BVS

novicom

BUSINESS VISIBILITY SUITE

Network & Business Edition

Precyzyjne narzędzie do wizualizacji procesów komunikacji sieciowej, modelowania usług biznesowych oraz infrastruktury teleinformatycznej

Zarządzanie zasobami IT jest podstawowym warunkiem skutecznych reakcji na incydenty w dynamicznie zmieniającym się cyber-środowisku. Przegląd zależności między adresacjami IP, dokonywany w określonym przedziale czasu pozwala - zarówno analitykom bezpieczeństwa, jak i operatorom SOC - zdobywać informacje w trakcie zabiegów serwisowych, a tym samym umożliwia dokonanie szybkiej identyfikacji oraz analizy, wykrytych w infrastrukturze sieciowej incydentów.

Business Visibility Suite (BVS) autorstwa firmy Novicom w wyjątkowy sposób łączy świat technologii IT oraz usług biznesowych organizacji, wykorzystując intuicyjne modelowanie zależności między obiema płaszczyznami. Kluczową wartością systemu jest w pełni zautomatyzowany process gromadzenia metadanych komunikacji sieciowej z uwzględnieniem zależności między urządzeniami IT oraz możliwość modelowania wskazanych usług biznesowych organizacji.

BVS POZWALA NA ZABEZPIECZENIE ZALEŻNOŚCI WYSTEPUJĄCYCH POMIĘDZY:

Usługami biznesowymi | **Usługami aplikacji** | **Usługami technicznymi** | **Urządzeniami IT**

Business Visibility Suite to narzędzie umożliwiające natychmiastową weryfikację i wizualizację komunikacji sieciowej adresu IP, celem przeprowadzenia błyskawicznej reakcji względem incdentu oraz identyfikacji takowych incydentów. Narzędzie pozwala również zrozumieć wpływ incydentu na procesy biznesowe organizacji, zapewniając szerszy kontekst w procesie ochrony przed cyber-zagrożeniami.

Za sprawą zautomatyzowanego procesu komunikacji sieciowej, będącego częścią BVS, można w prosty sposób dokonać rozpoznania w rzeczywistym stanie infrastruktury teleinformatycznej oraz zależnościach między zasobami IT organizacji (widoczność zasobów IT pośród urządzeń sieciowych). Narzędzie umożliwia wyszukanie danych wejsciowych, co pozwala dokonać błyskawicznej reakcji wobec wykrytego incydentu, biorąc pod uwagę jego wpływ na oferowane przez organizację usługi.

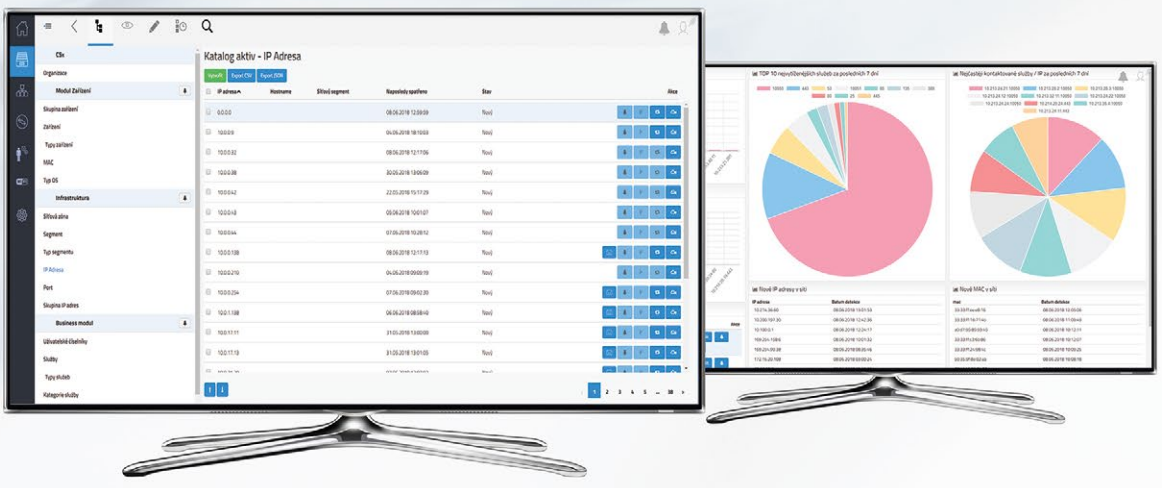
BVS firmy Novicom oferuje 2 moduły:

1. BVS Network Edition (moduł sieciowy): wizualizacja obecnego stanu infrastruktury IT oraz rejestrowanie komunikacji pomiędzy urządzeniami IT, które składają się na obraz zachowania sieci. Innymi słowy jest to wgląd w rodzaj ruchu w określonej lokalizacji sieciowej.

2. BVS Business Edition (moduł biznesowy) - przedłużenie możliwości modułu BVS Network Edition. Pozwala na modelowanie usług biznesowych i ich zależności w ramach infrastruktury IT, zapewniając dodatkowy i tym samym pełny kontekst sytuacji, w tym aktualną analizę krytycznych systemów i urządzeń IT oraz ich ważności w procesie zapewnienia kluczowych usług dla klientów końcowych.

Przegąd właściwości i możliwości narzędzia BVS firmy Novicom (Network & Business Edition)

Wizualizacja zasobów IT (assetów) w ramach infrastruktury komunikacyjnej	Określenie relacji miedzy obiektami, będącymi elementami procesu komunikacji sieciowej. Wersja Business narzędzia oferuje dodatkowo możliwość wizualnego modelowania zależności między usługami, aplikacjami i urządzeniami.
Graficzny interfejs	Możliwość analizowania zależności między obiektami w sieci w sposób hierarchiczny, począwszy od głównych węzłów i segmentów sieci, poprzez urządzenia określone konkretnymi adresami IP, kończywszy na opierających na nich usługach i portach, które z nimi korespondują (analiza typu drill-down).
Alertowanie	Alarmy aktywujące się w przypadku zmian w infrastrukturze. Powiadomienia o właścicielach zasobów. Powiadomienia dotyczące nowych, nieautoryzowanych narzędzi wprowadzone celem uniknięcia wystąpienia incydentów bezpieczeństwa.
Automatyczne gromadzienie metadanych urządzeń podłączonych do sieci i ich komunikacji z innymi elementami sieciowymi.	Wykorzystanie autonomicznej sondy, celem wydobycia metadanych przedstawiających komunikację sieciową i wizualizację sieci w czasie rzeczywistym. Podstawowe informacje dotyczące połączeń komunikacyjnych (segment sieci, źródło IP, destynacja IP, protokół, usługa destynacji - port komunikacyjny destynacji).
Możliwość tagowania nowych węzłów komunikacyjnych (urządzeń)	W celu grupowania elementów podlegających identycznym wymaganiom audytowym lub wewnętrznym wytycznym możliwe jest ich tagowanie.
Wizualizacja przychodzącej/ wychodzącej komunikacji określonego urządzenia IT	Adresy IP komunikujące się z portami innych urządzeń - komunikacja przychodząca do usług, które działają na portach konkretnych adresów IP
Repozytorium informacji o zasobach	• Nazwa zasobu • Typ zasobu • Identyfikator zasobu (opierający się np. na adresie IP, MAC, porcie, itd.) • Administrator zasobu • Metadane zdefiniowane przez użytkownika
Przegląd zasobów organizacji	Eksportowany do pliku XLS, CSV.
Timeline	Porównanie obecnego statusu infrastruktury IT do jej stanu z przeszłości w kontekście określonego przedziału czasowego (np. Poprzez podkreślenie nowo zidentyfikowanych zasobów).
Podgląd zdarzeń	Podgląd zdarzeń w formie interaktywnego, graficznego dashboardu (zakłada m.in. możliwość podejrzenia szczegółów konkretnego elementu).
Centralne wyszukiwanie pełnotekstowe (fulltext)	Opcja wyszukania urządzenia z wykorzystaniem jakiegokolwiek atrybutu.
Retencja danych i wydajność	Obsługa i przechowywanie dużego wolumenu danych wejściowych (ponad 10GB danych dziennie) oraz magazynowanie przez określony okres czasu kluczowych metadanych, wymaganych przy procesie dochodzeniowym w przypadku wystąpienia incydentu.
Customizowany dostęp do konkretnych części aplikacji	Autentykacja użytkownika, zabezpieczony dostęp do określonych elementów aplikacji na podstawie zdefiniowanych ról użytkowników.



BVS Network Edition

Moduł podstawowy: **BVS Network Edition** pomaga określić następujące zagadnienia:

- Jakie urządzenia są obecnie podłączone do sieci?
- Czy narzędzia te są autoryzowane?
- Które z urządzeń w sieci nie są dłużej wykorzytywane (tzw. dead woods)?
- Które połączenia zostały dopiero co nawiązane i które z urządzeń dokonują próby komunikacji? Czy jest to oznaka działania urządzenia, zarażonego złośliwym oprogramowaniem?
- Kto jest administratorem urządzenia?
- Jakie usługi działają w ramach sieci?
- Jakie inne urządzenia będą miały wpływ na dostępność urządzenia monitorowanego?
- Jaka jest historia komunikacji (profil) określonego urządzenia i jakie zmiany zostały wprowadzone?
- Jak wygląda grupa urządzeń, które komunikowały się z określonym adresem IP w zdefiniowanym okresie czasowym?
- Jakie zmiany zostały w ostatnim czasie dokonane na urządzeniu (otwarcie portów, zmiana ryzyka, podatności, itp.)?

BVS Network Edition - przypadki zastosowania:

1. **Migracja infrastruktury teleinformatycznej do chmury**
   > Lokalizacja zasobu (segment, właściciel, ryzyko)
   > Rozpoznanie wszystkich usług i zależności
   > Eksport macierzy komunikacji urządzenia
2. **Identyfikacja skali cyber-incydentu**
   > Organizacja otrzyma informację na temat możliwej kompromitacji systemu
   > Adresacja IP systemu jest wymieniona jako identyfikator
   > Narzędzie wizualizuje wszystkie urządzenia dotknięte incydentem w określonym okresie czasowym
3. **Implementacja NAC (Network Access Control)**
   > Natychmiastowe rozpoznanie aktualnego środowiska sieciowego pozwala na szybsze wdrożenie narzędzi NAC, w tym narzędzia AddNet firmy Novicom

BVS Business Edition - przypadki zastosowania:

1. **Wsparcie działań zespołów SOC**
   > Priorytetyzacja incdydentów i prowadzonego śledztwa pod kątem krytyczności zasobu dla organizacji
   > Błyskawiczna identyfikacja skali cyber-incydentu
   > Raportowanie z poziomu usług biznesowych
2. **Planowanie zmian infrastruktury z uwzględnieniem wpływu na utrzymanie ciągłości usług**
   > Szybkie przygotowanie Business Impact Analysis (BIA)
   > Identyfikacja i zarządzanie informacjami dotyczącymi aktualnych zasobów wraz określeniem usług, z którymi są związane
3. **Podstawy do optymalizacji infrastruktury IT**
   > Dane umozliwiajce rozróżnienie zasobów ktytycznych od tych pozbawionych tego znaczenia
   > Identyfikacja „Single Point of Failure"

BVS Business Edition

Moduł **Business Edition** swoją funkcjonalnością ukierunkowany jest na zespoły operacyjne SOC, managerów IT i personel odpowiedzialny za bezpieczeństwo cyfrowe organizacji, który nadzoruje proces dostarczania usług, ich dostępność, w tym połączenie ich z odpowiednimi zasobami IT i okreslenie możliwych wskaźników ryzyka.

- Stworzenie logicznej mapy zasobów, odzwierciedlającej usługi organizacji z poziomu technicznego, aplikacji i znaczenia biznesowego.
- Powiadomienia zmian w zasobach IT i ich wpływie na zdefiniowane usługi.
- Wizualne modelowanie zależności miedzy usługami biznesowymi, aplikacjami, usługami IT oraz zasobami (Business Impact Analysis - BIA) połączone z automatyzacją identyfikacji zasobu i jego zachowania.
- Identyfikacja wpływu zdarzeń operacyjnych na usługi biznesowe organizacji (scenariusze typu: what if?).
- Wgląd w wykryte w systemach IT podatności i ich znaczenia dla usług na nich opartych (piorytetyzacja procesu eliminacji ryzyk z najwyższym wskaźnikiem wpływu na krytyczne usługi organizacji).
- Zapewnienie ciągłości usług poprzez lepszy wgląd we wspierającą ją infrastrukturę IT.

Wartość dodana Novicom Business Visibility Suite (BVS)

- Proste i intuicyjne narzędzie, znacząco wspierające proces szybkiego wykrywania cyber-incydentów.
- Szybka orientacja w złożonym środowisku komunikacji sieciowej.
- Mapowanie zachowań infrastruktury i komunikacji sieciowej klienta celem byskawicznego aktywowania usług SOC.
- Identyfikacja infrastruktury sieciowej i urządzeń podłączonych do sieci (np. wykluczenie tzw. „shadow IT").
- Monitoring komunikacji sieciowej i Wi-Fi.
- Szybka identyfikacja relacji i zależności komunikacji sieciowej między urządzeniami IT w celu obniżenia czasu implementacji i konfiguracji narzędzi NAC (Network Access Control).
- Integracja z NAC umożliwia uzyskanie kompleksowej perspektywy, począwszy od poziomu usług biznesowych, skończywszy na obszarze zdefiniowanych urządzeń fizycznych.
- Wymaga minimalnej interakcji ze strony klienta, będąc wydajnym narzędziem w dostarczaniu podstawowych informacji, które dotyczą zakresu adresacji uwzględniającego komunikujące się ze sobą elementy.
- Identyfikuje i w prosty sposób utrzymuje informacje o związkach i zależnościach pomiędzy usługami biznesowymi / aplikacjami oraz infrastrukturą - byskawicznie definiując, które usługi są wystawione na ryzyko cyberzagrożeń.
- Przejrzysta i bezproblemowa migracja infrastruktury chmurowej dzięki podglądowi zależności między systemami, które mają podlegać migracji a główną infrastrukturą sieciową. Zapewnia to niezawodność migracji wszystkich potrzebnych systemów i zapobiega przestojom w procesie dostawy usług.
- Lepsze rozplanowanie kosztów obsługi urządzeń, z uwzględnieniem opartych na nich usług biznesowych i ryzyku na jakie są narażone.
- Oszczędność czasu jaka wiąże się z uzwględnieniem podstawowego kontekstu informacyjnego, przypisanego bezpośrednio do zasobu (nie trzeba za każdym razem przeszukiwać kilku narzędzi aby znaleźć konkretną informację).
- Błyskawiczne zdefiniowanie aktualnej „kondycji infrastruktury" oraz określenie potencjalnych zagrożeń bezpieczeństwa (podjęcie działań prewencyjnych wobec niekontrolowanego uruchomienia nowych usług sieciowych, itp.).
- Wsparcie działań w obszarze BIA (Business Impact Analysis).

Zespoły IT i SOC zmagają się z problemem podjęcia szybkiej reakcji wobec incydentu bezpieczeństwa ze względu na brak znajomości środowiska IT, które mają chronić.

Wymagania techniczne dla systemu BVS firmy Novicom

Poniższe urządzenia są instalowane w środowisku IT klienta:

- Fizyczna sonda do monitoringu połączeń sieciowych (standardowy stojak 1U, z dwoma interfejsami sieciowymi - dla danych SPAN / 10Gbit / interfejsy monitoringu przełączników sieciowych + 1Gbit / dla komunikacji serwera BVS).
- Opcjonalne fizyczne sondy Wi-Fi do monitoringu spektrum Wi-Fi (standardowe urządzenia Mini PC, kompatybilne z większością standardów Wi-Fi).
- Zarządzanie i kolektor na sprzęcie HW dostarczany razem z rozwiązaniem BVS lub w ramach własnych zasobów klienta.
- Wsparcie urządzeń VMware i fizycznych.
- Wykorzystanie sprawdzonego sprzętu Appliance Novicom.

Wdrożenie Novicom BVS

- Proces wdrożenia oparty jest na najlepszych praktykach zaczerpniętych z metodologii wdrożeniowej Novicom (Novicom Implementation Methodology - NIM).
- Podczas pierwszej fazy wdrożenia, w ramach sieci klienta zostaje zaimplementowana niezbędna infrastruktura BVS oraz uruchomiona sonda modułu BVS Network.
- Moduł BVS Business może zostać efektywnie wykorzystany po wykonaniu analizy BIA (Business Impact Analysis).

Współpraca w ramach zadań realizowanych w procesie wdrożenia Novicom BVS

- Podłączenie sond celem monitorowania przełączników (switchy) infrastruktury.
- Ustalenie zakresu definicyjnego dla monitorowanych segmentów.
- Interpretacja wybranych parametrów komunikacji do analizy.
- Zapewnienie połączenia pomiędzy komponentami BVS.
- Zapewnienie dostępu do kluczowych usług sieciowych - DNS i NTP.
- Zdalny dostęp dla dwukierunkowej komunikacji (2-way communication) oraz dostęp z/do urządzenia (Operator narzędzia BVS > Środowisko klienta; Środowisko klienta > Operator narzędzia BVS).

PL-2019-02

novicom
NETWORK MANAGEMENT HAS NEVER BEEN EASIER

Novicom, s.r.o.
Praga, Republika Czeska
www.novicom.eu
sales@novicom.eu

BVS