

# SECURE SOFT CORPORATION

**e-Secure Consulting Group**

**REPORTE MENSUAL OPERACIÓN DE CYBERSOC**

**Enero de 2022**

## Preparado para:



**Fecha:**

**${fecha\_actual}**

**El presente documento contiene información estrictamente privada y confidencial para Securesoft Corp S.A.C. y Banco Pichincha Colombia.**

## OBJETIVO

Este documento dará a conocer el estado de la gestión del servicio de monitoreo para el Banco Pichincha Colombia.

## ALCANCES

Este documento servirá como herramienta para verificar el correcto funcionamiento de los equipos, estado de las atenciones de los requerimientos y la recolección de eventos e información obtenida de las diferentes plataformas integradas en el SIEM en el mes de **enero**.

## ESTADO DE SALUD

## RESUMEN EVENTOS DE SALUD

## 

## FIREWALLS

## FIREWALL AMERICAS

${graph1208}

* *Se observa el uso de consumo de CPU durante el último mes es de 1.02%*
* *Se observa el uso de consumo de Disco durante el último mes es de 29.49%*
* *Se observa el uso de consumo de Memoria durante el último mes es de 18.79%*

## FIREWALL PANORAMA

${graph1203}

* *Se observa el uso de consumo de CPU durante el último mes es de 4.75%*
* *Se observa el uso de consumo de Disco durante el último mes es de 37.80%*
* *Se observa el uso de consumo de Memoria durante el último mes es de 79.38%*

## FIREWALL ZONA FRANCA

${graph1207}

* *Se observa el uso de consumo de CPU durante el último mes es de 1.00%*
* *Se observa el uso de consumo de Disco durante el último mes es de 20%*
* *Se observa el uso de consumo de Memoria durante el último mes es de 16.23%*

## COMPONENTES SIEM

## ESTADO DEL LICENCIAMIENTO

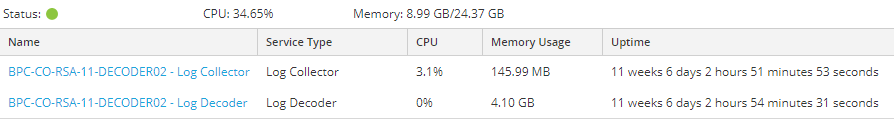
## 

## USO DE CPU Y MEMORIA ACTUAL

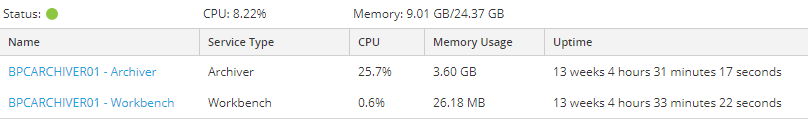
## Log Decoder 01

## 

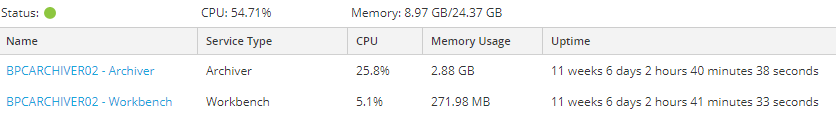
## Log Decoder 02



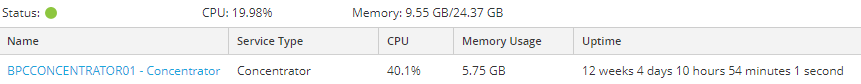
## Archiver 01



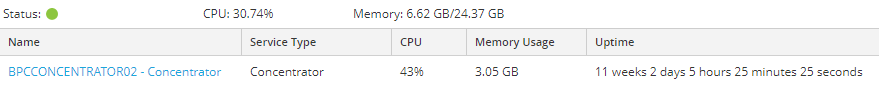
## Archiver 02



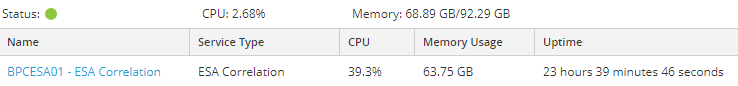
## Concentrator 01



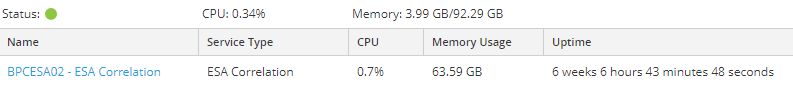
## Concentrator 02



## ESA 01

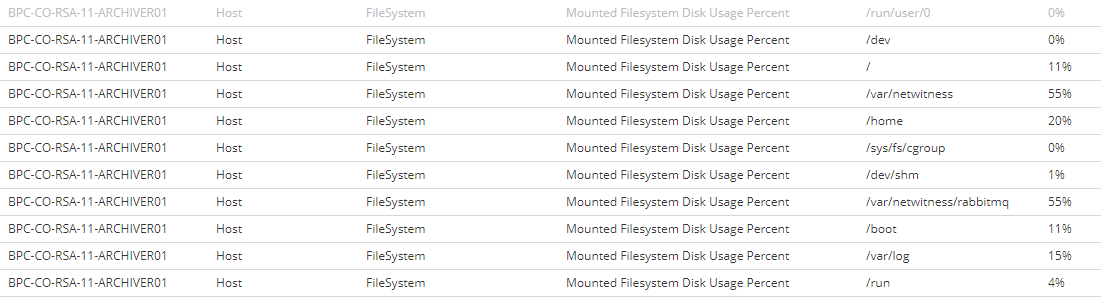


## ESA 02



## USO DE DISCO

* + 1. **Archiver 01**



## Archiver 02

## 

## Concentrator 01

## 

## Concentrator 02

## 

## ESA 01

## 

## ESA 02

## 

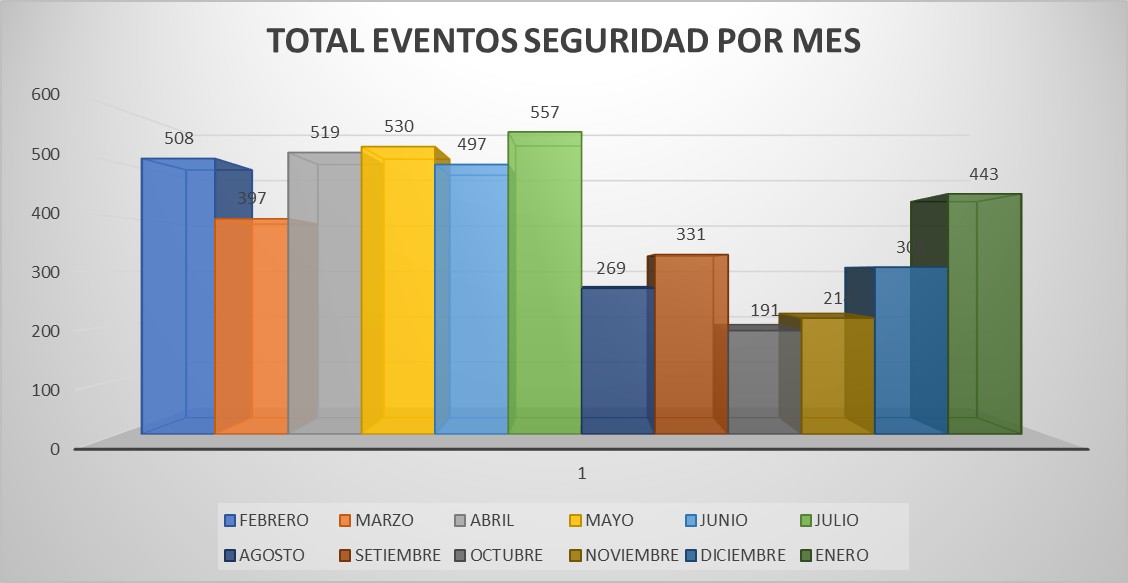
## Log decoder 01

## 

## Log decoder 02

## 

## RESUMEN EVENTOS DE SEGURIDAD



## EXABEAM

## ESTADO DE LOS RECURSOS

## 

## ESTADO DEL SISTEMA

## 

## USO DE DISCO

## 

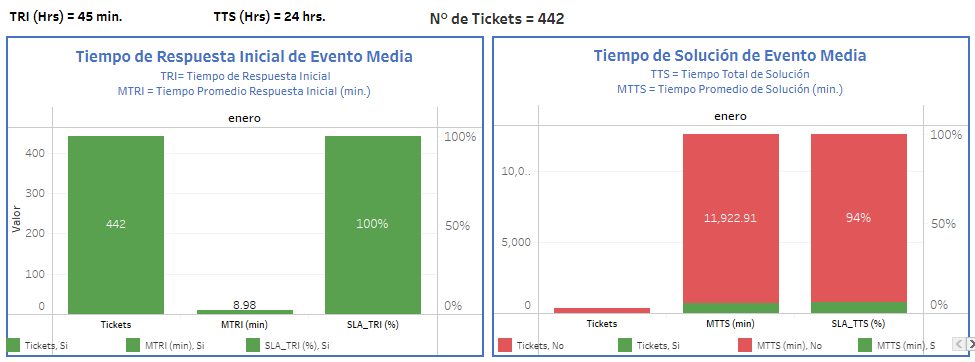
## 

## GESTION DEL SERVICIO

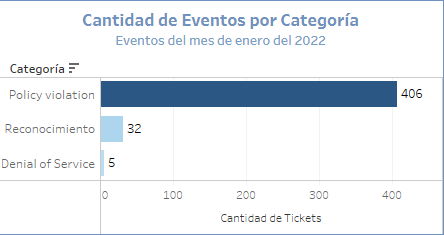
## Se ingresó a través de TABLEAU

## 

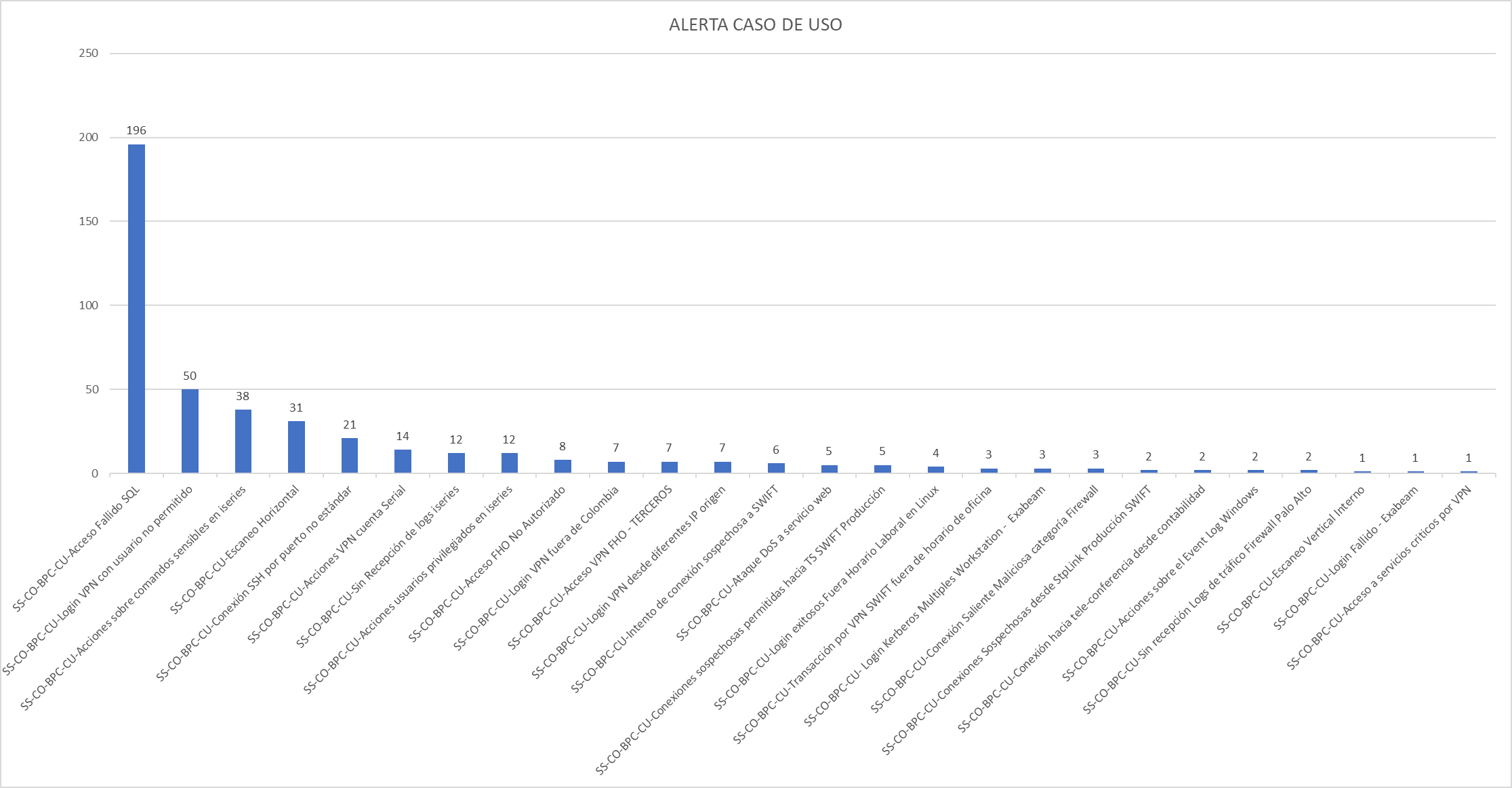
1. **SLA**



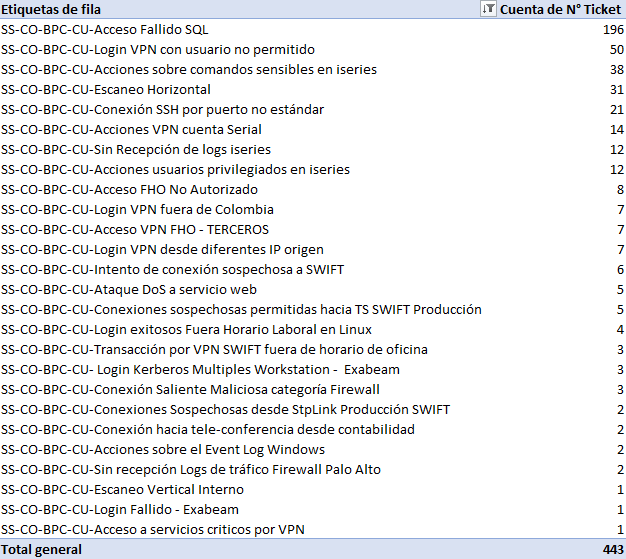
1. **ALERTAS POR CATEGORÍA**



1. **ALERTAS POR CASO DE USO**



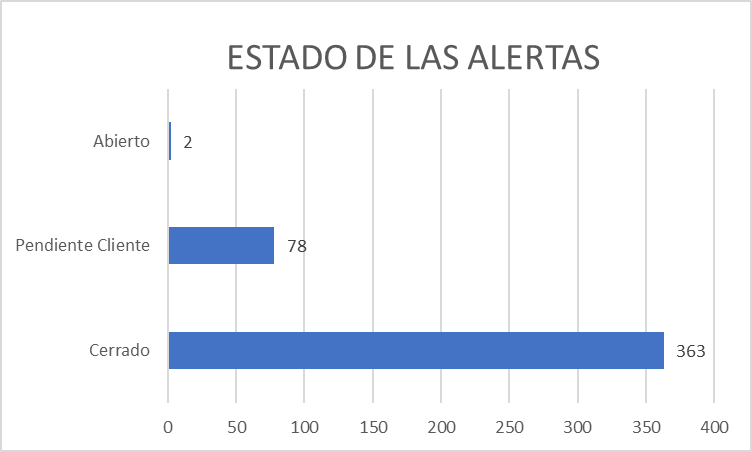
**Se agrega detalle debido a la cantidad de alertas.**



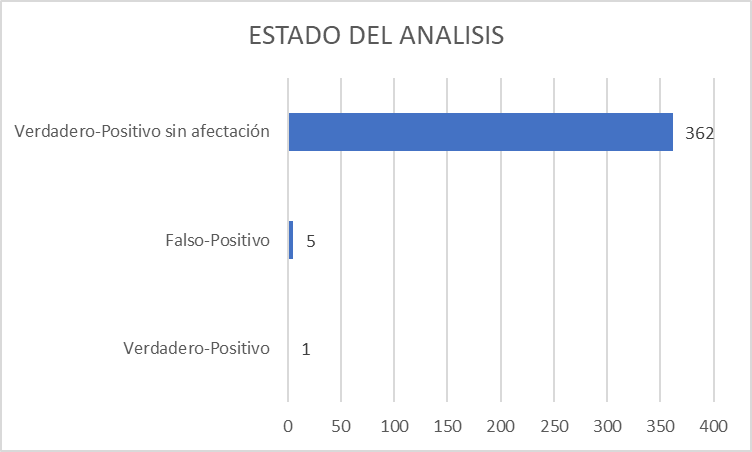
* **Detalle de alertas según los casos de uso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N° Ticket** | **Categoría** | **Caso\_Uso** | **Identificador** | **Status** |
| INC283664 | Policy violation | SS-CO-BPC-CU-Conexiones sospechosas permitidas hacia TS SWIFT Producción | Verdadero-Positivo sin afectación | Cerrado |
| INC280369 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC283648 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Falso-Positivo | Cerrado |
| INC286752 | Denial of Service | SS-CO-BPC-CU-Ataque DoS a servicio web |  | Pendiente Cliente |
| INC287121 | Policy violation | SS-CO-BPC-CU-Acciones sobre el Event Log Windows |  | Pendiente Cliente |
| INC272169 | Denial of Service | SS-CO-BPC-CU-Ataque DoS a servicio web | Verdadero-Positivo sin afectación | Cerrado |
| INC286914 | Denial of Service | SS-CO-BPC-CU-Ataque DoS a servicio web |  | Pendiente Cliente |
| INC280096 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC272676 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Verdadero-Positivo sin afectación | Cerrado |
| INC274557 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC274802 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC278468 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC286212 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276747 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado | Verdadero-Positivo | Cerrado |
| INC281961 | Policy violation | SS-CO-BPC-CU-Conexiones sospechosas permitidas hacia TS SWIFT Producción | Verdadero-Positivo sin afectación | Cerrado |
| INC279812 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC283951 | Policy violation | SS-CO-BPC-CU-Intento de conexión sospechosa a SWIFT |  | Pendiente Cliente |
| INC281960 | Policy violation | SS-CO-BPC-CU-Intento de conexión sospechosa a SWIFT |  | Pendiente Cliente |
| INC282317 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC279922 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC279943 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC279958 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC281583 | Policy violation | SS-CO-BPC-CU-Conexiones sospechosas permitidas hacia TS SWIFT Producción | Verdadero-Positivo sin afectación | Cerrado |
| INC275879 | Policy violation | SS-CO-BPC-CU-Login Fallido - Exabeam | Verdadero-Positivo sin afectación | Cerrado |
| INC282331 | Policy violation | SS-CO-BPC-CU-Acciones sobre el Event Log Windows |  | Pendiente Cliente |
| INC273451 | Policy violation | SS-CO-BPC-CU-Sin recepción Logs de tráfico Firewall Palo Alto | Falso-Positivo | Cerrado |
| INC273802 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Verdadero-Positivo sin afectación | Cerrado |
| INC273841 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Verdadero-Positivo sin afectación | Cerrado |
| INC285398 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Falso-Positivo | Cerrado |
| INC284942 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Falso-Positivo | Cerrado |
| INC277224 | Denial of Service | SS-CO-BPC-CU-Ataque DoS a servicio web |  | Pendiente Cliente |
| INC281366 | Policy violation | SS-CO-BPC-CU-Conexión Saliente Maliciosa categoría Firewall | Verdadero-Positivo sin afectación | Pendiente Cliente |
| INC281419 | Policy violation | SS-CO-BPC-CU-Conexión Saliente Maliciosa categoría Firewall | Verdadero-Positivo sin afectación | Pendiente Cliente |
| INC274728 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC278379 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries |  | Pendiente Cliente |
| INC274695 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC271798 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado | Verdadero-Positivo sin afectación | Cerrado |
| INC277361 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado | Verdadero-Positivo sin afectación | Cerrado |
| INC284530 | Reconocimiento | SS-CO-BPC-CU-Escaneo Vertical Interno | Verdadero-Positivo sin afectación | Cerrado |
| INC272253 | Policy violation | SS-CO-BPC-CU-Intento de conexión sospechosa a SWIFT | Verdadero-Positivo sin afectación | Cerrado |
| INC272190 | Policy violation | SS-CO-BPC-CU-Intento de conexión sospechosa a SWIFT | Verdadero-Positivo sin afectación | Cerrado |
| INC287155 | Policy violation | SS-CO-BPC-CU-Intento de conexión sospechosa a SWIFT |  | Pendiente Cliente |
| INC279771 | Policy violation | SS-CO-BPC-CU-Intento de conexión sospechosa a SWIFT |  | Pendiente Cliente |
| INC284562 | Denial of Service | SS-CO-BPC-CU-Ataque DoS a servicio web |  | Pendiente Cliente |
| INC279983 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC279998 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC280015 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC280027 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC280034 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC280046 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC280056 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC280067 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC276841 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC276204 | Policy violation | SS-CO-BPC-CU-Sin recepción Logs de tráfico Firewall Palo Alto | Verdadero-Positivo sin afectación | Cerrado |
| INC273632 | Policy violation | SS-CO-BPC-CU-Login VPN fuera de Colombia | Verdadero-Positivo sin afectación | Cerrado |
| INC279775 | Policy violation | SS-CO-BPC-CU-Conexiones sospechosas permitidas hacia TS SWIFT Producción | Verdadero-Positivo sin afectación | Cerrado |
| INC270877 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado | Verdadero-Positivo sin afectación | Cerrado |
| INC276215 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado | Verdadero-Positivo sin afectación | Cerrado |
| INC280060 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado |  | Pendiente Cliente |
| INC280158 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado |  | Pendiente Cliente |
| INC276142 | Policy violation | SS-CO-BPC-CU-Acceso FHO No Autorizado | Verdadero-Positivo sin afectación | Cerrado |
| INC278563 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC278314 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC270900 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC275179 | Policy violation | SS-CO-BPC-CU-Sin Recepción de logs iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276341 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC275859 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC276657 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC286026 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284106 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC281514 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal |  | Abierto |
| INC283145 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC283424 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC285447 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC283549 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC279043 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC276308 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC275729 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC279163 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284051 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen |  | Pendiente Cliente |
| INC281098 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen |  | Pendiente Cliente |
| INC282838 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen |  | Pendiente Cliente |
| INC276385 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC278988 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC279865 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC276265 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271583 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271854 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271860 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276628 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC284304 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC277536 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279173 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279852 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276005 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271846 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283087 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS |  | Pendiente Cliente |
| INC285653 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC286790 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC275971 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC277036 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC273082 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC274590 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC273678 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC274846 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC274232 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC273675 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC277052 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC274850 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274857 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274594 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274600 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274604 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273685 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273687 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274239 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274246 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273090 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273095 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270894 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270898 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271134 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271135 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC277016 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278132 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278133 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278655 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC277488 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278558 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274632 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273670 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC274226 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC277046 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC272925 | Policy violation | SS-CO-BPC-CU- Login Kerberos Multiples Workstation - Exabeam | Verdadero-Positivo sin afectación | Cerrado |
| INC273548 | Policy violation | SS-CO-BPC-CU- Login Kerberos Multiples Workstation - Exabeam | Verdadero-Positivo sin afectación | Cerrado |
| INC274177 | Policy violation | SS-CO-BPC-CU-Login exitosos Fuera Horario Laboral en Linux | Verdadero-Positivo sin afectación | Cerrado |
| INC274214 | Policy violation | SS-CO-BPC-CU-Login exitosos Fuera Horario Laboral en Linux | Verdadero-Positivo sin afectación | Cerrado |
| INC284598 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC283851 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC283857 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC283906 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286245 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286246 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286251 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285004 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Abierto |
| INC285005 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285124 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284501 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC281066 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC274219 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC279623 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC274172 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC272818 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC272987 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC281043 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC283231 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC279611 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC279616 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC283728 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen |  | Pendiente Cliente |
| INC271655 | Policy violation | SS-CO-BPC-CU-Conexión hacia tele-conferencia desde contabilidad | Verdadero-Positivo sin afectación | Cerrado |
| INC273569 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS | Verdadero-Positivo sin afectación | Cerrado |
| INC272210 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS | Verdadero-Positivo sin afectación | Cerrado |
| INC284582 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC286257 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC283253 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC281433 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC279571 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC282535 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC281540 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC280187 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC279629 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC273629 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC281594 | Policy violation | SS-CO-BPC-CU-Conexiones Sospechosas desde StpLink Producción SWIFT | Verdadero-Positivo sin afectación | Cerrado |
| INC279502 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC279533 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC276804 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC276808 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC276822 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC283847 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC277409 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC278055 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC272407 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC275504 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC276160 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC272344 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC274160 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC278057 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278116 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276832 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276853 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279481 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279696 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281528 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282527 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283153 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283167 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283245 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC280171 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273623 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275519 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275521 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276168 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271587 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271665 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270835 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270837 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272280 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272290 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272355 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273042 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281642 | Policy violation | SS-CO-BPC-CU-Conexiones Sospechosas desde StpLink Producción SWIFT | Verdadero-Positivo sin afectación | Cerrado |
| INC279780 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC279650 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC279302 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries |  | Pendiente Cliente |
| INC277972 | Policy violation | SS-CO-BPC-CU-Transacción por VPN SWIFT fuera de horario de oficina | Verdadero-Positivo sin afectación | Cerrado |
| INC277975 | Policy violation | SS-CO-BPC-CU-Transacción por VPN SWIFT fuera de horario de oficina |  | Pendiente Cliente |
| INC277984 | Policy violation | SS-CO-BPC-CU-Transacción por VPN SWIFT fuera de horario de oficina |  | Pendiente Cliente |
| INC286371 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286377 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286415 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285416 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284786 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284840 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Pendiente Cliente |
| INC272459 | Policy violation | SS-CO-BPC-CU-Login exitosos Fuera Horario Laboral en Linux | Verdadero-Positivo sin afectación | Cerrado |
| INC284907 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC273980 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC284831 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC286581 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC277273 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC278383 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC273838 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC282559 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC279276 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC286608 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284698 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284798 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC283522 | Policy violation | SS-CO-BPC-CU-Conexión hacia tele-conferencia desde contabilidad | Verdadero-Positivo sin afectación | Pendiente Cliente |
| INC276601 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS |  | Pendiente Cliente |
| INC276542 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen | Verdadero-Positivo sin afectación | Pendiente Cliente |
| INC275914 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen | Verdadero-Positivo sin afectación | Cerrado |
| INC277289 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC277335 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC277935 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278425 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278683 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282560 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282594 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282613 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279362 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281385 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281416 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283309 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283316 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283346 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282344 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282364 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282013 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282041 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273193 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272466 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272467 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270969 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270970 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270742 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC270743 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271744 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271745 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271182 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271184 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274420 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273198 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273340 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274651 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274652 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273497 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273508 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273768 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273773 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274727 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC273996 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274062 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279859 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC282836 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC282114 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC283152 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282766 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276261 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274066 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274309 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276963 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC279847 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC271514 | Policy violation | SS-CO-BPC-CU-Conexión Saliente Maliciosa categoría Firewall | Verdadero-Positivo sin afectación | Cerrado |
| INC276929 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC282138 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284102 | Policy violation | SS-CO-BPC-CU-Login VPN desde diferentes IP origen |  | Pendiente Cliente |
| INC279002 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC285341 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC285446 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC286681 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC276399 | Policy violation | SS-CO-BPC-CU-Acceso a servicios criticos por VPN | Verdadero-Positivo sin afectación | Cerrado |
| INC283716 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279020 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC273415 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276003 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC275779 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC279821 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC277696 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC282972 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC275892 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC275807 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC272004 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC271484 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC271584 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC286887 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries |  | Pendiente Cliente |
| INC286851 | Policy violation | SS-CO-BPC-CU-Conexiones sospechosas permitidas hacia TS SWIFT Producción | Verdadero-Positivo sin afectación | Cerrado |
| INC279793 | Policy violation | SS-CO-BPC-CU-Conexión SSH por puerto no estándar | Verdadero-Positivo sin afectación | Cerrado |
| INC281234 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC281240 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS |  | Pendiente Cliente |
| INC281878 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS |  | Pendiente Cliente |
| INC286544 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286546 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286557 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285883 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285886 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285895 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285241 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285279 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285309 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284651 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284687 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC281284 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281887 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281892 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281214 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282254 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282275 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC284628 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC280630 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC280635 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC280646 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC280661 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC281093 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC279916 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC279105 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC281927 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC285256 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC283981 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC283987 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC284012 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC280507 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279952 | Policy violation | SS-CO-BPC-CU- Login Kerberos Multiples Workstation - Exabeam | Verdadero-Positivo sin afectación | Cerrado |
| INC280642 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries |  | Pendiente Cliente |
| INC272755 | Policy violation | SS-CO-BPC-CU-Acciones usuarios privilegiados en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276715 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276717 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276589 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC272522 | Policy violation | SS-CO-BPC-CU-Login exitosos Fuera Horario Laboral en Linux | Verdadero-Positivo sin afectación | Cerrado |
| INC272682 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC272779 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276091 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276093 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC271994 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC276048 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Falso-Positivo | Cerrado |
| INC286210 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC272519 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC272673 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC287129 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC283401 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC286454 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC285795 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC278466 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC278761 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC279400 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC282399 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC280086 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC287089 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC286476 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC286186 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC286191 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286195 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286478 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286479 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC276121 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274757 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274759 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275338 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275344 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274493 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274499 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC274567 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272554 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272558 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC272663 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271922 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271043 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271046 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC284262 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC287094 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC287100 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC287118 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC280089 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282406 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282477 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC280723 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC283353 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC280149 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279403 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC279463 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278763 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278823 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278467 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC278526 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276692 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276708 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271820 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC276706 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284214 | Reconocimiento | SS-CO-BPC-CU-Escaneo Horizontal | Verdadero-Positivo sin afectación | Cerrado |
| INC283631 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC285948 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC281757 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC282773 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284040 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC284257 | Policy violation | SS-CO-BPC-CU-Login VPN con usuario no permitido | Verdadero-Positivo sin afectación | Cerrado |
| INC283795 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286720 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC285543 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC286012 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC275625 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275735 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275842 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC281468 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC282731 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC276923 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC271564 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275659 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275836 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC275909 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL | Verdadero-Positivo sin afectación | Cerrado |
| INC285551 | Policy violation | SS-CO-BPC-CU-Acceso Fallido SQL |  | Pendiente Cliente |
| INC280414 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC283618 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC284322 | Policy violation | SS-CO-BPC-CU-Acciones sobre comandos sensibles en iseries | Verdadero-Positivo sin afectación | Cerrado |
| INC271993 | Policy violation | SS-CO-BPC-CU-Acciones VPN cuenta Serial | Verdadero-Positivo sin afectación | Cerrado |
| INC283389 | Policy violation | SS-CO-BPC-CU-Acceso VPN FHO - TERCEROS |  | Pendiente Cliente |

1. **ESTADO DE LAS ALERTAS**

****

1. **ESTADO DEL ANALISIS DE LAS ALERTAS**

****

**CONCLUSIONES**

* Se observa que los componentes del SIEM se encuentran estables.
* Se observa los equipos Firewall estables durante el mes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 00 | ${Autor} | Supervisor CyberSOC | 23/02/2022 | Versión Inicial |