BVS

BUSINESS VISIBILITY SUITE

Network & Business Edition

Ein Tool zur klaren Visualisierung von Netzwerkkommunikation sowie zur Gestaltung von Geschäftsdienstleistungen und IT-Infrastrukturen.

Die Verwaltung von IT-Assets ist die Grundvoraussetzung für eine erfolgreiche Reaktion auf Vorfälle in einer sich schnell verändernden Cyberumgebung. Ein Überblick über die Beziehungen zwischen IP-Geräten im Zeitverlauf liefert sowohl Sicherheitsanalysten als auch SOC-Betreibern wichtige Informationen für potenzielle Service-Eingriffe, eine schnelle Identifizierung und die Untersuchung von Sicherheitsvorfällen in der Netzwerkinfrastruktur.

Novicom BVS verbindet auf ideale Art und Weise die Welt der IT-Technologie mit den Geschäftsprozessen des Unternehmens durch intuitive Darstellung der Abhängigkeiten zwischen diesen beiden Ebenen. Der Hauptvorteil von BVS ist eine automatisierte Metadatensammlung von Netzwerk-Kommunikationsbeziehungen zwischen IT-Geräten.

MIT BVS KÖNNEN SIE DIE FOLGENDEN BEZIEHUNGEN AUFRECHT ERHALTEN

Business Visibility Suite ist ein Tool zur unmittelbaren Überwachung und Visualisierung der Netzwerkkommunikation von IP-Geräten, das eine schnelle Reaktion auf Vorfälle und die Identifizierung von Sicherheitsvorfällen in der Infrastruktur ermöglicht. BVS hilft auch dabei, die Auswirkungen von Vorfällen auf bereitgestellte Geschäftsdienste zu verstehen und Sicherheitsbedrohungen zu verhindern.

Novicom BVS bietet die beiden folgenden Module an:

1. BVS Network Edition - die Darstellung des aktuellen Zustands der IT-Infrastruktur und die Erfassung der Kommunikation zwischen IT-Geräten liefern ein Gesamtbild des Netzwerkverhaltens - welche Art von Datenverkehr an einem bestimmten Ort stattfindet.

2. BVS Business Edition – erweitert die Fähigkeiten von BVS-Netzwerk-Edition. Es ermöglicht die Darstellung von Geschäftsdiensten und deren Abhängigkeiten von der IT-Infrastruktur, bietet einen aktuellen Überblick über die IT und eine Bewertung der kritischen IT-Geräte und deren Bedeutung für die Endkunden.

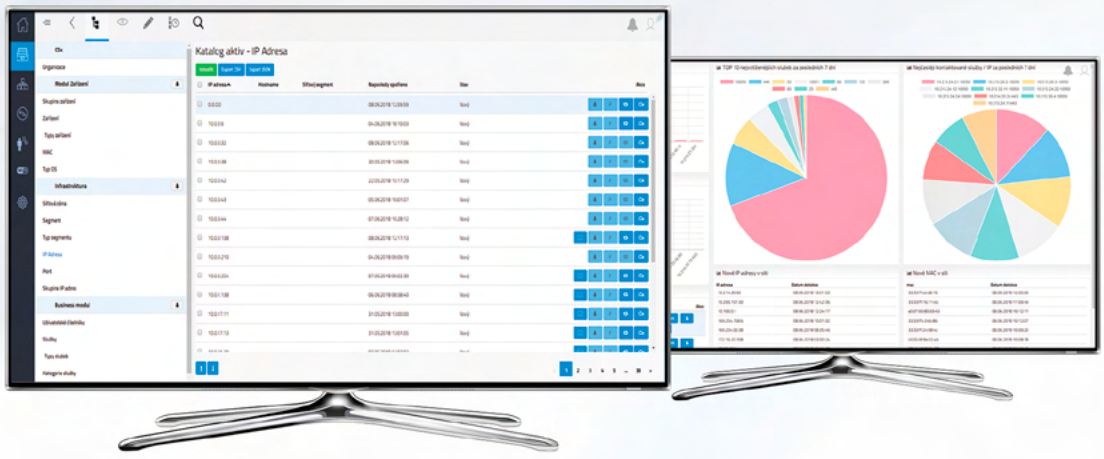
Wer kann BVS nutzen:

- IT (Infrastrukturoptimierung, Tagesbetrieb)
- IT-Sicherheit (analytische und forensische Aktivitäten, Untersuchung von Angriffsausbreitungsvektoren)
- Sicherheit (Geräte-Schwachstelle, Business Services, Risiko, Auswirkungen, Kontinuität)
- Inhaber von Anwendungen und Business Services
- Manager
- Security Operation Center (SOC)
- Systemintegratoren

IT- und SOC-Teams haben aufgrund mangelnder Kenntnisse über die zu schützende Umgebung Schwierigkeiten mit einer schnellen Reaktion auf Vorfälle.

Überblick über die Funktionen und Möglichkeiten von Novicom BVS (Netzwerk & Business Edition)

Visualisierung von IT-Geräten (Assets) innerhalb der Kommunikationsinfrastruktur	Identifizieren von Beziehungen zwischen Objekten, die Teil der Netzwerkkommunikation sind. Die Business Edition umfasst zusätzlich die visuelle Darstellung der Abhängigkeiten zwischen Diensten, Anwendungen und Geräten.
Grafische Schnittstelle	Möglichkeit, sich hierarchisch durch die Beziehungen zu bewegen, von den wichtigsten Knoten und Netzsegmenten über die IP-Geräte bis hin zu den darauf ausgeführten Diensten und den entsprechenden Ports (Drill-down).
Alarmierung	Warnungen bei Infrastrukturänderungen. Benachrichtigungen für Asset-Inhaber. Benachrichtigung über neue nicht autorisierte Geräte, um Sicherheitsvorfälle proaktiv zu vermeiden.
Automatisierte Metadaten-Erfassung von Geräten im Netzwerk und deren Kommunikation	Verwendung der autonomen Prüfeinrichtung zur Extraktion von Metadaten über die Netzkommunikation und deren Visualisierung fast in Echtzeit. Grundlegende Informationen über Kommunikationsverbindungen (Netzsegment, IP-Quelle, IP-Ziel, Protokoll, Zieldienst - Zielkommunikationsport).
Option zum Markieren neuer Knoten (Geräte)	Für die Gruppierung von Elementen, die unter dieselben Prüfungsanforderungen oder internen Richtlinien fallen, ist es möglich, benutzerdefinierte Tags hinzuzufügen.
Visualisierung der eingehenden/ausgehenden Kommunikation eines IT-Geräts	IP-Adresse, die mit Ports eines anderen Geräts kommuniziert – eingehende Kommunikation mit Diensten, die auf den Ports der IP-Adresse laufen.
Repository von Asset-Informationen	• Asset Name • Asset Typ • Asset-Kennung (basierend auf dem aktiven Typ, z. B. IP-Adresse, MAC, Port...) • Asset-Administrator • Benutzerdefinierte Metadaten
Überblick über das Organisationsvermögen	Export in XLS, CSV.
Zeitleiste	Vergleichen Sie den aktuellen Infrastrukturstatus mit einem Zeitabschnitt aus der Vergangenheit (z. B. durch Hervorheben neu identifizierter Assets).
Events-Übersicht	Warnmeldungen für neue, nicht genehmigte Geräte verhindern Vorfälle (Alarmierung).
Zentraler Gesamtbericht	Suchen Sie mit einem beliebigen Attribut nach Geräten.
Datenaufbewahrung und Leistung	Verarbeitung und Speicherung großer Datenmengen am Computer (über 10 GB Daten pro Tag) und Speicherung der wichtigsten Metadaten, die für die Untersuchung von Vorfällen erforderlich sind, über den erforderlichen Zeitraum hinweg.
Anpassbarer Zugriff auf bestimmte Anwendungsteile	Benutzerauthentifizierung, sicherer Zugang zu bestimmten Teilen der Anwendung auf der Grundlage von Benutzerrollen.



BVS Netzwerk Edition

Das Basismodul BVS Network Edition beantwortet die folgenden Fragen:

- Welche Geräte befinden sich derzeit im Netz?
- Sind diese Geräte zugelassen?
- Welche Geräte im Netzwerk werden nicht mehr verwendet? Welche Verbindungen werden neu hergestellt und welche Geräte versuchen zu kommunizieren? Gibt es bei einer dieser Verbindungen Anzeichen für ein Gerät mit bösartigem Verhalten?
- Wer ist der Geräteadministrator?
- Welche Dienste laufen im Netzwerk?
- Welche anderen Geräte wirken sich auf die Verfügbarkeit des überwachten Geräts aus?
- Wie ist die Kommunikationshistorie (Profil) des betreffenden Geräts und welche Änderungen wurden daran vorgenommen?
- Wie viele betroffene Geräte haben in der ausgewählten Zeit mit der angegebenen IP kommuniziert?
- Was sind die letzten Änderungen an einem Gerät? (offene Ports, Risikoänderung, Schwachstelle, usw.)?

BVS Network Edition Anwendungsfälle:

1. **Migration der IKT-Infrastruktur in die Cloud**
   > Standort der Assets (Segment, Eigentümer, Risiko)
   > Identifizierung aller Dienste und Abhängigkeiten
   > Export der Gerätekommunikationsmatrix
2. **Erkennen des Ausmaßes eines Cybervorfalls**
   > Das Unternehmen erhält Informationen über eine mögliche Kompromittierung seines Informationssystems
   > IP-Adresse des Systems wird als Kennung aufgeführt
   > BVS visualisiert alle betroffenen Geräte im ausgewählten Zeitrahmen
3. **Implementierung von NAC**
   > Unmittelbare Orientierung in der aktuellen Netzumgebung ermöglicht eine schnellere Bereitstellung von NAC-Tools, einschließlich ADDNET von Novicom

BVS Business Edition Anwendungsfälle:

1. **Unterstützen Sie die Arbeit des SOC-Teams**
   > Prioritätensetzung bei der Untersuchung von Vorfällen entsprechend der Kritikalität des Assets
   > Vorhersage von Angriffen in Bezug auf die Kritikalität von Assets
   > Schnelle Identifizierung des Ausmaßes eines Cybervorfalls
   Berichterstattung auf Ebene der Unternehmensdienste
   Unter anderem werden SOC-Betreiber sofort darüber informiert, ob ein infiziertes Gerät den hochkritischen Dienst beeinträchtigen könnte.
2. **Planung von Infrastrukturänderungen mit Auswirkungen auf die Servicekontinuität**
   > Priorisierung von Reparaturen und Patches für IT-Geräte
   > Schnelle Erstellung von Business Impact Analysen
   > Identifizierung und einfache Pflege von Informationen über die Existenz des Assets und seine Verbindung zu bestimmten durchgeführten Diensten
3. **Inputs zur Optimierung der IT-Infrastruktur**
   > Eingabe zur Trennung von kritischen und nicht kritischen Assets
   > Identifizierung des „Single Point of Failure“
3. **Dokumentation des Risikomanagements**
   > Informationen darüber, ob bestimmte geschäftskritische Dienste von besonders anfälligen Geräten abhängig sind

BVS Business Edition

Die BVS Business Edition eignet sich mit ihrem Fokus und ihrer Funktionalität für SOC-Mitarbeiter, IT-Manager und IT-Sicherheitsbeauftragte, die den Überblick über bereitgestellte Dienste, deren Verfügbarkeit, einschließlich Links zu unterstützenden IT-Ressourcen und möglichen Risikofaktoren behalten müssen.

BVS Business Edition bietet die folgenden Optionen:

- Erstellung logischer Assets, die die technischen, Anwendungs- und Geschäftsservices des Unternehmens darstellen.
- Benachrichtigung über Änderungen an IT-Beständen und deren Auswirkungen auf bestimmte Dienste.
- Visuelle Darstellung von Abhängigkeiten zwischen Geschäftsdiensten, Anwendungen, IT-Diensten und IT-Assets (Business Impact Analysis) mit automatischer Asset-Identifizierung und Asset-Verhalten.
- Identifizierung der Auswirkungen von Betriebsereignissen auf die Geschäftsdienste der Organisation (Was-wäre-wenn-Szenarien).
- Informationen über festgestellte Schwachstellen, BVS bezieht die Daten aus den Ergebnissen der Schwachstellenscanner.
- Übersicht über die möglichen Auswirkungen von Schwachstellen, die in den Assets der technischen IT-Ressourcen entdeckt wurden.
- Gewährleistung der Kontinuität der Dienste durch einen besseren Überblick über die Support-Infrastruktur.

Der Mehrwert von Novicom BVS - Business Visibility Suite

- Einfaches und intuitives Tool mit umfassender Unterstützung zur schnelleren Bewältigung von Cyber -Vorfällen.
- Schnelle Orientierung in einem komplexen Netzwerk-kommunikationsumfeld.
- Abbildung des Kommunikationsverhaltens der Kunden und die Netzinfrastruktur, um SOC
  - Dienste schnell einzuführen.
  - Identifizierung der Netzinfrastruktur und der Geräte, z. B. Beseitigung der „Schatten-IT“
- Überwachung von Wi-Fi und Netzwerkkommunikation
- Schnelle Identifizierung von Netzwerk-Kommunikationsbeziehungen zwischen IT-Geräten, um die Implementierungszeit und die Einstellung von Network Access Control-Tools zu reduzieren.
- Die Integration mit NAC ermöglicht eine umfassende Sicht von den Top Unternehmensdiensten bis hin zur Ebene der physisch identifizierbaren Geräte.
- Mindestanforderungen für die Interaktion mit Kunden sind grundlegende Informationen über Adressbereiche, die kommunizierende Elemente enthalten.
- Identifizierung und einfache Pflege von Beziehungen und Abhängigkeiten zwischen Geschäftsdiensten/ Anwendungen und der Infrastruktur - schnell herausfinden, welche Dienste von Sicherheitsbedrohungen gefährdet sind.
- Übersichtliche und nahtlose Migration der Cloud-Infrastruktur durch eine Übersicht der Kommunikationsabhängigkeiten.

BVS und aktive SOC

Novicom BVS ist ein wichtiger Bestandteil der Active SOC (Security Operation Center) -Strategie, die Novicom zusammen mit seinen SOC-Partnern auf dem Markt vorantreiben will.
Novicom BVS bildet zusammen mit dem Novicom ADDNET (Lösung für effizientes Management von Netzwerkdiensten und Netzwerkzugangskontrolle) und Novicom ELISA (ein Tool zum Abfangen und Auswerten von Cyber-Sicherheitsereignissen) ein ideales Portfolio, das eine schnelle und nahtlose Anbindung an den SOC-Service ermöglicht.

Technische Ressourcen für Novicom BVS

Die folgenden Geräte sind in der Kundenumgebung installiert:

- Physikalische Sonden zur Überwachung von Netzwerkverbindungen (Standard 1U in einem Rack, mit 2 Netzwerkschnittstellen - für SPAN-Daten / 10Gbit / Netzwerk-Switches Überwachungsschnittstellen + 1Gbit / für BVS-Server-Kommunikation)
- Optionale physische Wi-Fi-Sonden zur Überwachung des Wi-Fi-Spektrums (Standard-Mini-PC-Geräte, die mit den meisten Wi-Fi-Standards kompatibel sind)
- Management und Sammler von HW-Geräten, die zusammen mit der BVS-Lösung oder mit eigenen Ressourcen des Kunden geliefert werden
- Unterstützung für VMware und physische Geräte
- Bewährte Novicom APPLIANCE Hardware wird verwendet, Novicom BVS Implementierung
- Die Implementierung erfolgt nach den bewährten Verfahren der Novicom Implementation Methodology (NIM)
- In der ersten Phase wird die erforderliche BVS-Infrastruktur im Netz des Kunden eingerichtet und das Modul BVS Network gestartet
- Das BVS Business Modul kann nach der Business Impact Analyse effizient genutzt werden Zusammenarbeit bei Aufgaben während der Novicom BVS Implementierung.
- Sondenverbindung zu überwachten Infrastruktur -Switches (für das Modul IT-Infrastruktur)
- Definition des Anwendungsbereichs für überwachte Segmente
- Interpretation ausgewählter Mitteilungen, die Gegenstand der Analyse sind
- Sicherstellung der Verbindung zwischen BVS-Komponente
- Bereitstellung des Zugangs zu Kernnetzdiensten - DNS und NTP
- Fernzugriff für 2-Wege-Kommunikation und Zugriff auf/von dem Gerät (BVS-Gerätebetreiber > Kundenumgebung; Kundenumgebung > BVS-Gerätebetreiber)

novicom

Novicom, s.r.o.
Prag, Tschechische Republik
www.novicom.eu
sales@novicom.eu

BVS

NVC DE 2022-02