Desarrollo, vía validación y testeo de funcionalidades en entornos de fábrica red (SANTI)

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

InprOTech

Smart security for your industry

INPROTECH GUARDIAN

Registro de alertas

Fecha: 06/2024

Referencia documento: IN-Registro de alertas

Versión: 2.6

INDICE

Contenido

1 Introducción

InprOTech Guardian es un servicio de cibervigilancia de redes industriales cuyas capacidades de detección de amenazas se basan en tres estrategias:

- El empleo de heurísticos (reglas estáticas de detección de escenarios de posible compromiso).
- El uso de algoritmos de Machine learning (IA), para detectar desviaciones de comportamiento frente a un patrón preentrenado y específico de una red industrial concreta (la del cliente).
- La implementación de un IDS (Snort), con las firmas de detección de Cisco Talos, uno de los principales proveedores de ciberinteligencia del mercado, incluyendo las vulnerabilidades *zero-day* de Microsoft.

Mediante las anteriores, Guardian es capaz de identificar miles de escenarios de ataque, compromiso o anomalía de los sistemas y servicios presentes en la red industrial, con el fin de mitigar su eventual impacto.

En este documento, se indica a alto nivel cuáles son las alertas generadas por InprOTech Guardian, descripción, causas probables, consecuencias y acciones recomendadas, de tal manera que el cliente pueda tomar el mejor curso de acción con la mayor información posible.

2 Alarmas estáticas

2.1 Nuevo dispositivo

Alarma:	**Prioridad:**
"New device"	Crítica

Descripción:

Nueva dirección "MAC" localizada en la red de la organización.

Causas Probables:

Se ha detectado una nueva dirección "MAC", no registrada previamente, correspondiente a un equipo conectado a la red de la organización.

Consecuencias:

Posibilidad de intrusión a la red de la organización.

Acciones recomendadas:

Localizar el equipo que posee la "MAC" objeto de la alarma, verificar su identidad y legitimidad, y realizar el tratamiento que se considere oportuno de dicho equipo o conexión.
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación "Inprotech Guardian".

1. En caso de considerar la nueva dirección "MAC" como legítima y no querer que aparezca nuevamente el aviso en futuras conexiones, se deberá gestionar la alarma como silenciada. Así mismo, si se considera que el dispositivo pertenece a la red de la organización, éste deberá ser marcado como autorizado.

2. En el caso de aceptación de la nueva dirección "MAC" pero se quiera mantener las notificaciones en sus futuras conexiones, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.2 Nueva IP

Alarma:	**Prioridad:**
"New IP"	Advertencia

Descripción:

Nueva dirección "IP" localizada en la red de la organización.

Causas:

Se ha detectado una nueva dirección "IP", no registrada previamente, correspondiente a un equipo conectado a la red de la organización.

Consecuencias:

Posibilidad de intrusión a la red de la organización.

Solución:

Localizar el equipo que posee la "IP" objeto de la alarma, verificar su identidad y legitimidad, y realizar el tratamiento que se considere oportuno de dicho equipo o conexión.
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación "Inprotech Guardian".

1. En caso de considerar la nueva dirección "IP" como legítima y no querer que aparezca nuevamente el aviso en futuras conexiones, se deberá gestionar la alarma como silenciada. Así mismo, si se considera que el dispositivo pertenece a la red de la organización, éste deberá ser marcado como autorizado.

2. En el caso de aceptación de la nueva dirección "IP" pero se quiera mantener las notificaciones en sus futuras conexiones, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.3 Nueva Conexión

Alarma:	**Prioridad:**
"New Connection"	Advertencia

Descripción:

Comunicación a través de puerto no habitual del dispositivo.

Causas:

Se ha establecido una comunicación en el dispositivo, haciendo uso de uno de sus puertos no utilizado con anterioridad.

Consecuencias:

Posibilidad de acceso no deseado a la interfaz del dispositivo e intrusión a la red de la organización.

Solución:

Localizar el equipo que ha recibido comunicación a través de un puerto diferente a los utilizados con anterioridad. Verificar la legitimidad del dispositivo y realizar el tratamiento que se considere oportuno de dicho equipo o conexión.
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación "Inprotech Guardian".

1. En caso de considerar aceptable el uso del nuevo puerto, objeto de la alarma, del dispositivo y no querer que aparezca nuevamente el aviso en futuras conexiones a dicho puerto, se deberá gestionar la alarma como silenciada.

2. En el caso de aceptación de la comunicación en el dispositivo mediante el puerto, objeto de la alarma, pero se quiera mantener las notificaciones en futuras conexiones a dicho puerto, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.4 Anomalía en puerto de red

Alarma:	**Prioridad:**
"Network port anomaly"	Advertencia

Descripción:

Diferente protocolo de comunicaciones, al primero registrado, en un puerto del dispositivo.

Causas:

El sistema Guardian ha detectado una comunicación mediante un protocolo diferente al primero que se ha registrado, en uno de los puertos del dispositivo.

Consecuencias:

Posibilidad de acceso no deseado a la interfaz del dispositivo e intrusión a la red de la organización.

Solución:

Localizar el equipo que ha sufrido un cambio de protocolo de comunicación en uno de sus puertos, verificar su identidad y legitimidad, y realizar el tratamiento que se considere oportuno de dicho equipo o conexión.
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación Inprotech Guardian.

1. En caso de considerar aceptable el cambio de protocolo en el puerto, objeto de la alarma, del dispositivo y no querer que aparezca nuevamente el aviso en futuros cambios de protocolo en ese puerto, se deberá gestionar la alarma como silenciada.

2. En el caso de aceptación del cambio de protocolo de comunicación en el puerto, objeto de la alarma, pero se quiera mantener las notificaciones en futuros cambios de protocolo en ese puerto, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.5 Nueva IP pública

Alarma:	**Prioridad:**
"New public IP"	Advertencia

Descripción:

Dirección "IP" pública localizada en la red de la organización.

Causas:

Se ha detectado una dirección "IP" pública correspondiente a un dispositivo, conectada a la red de la organización.

Consecuencias:

Posibilidad de intrusión a la red de la organización.

Solución:

Localizar el equipo que posee la "IP" pública, objeto de la alarma, verificar su identidad y legitimidad, y realizar el tratamiento que se considere oportuno de dicho equipo o conexión.
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación "Inprotech Guardian".

1. En caso de considerar la dirección "IP" pública como legítima y no querer que aparezca nuevamente el aviso en futuras conexiones, se deberá gestionar la alarma como silenciada.

2. En el caso de aceptación de la dirección "IP" pública, pero se quiera mantener las notificaciones en sus futuras conexiones, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.6 Conexión con puerto IT

Alarma:	**Prioridad:**
"Connection with IT port"	Crítica

Descripción:

Comunicación de puerto IT en red OT

Causas:

Se ha establecido una comunicación de un puerto, de un dispositivo, declarado como IT dentro de la red OT de la organización.

Consecuencias:

Posibilidad de intrusión a la red OT de la organización.

Solución:

Localizar el dispositivo con puerto de comunicaciones declarado en la red IT y que se encuentra estableciendo comunicación dentro del entorno OT de la organización. Verificar su identidad y legitimidad, y realizar el tratamiento que se considere oportuno de dicho equipo.
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación Inprotech Guardian.

1. En caso de aceptar la comunicación del dispositivo con puerto de comunicaciones declarado como IT con equipos de la red OT de la organización, y no querer que aparezca nuevamente el aviso en futuras comunicaciones, se deberá gestionar la alarma como silenciada.

2. En el caso de aceptar la comunicación del dispositivo a través del puerto de comunicaciones declarado como IT con equipos de la red OT de la organización, pero se quiera mantener las notificaciones en futuras comunicaciones, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.7 Posible fingerprinting

Alarma:	**Prioridad:**
"Possible fingerprinting"	Advertencia

Descripción:

Dispositivo en busca de puertos de comunicación abiertos en la organización.

Causas:

El sistema Guardian ha detectado que la dirección IP de un dispositivo, externo o interno, está intentando establecer comunicación con diferentes "IPs" de equipos de la organización en busca de puertos abiertos.

Consecuencias:

Posibilidad de acceso no deseado a la interfaz de dispositivos e intrusión a la red de la organización.

Solución:

Localizar el equipo que posee la IP objeto de la alarma, verificar su identidad y realizar el tratamiento que se considere oportuno de dicho equipo.

Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación Inprotech Guardian.

1. Si se trata de un dispositivo legítimo y no se quiere que aparezca nuevamente el aviso en futuros intentos de conexión, se deberá gestionar la alarma como silenciada.

2. Si se trata de un dispositivo legítimo, pero se quiera mantener las notificaciones en sus futuros intentos de conexión, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.8 Posible ARP spoofing

Alarma:	**Prioridad:**
"Possible ARP spoofing"	Advertencia

Descripción:

Dispositivo con diferente correlación entre direcciones "IP" y "MAC".

Causas:

El sistema Guardian ha detectado que la dirección "MAC" de uno de los dispositivos no se corresponde con la dirección "IP" anteriormente registrada. Por lo cual, el equipo ha sufrido un cambio de dirección "IP".

Consecuencias:

Posibilidad de intrusión a la red de la organización.

Solución:

Localizar el equipo que ha sufrido un cambio de dirección "IP" respecto a su dirección "MAC".
Su localización se puede realizar haciendo un seguimiento en el mapa de red de la aplicación Inprotech Guardian.

1. En caso de considerar correcta la nueva dirección "IP" en el dispositivo y no querer que aparezca nuevamente el aviso en futuras comunicaciones, se deberá gestionar la alarma como silenciada. Así mismo, si se quiere asignar esa nueva dirección "IP" a la dirección "MAC" del dispositivo, se deberá de hacer su sustitución en los ajustes del dispositivo.

2. En el caso de aceptación de la nueva dirección "IP" al dispositivo pero se quiera mantener las notificaciones en sus futuras comunicaciones, se deberá gestionar la alarma como resuelta.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

2.9 Alerta de inactividad

Alarma:	**Prioridad:**
"Inactivity alert"	Emergencia

Descripción:

El módulo de gestión de alertas no recibe datos de la sonda de tráfico.

Causas:

Posible fallo en uno o varios puntos de la comunicación entre la sonda y el gestor de alertas.
Otro motivo podría ser un error de configuración por parte del administrador de los timeouts de eventos.
También debería considerarse la desconexión física del cable conectado al puerto espejo del switch de la fábrica, por donde se produce el sniffing.

Consecuencias:

Potencial pérdida de datos; Guardian deja de monitorear el tráfico, con el riesgo que eso conlleva.

Solución:

Comprobación física del equipo para descartar problemas de conexión. Si todo está OK, escalado a InprOtech para revisión interna desde interfaz de administración.

Enlace a fuente de información externa:

Manual de usuario InprOTech Guardian.

3 Alarmas de IA/ML

3.1 Alerta por correlación de algoritmos

Alarma:	**Prioridad:**
ML algorithm collision	*"{critical|alert}"* dependiendo de parámetros internos (threshold y severity_delta)
Descripción:	
Algunos algoritmos detectaron este suceso como una anomalía	
Causas:	
Varios algoritmos han detectado que un mismo evento es anómalo.	
Consecuencias:	
Posibilidad de intrusión a la red OT de la organización o comunicación anómala de alguno de sus elementos, puesto que se detecta una desviación con respecto a la línea base de comportamiento que el algoritmo había aprendido durante su entrenamiento.	
Solución:	
Revisión interna de la anomalía para determinar el alcance.	
Enlace a fuente de información externa:	
Manual de usuario InprOTech Guardian.	

3.2 Alerta por varias anomalías en dispositivo origen

Alarma:	**Prioridad:**
SRC Device generated {número mínimo de anomalías} anomalies	*"{critical|alert}"* dependiendo de parámetros internos (threshold y severity_delta)

Descripción:
Este dispositivo generó {número mínimo de anomalías} anomalias en {tiempo mínimo} seconds. -> Puede o no ser un ataque, pero es aconsejable estudiarlo o volver a entrenar.

Causas:
Un mismo dispositivo está siendo detectado como fuente de varias anomalías en un corto período de tiempo. También puede ser que el tráfico haya cambiado, porque se añada o quite algún dispositivo o porque se esté haciendo un nuevo producto industrial o incluso puede afectar cambios de turno si en el proceso hay intervención humana y sea necesario reentrenar.

Consecuencias:
Posibilidad de intrusión a la red OT de la organización o comunicación anómala de alguno de sus elementos, puesto que se detecta una desviación con respecto a la línea base de comportamiento que el algoritmo había aprendido durante su entrenamiento.

Solución:
Revisión interna de la anomalía para determinar el alcance.

Enlace a fuente de información externa:
Manual de usuario InprOTech Guardian.

3.3 Alerta por varias anomalías en dispositivo destino

Alarma:	**Prioridad:**
DST Device generated {número mínimo de anomalías} anomalies	*"{critical|alert}"* dependiendo de parámetros internos (threshold y severity_delta)

Descripción:
Este dispositivo generó {número mínimo de anomalías} anomalias en {tiempo mínimo} seconds. -> Puede o no ser un ataque, pero es aconsejable estudiarlo o volver a entrenar.

Causas:
Un mismo dispositivo está siendo detectado como destino de varias anomalías en un corto período de tiempo. También puede ser que el tráfico haya cambiado, porque se añada o quite algún dispositivo o porque se esté haciendo un nuevo producto industrial o incluso puede afectar cambios de turno si en el proceso hay intervención humana y sea necesario reentrenar.

Consecuencias:
Posibilidad de intrusión a la red OT de la organización o comunicación anómala de alguno de sus elementos, puesto que se detecta una desviación con respecto a la línea base de comportamiento que el algoritmo había aprendido durante su entrenamiento.

Solución:
Revisión interna de la anomalía para determinar el alcance.

Enlace a fuente de información externa:
Manual de usuario InprOTech Guardian.

3.4 IA/ML alarms (antiguo)

Alarma:	**Prioridad:**
Anomaly detected in {netflow/raw} traffic	*"{critical|alert}"* dependiendo de parámetros internos (threshold y severity_delta)
Descripción:	
Anomalía detectada usando el modelo *{algoritmo}*, puntuación: *{puntuación}*.	
Causas:	
El motor de IA del sistema Guardian ha detectado una anomalía en el tráfico de la red debido a una desviación de los patrones de comportamiento normales aprendidos previamente durante el entrenamiento.	
Consecuencias:	
Posibilidad de intrusión a la red OT de la organización o comunicación anómala de alguno de sus elementos, puesto que se detecta una desviación con respecto a la línea base de comportamiento que el algoritmo había aprendido durante su entrenamiento.	
Solución:	
Revisión interna de la anomalía para determinar el alcance.	
Enlace a fuente de información externa:	
Manual de usuario InprOTech Guardian.	

4 Alarmas de IDS

Alarma:	**Prioridad:**
{Campo alert message del IDS Snort}	"*{emergency|alert|error}*" dependiendo de la prioridad de la alerta del IDS
Descripción:	
{Campo alert message del IDS Snort}	
Causas:	
Consultar información adicional asociada en la base de datos de Snort, mediante el enlace proporcionado en el campo Valor de la alerta.	
Consecuencias:	
Consultar información adicional asociada en la base de datos de Snort, mediante el enlace proporcionado en el campo Valor de la alerta.	
Solución:	
Consultar información adicional asociada en la base de datos de Snort, mediante el enlace proporcionado en el campo Valor de la alerta.	
Enlace a fuente de información externa:	
Manual de usuario InprOTech Guardian, y base de datos de Snort (https://www.snort.org/rule_docs/).	

5 Alarmas UEBA/PM

5.1 Alerta UEBA

Alarma:	**Prioridad:**
Anomaly detected in lstm	(Warning/Alert) dependiendo de parámetros internos (threshold y severity_delta)
Descripción:	
Anomaly detected by lstm model. Scoring: {value}	
Causas:	
El motor de IA del sistema Guardian ha detectado una anomalía en el tráfico de la red debido a una desviación de los patrones de comportamiento normales aprendidos previamente durante el entrenamiento.	
Consecuencias:	
Posibilidad de intrusión a la red OT de la organización o comunicación anómala de alguno de sus elementos, puesto que se detecta una desviación con respecto a la línea base de comportamiento que el algoritmo había aprendido durante su entrenamiento.	
Solución:	
Revisión interna de la anomalía para determinar el alcance.	
Enlace a fuente de información externa:	
Manual de usuario InprOTech Guardian.	

5.2 Alerta PM

Alarma:	**Prioridad:**
Anomaly detected in process mining	(Warning/Alert) dependiendo de parámetros internos (threshold y severity_delta)
Descripción:	
Anomaly detected in process-mining model. Scoring: {value}	
Causas:	
El motor de IA del sistema Guardian ha detectado una anomalía en el tráfico de la red debido a una desviación de los patrones de comportamiento normales aprendidos previamente durante el entrenamiento.	
Consecuencias:	
Posibilidad de intrusión a la red OT de la organización o comunicación anómala de alguno de sus elementos, puesto que se detecta una desviación con respecto a la línea base de comportamiento que el algoritmo había aprendido durante su entrenamiento.	
Solución:	
Revisión interna de la anomalía para determinar el alcance.	
Enlace a fuente de información externa:	
Manual de usuario InprOTech Guardian.	

6 Pruebas proactivas de alertas

A continuación se indica cómo llevar a cabo tests proactivo que generen alertas, para verificar que las estrategias de detección de amenazas se están comportando conforme a lo esperado.

- *Al conectar un dispositivo con una MAC nueva en la red, debería generarse la alerta de NUEVO DISPOSITIVO.*
- *Al hacer que un dispositivo, nuevo o existente, levante una IP no registrada con anterioridad aparecería la de NUEVA IP.*
- *Al hacer una conexión contra un dispositivo en un puerto no utilizado en el pasado, aparecerá la de NUEVA CONEXIÓN.*
- *Al hacer una conexión contra un dispositivo en un puerto ya utilizado anteriormente pero un protocolo diferente (por ejemplo, http en puerto de https o a la inversa), tendríamos la alerta de ANOMALÍA EN PUERTO DE RED.*
- *Si se hace una conexión contra una IP pública desde un dispositivo, saltaría la alerta de NUEVA IP PÚBLICA.*
- *Si se ven comunicaciones dentro de la red OT en puertos habitualmente etiquetados como IT (por ejemplo http. La lista es: 20, 21, 22, 23, 25, 80, 443, 143, 445), se generará la alarma CONEXIÓN CON PUERTO IT.*
- *Si se hace un fingerprinting mediante TCP SYN contra un dispositivo por ejemplo con NMAP y sobrepasas los umbrales (por defecto más de 3 en 5 minutos), saltará la alerta de POSIBLE FINGERPRINTING.*
- *Si se cambia una asociación MAC-IP, se generará una alerta por POSIBLE ARP SPOOFING, con un período de descanso por defecto de 1h.*
- *Si se da un cambio significativo de comportamiento de la red con respecto a lo habitual, se darán una o varias alertas por ANOMALÍA EN EL TRÁFICO RAW/NETFLOW. Forzarlo, quizás sería tan fácil como insertar un dispositivo en la red y ponerlo a descargar una ISO de un sistema operativo, por ejemplo, o haciendo un fingerprinting mediante TCP SYN contra un dispositivo con NMAP, o cambiando asociaciones MAC-IP.*
- *Con respecto a las firmas del IDS, podría probarse cualquiera del listado, que se puede consultar aquí: https://www.snort.org/downloads#rules.*

* Se entiende que cada alerta se da para un contexto de red (IPs,MACs, puerto, protocolo) concreto, y luego hay un período de descanso definido en la configuración, por lo que si estamos en ese escenario, la alerta no se genera.