Do wykonania jest dostarczenie rozwiązania do obsługi incydentów w firmie. Incydenty, które będą zgłaszane do zespołu rozwiązującego incydenty:

- naruszenia finansowe (kradzieże i wyłudzenia)

- podejrzenie popełnienia czynności, które mogą skutkować niekorzystnie dla firmy (np. przekazanie informacji o obecnie składanych ofertach do konkurencji)

- podejrzenie przestępstwa

Obecnie także brakuje źródła centralnej informacji, co użytkownicy robią w systemach, w które mogą posłużyć do ewentualnych do incydentów. Systemy, z których będą pochodziły logi to:

* Rejestr czasu pracy
* BidMaster (system do zarządzani ofertami)
* System księgowy

Lista tych systemów może w czasie rozwoju wzrosnąć.

Takie informacje (logi z systemów) mogą posłużyć zespołowi do spraw bezpieczeństwa do wyrywkowego sprawdzania poczynań użytkownika lub posłużyć jako dowód podczas weryfikacji incydentu.

Część informacji, takich jak wyciąg z kont bankowych firmowych czy aktualnie składane oferty, są dostępne w systemach istniejących w firmie. Do tych systemów członkowie zespołu do obsługi incydentów mają dostęp. Nie będzie można tych danych pobierać do nowo powstającego systemu, ponieważ są to dane wrażliwe. Jednak do celów dowodowych można robić zrzuty ekranów z tych systemów, które mogą dowieść popełnienia wykroczenia przez pracownika. Taki zrzut ekranu wraz z adnotacją należy zapisać w systemie.

Każde zgłoszenie informacji musi przejść przez trzy etapy:

* Wstępna weryfikacja (czy zgłoszenie zawiera dostatecznie wystarczające informację do podjęcia weryfikacyjnego). Jeżeli ich brak, to należy wysłać żądanie o dodatkowe informacje do zgłaszającego.
* Weryfikacja właściwa (sprawdzenie wszystkich możliwych miejsc w celu weryfikacji zgłoszenia, kontakt z osobami, które mogą pomóc w weryfikacji zgłoszenia)
* Akceptacja wyników przeprowadzonego postępowania przez kierownika zespołu
* Wysłanie wyników przeprowadzonego dochodzenia do zgłaszającego

Wyjątkiem są weryfikacje wyrywkowe, które nie muszą przechodzić etapu wstępnej weryfikacji (ponieważ takiej dokonuje osoba, która decyduje się wszcząć dochodzenie).

W trakcie weryfikacji incydentu, może zajść konieczność komunikacji z osobą podejrzaną w celu wyjaśnienia zaistniałej sytuacji. Taka komunikacja powinna odbyć się za pomocą systemu i nie powinna być realizowana z prywatnego maila. Również komunikacja z osobami, które mogą dostarczyć nam materiałów dowodowych, powinna się się odbyć za pomocą systemu.

W trakcie pracy, pracownik zespołu weryfikacji incydentów może wyrywkowo przeglądać logi przesłane przez systemy, w celu sprawdzenia poczynań danego lub danych użytkowników. Przeglądanie logów ma odbywać się jako wygenerowanie raportu z logów. Raport taki ma być dostępny dla osoby generującej i jego kierownictwa. Na podstawie takiego raportu można rozpocząć dochodzenie (wyrywkowa weryfikacja).

Weryfikacje wyrywkowe, nie muszą przechodzić etapu wstępnej weryfikacji (ponieważ takiej dokonuje osoba, która decyduje się wszcząć dochodzenie).

Dodatkowo, system posiada mechanizm, który samodzielnie przeszukuje logi systemu i powiadamia o potencjalnie niebezpiecznych poczynaniach wykonywanych przez użytkowników (np. bardzo częste przeszukiwanie danych finansowych nie będąc pracownikiem stricte związany z pracami księgowymi). Wyszukanie takiej nieprawidłowości skutkuje automatycznym złożeniem zgłoszenia i podlega takim samym etapom, jak zgłoszenie złożone przez osobę.

Kierownik akceptuje wyniki dochodzenia przeprowadzonego przez pracownika zespołu do incydentów. Kierownik ma także możliwość zwrócenia dochodzenia do pracownika w celu doszczegółowienia dochodzenia.

//tutaj trochę na odwal się

Jeżeli brak wykrytych incydentów, zgłaszający jest powiadamiany o braku incydentu.

Jeżeli wykryto incydent, wysłanie powiadomienie do zgłaszającego o wynikach dochodzenia wraz z informacją o dalszych działaniach (o ile nie wpłynie to na dobro dochodzenia) i Ew. kontakt z kadrami w celu zwolnienia pracownika, jeżeli doszło do przestępstwa.

W firmie zespół działa obecnie w formie papierowej. Nie ma obecnie miejsca, w którym można by składować papierowe (lub z e-mail) wnioski o weryfikacje incydentu. Zamawiający chce stworzyć możliwość wprowadzenia do systemu starych wniosków. Miało by to posłużyć głównie do weryfikacji spraw, które zostały już zamknięte (np. w przypadku, gdy ktoś chciałby powrócić do starego zgłoszenia incydentu). Do takich spraw można dołączać załączniki (pdy, zrzuty ekranów etc)

Bardzo ważne jest też to, żeby pracownicy, który pracują w zespole bezpieczeństwa byli też rozliczani z każdej operacji, która będą wykonywać w nowo powstałym systemie.