Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

Opis przedmiotu zamówienia

1. System musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.

2. System musi zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.

3. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.

4. Dostarczone rozwiązanie musi być systemem klasy SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń. Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania.

5. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.

6. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.

7. System musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians).

8. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum: na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego i tabelarycznego.

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

9. Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.

10. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.

11. System musi pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, MS Word, MS Excel, jpg, png.

12. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.

13. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.

14. Dla zarejestrowanych zdarzeń/ incydentów system automatycznie wyznaczy ścieżkę ataku i zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.

15. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.

16. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).

17. Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.

18. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

19. W ramach obsługi zdarzeń/incydentów/podatności system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

organizację w przypadku materializacji zagrożenia.

20. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np.: przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.

21. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.

22. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.

23. System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.

24. System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:

a. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,

b. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,

c. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,

d. wyświetlanie lokalizacji zasobów określonego rodzaju,

e. wyświetlanie najbardziej narażonych zasobów teleinformatycznych,

f. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.

25. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).

26. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.

27. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.

28. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.

29. System musi umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstwie których listy te będą modyfikowane. System musi umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

wierszu np: login, adres IP, Aplikacja.

30. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych, system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.

31. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w scenariuszach obsługi incydentów. Scenariusze obługi incydentów muszą być uzależnione od ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).

32. System musi umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (tzw. Playbook'ach).

33. System musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:

a. wzbogacanie danych kontekstowych,
b. gromadzenie artefaktów danych związanych z incydentem,
c. współpraca z innymi członkami zespołu,
d. komunikacja w ramach zespołu,
e. wykonywanie czynności związanych z reakcją na incydent,
f. raportowanie przebiegu incydentu.

34. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów/podatności. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.

35. System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (tzw. Playbook'ów).

36. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.

37. System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego.

38. System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: indentyfikacja IoC.

39. System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów.

40. System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

incydentu.

41. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.

42. Parsowanie warunkowe i hierarchiczne musi być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich w warunkach.

43. Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.

44. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.

45. System musi zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email.

46. Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach.

47. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

48. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability.

49. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.

50. System musi posiadać predefiniowany zestaw parserów.

51. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych oraz formaty JSON, XML, CIS, LEEF, Syslog. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.

52. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.

53. System musi umożliwiać definiowanie zakresu i czasu uczenia, np.: analiza logowania użytkowników po

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu.

54. System musi mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence, Active Directory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika.

55. System musi posiadać funkcję „automatycznej korelacji", tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego", będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły.

56. System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.

57. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.

58. Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).

59. Rozwiązania SIEM, SOAR, narzędzia elektronicznej dokumentacji, oraz baza wiedzy mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

60. Interfejs użytkownika Systemu musi być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.

61. Funkcjonowanie rozwiązania musi być oparta w całości o architekture „on-premise", w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego.

62. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2019), Redhat/Oracle Linux (minimum 7.x).

63. Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.

64. System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z: MS SQL lub Oracle.

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

65. System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów.

66. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

67. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD, minimum to: nazwa użytkownika, login, e-mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane.

68. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

69. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).

70. System musi być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.

71. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.

72. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK.

73. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

74. Tworzenie raportów PDF musi posiadać opcje automatycznego harmonogramu, który w zadanym wcześniej momencie pozwoli na wysyłkę utworzonego raportu do zdefiniowanych odbiorców poczty email. Konfiguracja harmonogramu tworzenia raportów PDF i ich wysyłki powinna być dostępna poprzez graficzny interfejs użytkownika.

75. System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.

76. System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko).

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

77. Interfejs systemu powinien umożliwiać z poziomu jednego okna widoku weryfikację wszystkich działań użytkownika na osi czasu, które spowodowały wzrost ryzyka. Z poziomu tego widoku system umożliwi przejście do opisu konkretnego zdarzenia.

78. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.

79. System pozwoli na prezentację danych w postaci tzw. „Dashboard", tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.

80. System musi automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych, konta serwisowe, użytkowników uprzywilejowanych, użytkowników w randze kierowniczej i zarejestrowane stacje robocze celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu.

81. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.

82. System musi umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje.

83. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów.

84. System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany).

85. System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności.

86. System powinien mieć logikę automatycznego przypisywania zgłoszeń, minimum na podstawie dostępności operatora, jego obciążenia, oraz cech zasobu którego dotyczy incydent, minimum typ zasobu (np.: serwer lub stacja robocza), krytyczność oraz realizowane z jego udziałem usługi z katalogu usług.

87. System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.

88. System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.

89. System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamkniecie głównego

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach.

90. System musi pozwalać na określenie automatycznych oraz inicjowanych przez operatora reakcji na incydenty bezpieczeństwa i/lub zdarzenia, polegających na integracji z systemami zewnętrznymi w celu uzyskania dodatkowych informacji, dotyczących incydentu/zdarzenia lub podjęcia akcji zapobiegawczych.

91. System musi umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.)

92. System musi być wyposażony w moduł obsługi elektronicznej dokumentacji zbiorów danych osobowych, umożliwiający prowadzenie rejestru czynności i kategorii czynności przetwarzania danych osobowych, opisanych w Art. 30 RODO. Moduł może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania.

93. System w ramach modułu ochrony danych osobowych musi oferować możliwość:

a. szacowania ryzyka cyber zagrożeń dla zasobów IT przetwarzających dane osobowe;

b. szacowania ryzyka ryzyka utraty dostępności, poufności i integralności danych wykonywana dla poszczególnych celów przetwarzania (uwzględniająca zabezpieczenia techniczne i organizacyjne) wraz z oceną skutków dla ochrony danych osobowych (tzw. Data Protection Impact Assessment);

c. prowadzenia wykazów programów i systemów informatycznych, służących przetwarzaniu danych osobowych;

d. prowadzenia ewidencji osób upoważnionych, wraz z możliwością generowania upoważnień oraz oświadczeń o poufności;

e. prowadzenia ewidencji udostępnień danych osobowych;

f. rejestracji i obsługi roszczeń związanych z przetwarzaniem danych osobowych.

94. System musi umożliwiać zdefiniowanie obszarów przetwarzania zbiorów danych osobowych wraz z listą zastosowanych dla nich zabezpieczeń fizycznych.

95. System musi umożliwiać rejestrację zgłoszeń incydentów dotyczących danych osobowych związanych z poszczególnymi zbiorami, jednostkami organizacyjnymi, osobami, lokalizacjami oraz związanych z zasobami informatycznymi.

96. System musi uwzględniać obsługę incydentów danych osobowych zapewniając możliwość automatycznego ich wykrywania na podstawie logów z systemów informatycznych biorących udział w ich przetwarzaniu. System musi umożliwiać dostrojenie reguł wykrywania zarówno w kontekście informacji pozyskanych z logów jak i parametrów elektronicznej dokumentacji związanej z ich przetwarzaniem. Dedykowana obsługa pozwoli na automatyczne przydzielenie zespołu obsługi do incydentu, dotyczącego zasobu przetwarzającego dane osobowe oraz uruchomieniu adekwatnego scenariusza obsługi, np.: dla konsekwencji wycieku danych osobowych.

97. System SIEM oraz wszystkie moduły towarzyszące muszą umożliwiać równoczesną pracę co najmniej 10 operatorów oraz objąć monitoringiem min. 800 zasobów IT. Przez zasób IT rozumie się serwery fizyczne lub

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

serwery wirtualne oraz komputery użytkowników. Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.

98. System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.

99. Zamówienie realizowane będzie w okresie 18 miesięcy od dnia zawarcia umowy, zgodnie ze wzorem umowy. Wykonanie zamówienia zostanie podzielone na etapy:

a. Etap I – wdrożenie – w terminie do 6 miesięcy od dnia zawarcie umowy. Szczegółowy zakres i wytyczne Etapu I określa Załącznik nr 1;

b. Etap II – utrzymanie i wsparcie systemu – w okresie 12 miesięcy, od dnia podpisania protokołu odbioru.

100. Po zakończonym wdrożeniu należy zapewnić bezpłatne 4-dniowe certyfikowane szkolenia (5 x 8h) w zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać przeprowadzone dla maksymalnie 10 osób i uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządzanie incydentami bezpieczeństwa; korzystanie ze scenariuszy obsługi incydentów, kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.) – łącznie 3 dni (3x8h), oraz modułu ochrony danych osobowych – łącznie 1 dzień (1x8h). Szkolenia muszą być zakończone egzaminem i certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.

101. Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. szczegółową dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).

102. Wraz z systemem wykonawca dostarczy pakiet e-szkoleń z zakresu bezpieczeństwa teleinformatycznego i RODO zgodnie z poniższymi wymaganiami:

a) Szkolenie w wersji elektronicznej (e-learning) z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego oraz RODO. Szkolenia dedykowane dla pracowników biurowych (nietechnicznych) pracujących z komputerami i przetwarzających różnego rodzaju informacje o różnym poziomie poufności. Szkolenia muszą być w formie gotowego produktu dostarczanego Zamawiającemu bezzwłocznie po złożeniu zamówienia / podpisaniu umowy. Zamawiający musi mieć możliwość swobodnego wykorzystania szkoleń bez ograniczeń czasowych oraz liczby odbiorców. Szkolenia nie mogą być w formie usługi.

b) Szkolenie musi być w postaci oddzielnych lekcji dla każdej z kategorii z niżej opisanego zakresu. Szkolenie powinno zawierać minimum 500 slajdów. Czas jednej lekcji (tematu) powinien oscylować w granicach 15-30 min. Lekcje powinny być multimedialne z wykorzystaniem scenek rodzajowych z możliwością odtworzenia w postaci dźwiękowej z użyciem lektora. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej. Podczas lekcji powinna być na bieżąco weryfikowana wiedza (uwaga) użytkownika poprzez np. ćwiczenia sprawdzające. Forma e-lerning.

c) Szkolenie musi posiadać oddzielne lekcje dla co najmniej następujących zagadnień:

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

- Zakres temtyczny dla bezpieczeństwa teleinformatycznego

- Czym jest bezpieczeństwo informacji;
- Aspekty prawne związane z bezpieczeństwem informacji;
- Czym jest phishing? Przykłady aktualnych cyberataków i sposoby ochrony przed nimi
- Zasady korzystania z Internetu;
- Zasady korzystania z portali społecznościowych;
- Zasady korzystania z poczty elektronicznej i zagrożenia z tym związane;
- Zasady korzystania z bezpiecznych haseł;
- Zagrożenia i sposoby zabezpieczania sprzętu mobilnego;
- Metody pozyskiwania informacji (socjotechnika);
- Bezpieczeństwo w zakresie płatności elektronicznych;
- Bezpieczeństwo fizyczne w zakresie zabezpieczania pomieszczeń, dokumentacji, sprzętu IT;
- Czym jest ransomware i jak wygląda w praktyce;
- Jak bezpiecznie korzystać z menedżera haseł w praktyce;
- Uważaj by nie zostać „mułem finansowym”
- Bezprzewodowe życie.
- Praca zdalna - jak zrealizować ją bezpiecznie?
- Vishing… co to jest?
- Test z imiennym certyfikatem ukończenia kursu

- Zakres tematyczny dla RODO

- Wprowadzenie do ochrony danych osobowych.
- Słów kilka o prywatności.
- Ochrona danych osobowych nie tylko w pracy.
- Zasady przetwarzania danych osobowych.
- Zgoda na przetwarzanie danych osobowych.
- Profilowanie danych.
- Ochrona danych osobowych poprzez zarządzanie ryzykiem.
- Koncepcja ochrony prywatności od początku procesu.
- Dokumentacja przetwarzania danych osobowych.
- Jakie prawa przysługują MOJEJ OSOBIE?
- Zarządzanie incydentami.
- Ustawa sektorowa.
- Dane osobowe a kodeks pracy po zmianach wynikających z wejścia w życie ustawy sektorowej
- Monitoring wizyjny po wejściu w życie RODO
- Jest już RODO, czas na DODO – różnice między RODO, a DODO (dyrektywa policyjna)
- Test sprawdzający wiedzę z imiennym certyfikatem ukończenia kursu.

d) Forma szkolenia:

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

- Szkolenie musi posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia. Atrakcyjna forma to m.in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk – głos lektorów indywidualny dla każdej z postaci występujących w szkoleniu.
- Szkolenie musi posiadać interaktywną formę, zwiększającą zaangażowanie osób uczących się. Szkolenie musi zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu/ szkolenia.
- Lekcje szkolenia muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT i RODO. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników komputerów (np. wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych, właściwe postępowanie w razie incydentu, ustawy RODO) niż samą teorię bezpieczeństwa IT i RODO.
- Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.
- Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001.
- Forma szkolenia, grafika, animacja, postaci powinny być spójne i takie same dla zakresu tematycznego z bezpieczeństwa informacji i RODO.

e) **Wymagania techniczne:**
Szkolenie w wersji elektronicznej musi być zgodne ze standardem umożliwiającym prezentację na **platformie MOODLE w wersji 3 lub wyższej**. Szkolenie powinno być dostarczone w technologii HTML5. Szkolenia powinny być podzielone tematycznie w taki sposób, aby można było operować (zarządzać dostępnością, harmonogramem, treściami itp.) poszczególnymi tematami z osobna oraz dokonywać modyfikacji ze strony zamawiającego.
f) **Warunki licencji:** Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na szkolenie.

Szczegółowy zakres i wytyczne procesu wdrożenia systemu

1. Proces wdrożenia systemu określony w Etapie I powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania w okresie 6 miesięcy.

2. Proces wdrożeniowy podzielony zostanie są na 4 obszary:
a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);
b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR;

d. Obszar Danych Osobowych, zakładający zainstalowanie i skonfigurowanie modułu Ochrony Danych Osobowych i jego integracji z pozostałymi modułami systemu (tj. SIEM i SOAR).

3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:

a. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej);

b. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:

- konsultacje w przygotowaniu infrastruktury zamawiającego do instalacji systemu,
- instalację lub import maszyny wirtualnej typu „software appliance",
- zestawienie połączenia zdalnego,
- aktywację licencji,
- wstępną konfigurację,
- import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);

c. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:

- przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
- uruchomienie reguł wykrywania;

d. Prace audytowe, w tym:

- pasywną analizę transmisji sieciowej:
  - ruch z/do serwerów webowych i aplikacyjnych,
  - ruch z/do serwerów baz danych,
  - ruch z/do serwerów pocztowych,
  - ruch z/do kontrolerów domenowych,
  - ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
  - ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,
- konsultacje w ramach otrzymanych wyników;
- zebranie danych audytowych wymaganych do sporządzenia raportu;

e. Analizę podatności, w zakresie:

- integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;
- przygotowanie reguł priorytetów i importu krytycznych podatności;

f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:

- zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
- potencjalne wektory ataków dla wykrytych zagrożeń;
- wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
- rekomendacja zabezpieczeń;
- zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

g. Transfer wiedzy w formie spotkania podsumowującego, obejmujący interpretację przez analityka wyników analizy ujętej w raporcie z systemu;

4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:

a. Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła zdarzeń obejmują:

- zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);
- sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam)
- centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);
- kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;
- systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);
- system SIEM
- w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;

b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;

c. Podłączenie reguł detekcji;

d. Podłączenie i konfiguracja mechanizmów UEBA:

- integracja z Active Directory
- utworzenie profili użytkowników UBA
- utworzenie profili hostów EBA
- import reguł bezpieczeństwa UEBA, utworzenie customowych reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia
- obserwacja i doprecyzowanie postępu uczenia maszynowego, wykluczenie/ dodanie nowych reguł zdarzeń użytkowników/ hostów.

d. Dostrojenie systemu, w tym reguł priorytetyzacji zdarzeń i incydentów, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji;

5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać kolejno:

a. Pracę z konsultantem (m.in. wprowadzenie do scenariuszy wbudowanych w systemie, analizę wymaganych zmian, związanych z ich dostosowaniem; pomoc przy generowaniu API KEY dla wbudowanych akcji);

b. Konfigurację zespołów obsługi celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi;

c. Konfigurację mechanizmów powiadamiania;

6. Obszar Danych Osobowych zakłada przeprowadzenie następujących prac wdrożeniowych w zakresie modułu danych osobowych:

a. Przygotowania rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania – wprowadzenie min. 10 czynności/ kategorii czynności;

Biuro Projektu
ul. Nadbystrzycka 36B, pokój 118
20-618 Lublin
tel.: (+48 81) 538 43 49
e-mail: m.latkowska@pollub.pl
zprpl.pollub.pl

b. Wprowadzenia kluczowych usług przetwarzających dane osobowe – wprowadzenie min. 5 kluczowych usług;

c. Wprowadzenia przykładowych udostępnień - wprowadzenie min. 5 udostępnień;

d. Wprowadzenia przykładowych powierzeń - wprowadzenie min. 5 powierzeń;

e. Wprowadzenia przykładowych upoważnień - wprowadzenie min. 5 upoważnień;

f. Wprowadzenia jednostek organizacyjnych - wprowadzenie min. 10 jednostek;

g. Wprowadzenie stanowisk pracowników - wprowadzenie min. 5 stanowisk.