Pegaso – Descripción del producto

Contenido

Lista de tablas

Lista de Figuras

Introducción

Pegasus es una solución de inteligencia cibernética líder en el mundo que permite a las agencias de inteligencia y de aplicación de la ley extraer inteligencia valiosa de forma remota y encubierta desde prácticamente cualquier dispositivo móvil. Esta innovadora solución fue desarrollada por veteranos de las agencias de inteligencia de élite para proporcionar a los gobiernos una forma de abordar los nuevos desafíos de interceptación de comunicaciones en el campo de batalla cibernético altamente dinámico de hoy. Al capturar nuevos tipos de información de dispositivos móviles, Pegasus cierra una brecha tecnológica sustancial para brindar la inteligencia más precisa y completa para sus operaciones de seguridad.

Superar el desafío de la interceptación de teléfonos inteligentes

El mercado de comunicaciones móviles de rápido crecimiento y altamente dinámico, caracterizado por la introducción de nuevos dispositivos, sistemas operativos y aplicaciones prácticamente a diario, requiere un replanteamiento del paradigma de inteligencia tradicional. Estos cambios en el panorama de las comunicaciones plantean desafíos y obstáculos reales que deben superar las organizaciones de inteligencia y las fuerzas del orden en todo el mundo:

Cifrado: Uso extensivo de dispositivos y aplicaciones cifradas para transmitir mensajes

Abundancia de aplicaciones de comunicación: Caótico mercado de sofisticados aplicaciones, la mayoría de las cuales están basadas en IP y utilizan protocolos propietarios

Objetivo fuera del dominio de intercepción: las comunicaciones de los objetivos a menudo están fuera del dominio de intercepción de la organización o son inaccesibles (por ejemplo, los objetivos están en roaming, reuniones cara a cara, uso de redes privadas, etc.)

Enmascaramiento: uso de varias identidades virtuales que son casi imposibles de rastrear y rastrear

Reemplazo de SIM: Reemplazo frecuente de tarjetas SIM para evitar cualquier tipo de interceptación

Extracción de datos: la mayor parte de la información no se envía a través de la red ni se comparte con otras partes y solo está disponible en el dispositivo del usuario final

Implementación compleja y costosa: a medida que las comunicaciones se vuelven cada vez más complejas, se necesitan más interfaces de red. La configuración de estas interfaces con los proveedores de servicios es un proceso largo y costoso, y requiere regulación y estandarización.

Las soluciones de interceptación estándar no son suficientes

Hasta que se aborden y resuelvan los desafíos mencionados anteriormente, es probable que los objetivos criminales y terroristas estén "a salvo" de los sistemas de interceptación estándar y heredados, lo que significa que se está perdiendo inteligencia valiosa. Estas soluciones estándar (descritas en las secciones a continuación) brindan solo inteligencia parcial, lo que deja a las organizaciones con brechas de inteligencia sustanciales.

Interceptación pasiva

La interceptación pasiva requiere relaciones muy profundas y estrechas con los proveedores de servicios locales (proveedores de telefonía móvil, Internet y PSTN) y tradicionalmente ha permitido un seguimiento adecuado de los mensajes de texto y las llamadas de voz. Sin embargo, la mayoría de las comunicaciones contemporáneas se componen de tráfico basado en IP, que es extremadamente difícil de monitorear con interceptación pasiva debido a su uso de protocolos propietarios y de encriptación.

Incluso cuando se intercepta este tráfico, normalmente transporta cantidades masivas de datos técnicos que no están relacionados con el contenido real y los metadatos que se comunican. Esto no solo genera frustración en los analistas y pérdida de tiempo en la búsqueda de datos irrelevantes, sino que también proporciona una instantánea parcial (en el mejor de los casos) de las comunicaciones del objetivo. Además, la cantidad de interfaces requeridas para cubrir a los proveedores de servicios relevantes amplía el círculo de entidades expuestas a información confidencial y aumenta la posibilidad de fuga.

Intercepción táctica GSM

Las soluciones tácticas de interceptación GSM monitorean de manera efectiva las llamadas de voz y los mensajes de texto en las redes GSM. Cuando se implementan tecnologías celulares avanzadas (redes 3G y LTE), estas soluciones se vuelven menos eficientes. En tales casos, se requiere degradar violentamente el objetivo a una red basada en GSM, lo que afecta notablemente la experiencia y la funcionalidad del usuario.

Estas soluciones también requieren un equipo táctico de campo bien capacitado ubicado cerca del objetivo monitoreado. Por lo tanto, en la mayoría de los casos en los que se desconoce la ubicación del objetivo, estas soluciones se vuelven irrelevantes. En otros casos, colocar un equipo táctico cerca del objetivo puede representar un riesgo grave tanto para el equipo como para toda la operación de inteligencia.

Software malicioso (Malware)

Presuntamente, el malware proporciona acceso al dispositivo móvil del objetivo. Sin embargo, no es completamente transparente y requiere la participación del objetivo para instalarse en sus dispositivos.
Este tipo de participación generalmente toma la forma de múltiples confirmaciones y aprobaciones antes de que el malware sea funcional. Es poco probable que la mayoría de los objetivos se dejen engañar para que cooperen con el malware debido a su alto nivel de sensibilidad por la privacidad en sus comunicaciones.

Además, es probable que dicho malware sea vulnerable a la mayoría de los programas antivirus y antispyware disponibles en el mercado. Como tales, dejan rastros y se detectan con bastante facilidad en el dispositivo.

Ciberinteligencia para el mundo móvil

Pegasus es una solución de inteligencia cibernética líder en el mundo que permite a las agencias de inteligencia y de aplicación de la ley extraer inteligencia valiosa de forma remota y encubierta desde prácticamente cualquier dispositivo móvil. Esta innovadora solución fue desarrollada por veteranos de las agencias de inteligencia de élite para proporcionar a los gobiernos una forma de abordar los nuevos desafíos de interceptación de comunicaciones en el campo de batalla cibernético altamente dinámico de hoy.

Al capturar nuevos tipos de información de dispositivos móviles, Pegasus cierra una brecha tecnológica sustancial para brindar la inteligencia más precisa y completa para sus operaciones de seguridad. Esta solución es capaz de penetrar en los smartphones más populares del mercado basados en los sistemas operativos BlackBerry, Android, iOS y Symbian.

Pegasus implementa silenciosamente un software invisible ("agente") en el dispositivo de destino. Este agente luego extrae y transmite de forma segura los datos recopilados para su análisis. La instalación se realiza de forma remota (por aire), no requiere ninguna acción por parte del objetivo ni interacción con él, y no deja ningún tipo de rastro en el dispositivo.

Beneficios de Pegaso

Las organizaciones que implementan Pegasus pueden superar los desafíos mencionados anteriormente para lograr una recopilación de inteligencia móvil inigualable:

- Acceso ilimitado a los dispositivos móviles del objetivo: recopile información de forma remota y encubierta sobre las relaciones, la ubicación, las llamadas telefónicas, los planes y las actividades de su objetivo, en cualquier momento y lugar.
- Interceptar llamadas: monitorear de forma transparente las llamadas de voz y VoIP en tiempo real
- Supere las brechas de inteligencia: recopile tipos de información únicos y nuevos (por ejemplo, contactos, archivos, escuchas telefónicas ambientales, contraseñas, etc.) para brindar la inteligencia más precisa y completa
- Manejar contenido y dispositivos cifrados: superar el cifrado, SSL, propietario protocolos y cualquier obstáculo que presente el complejo mundo de las comunicaciones
- Supervisión de aplicaciones: controle una multitud de aplicaciones, incluidas Skype, WhatsApp, Viber, Facebook y Blackberry Messenger (BBM)
- Identifique objetivos: haga un seguimiento de los objetivos y obtenga información de posicionamiento precisa mediante GPS
- Independencia del proveedor de servicios: no hay cooperación con los operadores de redes móviles locales (OMN) es necesario
- Descubra identidades virtuales: Supervise constantemente el dispositivo sin preocuparse por cambio frecuente de identidades virtuales y reemplazo de tarjetas SIM
- Evite riesgos innecesarios: elimine la necesidad de proximidad física al objetivo o dispositivo en cualquier fase

Aspectos destacados de la tecnología

La solución Pegasus utiliza tecnología de punta especialmente desarrollada por veteranos de las agencias de inteligencia y de aplicación de la ley. Ofrece un amplio conjunto de características avanzadas y sofisticadas capacidades de recopilación de inteligencia que no están disponibles en las soluciones de interceptación estándar:

- Penetra en dispositivos basados en Android, BlackBerry, iOS y Symbian

Extrae contactos, mensajes, correos electrónicos, fotos, archivos, ubicaciones, contraseñas, lista de procesos y más

Accede a dispositivos protegidos con contraseña

Totalmente transparente al objetivo

No deja rastro en el dispositivo.

Consumo mínimo de batería, memoria y datos

Mecanismo de autodestrucción en caso de riesgo de exposición

Recupera cualquier archivo del dispositivo para un análisis más profundo

Arquitectura de Alto Nivel

El sistema Pegasus está diseñado en capas. Cada capa tiene su propia responsabilidad formando juntos una solución integral de recopilación y análisis de ciberinteligencia.

Las principales capas y bloques de construcción de los sistemas son:

Instalaciones: la capa de instalación se encarga de emitir nuevas instalaciones de agentes, actualizar y desinstalar agentes existentes.

Recopilación de datos: La capa de recopilación de datos se encarga de recopilar los datos del dispositivo instalado. Pegasus ofrece inteligencia integral y completa mediante el empleo de cuatro métodos de recopilación:

– Extracción de datos: extracción de todos los datos que existen en el dispositivo tras la instalación del agente

– Monitoreo Pasivo: Monitoree los nuevos datos de llegada al dispositivo

– Recopilación activa: active la cámara, el micrófono, el GPS y otros elementos para recopilar datos en tiempo real

– Recopilación basada en eventos: defina escenarios que activen automáticamente la recopilación de datos específicos

Transmisión de Datos: La capa de Transmisión de Datos se encarga de transmitir los datos recopilados de regreso a los servidores de comando y control, utilizando la forma más eficiente y segura.

Presentación y análisis: el componente Presentación y análisis es una interfaz de usuario que se encarga de presentar los datos recopilados a los operadores y analistas, convirtiendo los datos en inteligencia procesable. Esto se hace usando los siguientes módulos:

– Monitoreo en tiempo real: presenta datos recopilados en tiempo real de objetivos específicos o múltiples. Este módulo es muy importante cuando se trata de objetivos sensibles o durante actividades operativas, donde cada información que llega es crucial para la toma de decisiones.

– Análisis Offline: Mecanismo de consultas avanzadas que permite a los analistas consultar y recuperar cualquier información recopilada. El mecanismo avanzado proporciona herramientas para encontrar conexiones e información ocultas.

– Análisis geo-basado: presenta los datos recopilados en un mapa y realiza consultas geo-basadas.

– Reglas y alertas: defina reglas que activen alertas según los datos específicos que llegan o el evento que ocurrió.

Administración: El componente de administración se encarga de gestionar todo el permisos del sistema, seguridad y salud:

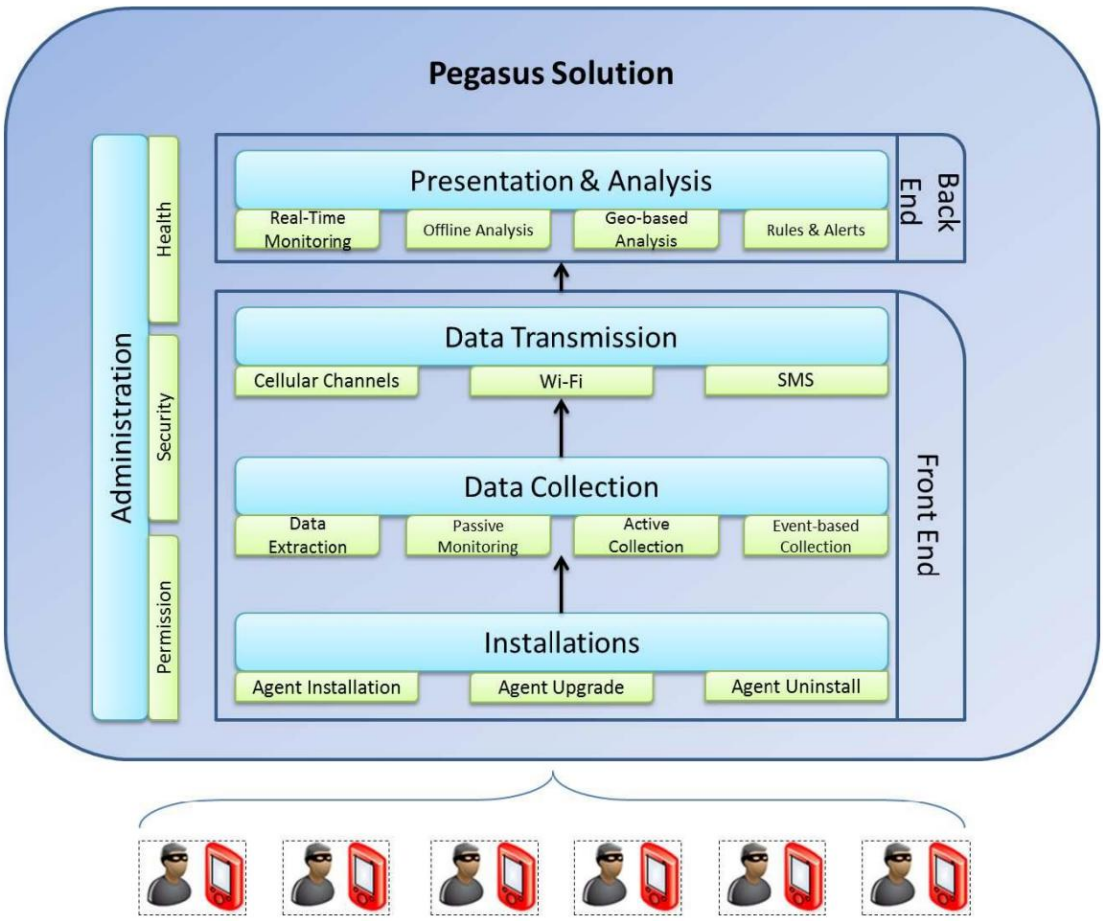
– Permiso: El mecanismo de permisos permite al administrador del sistema administrar los diferentes usuarios del sistema. Proporcione a cada uno de ellos el nivel de acceso adecuado solo a los datos que tienen permitido. Esto permite definir grupos en la organización que manejan solo uno o más temas y otros grupos que manejan diferentes temas.

– Seguridad: el módulo de seguridad supervisa el nivel de seguridad del sistema, asegurándose de que los datos recopilados se inserten en la base de datos del sistema limpios y seguros para una revisión futura.

– Salud: el componente de salud de la solución Pegasus supervisa el estado de todos los componentes y se asegura de que todo funcione sin problemas. Supervisa la comunicación entre las diferentes partes, el rendimiento del sistema, la disponibilidad de almacenamiento y alerta si algo funciona mal.

Las capas y los componentes del sistema se muestran en la Figura 1.

Figura 1: Arquitectura de alto nivel de Pegasus



Instalación del agente

Para comenzar a recopilar datos del teléfono inteligente de su objetivo, se debe instalar un componente basado en software ("Agente") de forma remota y encubierta en su dispositivo.

Propósito del agente

El "Agente", un componente basado en software, reside en los dispositivos de punto final de los objetivos monitoreados y su propósito es recopilar los datos para los que fue configurado. El agente es compatible con los sistemas operativos más populares: dispositivos basados en BlackBerry, Android, iOS (iPhone) y Symbian.

Cada agente es independiente y está configurado para recopilar información diferente del dispositivo y transmitirla a través de canales específicos en marcos de tiempo definidos. Los datos se envían de vuelta a los servidores de Pegasus de forma oculta, comprimida y cifrada.

El agente recopila continuamente la información del dispositivo y la transmitirá una vez que esté disponible una conexión a Internet confiable.

El cifrado de las comunicaciones, el uso de muchas aplicaciones y otros métodos de ocultamiento de las comunicaciones dejan de ser relevantes cuando se instala un agente en el dispositivo.

Vectores de instalación de agentes

Inyectar e instalar un agente en el dispositivo es la fase más sensible e importante de la operación de inteligencia que se lleva a cabo en el dispositivo de destino. Cada instalación debe planificarse cuidadosamente para garantizar su éxito. El sistema Pegasus admite varios métodos de instalación. La variedad de métodos de instalación responde a los diferentes escenarios operativos que son únicos para cada cliente, lo que resulta en la solución más completa y flexible.
Los siguientes son los vectores de instalación admitidos:

Instalación remota (rango libre):

Over-the-Air (OTA): un mensaje push se envía de forma remota y encubierta al dispositivo móvil. Este mensaje hace que el dispositivo descargue e instale el agente en el dispositivo. Durante todo el proceso de instalación, no se requiere la cooperación o participación del objetivo (p. ej., hacer clic en un enlace, abrir un mensaje) y no aparece ninguna indicación en el dispositivo. La instalación es totalmente silenciosa e invisible y el objetivo no puede impedirla. Esta es la singularidad de NSO, que diferencia significativamente la solución Pegasus de cualquier otra solución disponible en el mercado.

Mensaje de ingeniería social mejorado (ESEM): en los casos en que el método de instalación OTA no sea aplicable1, el operador del sistema puede optar por enviar un mensaje de texto normal (SMS) o un correo electrónico, atrayendo al objetivo para que lo abra. Un solo clic, planificado o no, en el enlace dará como resultado la instalación de un agente oculto. La instalación está completamente oculta y, aunque el objetivo hizo clic en el enlace, no se dará cuenta de que el software se está instalando en su dispositivo.

Las posibilidades de que el objetivo haga clic en el enlace dependen totalmente del nivel de

1 por ejemplo, algunos dispositivos no lo admiten; algunos proveedores de servicios bloquean los mensajes push; número de teléfono de destino en desconocido.

credibilidad del contenido. La solución Pegasus proporciona una amplia gama de herramientas para redactar un mensaje inocente y personalizado para atraer al objetivo a abrir el mensaje.

NOTA: Tanto los métodos OTA como ESEM solo requieren un número de teléfono o una dirección de correo electrónico que utilice el objetivo. No se necesita nada más para lograr una instalación exitosa del agente Pegasus en el dispositivo.

Cerca del objetivo (alcance limitado):

Elemento de red táctica: el agente de Pegasus se puede inyectar en silencio una vez que se adquiere el número utilizando un elemento de red táctica como la estación base transceptora (BTS). La solución Pegasus aprovecha las capacidades de tales herramientas tácticas para realizar una inyección e instalación remota del agente. Tomar una posición en el área del objetivo es, en la mayoría de los casos, suficiente para lograr la adquisición del número de teléfono. Una vez que el número está disponible, la instalación se realiza de forma remota.

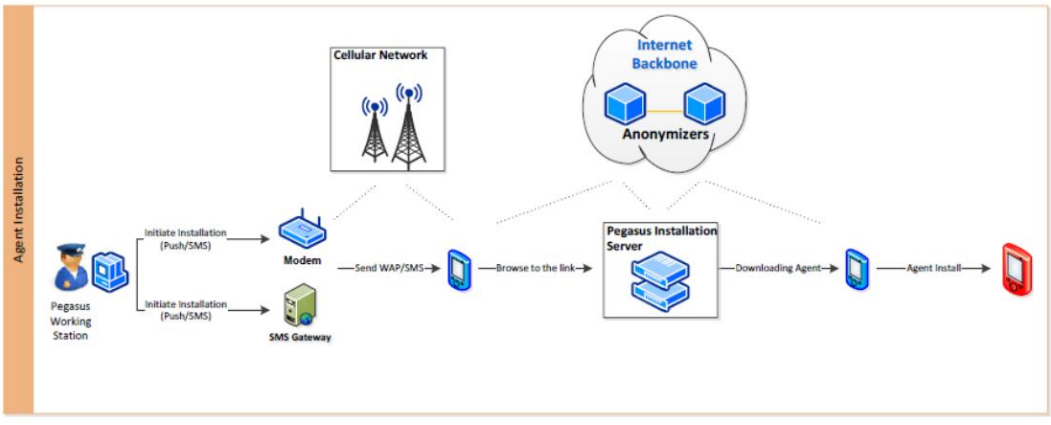
Físico: cuando el acceso físico al dispositivo es una opción, el agente de Pegasus puede ser inyectado manualmente e instalado en menos de cinco minutos. Después de la instalación del agente, la extracción de datos y el monitoreo de datos futuros se realizan de forma remota, proporcionando las mismas funciones que cualquier otro método de instalación.

NOTA: Las instalaciones tácticas y físicas generalmente se usan donde no hay disponible un número de teléfono o dirección de correo electrónico de destino.

Flujo de instalación del agente

El flujo de instalación del agente remoto se muestra en la Figura 2.

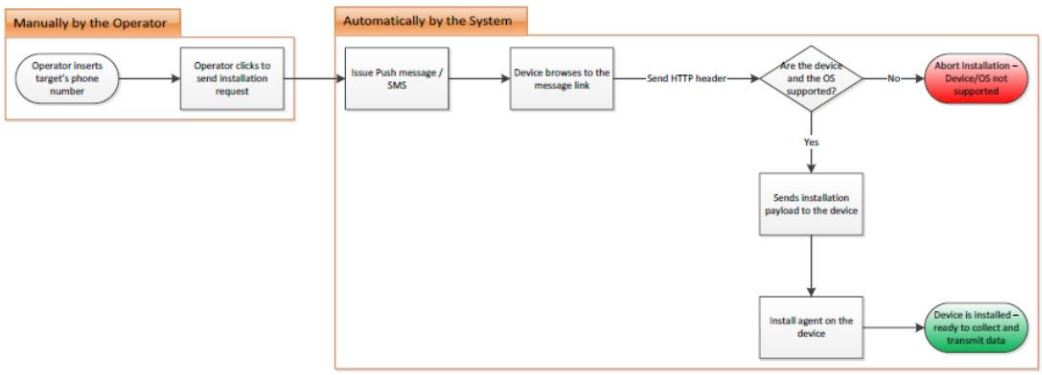
Figura 2: Flujo de instalación del agente



Para iniciar una nueva instalación, el operador del sistema Pegasus solo debe ingresar el número de teléfono de destino. El resto lo hace automáticamente el sistema, lo que resulta en la mayoría de los casos con un agente instalado en el dispositivo de destino.

El inicio de la instalación del agente se muestra en la Figura 3.

Figura 3: Inicio de la instalación del agente



Sistemas operativos y dispositivos compatibles

Operating System (OS)	OS Version	Device	Comments
Android	2.1 – 4.2	▪ Samsung Galaxy series ▪ Sony Ericsson Xperia series ▪ Others (refer to note below)	Support is based on local firmware versions, which must be defined with the customer
iOS	4.x – 6.1.4	▪ iPhone 4 ▪ iPhone 4S ▪ iPhone 5	
BlackBerry	5.0 – 7.1	▪ Curve (8520, 9300, 9350, 9360) ▪ Bold (9000, 9700, 9780, 9790, 9900, 9930) ▪ Torch (9800, 9810, 9850, 9860) ▪ Pearl (9100)	
Symbian	Version S60 OS9 3rd edition FP1, FP2, 5th edition and Symbian^3	Variety of devices	Support is based on local firmware versions, which must be defined with the customer

NOTA: Los dispositivos basados en Android a menudo se agregan a la lista compatible. Se puede enviar una lista actualizada a petición del cliente.

Fallo de instalación

La instalación a veces puede fallar debido a las siguientes razones:

1. Dispositivo no compatible: el dispositivo de destino no es compatible con el sistema (que aparece arriba).

2. Sistema operativo no compatible: el sistema operativo del dispositivo de destino no es compatible con el sistema.

3. Navegador no compatible: el navegador predeterminado del dispositivo fue reemplazado previamente por el objetivo. El sistema no admite la instalación desde navegadores que no sean el predeterminado del dispositivo (y también Chrome para dispositivos basados en Android).

En cualquiera de los casos mencionados anteriormente, si el operador inicia una instalación remota en un dispositivo, sistema operativo o navegador no compatible, la inyección fallará y la instalación se cancelará. En estos casos, el proceso finaliza con un navegador abierto en el dispositivo de destino que señala y muestra la página URL que definió el operador antes de la instalación.

El sistema identifica el dispositivo, el sistema operativo y el navegador mediante su agente de usuario HTTP. Si por alguna razón el agente de usuario fue manipulado por el objetivo, el sistema podría fallar correctamente identifique el dispositivo y el sistema operativo y proporcione la carga útil de instalación incorrecta. En tal caso, la inyección fallará y la instalación se cancelará, mostrando nuevamente la página URL mencionada anteriormente.

Recopilación de datos

Tras la instalación exitosa del agente, se monitorea y recopila una amplia gama de datos del dispositivo:

Textual: la información textual incluye mensajes de texto (SMS), correos electrónicos, registros de calendario, historial de llamadas, mensajería instantánea, lista de contactos, historial de navegación y más. La información textual suele ser estructurada y de tamaño reducido, por lo que es más fácil de transmitir y analizar.

Audio: la información de audio incluye llamadas interceptadas, sonidos ambientales (grabación de micrófono) y otros archivos de audio grabados.

Visual: la información visual incluye instantáneas de la cámara, recuperación de fotos y captura de pantalla.

Archivos: cada dispositivo móvil contiene cientos de archivos, algunos tienen un valor incalculable inteligencia, como bases de datos, documentos, videos y más.

Ubicación: Monitoreo continuo de la ubicación del dispositivo (Celular-ID y GPS).

La variedad de datos que recopila el sistema Pegasus se muestra en la Figura 4.

Figura 4: Datos recopilados

La recogida de datos se divide en tres niveles:

Extracción de datos inicial

Monitoreo pasivo

colección activa

Extracción de datos iniciales

Una vez que el agente se inyecta e instala correctamente en el dispositivo, los siguientes datos que residen y existen en el dispositivo se pueden extraer y enviar al centro de comando y control:

- Registros de SMS
- Detalles de contactos
- Historial de llamadas (registro de llamadas)
- Registros de calendario
- Correos electrónicos
- Mensajería instantánea
- Historial de navegación

A diferencia de otras soluciones de recolección de inteligencia que solo brindan monitoreo futuro de comunicaciones parciales, Pegasus permite la extracción de todos los datos existentes en el dispositivo. Como resultado, la organización se beneficia al acceder a datos históricos sobre el objetivo, lo que ayuda a construir una imagen de inteligencia completa y precisa.

NOTA: La extracción de datos inicial es una opción y no una obligación. Si a la organización no se le permite acceder a los datos históricos del objetivo, dicha opción puede desactivarse y el agente solo monitoreará los nuevos datos de llegada.

Monitoreo Pasivo

Desde el momento en que el agente se instaló correctamente, sigue monitoreando el dispositivo y recupera cualquier registro nuevo que esté disponible en tiempo real (o en una condición específica si se configura de manera diferente). A continuación se muestra la lista completa de datos que son monitoreados por el agente:

- Registros de SMS
- Detalles de contactos
- Historial de llamadas (registro de llamadas)
- Registros de calendario
- Correos electrónicos
- Mensajería instantánea
- Historial de navegación
- Seguimiento de ubicación (basado en ID de celda)

Colección activa

Además del monitoreo pasivo, luego de la instalación exitosa del agente, se encuentra disponible un amplio conjunto de funciones de recopilación activa. La recopilación activa se refiere a las solicitudes activas enviadas por el operador para recopilar información específica del dispositivo instalado. Este conjunto de características se denominan activas, ya que llevan su colección a pedido explícito del operador. La recopilación activa permite al operador realizar acciones en tiempo real en el dispositivo de destino, recuperando información única del dispositivo y del área circundante del objetivo, que incluye:

- Seguimiento de ubicación (basado en GPS)

Interceptación de llamadas de voz

recuperación de archivos

Grabación de sonido ambiental (grabación de micrófono)

toma de fotos

captura de pantalla

La recopilación activa diferencia a Pegasus de cualquier otra solución de recopilación de inteligencia, ya que el operador controla la información que se recopila. En lugar de simplemente esperar a que llegue la información, con la esperanza de que esta sea la información que estaba buscando, el operador recupera activamente información importante del dispositivo y obtiene la información exacta que estaba buscando.

Descripción de los datos recopilados

Los diferentes tipos de datos disponibles para extracción, monitoreo pasivo y recolección activa con sus respectivas características se enumeran en la Tabla 1.

Tabla 1: Características de la colección Descripción

Application Type	Features Description	Data Extraction	Passive / Active Collection
Instant Messaging (IM): 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	Agent extracts and monitors all the incoming and outgoing instant messages to/from the device. Full 1-on-1 conversation extraction and monitoring including group chat. Indication for file transfer (file name).	✔	✔
Location Tracking	The system provide two types of location information about the device: GPS: 1. Upon user request, a defined timeframe for sampling location is opened. GPS data is retrieved when applicable (available reception). In case GPS signal is not accessible, Cell-ID is retrieved. 2. If GPS is disabled by the target, the system enable it for sampling and immediately turn it off Cell-ID: Devices constantly transmit their location (Cell-ID) every time they communicate with the server. The retrieved location data is analyzed at the server and placed on map. Location-based queries and alerts are easily set.	✔	✔
Calendar	Agent extracts all the calendar records from the device and monitors any change or new event added to the calendar.	✔	✔
Contact details	Agent extracts all contacts available on the device. From this point the agent monitors any change/deletion of existing contacts and the addition of new contact.	✔	✔

Application Type	Features Description	Data Extraction	Passive / Active Collection
	The agent extracts and monitors all values assigned in each contact field that is available (based on vCard fields), including photo if assigned.		
Environmental sound recording (microphone recording)	The user can request to turn on the device microphone and listen in real-time to the surrounding sounds. The surrounding sounds are recorded and can be analyzed and replayed at a later stage. Turning on the microphone is based on an incoming silent call to the device from the server (PBX). Such call is allowed only after the agent assured that the device is in idle mode (device is not in active use and the screen is turned off). Any action by the target that turns on the screen will result in immediate call hang-up and cease of capturing surrounding sounds. No indication of the recording or the incoming silent call appears on the device at any point. The quality of the recording depends on the device's microphone sensitivity, the surrounding noise and the device model. This sensitivity varies between the different mobile phone models and is set by the phone manufacturer. Usually the content of a conversation held a few meters next to the device can be heard.	N/A[2]	✔
SMS	Agent extracts and monitors all the incoming and outgoing text messages (SMS).	✔	✔
Call Interception (call recording) – Android only	The user can request to record incoming and outgoing calls of the target device. The calls are recorded locally on the device and then sent to the system servers upon completion.	N/A	✔
Email: 1. Main email application in all platforms 2. Gmail application in Android	Agent extracts and monitors all the emails that reside on the device. The main email application (stock) on the device is monitored, thus all accounts which are defined there are monitored (e.g., exchange, Gmail, etc.). For Android-based devices both the main email stock application and the Gmail application are monitored.	✔	✔
File retrieval	Upon user request a full list of files and folders is extracted from the device (internal storage and SD card). When the operator spots a file of interest he can immediately request to retrieve it.	N/A	✔
Photo taking	Upon user request snapshots using the front and rear camera are taken from the device and sent to the servers. The snapshots are taken only after the agent assured that the	N/A	✔

2 Para las funciones de recopilación activa, los datos iniciales no se extraen antes de que el usuario inicie una solicitud.

Application Type	Features Description	Data Extraction	Passive / Active Collection
	device is in idle mode. During photo taking no indication appears on the device and flash is never used. The quality of the photo can be chosen by the operator to reduce data usage and faster photo transmission. Since flash is not used and the phone might be in motion or inside rooms with low light, the photos are sometimes out of focus.		
Screen capturing	Upon user request a screen capture is taken and sent to the Pegasus servers. The device screenshots can provide insights on the applications used by the target, wallpaper image used and more intimate information about the target.	N/A	✔
Browsing history	Agent extracts and monitors the history of browsed websites from the default browser of the device.	✔	✔
Browsing favorites	Agent extracts and monitors the favorites websites saved in the default browser of the device.	✔	✔
Call history (call log)	Agent extracts the history of all incoming/outgoing calls made to/from the device. The data includes the caller and callee numbers and the duration of the call. Calling attempts which did not result with a conversation will show duration of 0 (zero) seconds.	✔	✔
Device information	Upon agent installation all device, network and connection details are extracted to monitor the general information of the device, including battery level. This provides a summarized view to help understand at-a-glance the device status.	✔	✔

Los datos mencionados anteriormente son los datos potenciales que podría recopilar un agente. El agente recopilará los datos aplicables y disponibles en el dispositivo. Si una o más de las aplicaciones mencionadas anteriormente no existen y/o se eliminan del dispositivo, el agente operará de la misma manera. Recogerá los datos del resto de servicios y aplicaciones que estén en uso en el dispositivo. Además, todos los datos recopilados de la aplicación eliminada aún se guardarán en los servidores o en el agente, si aún no se transmitieron a los servidores.

Además, los datos mencionados anteriormente que recopila el agente cubren las aplicaciones más populares utilizadas en todo el mundo. Dado que la popularidad de las aplicaciones difiere de un país a otro, entiende que la extracción de datos y el monitoreo de otras aplicaciones serán necesarios a medida que evolucione el tiempo y los objetivos adopten nuevas aplicaciones. Cuando se plantea tal requisito, puede extraer con bastante facilidad los datos importantes de prácticamente cualquier aplicación a pedido del cliente y publicarlos como una nueva versión que estará disponible para el cliente.

Búfer de colección

El agente instalado monitorea los datos del dispositivo y los transmite a los servidores. Si la transmisión no es posible3 , el agente recopilará la nueva información disponible y la transmitirá cuando la conexión esté disponible. Los datos recopilados se almacenan en un búfer oculto y encriptado. Este búfer está configurado para alcanzar no más del 5 % del espacio libre disponible en el dispositivo. Por ejemplo, si el dispositivo monitoreado tiene 1 GB de espacio libre, el búfer puede almacenar hasta 50 MB. En caso de que el búfer haya alcanzado su límite, los datos más antiguos se eliminan y se almacenan nuevos datos (FIFO). Una vez que se han transmitido los datos, el contenido del búfer se elimina por completo.

.

3 No hay canales de datos disponibles; El dispositivo está en itinerancia; El dispositivo está apagado.

Transmisión de datos

De manera predeterminada, los datos recopilados (extracción de datos inicial, monitoreo pasivo y recopilación activa) se envían de regreso al centro de comando y control en tiempo real. Los datos se envían a través de canales de datos, donde Wi-Fi es la conexión preferida para usar cuando está disponible. En otros casos, los datos se transmiten a través de canales de datos celulares (GPRS, 3G y LTE). Se pensó más en los métodos de compresión y se centró en la transmisión de contenido textual siempre que fue posible.
Las huellas de datos son muy pequeñas y, por lo general, ocupan solo unos pocos cientos de bytes. Esto es para asegurarse de que los datos recopilados se transmitan fácilmente, asegurando un impacto mínimo en el dispositivo y en el plan de datos móviles de destino.

Si los canales de datos no están disponibles, el agente recopilará la información del dispositivo y la almacenará en un búfer dedicado, como se explica en la sección Recopilación de datos.

La transmisión de datos se detiene automáticamente en los siguientes escenarios:

- Batería baja: cuando el nivel de batería del dispositivo está por debajo del umbral definido (5 %), todos los procesos de transmisión de datos se detienen inmediatamente hasta que se recarga el dispositivo.
- Dispositivo en roaming: cuando el dispositivo está en roaming, los canales de datos móviles se vuelven caros, por lo que la transmisión de datos se realiza solo a través de Wi-Fi. Si no existe Wi-Fi, se detendrá la transmisión.

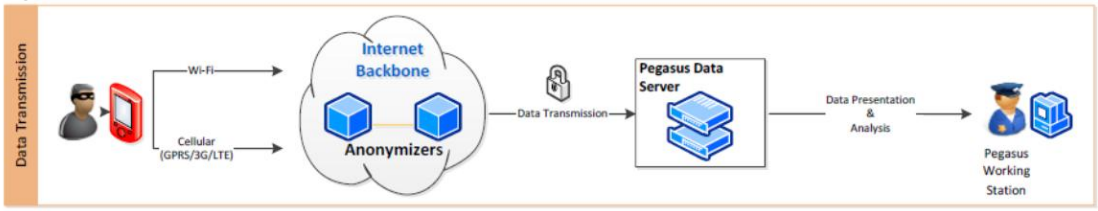
Cuando no hay canales de datos disponibles y no hay ninguna indicación de comunicación procedente del dispositivo, el usuario puede solicitar que el dispositivo se comunique y/o envíe algunos datos cruciales mediante mensajes de texto (SMS).

PRECAUCIÓN: La comunicación y/o transmisión de datos a través de SMS puede generar costos para el objetivo y aparecer en su informe de facturación, por lo que debe usarse con moderación.

La comunicación entre el agente y los servidores centrales es indirecta (a través de una red anonimizadora), por lo que el rastreo hasta el origen no es factible.

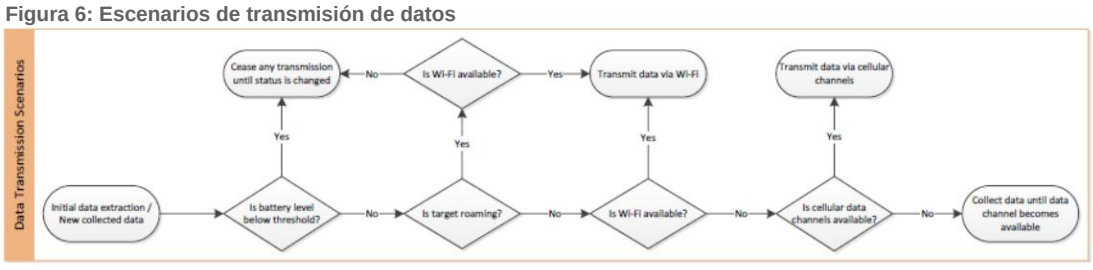
El proceso de transmisión de datos del sistema Pegasus se muestra en la Figura 5.

Figura 5: Proceso de transmisión de datos



Los canales y escenarios para la transmisión de los datos recopilados se muestran en la Figura 6.

Figura 6: Escenarios de transmisión de datos



Seguridad de transmisión de datos

Todas las conexiones entre los agentes y los servidores se cifran con algoritmos sólidos y se autentican mutuamente. Si bien el cifrado de datos es probablemente el problema más apremiante, se prestó especial atención para garantizar que se consuman los datos, la batería y la memoria mínimos dentro de los requisitos de los agentes. Esto está destinado a asegurarse de que el objetivo no plantee preocupaciones.

La detección de un agente operativo por parte del objetivo es casi imposible. El agente de Pegasus se instala en el nivel del kernel del dispositivo, está bien oculto y es imposible de rastrear por el software antivirus y antiespía.

Los datos transmitidos se cifran con cifrado simétrico AES de 128 bits.

Red de transmisión de anonimización de Pegasus

La transparencia del agente y la seguridad de la fuente son los principios rectores de la solución Pegasus. Para garantizar que el rastreo hasta la organización operativa sea imposible, se implementa la Red de transmisión anonimizadora (PATN) de Pegasus, una red de anonimizadores para atender a cada cliente. Los nodos PATN se distribuyen en diferentes lugares del mundo, lo que permite redirigir las conexiones de los agentes a través de diferentes rutas antes de llegar a los servidores de Pegasus. Esto asegura que las identidades de ambas partes que se comunican estén muy ocultas.

Presentación y análisis de datos

La recopilación exitosa de datos de cientos de objetivos y dispositivos genera cantidades masivas de datos para visualización, presentación y análisis. El sistema proporciona un conjunto de herramientas operativas para ayudar a la organización a transformar los datos en inteligencia procesable. Esto es para ver, ordenar, filtrar, consultar y analizar los datos recopilados. Las herramientas incluyen:

Análisis geográfico: realice un seguimiento de la ubicación histórica y en tiempo real del objetivo, vea varios objetivos en el mapa

Reglas y alertas: defina reglas para generar alertas sobre la llegada de datos importantes

Favoritos: marque eventos importantes y favoritos para una revisión posterior y un análisis más profundo

Tablero de inteligencia: vea aspectos destacados y estadísticas de las actividades del objetivo

Gestión de entidades : Gestione objetivos por grupos de interés (p. ej., drogas, terror, graves crimen, ubicación, etc.)

Análisis de línea de tiempo: revise y analice los datos recopilados de un período de tiempo particular

Búsqueda avanzada: Realice una búsqueda de términos, nombres, palabras clave y números para recuperar información específica

Los datos recopilados están organizados por grupos de interés (p. ej., grupo de drogas A, grupo terrorista B, etc.) y cada grupo consta de objetivos. Cada objetivo consta de varios dispositivos en los que algunos tienen agentes instalados.

Los datos recopilados se muestran en una interfaz de usuario intuitiva y fácil de usar y, cuando corresponde, emula la visualización popular de aplicaciones comunes. La interfaz de usuario intuitiva está diseñada para el trabajo diario. Los operadores pueden personalizar fácilmente el sistema para adaptarlo a sus métodos de trabajo preferidos, definir reglas y alertas para temas específicos de interés.

El operador puede optar por ver todos los datos recopilados de un objetivo específico o solo un tipo específico de información, como información de ubicación, registro de calendario, correos electrónicos o mensajes instantáneos.

La pantalla de monitoreo del calendario de Pegasus se muestra en la Figura 7.

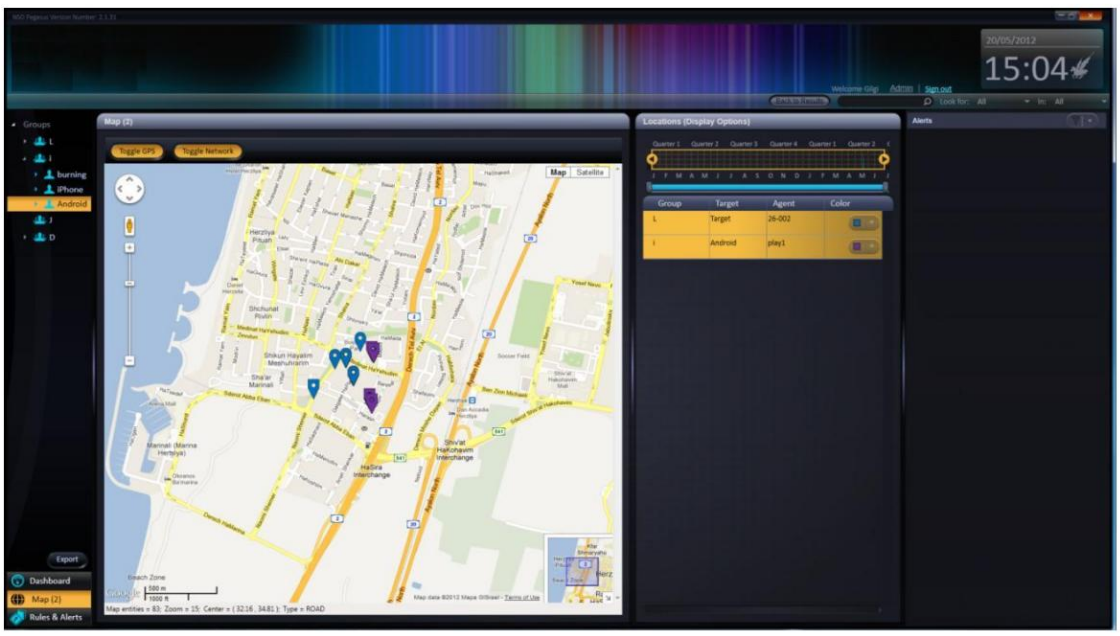
Figura 7: Monitoreo de Calendario

La pantalla de interceptación de llamadas y registro de llamadas de Pegasus se muestra en la Figura 8.

Figura 8: Registro de llamadas e intercepción de llamadas

La pantalla de seguimiento de ubicación de Pegasus se muestra en la Figura 9.

Figura 9: Seguimiento de ubicación



Los campos de presentación de los datos recopilados se enumeran en la Tabla 2.

Tabla 2: Presentación de los datos recopilados

Service / Application Type	Extracted data	Display method
Instant Messaging (IM): 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	▪ Chat participants (Names & phones) ▪ Conversation content ▪ Date & Time ▪ Attachments metadata (without the attachment)	▪ Grid ▪ Conversation mode
Location Tracking	▪ Data source (GPS/Cell-ID) ▪ Latitude ▪ Longitude ▪ Date & Time	▪ Grid ▪ Map: - On map display - Full trail - Type of location data (GPS or Cell-ID based)
Calendar	▪ Meeting subject ▪ Event date and start time	▪ Grid ▪ Monthly calendar view (emulates popular calendar clients)
Contact details	▪ Entire values stored in the contact entry including photo if available	▪ Grid ▪ Contact card with the entire details
Environmental sound recording (microphone recording)	▪ Recorded audio ▪ Recording Date & Time ▪ Duration	▪ Grid ▪ Playback interface
SMS	▪ Direction (incoming, outgoing) ▪ Contact name ▪ Phone number ▪ Message content ▪ Date & Time	▪ Grid
Call Interception	▪ Direction ▪ Contact name ▪ Phone number ▪ Duration ▪ Date & Time	▪ Grid ▪ Playback interface
Email: 1. Main email application in all platforms 2. Gmail application in Android	▪ From ▪ To ▪ CC ▪ BCC ▪ Subject ▪ Folder ▪ Account ▪ Message content ▪ Date & Time	▪ Grid ▪ HTML (emulates popular email clients)
File retrieval	▪ List of folders (tree) ▪ List of files (grid): ▪ Filename	▪ Grid ▪ Tree view

Service / Application Type	Extracted data	Display method
	▪ Modified date ▪ File size	
Photo taking	▪ Date & Time ▪ Photo	▪ Grid ▪ Photo viewer
Screen capturing	▪ Date & Time ▪ Screen capture image	▪ Grid ▪ Photo viewer
Browsing history	▪ Website name (as saved by the target, usually the default website name) ▪ Website URL address	▪ List
Browsing favorites	▪ Website name (as saved by the target, usually the default website name) ▪ Website URL address	▪ List
Call history (call log)	▪ Direction ▪ Contact name ▪ Phone number ▪ Duration ▪ Date & Time	▪ Grid
Device information	▪ Battery level ▪ Connection type (e.g., 3G, WiFi) ▪ MSISDN ▪ IMEI ▪ IMSI ▪ Device Manufacturer ▪ Device model ▪ Operating System version ▪ Installation date ▪ Last communication time ▪ Device current country ▪ Device home country ▪ Serving network ▪ Home serving network	▪ Dashboard

Reglas y Alertas

El módulo de Reglas y Alertas en el sistema alerta cuando ocurre un evento importante. Las reglas deben definirse con anticipación y ayudan a los operadores a revisar y tomar acciones en tiempo real, por ejemplo:

Geo-cercas: o

Acceder a la zona activa: alerta cuando el objetivo llega a una ubicación importante o

Abandonar la zona activa: alerta cuando el objetivo abandona una ubicación determinada

Las alertas de geo-cerca se basan en un perímetro alrededor de una ubicación determinada, donde el operador define el tamaño del perímetro.

Detección de reuniones: alerta cuando dos objetivos se encuentran (comparten la misma ubicación)

Detección de conexión:

- o Alerta cuando se envía un mensaje desde/hacia un número específico
- o Alerta cuando se realiza una llamada telefónica desde/hacia un número específico

Detección de contenido: alerta cuando se usa una palabra/término/palabra clave definida en un mensaje

Exportación de datos

El sistema está diseñado como un sistema de extremo a extremo, proporcionando a sus usuarios herramientas de recopilación y análisis. Sin embargo, entendemos que existen capacidades de análisis avanzadas y requisitos de fusión de datos de otras fuentes, por lo tanto, el sistema permite la exportación de la información recopilada y la integración perfecta con sistemas de análisis o back-end de terceros disponibles .

Mantenimiento de agentes

Una vez que el agente está instalado en un determinado dispositivo, debe mantenerse para admitir nuevas funciones y cambiar sus ajustes y configuraciones o desinstalarse cuando ya no proporciona inteligencia valiosa a la organización.

Actualización de agente

Cuando se lanzan las actualizaciones de los agentes, están disponibles para su instalación. Estos nuevos agentes ahora están listos para instalarse en los dispositivos de los nuevos objetivos o como actualizaciones para los agentes existentes instalados en los dispositivos de los objetivos. Estas actualizaciones brindan nuevas funcionalidades, corrección de errores, soporte para nuevos servicios o mejoran el comportamiento general de los agentes. Tales actualizaciones son cruciales para mantener el agente funcional y operativo en el progreso sin fin del mundo de las comunicaciones y especialmente en el campo de los teléfonos inteligentes.

Hay dos tipos de actualizaciones de agentes:

Actualización opcional: la actualización del agente no es obligatoria por el sistema. El usuario decide cuándo, en todo caso, actualizar el agente.

Actualización obligatoria: la actualización del agente es obligatoria por el sistema. El supervisor debe actualizar el agente; de lo contrario, no se monitoreará nueva información desde el dispositivo.

La actualización a veces requiere la instalación de un nuevo agente y, a veces, solo una pequeña actualización del agente existente. En ambos casos, el usuario es el único que decide cuándo realizar la actualización y, por lo tanto, debe planificarla en consecuencia.

Una vez que el usuario envió el comando para la actualización, el proceso debería llevar solo unos minutos. El proceso puede demorar más si el dispositivo está apagado o tiene una mala conexión de datos.
En cualquier caso, la actualización se realizará una vez que esté disponible una conexión de datos decente.

Configuración del agente

La configuración del agente se establece por primera vez durante su instalación. A partir de este punto, estas configuraciones sirven al agente, pero siempre se pueden cambiar si es necesario. La configuración incluye la dirección IP para transmitir los datos recopilados, la forma en que se envían los comandos al agente, el tiempo hasta que el agente se desinstala automáticamente (consulte el mecanismo de autodestrucción para obtener más detalles) y más.

Desinstalación del agente

Cuando se realiza la operación de inteligencia o en caso de que el objetivo ya no sea de interés para la organización, el componente basado en software ("Agente") en el dispositivo del objetivo se puede eliminar y desinstalar. La desinstalación es rápida, requiere una sola solicitud de usuario y no tiene un efecto mínimo en el dispositivo de destino. El usuario emite una solicitud de desinstalación del agente que se envía al dispositivo.

Una vez que el agente se desinstala de un determinado dispositivo, no deja rastros ni indicaciones de que alguna vez existió allí4. Siempre que el agente esté operativo en el dispositivo y exista una conexión entre él y los servidores, se puede desinstalar de manera fácil y remota.
.
La desinstalación siempre se puede realizar de forma remota, independientemente del método utilizado para la instalación. La desinstalación física también es una opción, si es necesario.

Desinstalar un agente no significa perder todos los datos recopilados: todos los datos recopilados durante el tiempo que el agente estuvo instalado en el dispositivo se mantendrán en los servidores para análisis futuros.

Mecanismo de autodestrucción

El sistema Pegasus contiene un mecanismo de autodestrucción para los agentes instalados. En general, entendemos que es más importante que la fuente no quede expuesta y que el objetivo no sospeche nada que mantener al agente con vida y trabajando. El mecanismo se activa en los siguientes escenarios:

Riesgo de exposición: En los casos en que exista una gran probabilidad de exposición del agente, automáticamente se activa un mecanismo de autodestrucción y se desinstala el agente.
El agente se puede volver a instalar en otro momento.

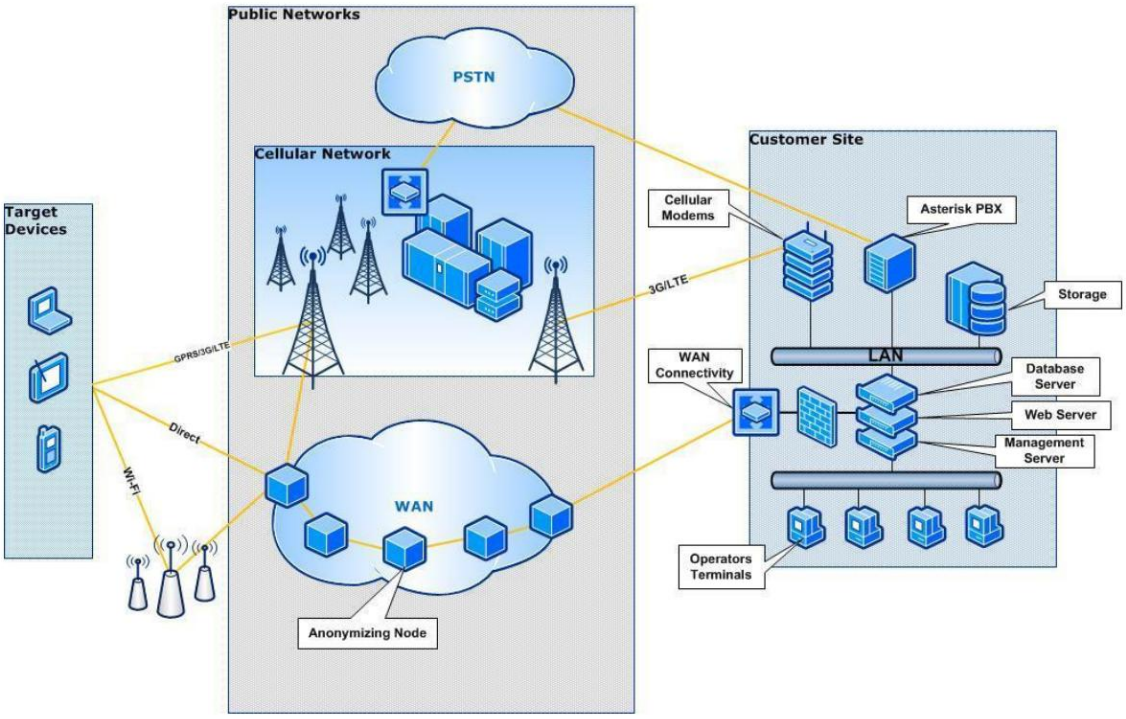
El agente no responde: en los casos en que el agente no responde y no se comunicó con los servidores durante mucho tiempo5, el agente se desinstalará automáticamente para evitar que se exponga o se use indebidamente.

4 En algunos casos, la desinstalación puede resultar en el reinicio del dispositivo. Si se reinicia, ocurre una vez que se realiza la eliminación del agente. El dispositivo aparece limpio sin ningún agente instalado.
5 El tiempo predeterminado es de 60 días, pero se puede reconfigurar para cualquier período de tiempo requerido

Arquitectura de soluciones

Los principales componentes arquitectónicos del sistema Pegasus se muestran en la Figura 10.

Figura 10: Arquitectura de la solución



Sitio del cliente

NSO es responsable de implementar y configurar el hardware y el software de Pegasus en las instalaciones del cliente, asegurándose de que el sistema funcione correctamente. A continuación se muestran los principales componentes instalados en el sitio del cliente:

Servidores WEB

Residiendo en las instalaciones del cliente, los servidores son responsables de lo siguiente:

- Instalación y monitoreo de agentes
- Mantenimiento de agentes: controle, configure y actualice de forma remota los agentes instalados
- Transmisión de datos: Recibir los datos recopilados transmitidos por los agentes instalados
- Atender las terminales de los operadores

Módulo de comunicaciones

El módulo de comunicaciones permite la interconectividad y conexión a internet a los servidores.

Módulo de comunicación celular

El módulo de comunicación celular permite la instalación remota del agente Pegasus en el dispositivo de destino utilizando módems celulares y/o puertas de enlace SMS.

Módulo de permisos

El módulo de gestión de permisos de Pegasus define y controla las funciones y el contenido disponible permitido para cada usuario en función de su función, rango y jerarquía.

Almacenamiento de datos

Los datos recopilados que fueron extraídos y monitoreados por los agentes se almacenan en un dispositivo de almacenamiento externo. Los datos están bien respaldados y con total resiliencia y redundancia para evitar fallas y tiempo de inactividad.

Seguridad de los servidores

Todos los servidores residen dentro de la red de confianza del cliente, detrás de las medidas de seguridad que pueda implementar, así como las medidas de seguridad que proporcionamos específicamente para el sistema.

Hardware

El hardware estándar del sistema se implementa en varios servidores conectados entre sí en un par de bastidores. El equipo se encarga del equilibrio de carga avanzado, la compresión de contenido, la gestión de conexiones, el cifrado, el enrutamiento avanzado y la supervisión del estado del servidor altamente configurable.

Consolas de operador

Los terminales de punto final (PC) del operador son la herramienta principal con la que los operadores activan el sistema Pegasus, inician instalaciones y comandos, y visualizan los datos recopilados.

Aplicación Pegaso

La aplicación Pegasus es la interfaz de usuario que está instalada en el terminal del operador. Proporciona a los operadores una variedad de herramientas para ver, ordenar, filtrar, administrar y alertar para analizar la gran cantidad de datos recopilados de los agentes de los objetivos.

Redes Públicas

Aparte de la instalación local de hardware y software en las instalaciones del cliente, el sistema Pegasus no requiere ninguna interfaz física con los operadores de redes móviles locales.
Sin embargo, dado que las instalaciones y los datos de los agentes se transfieren a través de las redes públicas, se asegura de que se transfiera de la manera más eficiente y segura, hasta los servidores del cliente:

Red anonimizadora

La red de transmisión anonimizada de Pegasus (PATN) se construye a partir de nodos de conectividad anónimos que se distribuyen en diferentes lugares del mundo, lo que permite que las conexiones de los agentes se dirijan a través de diferentes rutas antes de llegar a los servidores de Pegasus. Los nodos anonimizados sirven solo a un cliente y el cliente puede configurarlos si es necesario.

Ver más información en la sección Red de transmisión de anonimización de Pegasus.

Dispositivos de destino

La arquitectura mencionada anteriormente permite a los operadores emitir nuevas instalaciones, extraer, monitorear y recopilar activamente datos de los dispositivos de los objetivos. Vea más detalles en Sistemas operativos y dispositivos compatibles.

NOTA: El Pegasus es un sistema de inteligencia de misión crítica, por lo que es completamente redundante para evitar fallas y fallas. El sistema maneja grandes cantidades de datos y tráfico las 24 horas del día y es escalable para respaldar el crecimiento de los clientes y los requisitos futuros.

Hardware de la solución

Las especificaciones de hardware para operar el sistema Pegasus dependen de la cantidad de agentes instalados simultáneamente, la cantidad de estaciones de trabajo, la cantidad de datos almacenados y por cuánto tiempo deben almacenarse.

Todo el hardware necesario se suministra con el sistema en el momento de la implementación y puede requerir una personalización local que debe ser manejada por el cliente según nuestras instrucciones. Si es necesario, el cliente puede comprar el hardware según las especificaciones proporcionadas por nosotros.

Terminales de operadores

Los terminales de operador son PC de escritorio estándar, con las siguientes especificaciones:

- Procesador: Core i5
- Memoria: 3 GB RAM
- Disco duro: 320GB
- Sistema Operativo: Windows 7

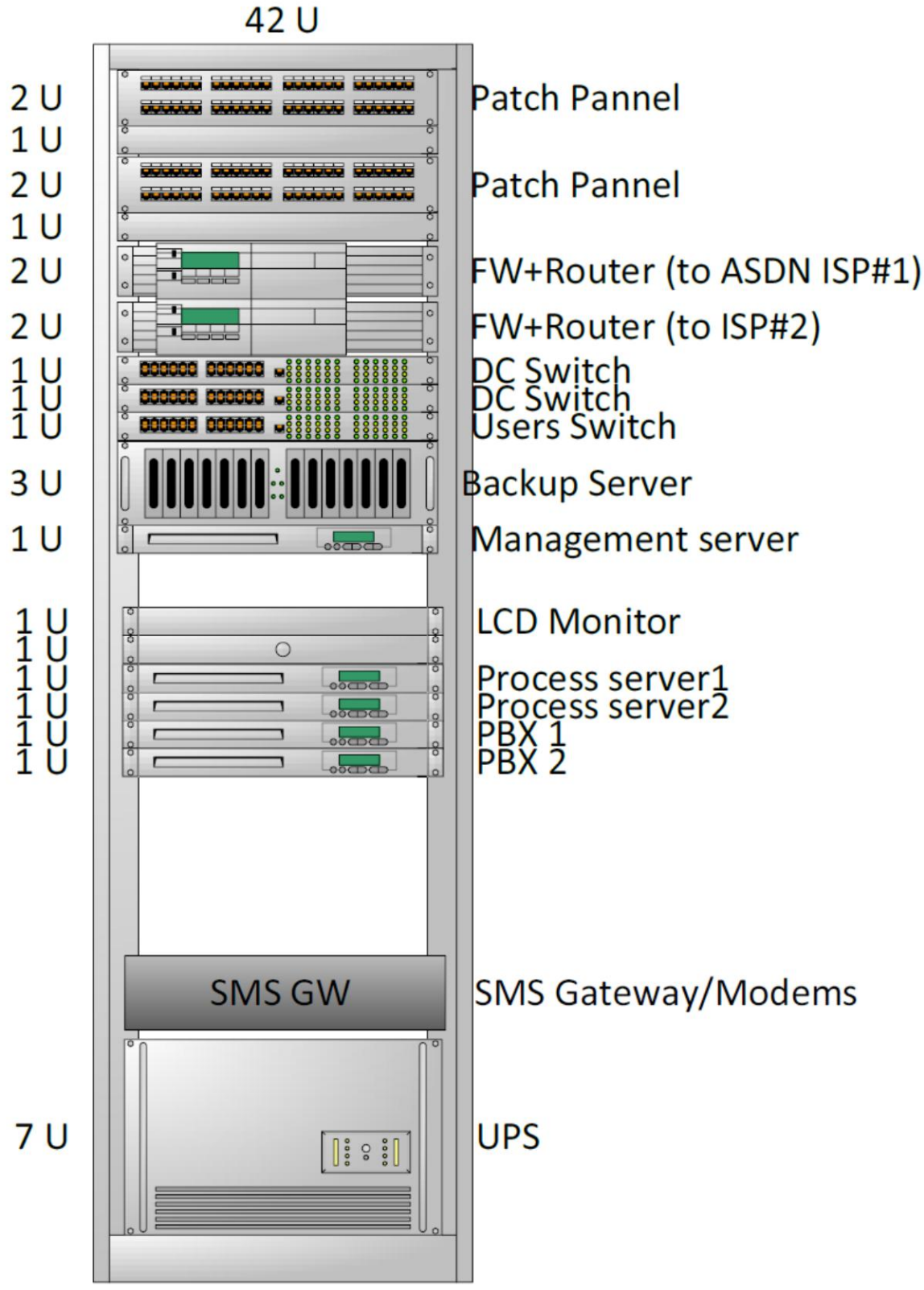
Hardware del sistema

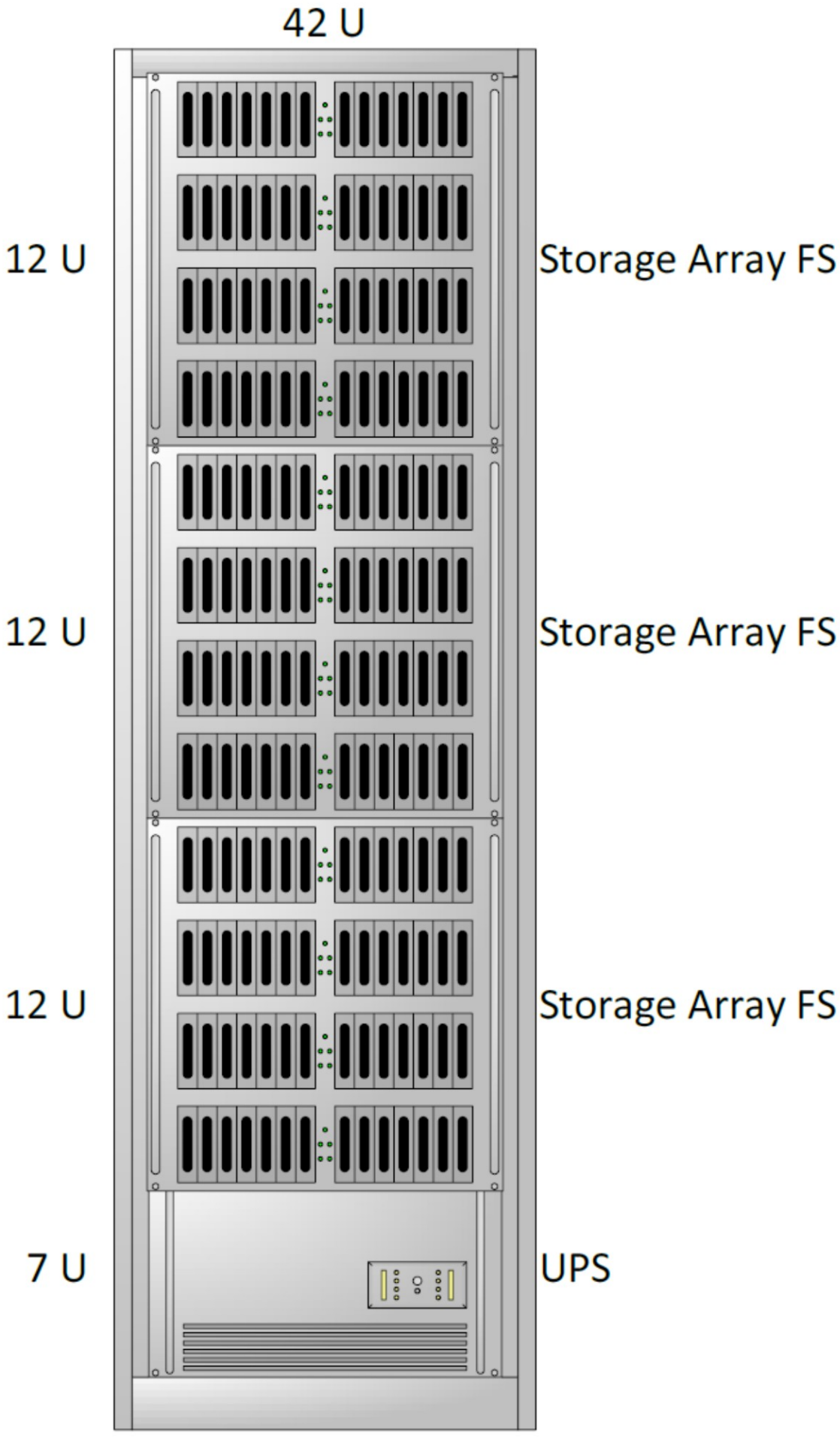
Para admitir completamente la infraestructura del sistema, se requiere el siguiente hardware:

- Dos unidades de gabinete 42U
- hardware de red
- 10 TB de almacenamiento
- 5 servidores estándar
- UPS
- Módems celulares y tarjetas SIM

El esquema de hardware del sistema se muestra en la Figura 11.

Figura 11: Hardware Pegasus





Configuración y capacitación del sistema

Somos responsables de la configuración y formación del sistema antes de su entrega al cliente.

Requisitos previos del sistema

La instalación exitosa del sistema Pegasus requiere las siguientes preparaciones de la sala de servidores:

- Espacio suficiente para albergar dos armarios de racks de 42U, 5x5x2,5 m (LxAnxAl)
- Habitación con aire acondicionado (18°C)
- Restricción de acceso
- Enrutamiento desde terminales de punto final a la sala de servidores
- Recepción de red celular confiable (al menos -95 dBm) 2 x tomacorrientes
- (20A) por rack
- 2 líneas ATM simétricas de diferentes ISP. Cada línea con un ancho de banda de 10 MB que contiene 8 direcciones IP estáticas externas:
  - o ISP n.º 1: red basada en fibra óptica o ISP n.º 2:
  - red basada en cable Ethernet de categoría 7 El sistema de misión crítica requiere dos redes paralelas para garantizar que la resiliencia del sistema y el tiempo de inactividad se mantengan en un mínimo absoluto.
- 2 conexiones E1 PRI, cada una contiene 10 extensiones (se recomiendan dos proveedores de servicios diferentes)
- 2 tarjetas SIM anónimas para cada operador de red móvil local
- Registro de servicios de terceros según sea necesario

Configuración del sistema

- La solución será implementada en el sitio del cliente por nuestro personal.
- La duración de la implementación generalmente requiere de 10 a 15 semanas laborales
- Se deben cumplir los requisitos previos del entorno operativo
- La configuración del sistema incluye la instalación de hardware y software, y además la integración al entorno y los sistemas locales
- Soporte y adaptaciones a las diferentes versiones de firmware de dispositivos locales

Capacitación

Tras la instalación del sistema, nuestro personal llevará a cabo sesiones completas de capacitación. La capacitación puede realizarse en el sitio o en cualquier otro lugar requerido por el cliente, incluida nuestra sede.
La sesión de entrenamiento incluye lo siguiente:

- Uso básico del sistema
- Arquitectura del sistema
- Funciones y uso avanzado del sistema

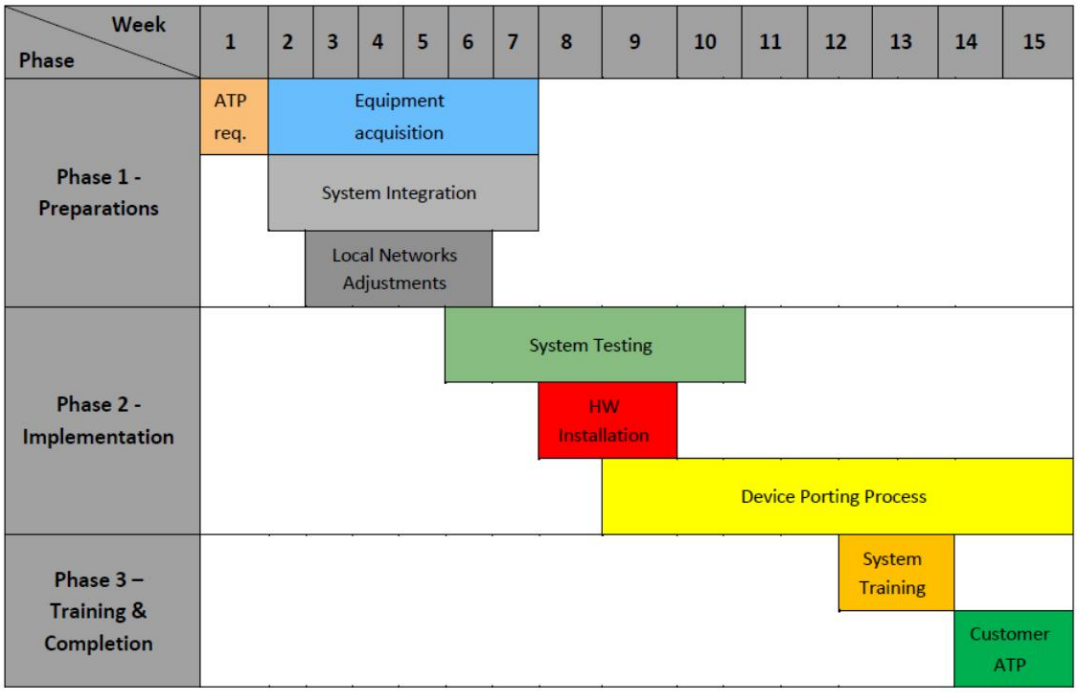
Ejercicios de simulación del mundo real

El número recomendado de asistentes es con respecto al número de consolas de operador instaladas.

Plan de implementación de alto nivel

El proceso de adaptación, instalación y prueba del sistema en el sitio de un nuevo cliente se enumera en la Tabla 3.

Tabla 3: Plan de implementación de Pegasus



Fase 1 – Preparativos:

Los requisitos para un Procedimiento de Prueba de Aceptación (ATP) se definen junto con el cliente

Adquisición y personalización de hardware y software para responder al cliente requisitos y necesidades

Cuando es necesario, el sistema Pegasus se integra con las infraestructuras y los sistemas locales

Adaptaciones del sistema a las redes móviles locales

Fase 2 – Implementación:

Pruebas del sistema

Instalación de hardware

Adaptaciones del sistema a versiones de firmware de dispositivos locales

Fase 3 - Formación y Finalización:

Entrenamiento detallado del sistema, práctica y simulación de escenarios de la vida real

Cliente ATP como se define durante la fase 1

Prueba de Aceptación del Sistema (SAT)

Hemos adquirido una experiencia sustancial en la instalación e implementación del sistema Pegasus.
El siguiente plan de prueba de aceptación verifica que el sistema funcione según lo requerido y valida que se haya entregado la funcionalidad correcta. Describe el alcance del trabajo a realizar y el enfoque adoptado para ejecutar las pruebas adecuadas para validar que el sistema funciona según lo acordado mutuamente con el cliente.

Las pruebas se dividen en 3 etapas:

Pruebas de funcionalidad

Pruebas de red y proveedores

Pruebas específicas a medida del cliente

Una vez que el sistema se ha implementado, probado y demostrado, se realiza una entrega oficial del sistema de nosotros al cliente.

Mantenimiento, soporte y actualizaciones

Proporcionamos, por defecto, un año de servicios de mantenimiento, soporte y actualizaciones. Estos servicios incluyen:

Mantenimiento y soporte

Brindamos servicios de mantenimiento y soporte de tres niveles que incluye:

- Nivel 1: problemas de operaciones del sistema estándar
  - o Asistencia telefónica y por correo electrónico
- Nivel 2: resolución proactiva de problemas técnicos o Ingenieros
  - dedicados inspeccionarán, examinarán y resolverán problemas técnicos comunes, poniendo sus mejores esfuerzos o Asistencia remota utilizando software de escritorio remoto y un privado virtual
  - Red (VPN) donde se solicite
- Nivel 3: corrección de errores y actualizaciones del sistema de fallas sustanciales del sistema
- Soporte telefónico: además de lo mencionado anteriormente, brindamos soporte telefónico y de correo electrónico apoyo a cualquier duda y problema que se plantee.

Además, el cliente podrá agregar el siguiente soporte:

- Asistencia in situ planificada o de emergencia
- Sistema de vigilancia de la salud

Actualizaciones

Tenemos lanzamientos de actualizaciones importantes para el sistema Pegasus varias veces al año. Estas actualizaciones suelen incluir:

- Nuevas características
- Compatibilidad con nuevos dispositivos/sistemas operativos
- Características personalizadas basadas en los requisitos del cliente
- Corrección de errores