

Spector 360.

Opis systemu i specyfikacja techniczna

Oprogramowanie Spector 360 zostało zaprojektowane z myślą o **monitoringu pracowników** i możliwości wygenerowania takich nieedytowalnych raportów, aby w razie potrzeby mieć możliwość uwiarygodnienia materiału zebranego przez ten system. Spector 360 archiwizuje strony internetowe odwiedzane przez osoby zatrudnione, wysłaną i otrzymaną korespondencję mailową, zapisy z czatów i komunikatorów, wszystkie wpisy wykonywane za pomocą klawiatury, przesłane pliki, wydrukowane i edytowane dokumenty czy uruchamiane aplikacje. Spector 360 **poprawi wydajność pracy i bezpieczeństwo organizacji** poprzez możliwość blokowania stron internetowych, portów, komunikatorów internetowych, a także tworzenie alertów z wcześniej zdefiniowanych słów kluczowych wysyłanych np. na **skrzynkę email administratora**.

Poprzez narzędzie pracujące jak kamera umożliwi **dokładny podgląd** tego co w danej chwili robił pracownik.

Spector 360 gromadzi informacje dotyczące aktywności internetowej i pracy z komputerem każdego z pracowników. Dane te zgromadzone w bazie są dostępne w każdej chwili. Można z nich wygenerować **ponad 50 rodzajów raportów**. Z każdego raportu natomiast, administrator może być przeniesiony jednym kliknięciem do informacji tekstowych, innych raportów lub Snapshotu z danej aktywności użytkownika.

Do najważniejszych cech oprogramowania Spector 360 należy:

- Pełna analiza aktywności użytkownika w trybie rzeczywistym.
 - Gromadzenie materiału zgodnie z zasadami informatyki śledczej.
 - Badanie integralności plików (np. binarnych, konfiguracyjnych), rejestrów itp. Program rejestruje pełną aktywność zalogowanego użytkownika. Rejestruje dostęp do wszystkich plików, znaki wpisywane z klawiatury, wykonuje zrzuty ekranu związane z każdą działalnością aplikacji/użytkownika. Dostępne są rozległe mechanizmy raportowania i przeglądania zdarzeń. Na podstawie zebranych informacji możliwa jest analiza i weryfikacja wszystkich wykonywanych operacji.
 - Badanie aktywności procesów zachodzących w systemie informatycznym (zmiany aktywności procesów, jakie programy/procesy są uruchamiane w trakcie sesji, itp.). Oprogramowanie potrafi śledzić pełną aktywność zalogowanego użytkownika oraz w ograniczonym zakresie działalność aplikacji działających w tle. Zainstalowanie lub uruchomienie jakiegokolwiek aplikacji zostanie zalogowane, z zastrzeżeniem, iż jeśli aplikacja jest nieautoryzowana i działa w tle to może być konieczna indywidualna analiza jej funkcjonalności.
 - Badanie, do jakich plików miał dostęp użytkownik/proces (np. jakie pliki zostały otwarte, itp.). Oprogramowanie loguje dostęp do wszystkich plików na poziomie aplikacji/procesów.
 - Badanie otwieranych gniazd do połączeń TCP, UDP, ICMP, itp. Oprogramowanie loguje otwieranie gniazd do połączeń TCP, UDP, ICMP, itp. w warstwie systemu.
 - Działanie w trybie ukrytym (stealth).
 - Funkcjonalność keyloggera. Następuje rejestracja znaków wpisywanych z klawiatury, zrzutów ekranu związanych z każdą działalnością aplikacji/użytkownika.
 - Wysyłanie wszystkich informacji na zdalny komputer w sposób bezpieczny. Rozwiązanie wspiera bezpieczeństwo poprzez szyfrowanie i autentyfikację.
 - Zdalne zarządzanie.
 - Możliwość alarmowania w czasie rzeczywistym (np. wysłanie e-maila o podejrzonej działalności, itp. z zastrzeżeniem do 10 minutowego opóźnienia ze względu na sposób działania oprogramowania łączący ze sobą skuteczność z optymalizacją obciążenia sprzętu i łącz.
 - Możliwość odtworzenia działań administratora, np. w przypadku analizy powłamaniamiowej.
 - Dostępne są rozbudowane raporty i głęboka analiza działań użytkownika systemu.
-

Szczegółowe funkcjonalności dotyczące monitoringu pracowników w trybie ukrytym:

1. Nagrywanie komunikacji email:

- Protokoły POP3/SMTP/IMAP,
- Natywnie MS Exchange i Outlook, Hotmail, Yahoo Mail, AOL Internet Email i innych webowych skrzynek pocztowych,
- Tworzenie kopi email wraz załącznikiem,
- Filtrowanie (od/do/źródło/załącznik/data/itp.), sortowanie i wyszukiwanie słów kluczowych,
- Przykładowe dostępne raporty:
 - i. Użytkownicy wysyłający i odbierający najwięcej emailów,
 - ii. Użytkownicy wysyłający najwięcej załączników,
 - iii. Użytkownicy wysyłający korespondencję do zdefiniowanych domen (np. konkurencji),
 - iv. Użytkownicy wysyłający emaile ze zdefiniowanym słowem kluczowym (np. porno, torrent i inne),
 - v. Domeny, na które były wysyłane / odbierane emaile.

2. Nagrywanie stron internetowych:

- Śledzenie aktywności użytkownika w Internecie,
- Wyszukiwanie słów kluczowych w adresie i treści strony,
- Przechwytywanie ściąganych plików (multimedia, oprogramowanie, nielegalne treści),
- Możliwość blokowania wejść na strony internetowe (tworzenie białych i czarnych list),
- Przykładowe dostępne raporty:
 - i. Najczęściej odwiedzane strony internetowe,
 - ii. Strony, na których użytkownicy spędzają najwięcej czasu,
 - iii. Użytkownicy odwiedzający najwięcej stron internetowych,
 - iv. Użytkownicy spędzający najwięcej czasu na przeglądaniu stron internetowych.

3. Nagrywanie transferów plików:

- Zarówno upload jak i download plików,
- Sesje HTTP, FTP, P2P (Kazaa, Limewire, itp.), transfer w ramach komunikatorów,
- Możliwość przechwytywania spyware, adware i innego malware, oraz treści zabronionych i niezgodnych z polityką firmy, np. multimediiów i oprogramowania,
- Informacja o używanym protokole transmisji, usługach, nazwach i typach plików,
- Przykładowe dostępne raporty w postaci wykresów:
 - i. Użytkownicy transferujący najwięcej plików,
 - ii. Użytkownicy ściągający najwięcej plików,
 - iii. Użytkownicy wysyłający najwięcej plików.

4. Nagrywanie słów wpisywanych w wyszukiwarkach internetowych:

- Zapis wyników z wielu wyszukiwarek (np. google.com, msn.com, yahoo.com, ask.com, altavista.com, gigablast.com, alltheweb.com, go.com, live.com, teoma.com i inne),
- Zapis dat i czasów wyszukiwania,
- Raport w postaci wykresów z najczęściej wpisywanych słów dla danego użytkownika,
- Przykładowe dostępne raporty:
 - i. Użytkownicy wyszukujący najczęściej,
 - ii. Najczęściej wybierane wyszukiwarki,
 - iii. Najczęściej wyszukiwane słowa.

5. Nagrywanie rozmów z czatów i komunikatorów internetowych:

- Wiele rodzajów komunikatorów (Skype, Miranda, Trillian, Gaim, AOL, IRC, MSN, AIM/ICQ, Yahoo, XMPP, Web IMs, OSCAR80, MSN Exchange i inne),
 - Możliwość wyszukiwania słów kluczowych,
 - Możliwość blokowania protokołów,
 - Przykładowe dostępne raporty:
 - i. Najczęściej używane komunikatory,
 - ii. Użytkownicy najczęściej użytkujący czaty i komunikatory.
-

6. Przechwytywanie **wpisów klawiaturowych**:

- Funkcjonalność keyloggera,
- Ukryte i prawdziwe wpisy blokowane przez aplikacje (np. hasła pod postacią * 'gwiazdka'),
- Kombinacje klawiszy (SHIFT + znak, CTRL + znak i inne),
- Kategoryzacja wpisów wg aplikacji, użytkownika, czasu, komputera itp.,
- Skanowanie wpisów po słowach kluczowych,
- Przykładowe dostępne raporty:
 - i. Użytkownicy wpisujący najwięcej znaków,
 - ii. Użytkownicy wpisujący najwięcej znaków do danych aplikacji (np. CRM, Office czy inne).

7. Kontrola **użytkowania oprogramowania**:

- Nagrywanie każdej uruchomionej aplikacji (np. CRM, pakietu office, przeglądarki, komunikatorów, aplikacji zabronionych),
- Przechwytywanie czasów załączenia, otwarcia, aktywności, użytkownika otwierającego aplikację, nazwę komputera,
- Informacja o czasach braku aktywności użytkownika,
- Przykładowe dostępne raporty:
 - i. Najczęściej uruchamiane aplikacje,
 - ii. Najczęściej używane aplikacje,
 - iii. Częstotliwość użytkowania danej aplikacji (np. CRM, Office, przeglądarka i inne),
 - iv. Trendy użytkowania danej aplikacji w czasie.

8. Informacje o **aktywności sieciowej użytkownika**:

- Wszystkie informacje o połączeniach sieciowych,
- Nagrywanie ruchu sieciowego; przechwytywanie: użytkownika, aplikacji, nazwy domeny, informacji o połączeniu: IP, czasów startu i czasów trwania, liczby połączeń, używanych portów, paczek wysłanych i odebranych,
- Identyfikacje streamów muzyki i video, wykrywanie stron z gramami on-line,
- Możliwość śledzenia podejrzanych połączeń,
- Przykładowe dostępne raporty:
 - i. Aplikacje, które charakteryzuje największy ruch sieciowy,
 - ii. Zużycie łącza przez dane domeny (np. Youtube, iTunes, Rapidshare, firmowa i inne),
 - iii. Zużycie przepustowości łącza przez danego użytkownika.

9. Nagrywanie **obiegu i historii dokumentów**:

- Nagrywanie dokumentów wg kategorii: utworzenie nowego pliku, nadpisanie, kasowanie, zmiana nazwy, kopiowanie na nośnik typu pendrive, CD/DVD, floppy, dysk sieciowy czy inne źródło, nagrywanie na dysku optycznym, drukowanie,
- Śledzenie specyficznych plików lub typów plików,
- Przykładowe dostępne raporty:
 - i. Użytkownicy kopiujący pliki na przenośne dyski,
 - ii. Typy plików przenoszone na przenośne dyski,
 - iii. Aktywności użytkownika dot. danego pliku (np. drukowanie, kopiowane i inne wykonywane na pliku „wyniki finansowe.xls”),
 - iv. Aktywności użytkowników dot. danego pliku (np. kto miał dostęp do pliku „plan marketingowy.doc”),

10. Kontrola **słów kluczowych**:

- Monitoring wszystkich wyspecyfikowanych słów kluczowych,
 - Ustawienie powiadomienia np. email,
 - Wykonanie Snapshot wpisu,
 - W alercie informacje o: słowie, czasie wpisu, zalogowanym użytkowniku, aplikacji, itp.,
 - Przykładowe dostępne raporty:
 - i. Najczęściej wpisywane zdefiniowane słowa kluczowe,
 - ii. Użytkownicy wpisujący dane słowa kluczowe,
 - iii. Aplikacje, w których zostało wpisane dane słowo kluczowe.
-

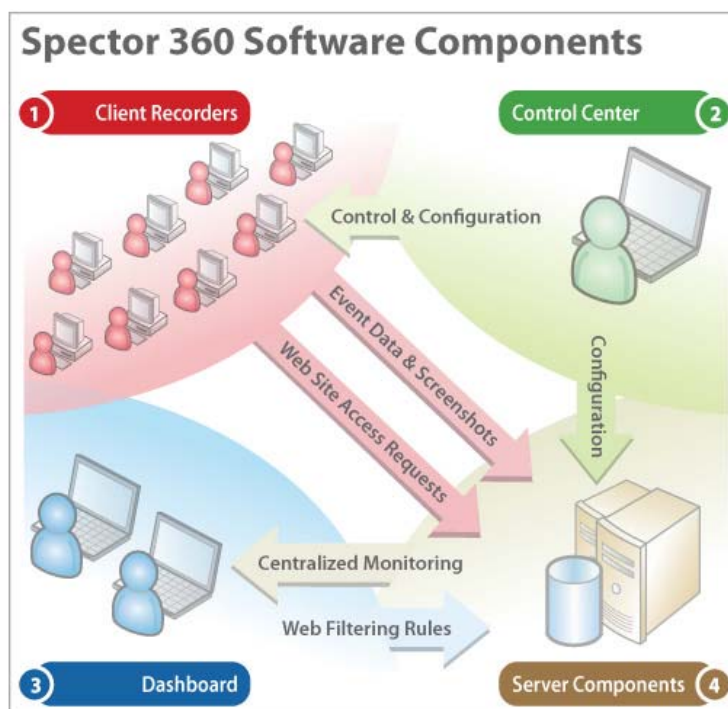
iv. Trendy alertów słów kluczowych w czasie.

11. Nagrywanie czasów aktywności pracowników:

- Nagrywanie czasów logowań, wylogowywań, aktywności i braku aktywności użytkownika,
- Tabela czasów aktywności użytkowników komputerów.

Architektura systemu:

System Spector 360 zbudowany jest z kilku komponentów niezbędnych do szybkiej, wydajnej i łatwej w obsłudze pracy.



1. **Client Recorders** to komponent zainstalowany i skonfigurowany na każdym komputerze użytkownika w sieci. Może być procesem działającym w trybie ukrytym, wtedy użytkownik nie będzie wiedział, że jest monitorowany. Komponent ten jest bardzo łatwy w konfiguracji pod poszczególnego użytkownika sieci zgodnie z polityką firmy (np. zablokowanie poszczególnych domen, portów, specyficznego ruchu, tworzenie alertów do słów kluczowych, itp.).
2. **Control Center** jest elementem odpowiedzialnym za konfigurację i zarządzanie poszczególnymi **Client Recorders**. Pozwala również na zdalną instalację i deinstalację klientów oprogramowania.
3. **Dashboard** to konsola administracji oprogramowaniem. Jest aplikacją graficzną opartą o .NET. Z poziomu **Dashboard** wysyła się zapytania do bazy danych SQL, aby uzyskać żądane informacje. Występuje możliwość zainstalowania więcej niż jednej konsoli administracyjnej przekazanej do kontroli innym osobom, np. do monitoringu poszczególnych działów w firmie. **Dashboard** i **Control Center** mogą być instalowane na tej samej maszynie, ale nie jest to zalecane ze względów bezpieczeństwa.
4. **Server Components**. Występują 4 softwareowe komponenty serwerowe. Wszystkie mogą znajdować się na jednej maszynie lub być dystrybuowane w sieci dla zwiększenia wydajności.
 - a. Primary Server. Rezyduje z reguły na tym samym serwerze co baza SQL i odpowiada za takie usługi jak upgrade i update narzędzia i wszystkich **Client Recorders**.
 - b. SQL Serwer i Baza Danych. Służy do przechowywania wszystkich zebranych informacji z monitorowanych komputerów. Jej zarządzaniem, włączając w to backupy i archiwizację zajmuje się **Dashboard**.
 - c. Data Vault. To element, do którego wszystkie **Client Recorders** wysyłają informacje w predefiniowanych interwałach czasowych. Następnie ten składa całość skategoryzowanych informacji do bazy danych.

- d. Web Filter Service. Jest komponentem odpowiedzialnym za blokowanie i udzielanie dostępu do danych stron internetowych zgodnie z ustalonymi regułami. Tworzone filtry mogą dotyczyć wszystkich użytkowników, grup użytkowników lub pojedynczego pracownika. Filtry tworzone są w [Dashboard](#).

Szkolenie z zakresu obsługi oprogramowania Spector 360.

Skrócona agenda:

1. Wdrożenie oraz konfiguracja usług wchodzących w skład programu Spector360
 - omówienie usług
 - instalacja poszczególnych usług
 - konfiguracja
 - diagnostyka
 2. Omówienie oraz konfiguracja programu monitorującego
 - przygotowanie konfiguracji programu
 - dystrybucja oprogramowania monitorującego
 - diagnostyka
 3. Omówienie programów wchodzących w skład Spector360
 - Control Center (omówienie poszczególnych funkcji programu: instalacja programu, zarządzanie zainfekowanymi komputerami, rozwiązywanie problemów)
 - Dashborad (omówienie poszczególnych funkcji programu: zarządzanie użytkownikami – przypisywanie uprawnień, analiza zgromadzonych danych, zarządzanie bazą danych)
 4. Przedstawienie metodologii przeprowadzania analizy
 - wykorzystanie słów kluczy
 - alerty
 - analiza pracy poszczególnego pracownika
-