

SZKOLENIE DWUDNIOWE — DZIEŃ 2 z 2



Cyberbezpieczeństwo w praktyce

CompTIA Security+ SY0-701 z laboratoriami CertMaster Labs

29.09.2026

07:00–15:00

Zdalnie (MS Teams)

Poziom średniozaawansowany

6 laboratoriów

8 godzin dydaktycznych · 7 modułów · zestaw laboratoriów oraz ćwiczeń praktycznych · pre-test i post-test · zaświadczenie i certyfikat

Agenda Dnia 2 — 13 pozycji harmonogramu BUR

OTWARCIE

Godziny zgodne z kartą usługi nr 2026/09/04/204299/3790068. Blok = zajęcia merytoryczne, LAB = laboratorium CertMaster Labs.

07:00–07:45 · Otwarcie, recap+quiz z Dnia 1, Monitoring i SIEM: architektura, logi, korelacja

Blok 7

07:45–08:30 · LAB 11.2.1 System Monitoring

Laboratorium

08:30–08:45 · Przerwa

08:45–09:30 · IAM: RBAC, Least Privilege, MFA/2FA, PAM, Zero Trust Architecture, ZTNA vs VPN

Blok 8

09:30–10:15 · Detekcja incydentów: IOC/IOA, playbooki SIEM. LAB 12.1.1 IR Detection

Blok 8 cd. + LAB

10:15–10:30 · Przerwa

10:30–11:15 · Forensics sieciowy: Wireshark, tcpdump, MitM, C2. LAB 12.3.1 Network Sniffers

Blok 9 + LAB

11:15–12:00 · Reagowanie na malware: IOC, izolacja, eliminacja. LAB 13.1.1 Malware Response

Blok 10 + LAB

12:00–12:30 · Przerwa obiadowa

12:30–13:15 · Playbooki IR i SOAR: automatyzacja, MTTD/MTTR. LAB 14.1.1 Playbook

Blok 11 + LAB

13:15–14:00 · BCP/DR: BIA, MTD/RTO/RPO/WRT, reguła 3-2-1-1-0. LAB 7.1.1 Backups

Blok 12 + LAB

14:00–14:30 · NISZ/UoKSC/CRA dla specjalistów IT, mapa certyfikacji, ścieżki kariery

Blok 13

14:30–15:00 · Walidacja: podsumowanie szkolenia i Q&A

Zamknięcie

Recap Dnia 1 — szybkie powtórzenie

Dziesięć pytań, dziesięć minut — utrwalamy fundament przed przejściem do operacji bezpieczeństwa.

1

1. Różnica: zagrożenie, podatność, ryzyko, incydent?

Zagrożenie działa NA podatność; ryzyko to iloczyn prawdopodobieństwa i wpływu; incydent to materializacja.

2

2. Czym różni się szyfrowanie symetryczne od asymetrycznego?

Symetryczne: jeden klucz, szybkie (AES). Asymetryczne: para kluczy, wolniejsze, rozwiązuje problem dystrybucji klucza (RSA/ECC).

3

3. Co gwarantuje Perfect Forward Secrecy?

Kompromitacja klucza prywatnego serwera NIE odszyfrowuje przechwyconych wcześniej sesji.

4

4. SYN scan a TCP Connect scan — różnica?

SYN (half-open) nie kończy handshake, szybszy i mniej widoczny; TCP Connect kończy pełne połączenie, w pełni logowany.

5

5. Co to jest Broken Access Control (A01 OWASP)?

Użytkownik uzyskuje dostęp do zasobów/funkcji poza swoimi uprawnieniami.

6

6. Stateful firewall a NGFW — kluczowa różnica?

Stateful śledzi stan połączeń warstwy 3–4; NGFW dodaje inspekcję warstwy aplikacji, IPS, świadomość tożsamości/aplikacji.

7

7. Co mierzy CVSS, a czego NIE mówi?

CVSS Base mierzy teoretyczną krytyczność podatności — NIE mówi, czy jest faktycznie wykorzystywana w atakach (do tego EPSS/CISA KEV).

Monitoring bezpieczeństwa: cel i architektura SIEM

Nie da się zareagować na to, czego się nie widzi — monitoring to fundament operacji bezpieczeństwa.

SIEM (Security Information and Event Management)

centralna platforma zbierająca, normalizująca i korelująca logi z całej infrastruktury w jednym miejscu.

Dwie funkcje w jednej nazwie

SIM (Security Information Management) — długoterminowe przechowywanie i raportowanie; SEM (Security Event Management) — analiza czasu rzeczywistego i alertowanie.

Dlaczego centralizacja jest konieczna

pojedynczy incydent zostawia ślady rozproszone po dziesiątkach systemów; bez korelacji w jednym miejscu żaden analityk nie połączy faktów na czas.

Normalizacja logów

różne systemy logują w różnych formatach; SIEM sprowadza je do wspólnego schematu (np. CEF, LEEF), żeby można je było porównywać i korelować.

Retencja

wymogi regulacyjne (w tym UoKSC) i śledztwa powypadkowe wymagają przechowywania logów przez określony czas — typowo miesiące, nie dni.

Zasada podstawowa: „jeśli zdarzenie nie zostało zalogowane, nie wydarzyło się” — z punktu widzenia dowodowego i operacyjnego. Widoczność (visibility) to pierwszy warunek jakiegokolwiek obrony.

Źródła logów: skąd SIEM czerpie dane

Jakość korelacji zależy bezpośrednio od tego, jak kompletne i różnorodne są źródła.

Logi systemowe i aplikacyjne

- **Windows Event Log** — zdarzenia logowania (ID 4624/4625), zmiany uprawnień, uruchamianie procesów — podstawowe źródło dla środowisk Windows.
- **syslog** — standard logowania w systemach Unix/Linux oraz urządzeniach sieciowych (routery, firewalle) — format tekstowy, przesyłany zwykle po UDP 514 lub TLS.
- **Logi aplikacyjne** — serwery WWW, bazy danych, aplikacje biznesowe — źródło informacji o próbach ataków na warstwę aplikacji (np. wzorce SQL Injection w logach serwera).

Telemetria sieciowa

- **NetFlow / IPFIX** — metadane o przepływach sieciowych (kto, z kim, ile danych, jak długo) — bez zawartości pakietów, więc lekkie i skalowalne.
- **Logi firewalla i IDS/IPS** — zablokowany/dozwolony ruch, sygnatury wykrytych ataków — bezpośrednie źródło alertów o próbach włamania.
- **DNS i proxy** — zapytania domenowe i ruch webowy — kluczowe dla wykrywania komunikacji ze złośliwą infrastrukturą C2, o czym powiemy przy forensics.

Reguły korelacji i alert fatigue

Surowe logi to dane. Reguła korelacji zamienia dane w sygnał, na który warto zareagować.

Reguła korelacji

logika łącząca pojedyncze zdarzenia w sensowny wzorzec, np. „5 nieudanych logowań z jednego IP w ciągu 2 minut, po których nastąpiło udane logowanie” → prawdopodobny brute force.

Próg i okno czasowe

każda reguła ma parametry: ile zdarzeń, w jakim czasie. Zbyt niski próg generuje szum, zbyt wysoki przepuszcza realne ataki.

Alert fatigue

zjawisko, w którym analityk zalany setkami alertów dziennie zaczyna je ignorować lub odrzucać bez dogłębnej analizy — statystycznie jedna z głównych przyczyn przeoczonych realnych incydentów.

Strojenie reguł (tuning)

ciągły proces dostosowywania progów i wykluczeń (whitelisting znanych, legalnych wzorców) w celu redukcji liczby fałszywych alarmów bez utraty wykrywalności.

Priorytetyzacja alertów

nie każdy alert wymaga natychmiastowej reakcji; klasyfikacja wg krytyczności (podobnie jak CVSS dla podatności) pozwala analitykowi skupić się na tym, co najważniejsze.

Za chwilę w laboratorium: sami skonfigurują Państwo regułę korelacji i zobaczą, jak zmiana progu wpływa na liczbę generowanych alertów.

LAB 11.2.1 System Monitoring

LAB 11.2.1

System Monitoring

Konfiguracja monitorowania systemu, analiza logów zdarzeń i utworzenie reguły alertowej w symulowanym środowisku SIEM.

Czas: 45 min (07:45–08:30)

Domena SY0-701: Domena 4 — Security Operations (monitoring i wykrywanie)

Kroki laboratorium

1. Zaloguj się do modułu 11.2.1 w CertMaster Labs.
2. Przejrzyj strumień logów napływających z symulowanych źródeł (host, firewall, uwierzytelnianie).
3. Zidentyfikuj wzorzec wielokrotnych nieudanych logowań w krótkim oknie czasowym.
4. Skonfiguruj regułę korelacji: próg liczby zdarzeń i okno czasowe wyzwalające alert.
5. Przetestuj regułę na symulowanym ruchu i zweryfikuj, czy alert generuje się poprawnie.
6. Skoryguj próg, aby zredukować liczbę fałszywych alarmów bez utraty wykrywalności realnego ataku.

Na co zwrócić uwagę

- **Kompromis próg/szum** — każda zmiana progu w jedną stronę redukuje fałszywe alarmy, ale zwiększa ryzyko przeoczenia subtelniejszego ataku — nie ma ustawienia idealnego, tylko świadomy kompromis.
- **Kontekst decyduje** — ta sama liczba nieudanych logowań może być normalna dla systemu testowego i krytyczna dla systemu produkcyjnego z danymi finansowymi.
- **Dokumentacja reguły** — każda skonfigurowana reguła powinna mieć udokumentowane uzasadnienie progu — ułatwia to przyszłe strojenie i audyt.

SIEM vs SOAR vs XDR — terminologia, która się myli

Trzy akronimy, trzy różne role w tym samym ekosystemie operacji bezpieczeństwa.

SIEM i XDR

- **SIEM** — zbiera, normalizuje i koreluje logi z całej infrastruktury (podejście „szerokie”, źródło danych: dowolne logi). To, co poznaliśmy dziś.
- **XDR (Extended Detection and Response)** — nowsza kategoria, głębiej zintegrowana z konkretnymi punktami końcowymi, siecią i chmurą tego samego producenta — mniej uniwersalna, ale często skuteczniejsza w detekcji dzięki natywnej integracji.
- **EDR (Endpoint Detection and Response)** — podzbiór XDR skupiony wyłącznie na stacjach roboczych/serwerach — poprzednik koncepcyjny XDR.

SOAR — automatyzacja reakcji

- **SOAR (Security Orchestration, Automation and Response)** — nie zbiera logów samodzielnie — konsumuje alerty z SIEM/XDR i automatyzuje kolejne kroki reagowania (np. izolację hosta).
- **Orkiestracja** — łączenie wielu narzędzi bezpieczeństwa (firewall, EDR, IAM) w jeden zautomatyzowany przepływ pracy przez API.
- **Playbook jako kod** — reguła reakcji zapisana jako zautomatyzowana sekwencja kroków — temat, który rozwiniemy szczegółowo w bloku jedenastym.

IAM: tożsamość, uwierzytelnianie, autoryzacja

Trzy różne pytania, trzy różne mechanizmy — mylenie ich to jeden z najczęstszych błędów projektowych.

Identyfikacja

„kim twierdzisz, że jesteś?” — podanie loginu, adresu e-mail lub innego identyfikatora, bez dowodu.

Uwierzytelnianie (authentication)

„udowodnij to” — weryfikacja tożsamości przez co najmniej jeden czynnik: coś, co wiesz (hasło), coś, co masz (token), coś, czym jesteś (biometria).

Autoryzacja (authorization)

„co wolno ci zrobić?” — po potwierdzeniu tożsamości, system decyduje, do jakich zasobów użytkownik ma dostęp.

Rozliczalność (accounting/auditing)

„co faktycznie zrobiłeś?” — logowanie działań użytkownika, umożliwiające późniejsze dochodzenie i audyt (czwarty element modelu AAA).

IAM (Identity and Access Management)

całościowy system zarządzający cyklem życia tożsamości: utworzenie konta, przypisanie uprawnień, zmiana roli, dezaktywacja przy odejściu.

Częsty błąd projektowy: silne uwierzytelnianie (MFA) bez rozsądnej autoryzacji nie chroni przed nadużyciem — użytkownik może być „na pewno tym, za kogo się podaje” i wciąż mieć dostęp do zbyt wielu zasobów.

RBAC i zasada najmniejszych uprawnień (Least Privilege)

Modele kontroli dostępu, które w praktyce decydują o skali szkód po przejęciu konta.

1

RBAC (Role-Based Access Control)

Uprawnienia przypisane do roli (np. „Księgowość”, „IT Admin”), nie do konkretnej osoby — zmiana stanowiska = zmiana roli, nie ręczne przepisywanie dziesiątek uprawnień.

2

Least Privilege (najmniejsze uprawnienia)

Użytkownik/proces dostaje wyłącznie te uprawnienia, które są absolutnie niezbędne do wykonania zadania — nic „na zapas”.

3

Separation of Duties (rozdzielenie obowiązków)

Krytyczne procesy (np. zatwierdzanie i wykonanie przelewu) rozdzielone między co najmniej dwie osoby — utrudnia nadużycie wymagające zмовy.

4

ABAC (Attribute-Based Access Control)

Model bardziej granularny niż RBAC: decyzja o dostępie zależy od atrybutów (pora dnia, lokalizacja, typ urządzenia) — fundament praktyczny Zero Trust.

5

Przegląd uprawnień (access review)

Regularny, udokumentowany audyt: kto ma dostęp do czego i czy to wciąż uzasadnione — przeciwdziała „pełzającym uprawnieniom” (privilege creep).

MFA/2FA: TOTP kontra FIDO2/WebAuthn

Nie każde „drugie hasło” jest równie odporne na phishing — różnica ma znaczenie praktyczne.

TOTP (Time-based One-Time Password)

- **Mechanizm** — aplikacja (np. Google Authenticator) generuje 6-cyfrowy kod, zmieniający się co 30 sekund, na podstawie współdzielonego sekretu i aktualnego czasu.
- **Zaletą** — prostota wdrożenia, brak dodatkowego sprzętu, działa offline.
- **Słaba strona** — podatny na phishing w czasie rzeczywistym (real-time relay/adversary-in-the-middle) — atakujący może przechwycić kod i natychmiast go użyć.

FIDO2 / WebAuthn (klucze U2F)

- **Mechanizm** — klucz sprzętowy (np. YubiKey) lub uwierzytelnianie platformowe (Windows Hello, Touch ID) wykorzystuje kryptografię asymetryczną powiązaną z konkretną domeną.
- **Odporność na phishing** — klucz prywatny nigdy nie opuszcza urządzenia, a podpis jest związany z domeną (origin binding) — fałszywa strona nie może „wyłudzić” ważnego podpisu.
- **Rekomendacja CISA/NIST** — FIDO2 uznawany za „phishing-resistant MFA” — rekomendowany standard dla kont uprzywilejowanych.

PAM: zarządzanie kontami uprzywilejowanymi

Konta administratora to najwyższej wartości cel dla każdego atakującego — wymagają osobnego reżimu kontroli.

PAM (Privileged Access Management)

wyspecjalizowana kategoria narzędzi i procesów do zabezpieczania, monitorowania i kontrolowania kont z podwyższonymi uprawnieniami (admin, root, service account).

Just-In-Time Access

uprawnienia uprzywilejowane przyznawane tylko na czas trwania konkretnego zadania, a nie na stałe — po zakończeniu automatycznie wygasają.

Session recording

nagrywanie/logowanie każdej sesji administracyjnej dla celów audytu i śledztwa powypadkowego.

Vaulting haseł

hasła kont uprzywilejowanych przechowywane w zaszyfrowanym „sejfie”, rotowane automatycznie po każdym użyciu — administrator nie zna hasła na stałe.

Konta serwisowe (service accounts)

często pomijane w audytach, a mają szerokie uprawnienia i rzadko zmieniane hasła — statystycznie częsty wektor eskalacji uprawnień po pierwszym włamaniu.

Dla egzaminu: PAM to nie to samo co IAM — IAM zarządza WSZYSTKIMI tożsamościami, PAM to wyspecjalizowana podkategoria skupiona wyłącznie na kontach o podwyższonym ryzyku.

Zero Trust Architecture wg NIST SP 800-207

„Nigdy nie ufaj, zawsze weryfikuj” — filozofia zastępująca klasyczny model obwodowy.

Model klasyczny (perimeter-based)

„zamek i fosa” — silna ochrona na granicy sieci, pełne zaufanie do wszystkiego, co już wewnątrz. Problem: po przełamaniu obwodu atakujący ma swobodę ruchu.

Zero Trust — założenie wyjściowe

żadne urządzenie ani użytkownik nie są domyślnie zaufani, niezależnie od tego, czy znajdują się „wewnątrz” czy „na zewnątrz” sieci.

Weryfikacja ciągła (continuous verification)

każde żądanie dostępu do zasobu jest weryfikowane osobno, w czasie rzeczywistym, na podstawie tożsamości, stanu urządzenia i kontekstu — nie jednorazowo przy logowaniu.

Mikrosegmentacja jako realizacja

sieć podzielona na małe, izolowane strefy (temat z wczorajszego dnia) — Zero Trust to filozofia, mikrosegmentacja to jeden z jej mechanizmów wdrożeniowych.

PEP i PDP

Policy Enforcement Point (egzekwuje decyzję) i Policy Decision Point (podejmuje decyzję o dostępie) — architektoniczny rdzeń modelu wg NIST SP 800-207.

Powrót do wczoraj: wspominaliśmy Zero Trust przy segmentacji sieci — dziś widzimy pełny obraz: to nie produkt do kupienia, tylko architektura budowana z IAM, MFA, mikrosegmentacji i ciągłego monitoringu razem.

ZTNA kontra klasyczny VPN

Zero Trust Network Access — praktyczna realizacja Zero Trust dla dostępu zdalnego.

VPN klasyczny

- **Model dostępu** — po nawiązaniu połączenia użytkownik otrzymuje dostęp do całego segmentu sieci, jakby fizycznie siedział w biurze.
- **Zaufanie** — jednorazowa weryfikacja przy nawiązaniu połączenia — brak ciągłej reoceny w trakcie trwania sesji.
- **Ryzyko** — skompromitowane urządzenie zdalne z aktywnym VPN staje się bramą do całej wewnętrznej sieci (lateral movement).

ZTNA (Zero Trust Network Access)

- **Model dostępu** — dostęp przyznawany do pojedynczej aplikacji/zasobu, nigdy do całego segmentu sieci — zasada najmniejszych uprawnień zastosowana do sieci.
- **Zaufanie** — weryfikacja tożsamości i stanu urządzenia przy każdym żądaniu dostępu do zasobu, nie tylko na starcie sesji.
- **Widoczność sieci** — użytkownik nie „widzi” topologii wewnętrznej sieci — ogranicza to rekonesans nawet dla legalnego, ale skompromitowanego konta.

Detekcja incydentów: IOC kontra IOA

Dwa różne pytania stawiane danym: „co już się stało?” kontra „co się właśnie dzieje?”

IOC (Indicator of Compromise)

dowód, że doszło już do kompromitacji: konkretny hash złośliwego pliku, adres IP serwera C2, podejrzana domena, nietypowy wpis w rejestrze systemowym.

Charakter IOC

retrospektywny/statyczny — porównujemy obserwowane dane z bazą znanych, już udokumentowanych wskaźników ataku (np. feedy threat intelligence).

IOA (Indicator of Attack)

wzorzec zachowania sugerujący trwający atak, niezależnie od konkretnego narzędzia: np. proces biurowy nagle uruchamiający PowerShell z podwyższonymi uprawnieniami.

Charakter IOA

behawioralny/dynamiczny — wykrywa nowe, nieznane wcześniej ataki po wzorcu zachowania, nie po konkretnej sygnaturze.

Komplementarność

dojrzały SOC wykorzystuje oba podejścia: IOC do szybkiej identyfikacji znanych zagrożeń, IOA do wykrywania nowych, jeszcze nieudokumentowanych technik.

Ograniczenie IOC: atakujący zmieniający hash pliku albo adres IP serwera C2 (co jest trywialne) automatycznie omija detekcję opartą wyłącznie na IOC — dlatego IOA staje się coraz ważniejsze.

Klasyfikacja alertów: true/false positive/negative

Macierz, na podstawie której analityk podejmuje decyzję — i którą egzamin regularnie testuje.

1

True Positive (prawdziwie pozytywny)

System poprawnie wykrył realny atak i wygenerował alert. Pożądany wynik — reagujemy.

2

False Positive (fałszywie pozytywny)

System wygenerował alert, choć nie było realnego ataku (np. legalne narzędzie administracyjne wygląda jak malware). Źródło alert fatigue.

3

True Negative (prawdziwie negatywny)

System poprawnie NIE wygenerował alertu, bo faktycznie nie było ataku. Pożądany, choć niewidoczny wynik.

4

False Negative (fałszywie negatywny)

Najgroźniejsza kategoria: realny atak miał miejsce, a system NIE wygenerował żadnego alertu. Atak pozostaje niewykryty.

LAB 12.1.1 IR Detection

LAB 12.1.1

IR Detection

Analiza zestawu wygenerowanych alertów SIEM i klasyfikacja każdego jako true/false positive na podstawie dostępnego kontekstu.

Czas: 45 min (09:30–10:15)

Domena SY0-701: Domena 4 — Security Operations (detekcja i klasyfikacja incydentów)

Kroki laboratorium

1. Zaloguj się do modułu 12.1.1 w CertMaster Labs.
2. Przejrzyj zestaw dziesięciu wygenerowanych alertów SIEM wraz z towarzyszącym kontekstem (logi źródłowe, czas, użytkownik).
3. Dla każdego alertu zdecyduj: true positive czy false positive, uzasadniając decyzję konkretnym elementem kontekstu.
4. Zidentyfikuj wśród alertów co najmniej jeden pasujący do wzorca IOC i jeden pasujący do wzorca IOA.
5. Wskaż, które alerty wymagają natychmiastowej eskalacji, a które mogą poczekać do przeglądu okresowego.
6. Podsumuj: ile alertów było prawdziwych, ile fałszywych — oblicz orientacyjny wskaźnik false positive rate dla tego zestawu.

Na co zwrócić uwagę

- **Kontekst jest wszystkim** — ten sam surowy alert może być true lub false positive w zależności od tego, kto, kiedy i z jakiego urządzenia wykonał daną akcję.
- **Nie każdy true positive to katastrofa** — klasyfikacja krytyczności następuje po potwierdzeniu, że alert jest prawdziwy — priorytetyzacja to osobny krok.
- **Wskaźnik false positive rate** — metryka realnie używana do oceny jakości strojenia reguł SIEM w danej organizacji — wysoki wskaźnik to sygnał do dalszego tuningu.

Debrief: strojenie SIEM i redukcja fałszywych alarmów

Od klasyfikacji pojedynczych alertów do systematycznego procesu poprawy jakości detekcji.

Whitelisting kontekstowy

znane, legalne wzorce (np. skrypty administracyjne uruchamiane cyklicznie) dodawane jako wyjątki, żeby nie generowały powtarzalnego szumu.

Wzbogacanie alertu (enrichment)

automatyczne dołączanie dodatkowego kontekstu do alertu (reputacja IP, geolokalizacja, historia użytkownika) — przyspiesza decyzję analityka.

Baseline zachowania

ustalenie, co jest „normalne” dla danego użytkownika/systemu, zanim zaczną się wykrywać odchylenia — bez baseline IOA jest niemożliwe do zrealizowania.

Iteracyjność procesu

strojenie SIEM to nie jednorazowy projekt wdrożeniowy, tylko ciągły proces — środowisko i wzorce ataków zmieniają się nieustannie.

Forensics sieciowy: metodyka i narzędzia

Ruch sieciowy nie kłamie — analiza pakietów dostarcza dowodów, których logi aplikacyjne mogą nie zawierać.

Network forensics

przechwytywanie i analiza ruchu sieciowego w celu rekonstrukcji przebiegu incydentu — co, kiedy, z kim, jaką ilością danych.

Wireshark

narzędzie graficzne do głębokiej analizy przechwyconych pakietów (PCAP) — dekodowanie protokołów warstwa po warstwie, filtrowanie po adresie, porcie, zawartości.

tcpdump

narzędzie wiersza poleceń do przechwytywania ruchu na żywo — lżejsze, skryptowalne, standard na serwerach bez interfejsu graficznego.

PCAP (Packet Capture)

standardowy format pliku przechowujący przechwycony ruch — przenośny między narzędziami, podstawowy artefakt dowodowy w śledztwie sieciowym.

łańcuch dowodowy (chain of custody)

udokumentowana historia: kto, kiedy, jak przechwycił i przechowywał dowód — krytyczne, jeśli materiał ma trafić do postępowania formalnego.

Zasada praktyczna: analiza logów aplikacyjnych mówi, co system ZAREJESTROWAŁ; analiza ruchu sieciowego pokazuje, co FAKTYCZNIE się wydarzyło na drucie — te dwa źródła bywają rozbieżne, gdy atakujący manipuluje logami.

Wzorce ruchu ataku: MitM, C2, eksfiltracja danych

To, czego konkretnie szukamy w przechwyconym ruchu — mechanika, nie tylko nazwa ataku.

1

Ślady ARP Spoofing / MitM

Zduplikowane lub sprzeczne odpowiedzi ARP dla tego samego adresu IP; nietypowy adres MAC odpowiadający za bramę sieciową.

2

Beaconing (regularna komunikacja C2)

Cykliczne, powtarzalne połączenia wychodzące do tego samego zewnętrznego adresu/domeny w stałych odstępach czasu — charakterystyczny wzorec złośliwego oprogramowania „meldującego się” do serwera dowodzenia.

3

DNS tunneling

Nietypowo długie lub częste zapytania DNS, zawierające zakodowane dane — technika eksfiltracji danych lub komunikacji C2 przez protokół zwykle niefiltrowany przez firewalla.

4

Eksfiltracja danych

Nagły, nietypowo duży transfer danych wychodzących (upload) od pojedynczego hosta, szczególnie poza standardowymi godzinami pracy.

5

Skanowanie wewnętrzne (internal reconnaissance)

Host generujący dużą liczbę połączeń do wielu różnych wewnętrznych adresów IP/portów w krótkim czasie — sygnał ruchu bocznego (lateral movement) po wstępnym włamaniu.

LAB 12.3.1 Network Sniffers

LAB 12.3.1

Network Sniffers

Przechwycenie i analiza ruchu sieciowego przy użyciu Wireshark/tcpdump w celu identyfikacji wzorca ataku w symulowanym środowisku.

Czas: 45 min (10:30–11:15)

Domena SY0-701: Domena 4 — Security Operations (forensics sieciowy)

Kroki laboratorium

1. Zaloguj się do modułu 12.3.1 w CertMaster Labs.
2. Przechwycić ruch sieciowy na przydzielonym interfejsie za pomocą narzędzia sniffującego.
3. Zastosuj filtr, aby wyizolować ruch związany z podejrzanym hostem.
4. Zidentyfikuj wzorzec beaconingu lub inny wskaźnik komunikacji C2 w przechwyconym ruchu.
5. Wyodrębnij kluczowe artefakty: adres IP/domenę C2, częstotliwość komunikacji, ilość przestanych danych.
6. Przygotuj krótkie podsumowanie ustaleń w formie odpowiedniej do przekazania zespołowi reagowania na incydenty.

Na co zwrócić uwagę

- **Filtrowanie to umiejętność kluczowa** — w realnym ruchu produkcyjnym surowy PCAP zawiera tysiące pakietów; bez precyzyjnych filtrów analiza jest praktycznie niewykonalna w rozsądnym czasie.
- **Szyfrowany ruch nie jest „nieanalizowalny”** — nawet bez odszyfrowania treści TLS, metadane (częstotliwość, wolumen, docelowy adres) ujawniają wzorzec beaconingu.
- **Ustalenia jako wejście do IR** — wynik analizy forensycznej bezpośrednio zasila decyzję o izolacji hosta, którą omówimy w kolejnym bloku.

Debrief: od przechwyconego pakietu do wniosku

Analiza forensyczna kończy się dopiero wtedy, gdy ustalenia stają się decyzją operacyjną.

Korelacja z innymi źródłami

sam PCAP rzadko wystarcza — zestawienie z logami hosta i SIEM z bloku siódmego daje pełny obraz przebiegu incydentu.

Fałszywe wskazania w ruchu sieciowym

nie każde regularne, cykliczne połączenie to beaconing malware — legalne oprogramowanie też regularnie „telefonuje do domu” (aktualizacje, telemetria producenta).

Timeline incydentu

chronologiczne zestawienie wszystkich ustalonych zdarzeń (pierwszy kontakt, eskalacja, eksfiltracja) — podstawowy artefakt każdego formalnego raportu z incydentu.

Od forensics do reagowania

analiza retrospektywna (co się stało) musi przełożyć się na decyzję operacyjną (co robimy teraz) — bez tego przejścia forensics jest ćwiczeniem akademickim.

Cykl życia reagowania na incydent (NIST SP 800-61)

Sześć faz, w które wpisuje się każde kolejne szczegółowe działanie omawiane dzisiaj.

1. Przygotowanie (Preparation)

procedury, narzędzia, przeszkolony zespół, zdefiniowane role — zanim cokolwiek się wydarzy.

2. Detekcja i analiza (Detection & Analysis)

to, o czym mówiliśmy w blokach siódmym i dziewiątym: rozpoznanie, że incydent faktycznie ma miejsce, i wstępna klasyfikacja jego skali.

3. Powstrzymanie (Containment)

ograniczenie zasięgu szkód — izolacja zainfekowanego hosta, zanim atak rozprzestrzeni się dalej.

4. Eliminacja (Eradication)

usunięcie przyczyny źródłowej: złośliwego oprogramowania, wykorzystanej podatności, nieautoryzowanego dostępu.

5. Odtworzenie (Recovery)

bezpieczne przywrócenie systemów do normalnej pracy, z weryfikacją, że zagrożenie faktycznie zostało usunięte.

6. Wnioski (Lessons Learned)

formalne podsumowanie po incydencie — co zadziałało, co nie, jakie zmiany wdrożyć, żeby uniknąć powtórki.

Model cykliczny, nie liniowy: wnioski z fazy szóstej zasilają z powrotem fazę pierwszą — przygotowanie na kolejny incydent. NIST SP 800-61 przedstawia to jako pętlę, nie linię prostą.

Reagowanie na malware: izolacja i eliminacja

Fazy powstrzymania i eliminacji zastosowane konkretnie do infekcji złośliwym oprogramowaniem.

Izolacja hosta (containment)

odcięcie zainfekowanej maszyny od sieci (fizycznie lub przez segmentację/VLAN) — priorytet: zatrzymać rozprzestrzenianie, nie od razu wyłączać zasilanie.

Dlaczego NIE wyłączamy zasilania od razu

wyłączenie niszczy zawartość pamięci RAM — cenny materiał dowodowy (aktywne procesy, klucze szyfrowania w pamięci) bezpowrotnie znika.

Identyfikacja szczepu (IOC malware)

hash pliku, nazwa procesu, wzorec sieciowy — porównanie z bazami threat intelligence w celu zrozumienia charakteru zagrożenia.

Eliminacja

usunięcie złośliwych plików, zatrzymanie procesów, usunięcie mechanizmów trwałości (persistence — np. wpisy autostartu, zaplanowane zadania).

Weryfikacja czystości przed odtworzeniem

ponowne skanowanie i monitorowanie przed przywróceniem hosta do sieci produkcyjnej — pochopne odtworzenie to najczęstsza przyczyna nawrotu infekcji.

Częsty błąd operacyjny: odtworzenie systemu „na szybko” z ostatniego dostępnego backupu bez pewności, że backup sam nie jest już zainfekowany — temat, do którego wrócimy w bloku o BCP/DR.

Forensics pamięci kontra forensics dysku

Dwa różne źródła dowodowe — ulotne i trwałe — potrzebne razem do pełnego obrazu incydentu.

Forensics pamięci (memory forensics)

- **Co przechwytujemy** — zrzut (dump) zawartości pamięci RAM w momencie aktywnej infekcji.
- **Dlaczego to pilne** — dane ulotne (volatile) — znikają bezpowrotnie po wyłączeniu zasilania. Zasada: „order of volatility” — zbieramy najpierw to, co znika najszybciej.
- **Co znajdziemy** — aktywne procesy (w tym ukryte przed listą procesów systemu), połączenia sieciowe w toku, czasem klucze szyfrowania w pamięci.

Forensics dysku (disk forensics)

- **Co przechwytujemy** — pełny, bitowy obraz (image) dysku — kopia identyczna co do bitu z oryginałem.
- **Dlaczego to trwałe** — dane nieulotne — przetrwają wyłączenie zasilania, dają więcej czasu na analizę bez presji.
- **Co znajdziemy** — usunięte (ale nienadpisane) pliki, historię systemu plików, metadane (znaczniki czasu utworzenia/modyfikacji), artefakty rejestru systemowego.

LAB 13.1.1 Malware Response

LAB 13.1.1

Malware Response

Przeprowadzenie pełnego scenariusza reagowania na infekcję złośliwym oprogramowaniem — od detekcji, przez izolację, po dokumentację.

Czas: 45 min (11:15–12:00)

Domena SY0-701: Domena 4 — Security Operations (reagowanie na incydenty, forensics)

Kroki laboratorium

1. Zaloguj się do modułu 13.1.1 w CertMaster Labs.
2. Przeanalizuj alert wskazujący na aktywną infekcję hosta.
3. Podejmij i uzasadnij decyzję o izolacji hosta od sieci.
4. Zidentyfikuj IOC szczepu malware (hash, nazwa procesu, wzorzec sieciowy) i porównaj z bazą referencyjną.
5. Wskaż kroki eliminacji, w tym usunięcie mechanizmu trwałości (persistence).
6. Sporządź dokumentację incydentu: chronologię działań, ustalone IOC, rekomendację przed odtworzeniem systemu.

Na co zwrócić uwagę

- **Kolejność działań ma znaczenie** — izolacja PRZED zbieraniem dowodów z pamięci, zbieranie dowodów PRZED eliminacją, eliminacja PRZED odtworzeniem — odwrócenie kolejności niszczy dowody lub przedłuża infekcję.
- **Dokumentacja w czasie rzeczywistym** — zapisywanie działań na bieżąco, nie z pamięci po fakcie — pod presją czasu szczegóły się zacierają.
- **To pełna próba generalna** — to laboratorium łączy detekcję, forensics i eliminację w jeden spójny scenariusz — dokładnie taki, jaki może się wydarzyć w realnej pracy.

Debrief: dokumentacja incydentu jako dowód

Raport z incydentu to nie formalność — to artefakt, na który polega organizacja, ubezpieczyciel i regulator.

Kto czyta raport z incydentu

zespół techniczny (żeby zrozumieć, co się stało), zarząd (żeby ocenić skutki biznesowe), czasem ubezpieczyciel cyber i regulator (NIS2/UoKSC — temat po południu).

Fakty, nie interpretacje

raport opisuje ustalone fakty i chronologię; wnioski i rekomendacje są jasno oddzielone od samego opisu zdarzeń.

Kompletność mimo presji czasu

pokusa „dopiszemy szczegóły później” prowadzi do luk, których nikt później nie uzupełnia — stąd znaczenie dokumentowania na bieżąco.

Raport jako materiał szkoleniowy

dobrze udokumentowany incydent staje się materiałem do wewnętrznych szkoleń i testowania kolejnych playbooków — bezpośrednio wraca w kolejnym bloku.

Playbooki IR: co to jest i dlaczego działa

Ustandaryzowana odpowiedź na powtarzalny scenariusz — spokój proceduralny w chwili kryzysu.

Playbook (runbook)

udokumentowana, krok po kroku sekwencja działań dla konkretnego, powtarzalnego typu incydu (np. „wykryty ransomware”, „phishing zgłoszony przez pracownika”).

Dlaczego nie improwizujemy w chwili kryzysu

pod presją czasu i stresu nawet doświadczony analityk pomija kroki — playbook to zewnętrzna pamięć proceduralna, niezależna od stanu emocjonalnego zespołu.

Struktura typowego playbooku

kryteria wyzwolenia (kiedy go uruchomić), role i odpowiedzialności, kolejne kroki decyzyjne, kryteria eskalacji, kryteria zamknięcia.

Playbook to dokument żywy

aktualizowany po każdym incydencie (faza „wniośki” z cyklu NIST 800-61) i regularnie testowany — nieaktualny playbook bywa gorszy niż jego brak.

Playbook a checklist

playbook zawiera punkty decyzyjne (jeśli X, to Y) — nie jest sztywną, liniową listą kontrolną bez rozgałęzień.

Powiązanie z wczoraj: playbook „wykryty ransomware” bezpośrednio odwołuje się do sekwencji izolacja→forensics→eliminacja, którą przećwiczyliśmy w poprzednim laboratorium.

SOAR: automatyzacja reagowania

Playbook zapisany jako kod — wykonywany przez system w sekundy, nie przez człowieka w minuty.

Od playbooku papierowego do playbooku zautomatyzowanego

SOAR przekształca udokumentowaną procedurę w sekwencję kroków wykonywanych automatycznie przez system, bez czekania na ręczne działanie analityka.

Przykład automatyzacji

alert o malware na hoście → SOAR automatycznie izoluje host w sieci → pobiera zrzut pamięci → powiadamia analityka z gotowym kontekstem, zamiast zaczynać od zera.

Human-in-the-loop vs pełna automatyzacja

w praktyce większość organizacji stosuje model pośredni: automatyczne kroki niskiego ryzyka (zbieranie danych), decyzje wysokiego ryzyka (np. wyłączenie serwera produkcyjnego) wymagają zatwierdzenia człowieka.

Integracja przez API

SOAR łączy się z firewallem, EDR, systemem IAM i wieloma innymi narzędziami przez ich interfejsy programistyczne, orkiestrując działania między nimi.

Korzyść skalowalności

zespół SOC obsługujący tysiące alertów dziennie fizycznie nie jest w stanie ręcznie przeanalizować każdego — automatyzacja pierwszej reakcji jest jedynym sposobem, by nadążyć.

Metryki SOC: MTTD, MTTR, MTTC

Liczby, którymi mierzy się dojrzałość operacyjną centrum bezpieczeństwa.

1

MTTD (Mean Time to Detect)

Średni czas od momentu wystąpienia incydentu do jego wykrycia. Im niższy, tym krócej atakujący działa niezauważony.

2

MTTR (Mean Time to Respond/Resolve)

Średni czas od wykrycia incydentu do jego pełnego rozwiązania — obejmuje powstrzymanie, eliminację i odtworzenie.

3

MTTC (Mean Time to Contain)

Średni czas od wykrycia do skutecznego powstrzymania (containment) — węższa metryka niż MTTR, mierzy tylko pierwszą, krytyczną reakcję.

4

Dlaczego automatyzacja obniża te metryki

Kroki wykonywane automatycznie przez SOAR (sekundy) zamiast ręcznie przez człowieka (minuty/godziny) bezpośrednio skracają MTTD, MTTC i MTTR.

LAB 14.1.1 Playbook

LAB 14.1.1

Playbook

Wykonanie gotowego playbooku dla scenariusza phishing/ransomware w symulowanym środowisku SOAR.

Czas: 45 min (12:15–13:00)

Domena SY0-701: Domena 4 — Security Operations (automatyzacja reagowania)

Kroki laboratorium

1. Zaloguj się do modułu 14.1.1 w CertMaster Labs.
2. Zapoznaj się ze scenariuszem: pracownik zgłasza podejrzaną e-mail, który następnie okazuje się początkiem ataku ransomware.
3. Uruchom właściwy playbook zgodnie z kryteriami wyzwolenia.
4. Przejdź przez kolejne kroki decyzyjne playbooku, zatwierdzając kroki wymagające interwencji człowieka (human-in-the-loop).
5. Zaobserwuj, które kroki zostały wykonane automatycznie, a które wymagały Twojej decyzji — i dlaczego akurat te.
6. Zamknij incydent zgodnie z kryteriami zamknięcia playbooku i zanotuj czas, jaki upłynął od wykrycia do powstrzymania (Twój „MTTC”).

Na co zwrócić uwagę

- **Playbook jako połączenie wszystkiego z dzisiaj** — ten scenariusz łączy detekcję (blok 8), forensics (blok 9), reagowanie na malware (blok 10) w jeden, zautomatyzowany przepływ.
- **Granica automatyzacji jest świadomym wyborem** — zwróćcie uwagę, które kroki playbook automatyzuje w pełni, a które celowo zatrzymuje się na zatwierdzeniu człowieka — to projektowa decyzja, nie ograniczenie techniczne.
- **Mierzalność** — to laboratorium pokazuje namacalnie, jak automatyzacja przekłada się na konkretną, zmierzoną wartość MTTC, nie tylko na abstrakcyjną deklarację „jesteśmy szybsi”.

Debrief: playbook phishing/ransomware w praktyce

Od pojedynczego zgłoszenia pracownika do w pełni udokumentowanego, zamkniętego incydentu.

Wartość czujnego pracownika

ten scenariusz zaczął się od zgłoszenia człowieka, nie od automatycznego alertu SIEM — szkolenie użytkowników (wczorajszy temat) bezpośrednio skraca MTTD.

Playbook nie eliminuje potrzeby eksperckiej wiedzy

automatyzuje powtarzalne kroki, ale decyzje wymagające kontekstu biznesowego wciąż wymagają doświadczonego analityka.

Każde wykonanie playbooku to okazja do jego poprawy

po zamknięciu incydentu wraca faza „wnioski” z cyklu NIST — czy playbook zadziałał optymalnie, czy wymaga korekty.

Od operacji do ciągłości działania

jeśli mimo wszystkich tych mechanizmów ransomware zdąży zaszyfrować dane, kolejna linia obrony to kopie zapasowe i plan odtworzenia — temat następnego bloku.

BCP i DR: różnica i miejsce w cyklu zarządzania kryzysowego

Dwa powiązane, ale odrębne plany — jeden dla biznesu, drugi dla IT.

BCP (Business Continuity Plan)

plan ciągłości działania — jak organizacja jako CAŁOŚĆ kontynuuje krytyczne funkcje biznesowe podczas i po zakłóceniu (niekoniecznie cybernetycznym — pożar, pandemia, awaria zasilania).

DR (Disaster Recovery)

plan odtworzenia po awarii — węższy, techniczny podzbiór BCP skupiony konkretnie na przywróceniu systemów IT i danych.

Relacja

DR jest częścią składową BCP, nie jego odpowiednikiem — BCP obejmuje też np. alternatywne lokalizacje pracy, komunikację kryzysową, łańcuch decyzyjny.

Dlaczego ten temat wraca po ransomware

skuteczny atak ransomware to jeden z najczęstszych realnych wyzwalaczy planu DR we współczesnych organizacjach.

Punkt wyjścia planowania

żaden plan BCP/DR nie powstaje w próżni — zaczyna się od analizy wpływu na biznes, BIA, o której za chwilę.

Dla egzaminu: pytanie rozróżniające BCP od DR to klasyczny wzorec SY0-701 — BCP = organizacja/biznes, DR = systemy/dane, DR $\subset$ BCP.

BIA: Business Impact Analysis

Zanim zaplanujemy odtworzenie, musimy wiedzieć, co jest naprawdę krytyczne — i ile kosztuje jego brak.

BIA (Business Impact Analysis)

systematyczna analiza identyfikująca krytyczne procesy biznesowe i szacująca skutki (finansowe, operacyjne, reputacyjne) ich niedostępności w czasie.

Cel praktyczny

BIA odpowiada na pytanie „ile możemy sobie pozwolić NIE mieć dostępu do systemu X, zanim szkody staną się nieakceptowalne?” — to bezpośrednio wyznacza metryki z kolejnego slajdu.

Klasyfikacja krytyczności procesów

nie wszystkie systemy są równie ważne — BIA porządkuje je wg priorytetu odtworzenia, unikając marnowania zasobów na ochronę systemów mało krytycznych kosztem kluczowych.

Zależności między systemami

BIA mapuje, które systemy zależą od innych (np. aplikacja księgowa wymaga działającej bazy danych i usługi uwierzytelniania) — kolejność odtwarzania musi to respektować.

Powiązanie z wczoraj: BIA to biznesowy odpowiednik oceny ryzyka, którą omawialiśmy przy podstawowych pojęciach — łączy prawdopodobieństwo zakłócenia z jego realnym wpływem na organizację.

Metryki ciągłości: MTD, RTO, RPO, WRT

Cztery liczby, które BIA przekłada na konkretne cele techniczne dla planu DR.

1

MTD (Maximum Tolerable Downtime)

Maksymalny czas, przez jaki proces biznesowy może być niedostępny, zanim skutki staną się nieakceptowalne (np. utrata klienta, kara umowna) — punkt wyjścia dla pozostałych metryk.

2

RTO (Recovery Time Objective)

Docelowy czas, w jakim system MUSI zostać przywrócony do działania po awarii — zawsze krótszy niż MTD, żeby zostawić margines bezpieczeństwa.

3

RPO (Recovery Point Objective)

Maksymalna akceptowalna ilość utraconych danych, mierzona w czasie — „ile danych możemy stracić?”. RPO 1h = backup musi być wykonywany co najwyżej co godzinę.

4

WRT (Work Recovery Time)

Czas potrzebny PO technicznym przywróceniu systemu na weryfikację integralności danych i pełny powrót do normalnej pracy biznesowej — często pomijany w planowaniu.

5

Zależność matematyczna

$MTD \geq RTO + WRT$. Jeśli suma RTO i WRT przekracza MTD, plan DR jest teoretycznie niewykonalny w akceptowalnym czasie — sygnał do inwestycji w szybsze odtwarzanie.

Strategie odtwarzania: hot / warm / cold site

Kompromis między kosztem utrzymania a szybkością odtworzenia — wybór zależny bezpośrednio od RTO.

Hot site i warm site

- **Hot site** — w pełni zdublowana, gotowa do natychmiastowego przejęcia infrastruktura, z aktualnymi danymi (replikacja w czasie rzeczywistym) — RTO liczone w minutach, ale najwyższy koszt utrzymania.
- **Warm site** — częściowo skonfigurowana infrastruktura zapasowa, dane synchronizowane okresowo (nie w czasie rzeczywistym) — RTO liczone w godzinach, koszt pośredni.

Cold site i chmura

- **Cold site** — lokalizacja zapasowa z podstawową infrastrukturą (zasilanie, sieć), ale bez skonfigurowanych systemów ani aktualnych danych — RTO liczone w dniach, najniższy koszt utrzymania.
- **Chmura jako czwarta opcja (DRaaS)** — Disaster Recovery as a Service — elastyczne skalowanie zasobów zapasowych na żądanie, coraz częściej zastępuje klasyczne, fizyczne warm/cold site.

Reguła 3-2-1-1-0 backupu

Ewolucja klasycznej zasady 3-2-1 o dwa elementy odpowiadające bezpośrednio na zagrożenie ransomware.

3 — trzy kopie danych

oryginał plus co najmniej dwie kopie zapasowe — pojedyncza kopia to brak realnej ochrony.

2 — dwa różne nośniki/media

kopie przechowywane na co najmniej dwóch różnych typach nośników (np. dysk lokalny + chmura) — ogranicza ryzyko awarii wspólnej dla jednego typu nośnika.

1 — jedna kopia poza siedzibą (offsite)

co najmniej jedna kopia fizycznie/logicznie oddalona od lokalizacji podstawowej — chroni przed zdarzeniami lokalnymi (pożar, powódź, kradzież).

1 — jedna kopia offline/immutable

element DODANY w reakcji na ransomware: co najmniej jedna kopia fizycznie odłączona od sieci lub niemodyfikowalna (immutable storage) — ransomware nie może zaszyfrować tego, do czego nie ma dostępu sieciowego.

0 — zero błędów przy weryfikacji

kopia zapasowa musi być regularnie testowana przez faktyczne odtworzenie — backup, który nigdy nie był testowany, to nadzieja, nie plan.

Dlaczego to rozwinięcie było konieczne: klasyczna reguła 3-2-1 zakładała zagrożenia fizyczne (pożar, awaria dysku) — nowoczesny ransomware aktywnie poszukuje i szyfruje TAKŻE podłączone sieciowo kopie zapasowe.

LAB 7.1.1 Backups

LAB 7.1.1

Backups

Konfiguracja strategii backupu zgodnej z regułą 3-2-1-1-0, wykonanie testu odtworzenia i weryfikacja integralności danych.

Czas: 45 min (13:00–13:45)

Domena SY0-701: Domena 4 — Security Operations (ciągłość działania i odtwarzanie)

Kroki laboratorium

1. Zaloguj się do modułu 7.1.1 w CertMaster Labs.
2. Skonfiguruj harmonogram backupu zgodny z zadaniem RPO dla przydzielonego systemu.
3. Skonfiguruj przechowywanie kopii zgodnie z regułą 3-2-1-1-0 (różne nośniki, offsite, offline/immutable).
4. Zasymuluj awarię/utratę danych na systemie źródłowym.
5. Wykonaj pełny test odtworzenia z kopii zapasowej i zmierz rzeczywisty czas odtworzenia.
6. Zweryfikuj integralność odtworzonych danych i porównaj zmierzony czas z zadaniem RTO.

Na co zwrócić uwagę

- **Zmierzony czas kontra deklarowany RTO** — jeśli rzeczywisty czas odtworzenia przekracza zadeklarowane RTO, plan DR wymaga korekty — to właśnie po to testujemy, nie zakładamy.
- **Weryfikacja integralności to osobny krok** — samo „odtworzenie się powiodło” nie wystarczy — dane muszą być kompletne i niezmodyfikowane, inaczej odtworzenie jest pozorne.
- **To ostatnie laboratorium dzisiejszego dnia** — domyka pełny cykl: prewencja (wczoraj) → detekcja/reagowanie (dziś rano) → ciągłość działania (teraz), gdy wszystko inne zawiedzie.

Debrief: test odtworzenia jako jedyny dowód, że backup działa

Posiadanie kopii zapasowej i posiadanie działającego planu odtworzenia to dwie różne rzeczy.

„Backup istnieje” to za mało

jedynym wiarygodnym dowodem sprawności planu DR jest udokumentowany, regularnie powtarzany test pełnego odtworzenia, nie sam fakt wykonywania kopii.

Testy powinny być zaplanowane cyklicznie

nie tylko raz, przy wdrożeniu — środowisko IT zmienia się, plan nieaktualizowany i nietestowany traci wiarygodność z czasem.

Dokumentowanie wyników testu

zmierzony czas odtworzenia i wynik weryfikacji integralności to dane wejściowe do przeglądu i ewentualnej korekty całej strategii DR.

Most do popołudnia

BCP/DR to obowiązek, który wraca wprost w wymogach regulacyjnych UoKSC, o których porozmawiamy w ostatnim bloku merytorycznym dzisiejszego dnia.

NIS2 i UoKSC: dyrektywa unijna a ustawa krajowa

BLOK 13

Ostatni blok merytoryczny — regulacje z perspektywy praktycznej specjalisty IT, nie prawnika.

NIS2 (dyrektywa UE 2022/2555)

akt unijny wyznaczający ramowe wymogi cyberbezpieczeństwa dla państw członkowskich; wejście w życie 16.01.2023, każde państwo wdraża ją do prawa krajowego.

UoKSC (Ustawa o Krajowym Systemie Cyberbezpieczeństwa)

polska implementacja NIS2 — to właśnie ten akt prawny, nie sama dyrektywa unijna, nakłada bezpośrednie, egzekwowalne obowiązki na polskie organizacje. Aktualny tekst: Dz.U. z 2026 r. poz. 252.

Dlaczego to rozróżnienie ma znaczenie praktyczne

w rozmowie z prawnikiem czy audytorem podstawą prawną konkretnego obowiązku w Polsce jest UoKSC (z numerem artykułu), nie sama dyrektywa NIS2.

Zakres podmiotowy

UoKSC dotyczy organizacji zakwalifikowanych jako podmiot kluczowy (PK) lub podmiot ważny (PW) — nie każdej firmy w Polsce.

Cel tego bloku: nie zastąpi porady prawnej — celem jest, żeby specjalista IT rozumiał, z czym wiążą się te przepisy operacyjnie, i wiedział, kiedy skonsultować się z działem prawnym/DPO.

Kim jest podmiot kluczowy i podmiot ważny (PK/PW)

Kwalifikacja zależy od sektora działalności i wielkości organizacji — sprawdzana wg polskich załączników do UoKSC.

1

Załącznik 1 UoKSC — 10 sektorów „kluczowych”

m.in. Energia, Transport, Bankowość i infrastruktura rynków finansowych, Ochrona zdrowia, Zaopatrzenie w wodę pitną, Infrastruktura cyfrowa, Zarządzanie usługami ICT, Podmioty publiczne.

2

Załącznik 2 UoKSC — 9 sektorów „ważnych”

m.in. Usługi pocztowe, Gospodarowanie odpadami, Produkcja/dystrybucja chemikaliów, Produkcja żywności, Produkcja, Dostawcy usług cyfrowych, Podmioty publiczne samorządowe.

3

Kryterium wielkości

Poza przynależnością sektorową liczy się wielkość organizacji (liczba zatrudnionych, obrót/suma bilansowa) — próg średniego/dużego przedsiębiorstwa.

4

Podmiot publiczny — kategoria szczególna

Występuje w OBU załącznikach — praktycznie każda jednostka administracji publicznej podlega UoKSC niezależnie od wielkości.

5

Praktyczna wskazówka

Jeśli Państwa organizacja nie wie, czy podlega UoKSC — pierwszy krok to sprawdzenie przynależności sektorowej wg załączników 1/2, nie zgadywanie.

Obowiązki organizacyjne: środki bezpieczeństwa wg NIS2 art. 21(2)

Dyrektywa unijna wyznacza kategorie ramowe — polska UoKSC (art. 8) rozwija je w bardziej szczegółowy katalog.

1

Analiza i zarządzanie ryzykiem

Systematyczna ocena ryzyka jako punkt wyjścia — dokładnie ta logika, o której mówiliśmy pierwszego dnia (zagrożenie × podatność × wpływ).

2

Obsługa incydentów

Procedury wykrywania, klasyfikacji i reagowania — bezpośrednio to, czym zajmowaliśmy się przez cały dzisiejszy dzień.

3

Ciągłość działania i zarządzanie kryzysowe

BCP/DR, kopie zapasowe, odtwarzanie po awarii — temat, który właśnie zamknęliśmy w bloku dwunastym.

4

Bezpieczeństwo łańcucha dostaw

Ocena bezpieczeństwa dostawców i podwykonawców ICT — temat, który wraca też przy CRA za chwilę.

5

Bezpieczeństwo w cyklu życia systemów (SDLC)

Uwzględnienie bezpieczeństwa w nabywaniu, rozwoju i utrzymaniu systemów — dokładnie DevSecOps, o którym mówiliśmy wczoraj.

6

Cyberhigiena, szkolenia i kryptografia

Świadomość personelu, regularne szkolenia, polityki szyfrowania danych — łączy tematy z obu dni szkolenia.

7

Kontrola dostępu, MFA i bezpieczeństwo zasobów ludzkich

IAM, MFA, zasady bezpieczne dla personelu — dokładnie blok ósmy dzisiejszego dnia.

Odpowiedzialność kierownika podmiotu i Pełnomocnik ds. Cyberbezpieczeństwa

Zgodność regulacyjna to nie wyłącznie sprawa działu IT — UoKSC nakłada osobistą odpowiedzialność na kierownictwo.

Odpowiedzialność kierownika podmiotu (art. 8c UoKSC)

kierownik podmiotu kluczowego/ważnego odpowiada osobiście za nadzór nad cyberbezpieczeństwem — delegowanie zadań na inną osobę NIE zwalnia go z tej odpowiedzialności.

Zakres decyzji kierownika (art. 8d UoKSC)

decyzje w zakresie systemu zarządzania bezpieczeństwem informacji, zapewnienie środków finansowych, przydział i nadzór zadań, zapewnienie świadomości personelu, nadzór nad zgodnością z prawem.

Obowiązkowe szkolenie kierownika (art. 8e UoKSC)

kierownik podmiotu ma obowiązek odbyć szkolenie z cyberbezpieczeństwa co najmniej raz w roku kalendarzowym — udokumentowane.

Pełnomocnik ds. Cyberbezpieczeństwa

funkcja operacyjna wyznaczana praktycznie w podmiotach publicznych — punkt kontaktowy i osoba nadzorująca bieżące wdrażanie wymogów, choć to kierownik pozostaje odpowiedzialny formalnie.

Uwaga metodologiczna: dokładny numer artykułu regulującego funkcję Pełnomocnika w aktualnym, znowelizowanym tekście UoKSC proszę zweryfikować bezpośrednio w ustawie przed wykorzystaniem w dokumentacji — w tym materiale skupiamy się na funkcji, nie na precyzyjnym numerze przepisu.

Zgłaszanie incydentów: 24h / 72h / 1 miesiąc

Precyzyjna terminologia i terminy wynikające wprost z art. 11 UoKSC — częsty punkt nieporozumień.

Incydent poważny

poprawna, ustawowa nazwa kategorii wyzwalającej obowiązek zgłoszenia (art. 2 pkt 7 UoKSC) — NIE „incydent znaczący”, mimo że to drugie określenie bywa powszechnie, błędnie używane.

24 godziny — wczesne ostrzeżenie

wstępne, szybkie powiadomienie właściwego CSIRT sektorowego o wystąpieniu incydentu poważnego (art. 11 ust. 1 pkt 4 UoKSC).

72 godziny — zgłoszenie incydentu poważnego

pełniejsze zgłoszenie z dodatkowymi szczegółami, w tym wstępną oceną skutków (art. 11 ust. 1 pkt 4a UoKSC).

1 miesiąc — sprawozdanie końcowe

liczony od momentu zgłoszenia z 72h — pełny raport z przebiegiem incydentu, podjętymi działaniami i wnioskami (art. 11 ust. 1 pkt 4c UoKSC).

Adresat zgłoszeń

właściwy CSIRT sektorowy (CSIRT NASK, CSIRT GOV lub CSIRT MON, w zależności od sektora) — nie dowolny organ.

Dlaczego to wraca dziś: te terminy to bezpośrednie regulacyjne uzupełnienie procesu reagowania na incydenty, który ćwiczyliśmy praktycznie w laboratoriach 12.1.1, 13.1.1 i 14.1.1 — dokumentacja z tamtych ćwiczeń to materiał wejściowy do takiego zgłoszenia.

CRA: SBOM i zgłaszanie podatności produktu

Cyber Resilience Act — regulacja skupiona na PRODUKCIE cyfrowym, nie na organizacji, która go używa.

SBOM (Software Bill of Materials)

- **Co to jest** — formalny, ustrukturyzowany wykaz wszystkich komponentów (bibliotek, zależności) wchodzących w skład danego produktu z oprogramowaniem.
- **Po co** — gdy w popularnej bibliotece ujawni się nowe CVE, SBOM pozwala natychmiast sprawdzić, które własne produkty faktycznie z niej korzystają — bez tego trzeba by przeszukiwać kod ręcznie.
- **Powiązanie z SCA** — narzędzia Software Composition Analysis, o których mówiliśmy wczoraj przy DevSecOps, to praktyczny sposób automatycznego generowania i utrzymywania SBOM.

Zgłaszanie podatności (CVD/VDP)

- **CVD (Coordinated Vulnerability Disclosure)** — proces skoordynowanego ujawniania podatności: badacz zgłasza lukę producentowi prywatnie, producent ma czas na łatkę, zanim szczegóły staną się publiczne.
- **VDP (Vulnerability Disclosure Policy)** — formalna polityka producenta opisująca, jak i gdzie zgłaszać znalezione podatności w jego produktach — CRA wymaga jej posiadania od producentów.
- **Zgłaszanie aktywnie wykorzystywanych podatności** — CRA nakłada na producentów obowiązek szybkiego zgłaszania do odpowiednich instytucji unijnych podatności aktualnie wykorzystywanych w atakach.

NIS2/UoKSC kontra CRA: organizacja kontra produkt

Ten sam podmiot może podlegać obu regulacjom jednocześnie, w dwóch różnych rolach.

NIS2/UoKSC — perspektywa operatora

jak organizacja zarządza bezpieczeństwem swoich systemów i procesów — obejmuje m.in. ciągłość działania, BCP/DR, o których mówiliśmy w bloku dwunastym.

CRA — perspektywa producenta

jakie cechy bezpieczeństwa musi mieć sam produkt cyfrowy wprowadzany na rynek, zanim trafi do klienta — obejmuje zarządzanie ryzykiem produktu i łańcuch dostaw komponentów.

Istotne rozróżnienie: CRA nie obejmuje BCP/DR

ciągłość działania i odtwarzanie po awarii to wyłącznie wymóg organizacyjny NIS2/UoKSC; CRA reguluje bezpieczeństwo produktu, nie proces jego odtwarzania u klienta.

Jeden podmiot, dwie role naraz

firma produkująca oprogramowanie i jednocześnie kwalifikująca się jako podmiot ważny wg UoKSC podlega OBU regulacjom jednocześnie, w dwóch różnych rolach — producenta i operatora.

Praktyczna checklista dla specjalisty IT: „Czy zarządzam systemami organizacji?” → myśl NIS2/UoKSC. „Czy tworzę/dostarczam produkt z komponentem cyfrowym?” → myśl CRA. Często odpowiedź brzmi: obie naraz.

Mapa certyfikacji CompTIA

Security+ jako jeden punkt na znacznie szerszej ścieżce certyfikacyjnej CompTIA.

1

Poziom podstawowy: A+, Network+

Fundamenty sprzętu, systemów operacyjnych i sieci — zalecany punkt startowy dla osób bez wcześniejszego doświadczenia w IT.

2

Security+ — punkt, w którym dziś jesteśmy

Pierwszy poziom specjalizacji w bezpieczeństwie, uznawany szeroko w branży i akceptowany przez amerykański Departament Obrony (DoD 8570) jako spełniający wymóg bazowy.

3

CySA+ (Cybersecurity Analyst)

Naturalny następny krok po Security+ — pogłębia dokładnie to, czym zajmowaliśmy się dzisiaj: monitoring, detekcję, analizę zagrożeń, reagowanie na incydenty.

4

PenTest+

Ścieżka ofensywna — testy penetracyjne, etyczny hacking, techniki ataku poznane teoretycznie wczoraj, tu rozwijane praktycznie i systematycznie.

5

CASP+ (SecurityX)

Poziom ekspercki — architektura bezpieczeństwa przedsiębiorstwa, zarządzanie ryzykiem na poziomie organizacyjnym, nie tylko technicznym.

Ścieżki kariery w cyberbezpieczeństwie

Security+ jako wspólny fundament dla kilku różnych, dobrze zdefiniowanych kierunków rozwoju zawodowego.

Analitik SOC (Tier 1 → Tier 2 → Tier 3)

ścieżka operacyjna, dokładnie ta, którą praktykowaliśmy dzisiaj — monitoring, detekcja, coraz bardziej samodzielna analiza i reagowanie na kolejnych poziomach.

Specjalista ds. bezpieczeństwa aplikacji (AppSec)

pogłębienie wczorajszego bloku czwartego: OWASP, SAST/DAST/SCA, współpraca z zespołami deweloperskimi nad DevSecOps.

Inżynier/Architekt bezpieczeństwa sieci

pogłębienie bloków trzeciego i piątego z wczoraj: projektowanie segmentacji, firewalli nowej generacji, architektury Zero Trust.

Specjalista GRC (Governance, Risk, Compliance)

pomost między techniką a dzisiejszym blokiem regulacyjnym — zarządzanie zgodnością z NIS2/UoKSC/CRA, audyty, polityki bezpieczeństwa.

Pentester / Red Teamer

ścieżka ofensywna, naturalnie prowadząca do PenTest+ — systematyczne testowanie bezpieczeństwa z perspektywy atakującego.

Refleksja na koniec: proszę zastanowić się, który blok z tych dwóch dni wzbudził w Państwu największe zainteresowanie — to często najlepsza wskazówka co do naturalnego kierunku dalszego rozwoju zawodowego.

Co dalej: przygotowanie do egzaminu SY0-701

To szkolenie to solidny fundament — droga do zdania egzaminu wymaga jeszcze systematycznego powtórzenia.

Struktura egzaminu — przypomnienie z Dnia 1

dziewięćdziesiąt pytań, dziewięćdziesiąt minut, pięć domen o różnej wadze (12%/22%/18%/28%/20%).

Materiały otrzymane w ramach szkolenia

prezentacje slajdów z obu dni, arkusz ćwiczeń (gap analysis, rejestr ryzyk, wzór procedury IR), mapa certyfikacji, lista zasobów do dalszej nauki.

Dalsza nauka — zasoby zewnętrzne

CERT Polska, NIST (publikacje SP 800), ENISA, polskie portale branżowe (np. sekurak.pl) — regularnie aktualizowane źródła wiedzy.

Znaczenie pytań performance-based

część pytań na egzaminie to nie tylko wybór odpowiedzi, ale symulacje praktyczne — dokładnie dlatego dwanaście laboratoriów w tym szkoleniu miało znaczenie wykraczające poza samą teorię.

Realistyczny harmonogram

większość zdających poświęca dodatkowe 4–8 tygodni samodzielnego powtórzenia po szkoleniu tego typu, zanim podejdzie do egzaminu.

Podsumowanie Dnia 2 i całego szkolenia

Od prewencji, przez detekcję i reagowanie, po ciągłość działania i zgodność regulacyjną — pełny cykl bezpieczeństwa.

Monitoring i SIEM

widoczność jako warunek konieczny każdej dalszej reakcji; korelacja, strojenie reguł, walka z alert fatigue.

IAM i Zero Trust

od modelu zamku i fosy do ciągłej weryfikacji każdego żądania — tożsamość jako nowy obwód bezpieczeństwa.

Detekcja i forensics

IOC kontra IOA, klasyfikacja alertów, analiza ruchu sieciowego jako niezależne źródło prawdy o przebiegu incydentu.

Reagowanie i automatyzacja

cykl NIST SP 800-61, playbooki jako proceduralna pamięć zespołu, SOAR jako mnożnik skali.

Ciągłość działania i regulacje

BCP/DR jako ostatnia linia obrony, NIS2/UoKSC/CRA jako formalne ramy tego wszystkiego, o czym mówiliśmy przez dwa dni.

Największa lekcja tych dwóch dni: bezpieczeństwo to nie pojedynczy produkt ani jednorazowy projekt — to spójny, cykliczny proces: prewencja → detekcja → reagowanie → wnioski → z powrotem do prewencji.

Walidacja, Q&A i zamknięcie szkolenia

Test teoretyczny z wynikiem generowanym automatycznie — zgodnie z metodą walidacji z karty usługi BUR.

Test teoretyczny (walidacja)

zgodnie z kartą usługi, każdy z siedmiu efektów uczenia się jest weryfikowany testem teoretycznym z wynikiem generowanym automatycznie.

Pytania otwarte

czas na dowolne pytania dotyczące materiału z obu dni, laboratoriów, ścieżki dalszej nauki lub samego egzaminu SY0-701.

Zaświadczenie ukończenia szkolenia

warunek: obecność na co najmniej 80% zajęć — zgodnie z warunkami uczestnictwa karty usługi BUR.

Materiały do pobrania

slajdy z obu dni, arkusz ćwiczeń, mapa certyfikacji i lista zasobów zostaną przekazane Państwu po zakończeniu szkolenia.

Kontakt po szkoleniu

w razie pytań po zakończeniu kursu zachęcam do kontaktu — dane kontaktowe podane są w karcie usługi i materiałach szkoleniowych.

Dziękuję za te dwa dni: za aktywny udział, dobre pytania i pracę w laboratoriach — powodzenia na egzaminie CompTIA Security+ SY0-701.

ZAKOŃCZENIE SZKOLENIA

Pytania i odpowiedzi

Wracamy do pytań zaparkowanych w trakcie obu dni oraz do tych, które pojawiły się przy ćwiczeniach.

✓ Konsultacja poszkoleniowa: 30 minut on-line w ciągu 30 dni – umów ją mailowo



Dziękuję za udział w szkoleniu

ltmastery.com@gmail.com · Dostawca Usług w Bazie Usług Rozwojowych, ID 204299

Źródła: wykaz-ksc.gov.pl · gov.pl/cyber · cert.pl · enisa.europa.eu