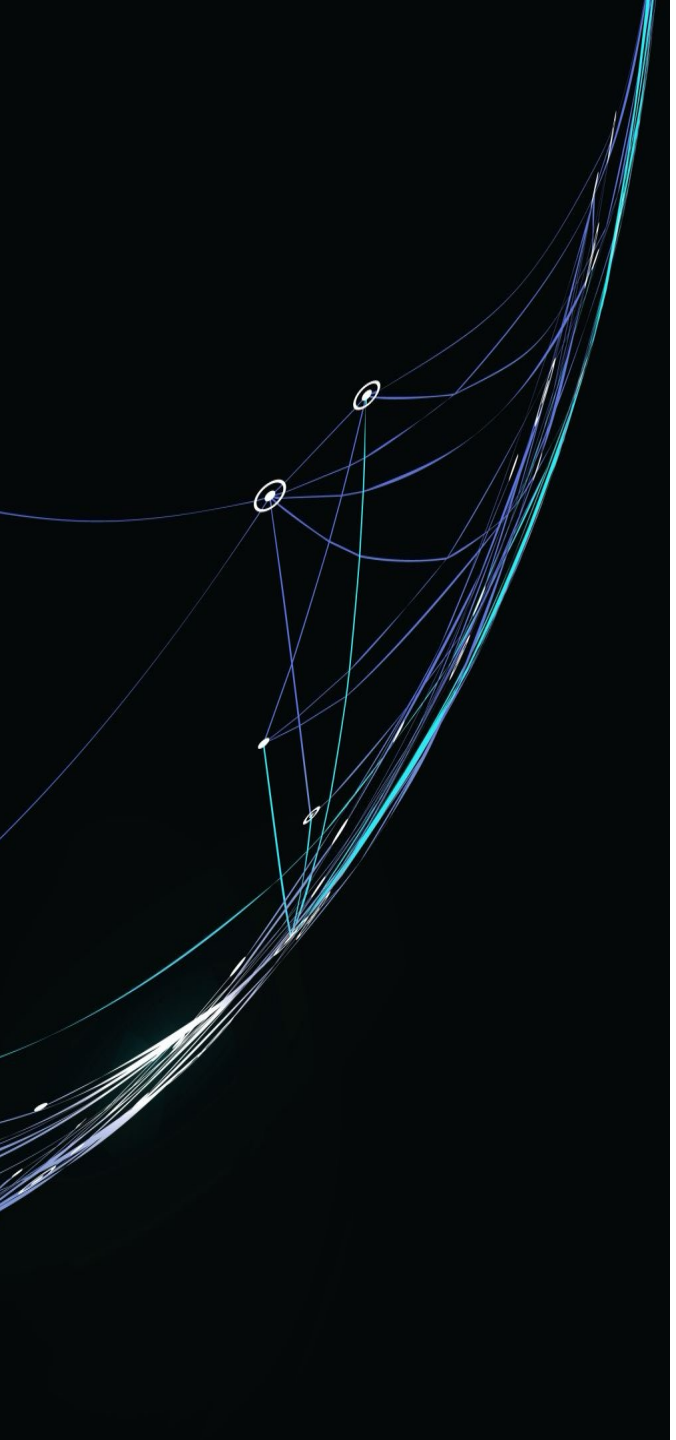
Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Przy ustalaniu środków zarządzania ryzykiem w cyberbezpieczeństwie:
  - Identyfikujemy wszystkie zagrożenia(!)
  - Obejmujemy ochroną przed incydentami sieci i systemy informatyczne;
  - Obejmujemy ochroną przed incydentami środowisko fizyczne tych systemów.



Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Środki zarządzania ryzykiem w cyberbezpieczeństwie obejmują co najmniej następujące elementy:
  - **politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;**
  - obsługę incydentu;
  - ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;
  - bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
  - bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;



Środki zarządzania ryzykiem w cyberbezpieczeństwie

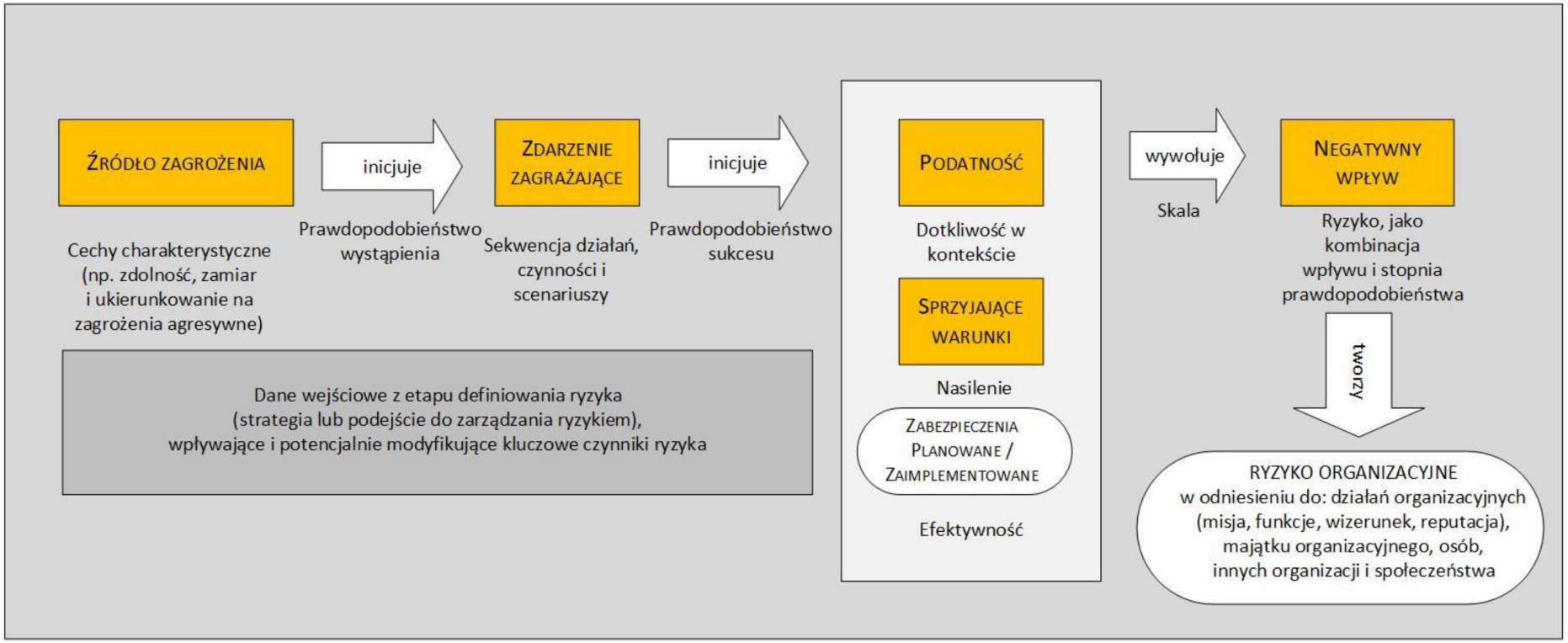
- Środki zarządzania ryzykiem w cyberbezpieczeństwie obejmują co najmniej następujące elementy:
  - **polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;**
  - podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;
  - polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
  - bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
  - w stosownych przypadkach - stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Szacowanie ryzyka

- NIST SP 800-30 Przewodnik dotyczący postępowania w zakresie szacowania ryzyka.
- ISO/IEC 27005 to norma mówiąca o zarządzaniu ryzykiem i aktywami
- Niezależnie od wyboru standardu i metodologii szacowania ryzyka, należy wziąć pod uwagę ryzyka w szczególności:
  - związane z utrzymaniem i bezpieczną eksploatacją systemu;
  - związane z bezpieczeństwem fizycznym i środowiskowym;
  - dotyczące ciągłości dostaw usług wspomagających systemy podmiotu kluczowego i ważnego

Szacowanie ryzyka

- NIST SP 800-30 Przewodnik dotyczący postępowania w zakresie szacowania ryzyka.



Szacowanie ryzyka

- NIST SP 800-30 - proces szacowania ryzyka.
  - Etap 1. Przygotowanie do szacowania ryzyka.
  - Etap 2. Ocena postępowania – identyfikacja źródeł zagrożeń, podatności, prawdopodobieństwa oraz wpływu, ustalenie ryzyka, określenie wpływu na **poufność, integralność oraz dostępność, uwzględnienie atrybutów cyberbezpieczeństwa**.
  - Etap 3. Przekazywanie wyników.
  - Etap 4. Utrzymanie wyników szacowania.

Szacowanie ryzyka

- Atrybuty cyberbezpieczeństwa
  - **Identify –** uzyskanie informacji organizacyjnych, aby zarządzać ryzykiem cyberbezpieczeństwa
  - **Protect –** opracowanie i uruchomienie odpowiednich zabezpieczeń prewencyjnych
  - **Detect –** opracowanie i uruchomienie działań niezbędnych do zidentyfikowania wystąpienia zdarzenia cyberbezpieczeństwa
  - **Respond –** opracowanie i wdrożenie działań niezbędnych w przypadku wykrycia zdarzenia cyberbezpieczeństwa
  - **Recover –** opracowanie i wdrożenie działań w celu utrzymania procedur i planów niezbędnych do przywrócenia uszkodzonych systemów, zasobów i danych w wyniku zdarzenia cyberbezpieczeństwa

- **Preventive** – zabezpieczenie, które ma na celu zapobieganie wystąpieniu incydentu bezpieczeństwa informacji.
- **Detective –** zabezpieczenie stosowane w przypadku wystąpienia incydentu bezpieczeństwa informacji.
- **Corrective** – zabezpieczenie działające po wystąpieniu incydentu bezpieczeństwa informacji.

Szacowanie ryzyka

- Przeglądanie zabezpieczeń według innych atrybutów.
  - **Zabezpieczenia** mogą być **zastąpione.**
  - Zabezpieczenia mogą be wybrane ze względu na **posiadanie określonych atrybutów**. Jeśli mamy ograniczony budżet, kosztowne zabezpieczenia mogą zostać odrzucone i zastąpione przez kilka innych o podobnych atrybutach.

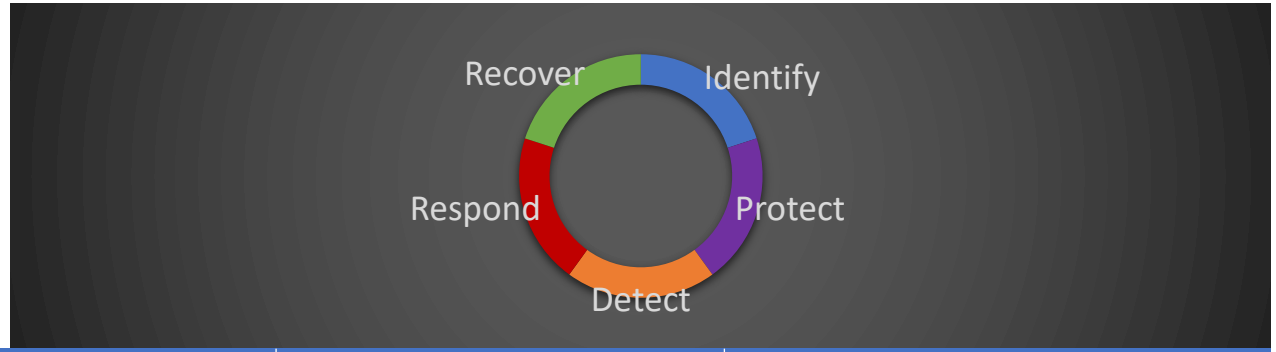
Szacowanie ryzyka

- **Wybranie zabezpieczeń w celu uzyskania właściwej skuteczności**.
  - Atrybuty użyte w ISO/IEC 27002:2022 (#Preventive, #Detective, #Corrective, #Identify, #Protect, #Detect, #Respond, #Recover) mogą być używane jako środek do sprawdzenia potencjalnych luk w strukturze zabezpieczeń.
  - **Przykład.** mogą istnieć odpowiednie środki w celu wykrycia zdarzeń związanych z bezpieczeństwem informacji, ale niewystarczające środki, aby zapobiegać incydentom związanym z bezpieczeństwem informacji.
  - **Przykład**. Przewaga środków proceduralnych z niewielką liczbą zabezpieczeń technologicznych może wskazywać na niską skuteczność zastosowanej struktury zabezpieczeń.

Szacowanie ryzyka

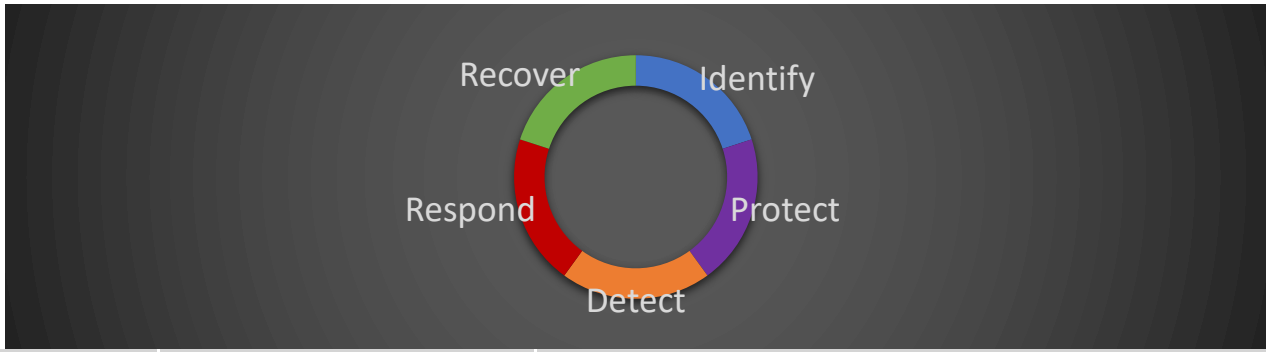
- **Wybranie zabezpieczeń w celu uzyskania właściwej skuteczności**.
  - Atrybuty użyte w ISO/IEC 27002:2022 (#Preventive, #Detective, #Corrective, #Identify, #Protect, #Detect, #Respond, #Recover) mogą być używane jako środek do sprawdzenia potencjalnych luk w strukturze zabezpieczeń.
  - **Przykład.** Wdrożono narzędzia w celu zautomatyzowanej reakcji na znane zagrożenia, jednak cześć zdarzeń pozostaje niewykryta z uwagi na brak reagowania na alerty i brak wglądu w logi zdarzeń systemów XDR czy SIEM.

Narzędzia cyberbezpieczeństwa



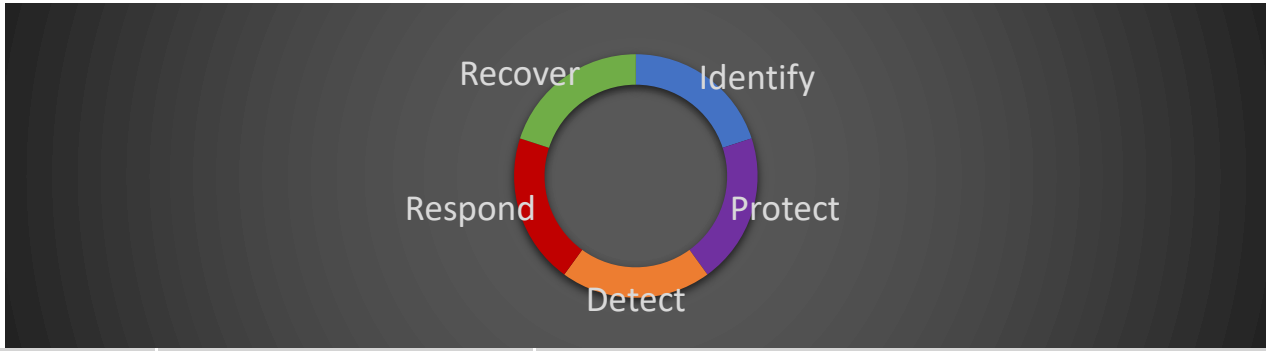
ISO/IEC 27002 control identifier	Control name	Information security properties	Cybersecurity concepts
5.15	Access control	#Confidentiality #Integrity #Availability	#Protect
5.18	Access rights	#Confidentiality #Integrity #Availability	#Protect
5.24	Information security incident management planning and preparation	#Confidentiality #Integrity #Availability	#Respond #Recover
5.25	Assessment and decision on information security events	#Confidentiality #Integrity #Availability	#Detect #Respond
5.26	Response to information security incidents	#Confidentiality #Integrity #Availability	#Respond #Recover
5.32	Intellectual property rights	#Confidentiality #Integrity #Availability	#Identify
6.3	Information security awareness, education and training	#Confidentiality #Integrity #Availability	#Protect
6.7	Remote working	#Confidentiality #Integrity #Availability	#Protect
7.9	Security of assets off-premises	#Confidentiality #Integrity #Availability	#Protect
8.2	Privileged access rights	#Confidentiality #Integrity #Availability	#Protect
8.7	Protection against malware	#Confidentiality #Integrity #Availability	#Protect #Detect
8.8	Management	#Confidentiality #Integrity #Availability	#Identify #Protect
8.12	Data leakage prevention	#Confidentiality	#Protect #Detect
8.15	Logging	#Confidentiality #Integrity #Availability	#Detect
8.16	Monitoring activities	#Confidentiality #Integrity #Availability	#Detect #Respond
8.18	Use of privileged utility programs	#Confidentiality #Integrity #Availability	#Protect
8.19	Installation of software on operational systems	#Confidentiality #Integrity #Availability	#Protect
8.20	Networks security	#Confidentiality #Integrity #Availability	#Protect #Detect
8.22	Segregation of networks	#Confidentiality #Integrity #Availability	#Protect
8.23	Web filtering	#Confidentiality #Integrity #Availability	#Protect
8.26	Application security requirements	#Confidentiality #Integrity #Availability	#Protect

Narzędzia cyberbezpieczeństwa



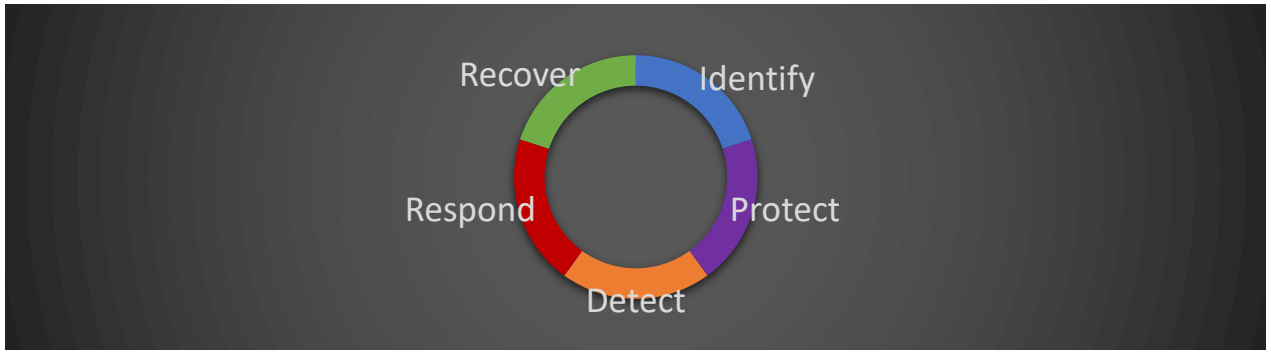
Nazwa systemu	Pkt. ISO/IEC 27001 Zał. A	NIST CSF	Opis ISO/IEC 27001 Zał. A
EDR (Endpoint Detection and Response)	8.7	#Protect #Detect	Protection against malware
	5.26	#Respond #Recover	Response to information security incidents
NDR (Network Detection and Response)	8.20	#Protect #Detect	Networks security
	5.26	#Respond #Recover	Response to information security incidents
XDR (Extended Detection and Response)	8.7	#Protect #Detect	Protection against malware
	5.26	#Respond #Recover	Response to information security incidents
	8.20	#Protect #Detect	Networks security
NAC (Network Access Control)	8.20	#Protect #Detect	Networks security
	8.22	#Protect	Segregation of networks
UEBA (User Entity Behavior Analytics)	8.16	#Detect #Respond	
SIEM (Security Information and Event Management)	8.15	#Detect	Logging
	5.26	#Respond #Recover	Response to information security incidents
	8.16	#Detect #Respond	Monitoring activities
AV (Antivirus)	8.7	#Protect #Detect	Protection against malware
PAM (Privileged Access Management)	8.18	#Protect	Use of privileged utility programs
	8.2	#Protect	Privileged access rights
IAM (Identity and Access Management)	5.15	#Protect	Access control
	5.18	#Protect	Access rights
DLP (Data Loss Prevention)	8.12	#Protect #Detect	Data leakage prevention
	5.32	#Identify	Intellectual property rights

Narzędzia cyberbezpieczeństwa



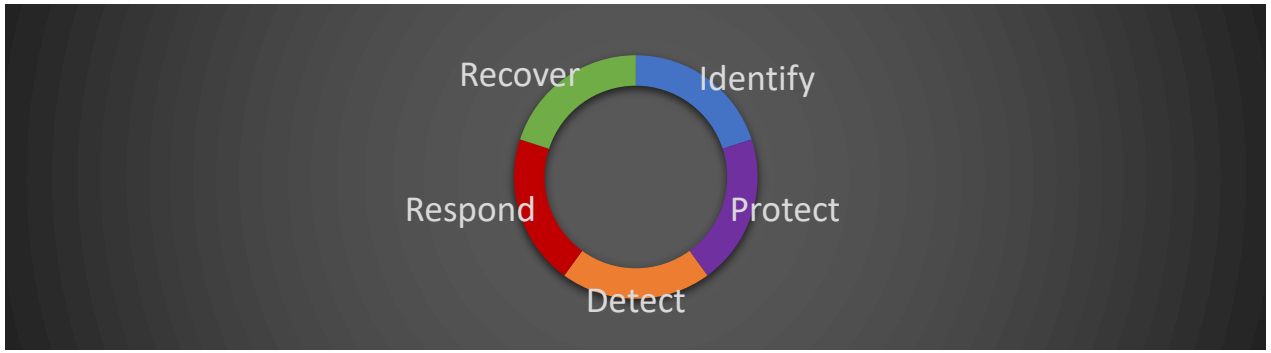
Nazwa systemu	Pkt. ISO/IEC 27001 Zał. A	NIST CSF	Opis ISO/IEC 27001 Zał. A
VPN (Virtual Private Network)	6.7	#Protect	Remote working
WAF (Web Application Firewall)	8.26	#Protect	Application security requirements
Sandbox	8.7	#Protect #Detect	Protection against malware
MDM (Mobile Device Management)	8.12	#Protect #Detect	Data leakage prevention
	7.9	#Protect	Security of assets off-premises
	8.7	#Protect #Detect	Protection against malware
SOAR (Security Orchestration Automation and Response)	8.7	#Protect #Detect	Protection against malware
	8.26	#Protect	Response to information security incidents
	5.7	#Identify #Detect #Respond	Threat intelligence
Vulnerability scanner	8.8	#Identify #Protect	Vulnerability management
Patch Management System	8.8	#Identify #Protect	Patch management
EMS (Endpoint Management System)	8.19	#Protect	Installation of software on operational systems
	5.32	#Identify	Intellectual property rights
Platforma szkoleniowa	6.3	#Protect	Information security awareness, education and training
TIP	5.7	#Identify #Detect #Respond	Threat intelligence
VPN (Virtual Private Network)	6.7	#Protect	Remote working
NGFW (Next-Generation Firewall)	8.22	#Protect	Segregation of networks
	8.23	#Protect	Web filtering
	8.32	#Protect	Change management
	5.23	#Protect	Information security for use of cloud services

Środki bezpieczeństwa



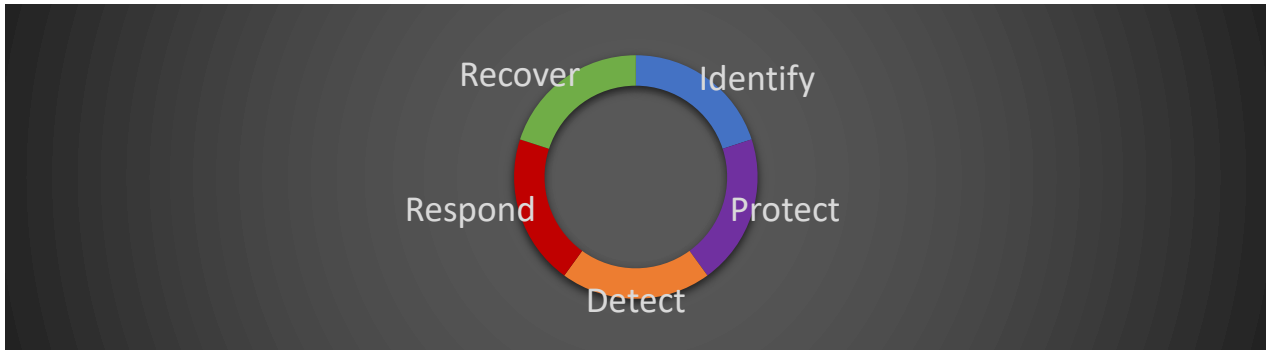
- **EDR (Endpoint Detection and Response)**. Narzędzie do wykrywania i reagowania w endpointach.
  - **Monitorowanie endpointów**. Ciągłe obserwowanie aktywności na urządzeniach końcowych w poszukiwaniu oznak kompromitacji.
  - **Analiza zachowań**. Użycie analizy behawioralnej do wykrywania nietypowych zachowań.
  - **Izolacja urządzeń**. Możliwość szybkiego izolowania urządzenia od reszty sieci w przypadku wykrycia infekcji.
  - **Remediacja**. Automatyczne lub manualne działania mające na celu usunięcie zagrożeń i przywrócenie normalnego funkcjonowania urządzeń.
  - **Automatyzacja odpowiedzi**. Może automatycznie reagować na wykryte zagrożenia, izolując zainfekowane urządzenia, blokując szkodliwy ruch lub uruchamiając procedury naprawcze.

Środki bezpieczeństwa



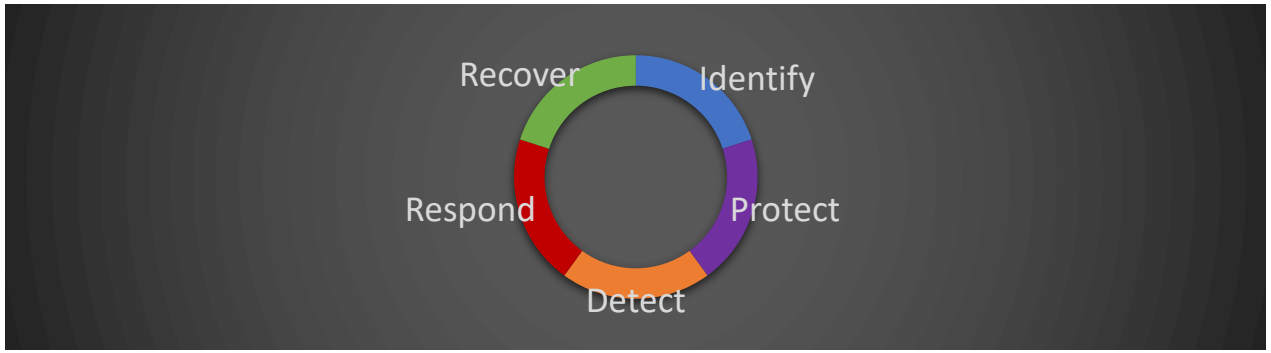
- **NDR (Network Detection and Response)**. Narzędzie do wykrywania i reagowania na zagrożenia sieciowe.
  - **Skanowanie ruchu w czasie rzeczywistym**. NDR ciągle monitoruje ruch sieciowy i identyfikuje wzorce lub aktywności, które mogą wskazywać na potencjalne zagrożenia lub ataki.
  - **Zaawansowane techniki wykrywania**. Wykorzystuje metody oparte na sygnaturach, analizie anomalii oraz zachowaniach.
  - **Analiza zachowań**. Analizuje zachowania w sieci, aby wykryć anomalie, które mogą ujawniać skomplikowane ataki, takie jak lateral traffic, exfiltracja danych czy ransomware.
  - **Automatyzacja odpowiedzi**. Może automatycznie reagować na wykryte zagrożenia np. poprzez izolację urządzenia oraz blokadę ruchu sieciowego.

Środki bezpieczeństwa



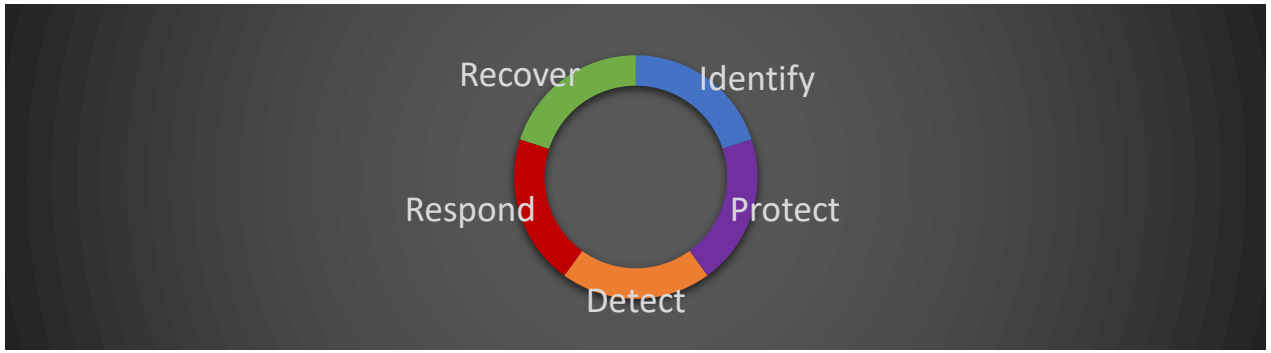
- **XDR (Extended Detection and Response)**. Narzędzie łączące wykrywanie i reakcję na zagrożenia.
  - **Integracja zabezpieczeń**. Łączy dane z różnych narzędzi bezpieczeństwa: antywirus, firewall, EDR, NDR.
  - **Automatyzacja odpowiedzi**. Automatycznie reaguje na wykryte zagrożenia.
  - **Analiza ruchu w sieci**. Zapewnia kompleksowy widok na działania w sieci.
  - **Zaawansowana analiza**. Wykorzystuje zaawansowane techniki analizy danych np. uczenie maszynowe, przez co umożliwia na identyfikację skomplikowanych ataków.
  - **Automatyzacja odpowiedzi**. Może automatycznie reagować na wykryte zagrożenia, izolując zainfekowane urządzenia, blokując szkodliwy ruch lub uruchamiając procedury naprawcze.

Środki bezpieczeństwa



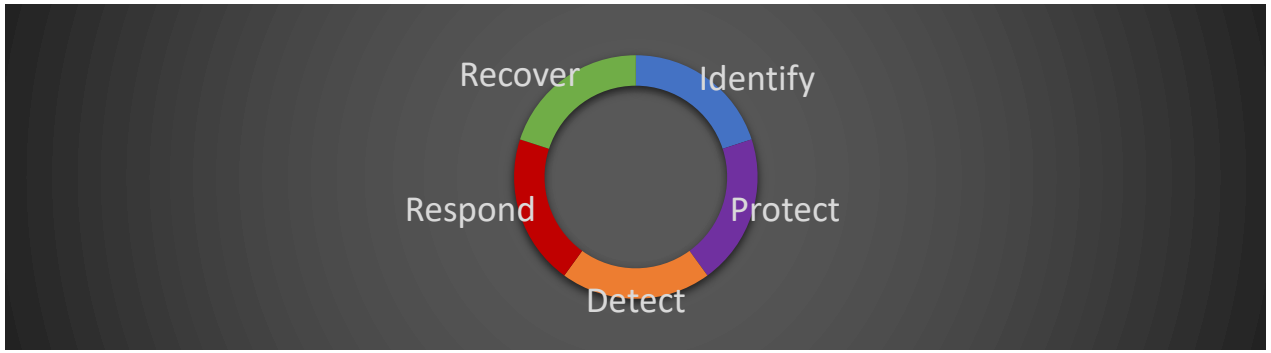
- **SIEM (Security Information and Event Management)**. Narzędzie do wykrywania i reagowania na zagrożenia sieciowe.
  - **Agregacja danych**. Zbiera dane z różnych źródeł w infrastrukturze IT.
  - **Analiza w czasie rzeczywistym**. Monitoruje aktywność w sieci w czasie rzeczywistym i umożliwia szybką detekcję anomalii.
  - **Korelacja zdarzeń**. Łączy informacje z różnych systemów.
  - **Alerty i powiadomienia**. Automatycznie generuje alerty w przypadku wykrycia podejrzanej aktywności.
  - **Raportowanie i audyt**. Zapewnia szczegółowe raporty dotyczące zdarzeń bezpieczeństwa.

Środki bezpieczeństwa



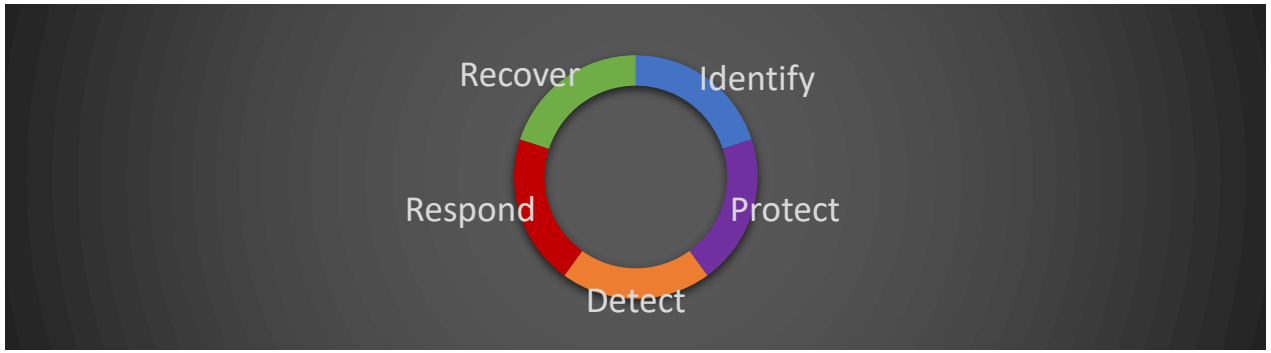
- **EDR** zapewnia wysoki poziom szczegółowości, ale nie obejmuje niezarządzanych punktów końcowych lub punktów końcowych, które nie mogą uruchomić agenta (np. drukarki, bezserwerowe środowiska chmurowe).
- **NDR** ma bardzo szeroki wgląd w ruch sieciowy sieć, ale nie monitoruje szczegółowo, co dzieje się w punktach końcowych.
- **XDR** łączy wykrywanie EDR i NDR, wprowadza automatyzację w celu przyspieszenia reagowania i ma na celu ułatwienie wykrywania wyrafinowanych ataków.
- **SIEM –** konfiguracja zajmuje więcej czasu i więcej wysiłku w utrzymaniu niż którekolwiek z powyższych narzędzi, ale co najważniejsze, zapewnia znacznie wyższy poziom dostosowywania w razie potrzeby, a także łatwo dostępne surowe dane dziennika. XDR brakuje głębi dostosowywania, którą można osiągnąć za pomocą narzędzi SIEM.

Środki bezpieczeństwa



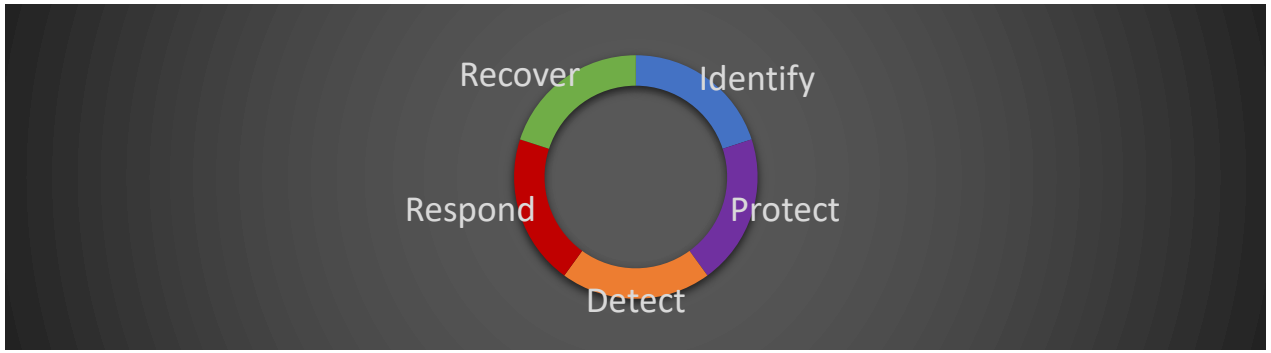
- **NAC (Network Access Control)**.
  - **Polityki dostępu do sieci**. Umożliwia definiowanie i egzekwowanie polityk kontroli dostępu do sieci na podstawie tożsamości użytkownika i stanu urządzenia.
  - **Inspekcja urządzeń**. Przed przyznaniem dostępu sprawdza podłączane urządzenia czy spełniają określone wymagania bezpieczeństwa.
  - **Zarządzanie gośćmi.** Umożliwia bezpieczne zarządzanie dostępem dla urządzeń gości.
  - **Segmentacja sieci**. Pomaga w izolowaniu urządzeń i użytkowników w różnych segmentach.
  - **Reagowanie na incydenty**. Automatyzuje odpowiedzi na wykryte zagrożenia w sieci.

Środki bezpieczeństwa



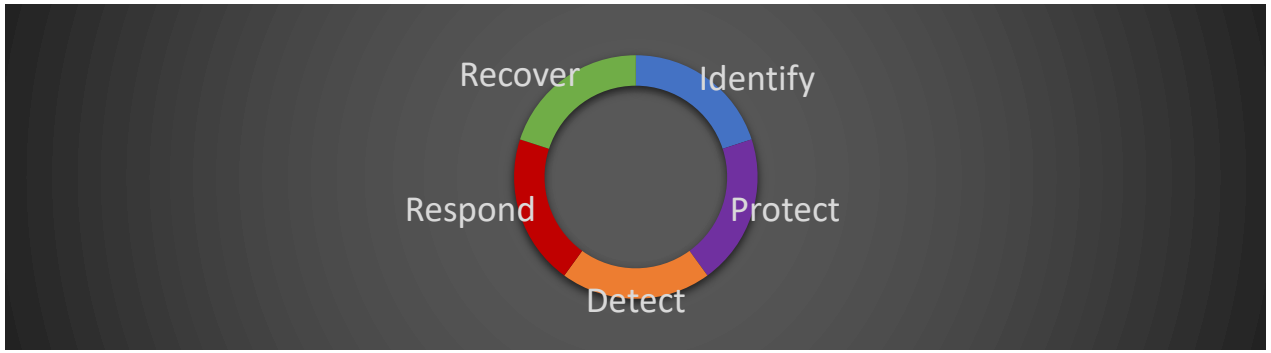
- **PAM (Privileged Access Management)**.
  - **Zarządzanie dostępem uprzywilejowanym**. Kontroluje dostęp do krytycznych systemów i zasobów dla uprzywilejowanych użytkowników.
  - **Monitoring i audyt**. Rejestruje działania wykonywane przez użytkowników uprzywilejowanych; śledzi wykonywane działania i np. wydawane polecenia w shell/cmd.
  - **Automatyczne wygaszanie sesji**. Automatycznie zamyka aktywne sesje.
  - **Wieloskładnikowe uwierzytelnienie**. Wymaga od użytkowników uprzywilejowanych stosowania wieloskładnikowego uwierzytelnienia.
  - **Ścisłe polityki bezpieczeństwa**. Umożliwia tworzenie i egzekwowanie skonfigurowanych polityk dostępu.

Środki bezpieczeństwa



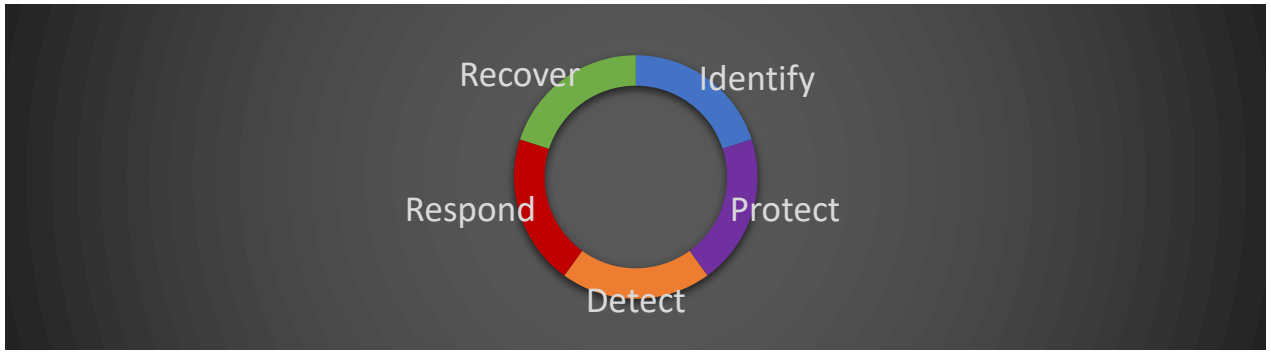
- **IAM (Identity and Access Management)**.
  - **Zarządzanie tożsamościami**. Centralne zarządzanie tożsamością użytkowników, włącznie z uwierzytelnianiem i autoryzacją.
  - **Polityki dostępu**. Definiowanie i egzekwowanie polityk dostępu do zasobów.
  - **Wieloskładnikowe uwierzytelnienie**.
  - **Zarządzanie sesjami**. Monitoruje i kontroluje uwierzytelnione sesje.
  - **Audyt i raportowanie**. Zapewnia śledzenie i raportowanie dotyczące działań użytkowników i dostępu do zasobów.

Środki bezpieczeństwa



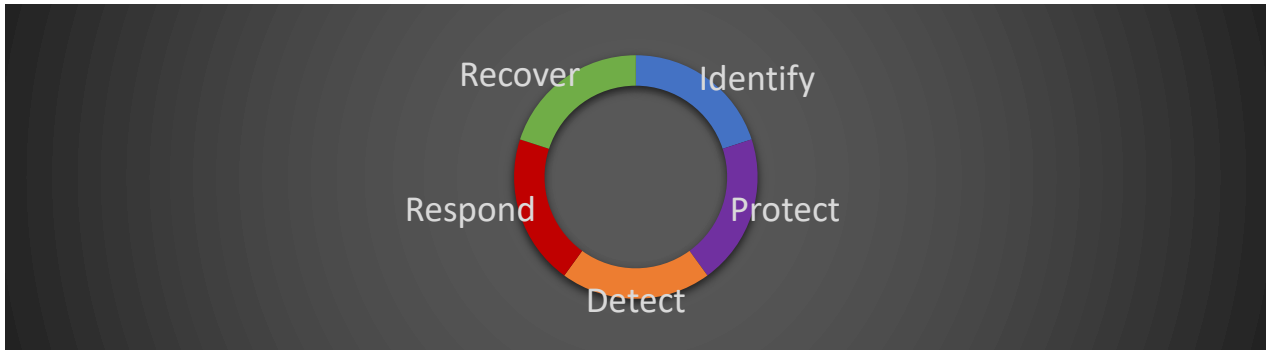
- **DLP (Data Loss Prevention)**.
  - **Monitorowanie danych**. Śledzi przepływ i miejsca wykorzystania danych.
  - **Blokowanie transmisji**. Automatycznie monitoruje i blokuje próby wysyłki wrażliwych danych poza organizację.
  - **Klasyfikacja danych**. Pomaga w identyfikacji i klasyfikacji wrażliwych danych.
  - **Oznaczanie danych**. Pozwala na oznaczanie wrażliwych danych.

Środki bezpieczeństwa



- **SOAR (Security Orchestration Automation and Response)**.
  - **Orkiestracja narzędzi bezpieczeństwa**. Integruje różne narzędzia bezpieczeństwa, automatyzując przepływ zadań i reakcję na incydenty.
  - **Automatyzacja odpowiedzi**. Automatyzuje procesy reagowania na incydenty.
  - **Zarządzanie planami reagowania**. Umożliwia zarządzanie incydentami bezpieczeństwa od identyfikacji zdarzenia po zamknięcie.
  - **Analiza po incydencie**. Pozwala na analizę po zdarzeniach i lepsze przygotowanie działań doskonalących.

Środki bezpieczeństwa



- **MDM (Mobile Device Management)**.
  - **Zarządzanie urządzeniami mobilnymi**. Umożliwia centralne zarządzanie i monitorowanie urządzeń mobilnych używanych w ramach organizacji.
  - **Reguły bezpieczeństwa**. Egzekwuje zasady bezpieczeństwa, takie jak szyfrowanie, ochrona hasłem i blokowanie urządzeń.
  - **Zdalne czyszczenie danych**. Pozwala na zdalne usunięcie danych z urządzenia, które zostało zgubione lub skradzione.
  - **Zarządzanie aplikacjami**. Kontroluje, które aplikacje mogą być instalowane na urządzeniach.

Dziękuję za uwagę