DODATEK B

Formularze

METKA DOWODU

Data	*Numer sprawy*	*Numer metki*
Wymagana zgoda ☐ *Tak* ☐ *Nie*	*Podpis osoby wyrażającej zgodę*	*Kod kreskowy dowodu*

Opis elementów (wliczając nadzorcę)

Opis kontenera

Osoba otrzymująca dowód	*Podpis*

INFORMACJE O OBSŁUDZE DOWODU

Zrzeczenie się przez *Lokalizacja*	*Data/godzina*	*Powód*	*Otrzymany przez* *Lokalizacja*
Od *Lokalizacja*	*Data/godzina*	*Powód*	*Do* *Lokalizacja*
Od *Lokalizacja*	*Data/godzina*	*Powód*	*Do* *Lokalizacja*
Od *Lokalizacja*	*Data/godzina*	*Powód*	*Do* *Lokalizacja*
Od *Lokalizacja*	*Data/godzina*	*Powód*	*Do* *Lokalizacja*
Od *Lokalizacja*	*Data/godzina*	*Powód*	*Do* *Lokalizacja*
Ostateczne rozporządzenie dowodem		*Data* *Podpis*	

OPIS SYSTEMU KLIENTA

Data	*Numer sprawy*	*Numer metki dowodu*
Kierownik projektu		

INFORMACJE O PROCESORZE I OBUDOWIE

Marka/model
Numer seryjny

UWAGI

OPIS SYSTEMU BĘDĄCEGO ŹRÓDŁEM DOWODÓW

Data	*Numer sprawy*	*Numer metki dowodu*

Nadzorca	*Lokalizacja*

INFORMACJE O SYSTEMIE BIOS

Typ/wersja systemu BIOS	*Data/godzina wydania systemu BIOS*
Kolejność rozruchowa	*Skalibrowana data/godzina*

INFORMACJE O PROCESORZE I OBUDOWIE

Marka/model	*Pamięć*
Numer seryjny	*Procesor*
Uwagi	

PRZECHOWYWANIE DANYCH

DRIVE 0

Ustawienia zworek	*Marka/model*	*Pojemność*
	Numer seryjny	
	Uwagi	
	Rodzaj obrazu ☐ *EnCase* ☐ *dd/surowy* ☐ *Inny*	

Czas tworzenia	*Początek*	*Koniec*	*Czas trwania*
Oryginalny skrót napędu			
Skrót EnCase			

DRIVE 1

Ustawienia zworek	*Marka/model*	*Pojemność*
	Numer seryjny	
	Uwagi	
	Rodzaj obrazu ☐ *EnCase* ☐ *dd/surowy* ☐ *Inny*	

Czas tworzenia	*Początek*	*Koniec*	*Czas trwania*
Oryginalny skrót napędu			

UWAGI

DANE ANALITYKA

Nazwisko	*Data*	*Podpis*

Arkusz wykrycia incydentu

NR SPRAWY: _____ **DATA:** _____

Informacje kontaktowe	
☐	**Osoba wypełniająca ten formularz** **Nazwisko:** _____ **Nr telefonu:** _____ **Inne:** _____

Źródło danych dotyczących wykrycia	
☐	**Data wykrycia:** _____
☐	**Rodzaj wykrycia:** **Automatyczny / Przez człowieka / Inny**
☐	**Nazwa źródła:** _____

Szczegółowe informacje	
☐	**Recenzja wykrycia?** **Tak / Nie** **Nazwisko recenzenta:** _____ **Przejrzano surowe dane/alarm?** **Tak / Nie** **Wykrycie wydaje się słuszne?** **Tak / Nie / Brak pewności**

Arkusz wykrycia incydentu

NR SPRAWY: _____ **DATA:** _____

Źródło danych	
☐	**Data instalacji:** _____
☐	**Data ostatniej aktualizacji lub konserwacji:** _____
☐	**Typowa częstotliwość błędów:** **Wysoka / Średnia / Niska**

Przechowywanie dowodów/danych	
☐	**Normalny czas przechowywania danych:** _____
☐	**Czy dane dotyczące wykrycia zostały zachowane?** **Tak / Nie** **Data zapisania:** _____ **Kontakt:** _____

Arkusz podstawowych informacji o incydencie

NR SPRAWY: _____ **DATA:** _____

Informacje dotyczące daty	
☐	**Data zgłoszenia incydentu:** _____
☐	**Data wykrycia incydentu:** _____

Informacje kontaktowe	
☐	**Osoba wypełniająca ten formularz** **Nazwisko:** _____ **Nr telefonu:** _____ **Inne:** _____
☐	**Osoba zgłaszająca incydent** **Nazwisko:** _____ **Nr telefonu:** _____ **Inne:** _____
☐	**Osoba wykrywająca incydent** **Nazwisko:** _____ **Nr telefonu:** _____ **Inne:** _____

Arkusz podstawowych informacji o incydencie

NR SPRAWY: _____ **DATA:** _____

Podsumowanie	
☐	**Status incydentu:** _____
☐	**Typ incydentu:** _____
☐	**Sposób wykrycia:** _____
☐	**Dotknięte systemy**
☐	**Osoby wiedzące o incydencie**
☐	**Ograniczenia dotyczące rozpowszechniania informacji:** _____

Arkusz informacji o szkodliwym programie

NR SPRAWY: _____ **DATA:** _____

Informacje kontaktowe	
☐	**Osoba wypełniająca ten formularz** **Nazwisko:** _____ **Nr telefonu:** _____ **Inne:** _____

Wykrycie	
☐	**Data wykrycia:** _____ **System:** _____ **Sposób wykrycia:** _____ **Szczegóły dot. wykrycia:** _____ **Czy wirus jest aktywny?** **Tak / Nie / Nie wiadomo**

Właściwości pliku	
☐	**Nazwa pliku:** _____ **Rozmiar:** _____ **Katalog:** _____ **Suma kontrolna (podać typ):** _____

Arkusz informacji o szkodliwym programie

NR SPRAWY: _____ DATA: _____

Inne pytania	
ANALIZA **Stan analizy; czy wirus został przeanalizowany pod kątem sieciowych i hostowych wskaźników zagrożenia**	
DYSTRYBUCJA **Czy wirus został przesłany do firm zewnętrznych przez proces automatyczny lub pracownika? Jeśli tak, należy podać nazwy wszystkich zewnętrznych jednostek i opisać cel przekazania im danych**	
PRZECHOWYWANIE **Czy została zachowana kopia wirusa (ręcznie lub w procesie kwarantanny)?**	

Arkusz danych dotyczących sieci

NR SPRAWY: _____ DATA: _____

Informacje kontaktowe

Osoba wypełniająca formularz

Nazwisko: _____

Nr telefonu: _____

Inne: _____

Istotne adresy IP i domeny

#	Data znalezienia	Adres IP lub domena
1		
2		
3		
4		
5		
6		
7		
8		
9		

#	Data	Monitorowanie	Blokada	Czarna dziura	Inne (opis)
1					
2					
3					
4					
5					
6					
7					
8					
9					

Arkusz danych dotyczących sieci

NR SPRAWY: _____ DATA: _____

Inne pytania	
MONITOROWANIE **Sprawdzić, czy prowadzony jest monitoring. Sprawdzić, czy administratorzy sieci włączyli urządzenia do przechwytywania ruchu sieciowego, kto się tym zajmuje, gdzie się to odbywa (fizycznie i logicznie), gdzie są składowane dane oraz kto ma do nich dostęp. Wyjaśnić reguły filtrowania przechwytywanych danych, napisać, czy zrzut zawiera pełną treść sesji, czy tylko informacje nagłówkowe (połączenia).**	
PRZECHOWYWANIE INFORMACJI **Jeśli zachowywane są jakiekolwiek dane, napisać w jaki sposób jest to robione i gdzie znajduje się magazyn. Podobnie jak przy podawaniu szczegółów dotyczących indywidualnych systemów, należy zadbać o prawidłowe obchodzenie się z danymi dotyczącymi sieci.**	