Guía de referencia de resolución de problemas de soluciones de amenazas avanzadas

Contenido

Introducción

En este documento se describen los enlaces de documentación de las soluciones de amenazas avanzadas (ATS) para productos como Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR) y Cisco SecureX.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El siguiente artículo es una guía de referencia para la configuración/resolución de problemas de productos de soluciones de amenazas avanzadas. Se puede hacer referencia a este artículo antes de iniciar Cisco TAC.

Enlaces de documentación de Cisco Secure Endpoint

Portales de productos	Artículos relacionados	Etiquetas
Nube pública Nube de Estados Unidos Nube de UE Nube APJC	Documentación general	Documentation
	Direcciones de servidor necesarias para un terminal seguro adecuado y operaciones de análisis de malware seguro	Configuration
	Directiva de soporte de conector de terminal seguro	Documentation
	Guía del usuario de Cisco Security Account	Documentation
	Configuración de la autenticación de dos factores en un terminal seguro	Configuration

	Metodología y prácticas recomendadas para la implementación de terminales seguros		Configuration
	Derecho para un terminal seguro		Configuration
	Activar el inicio de sesión seguro para cuentas de seguridad de Cisco		Configuration
	Correos electrónicos de notificación de terminales seguros		Configuration
	Configurar y administrar exclusiones en un terminal seguro	Video	Configuration
	Cambios en la lista de exclusión mantenida por Cisco para Secure Endpoint Console		Configuration
	Prácticas recomendadas para las exclusiones de terminales seguros		Configuration
	Configuración de una lista de detección personalizada sencilla en Secure Endpoint Portal		Configuration
	Secure Endpoint Console y el filtro visto por última vez		Troubleshooting
	Exportar listas de bloqueo de aplicaciones desde Secure Endpoint Portal con API		Configuration
	Cómo crear un flujo de eventos con API de terminales seguras		Configuration
	¿Cómo se envía un archivo en Secure Malware Analytics desde Secure Endpoint Portal?		Troubleshooting
	Inscripción y habilitación de la búsqueda avanzada orbital en la implementación de terminales seguros		Documentation
	Troubleshooting de fallas de actualización de definiciones TETRA		Troubleshooting
	Integración segura de terminales con Splunk		Configuration
	Configurar notificación de elementos emergentes en un terminal seguro		Configuration
	Solucionar problemas de eventos de análisis de archivos falsos positivos en un terminal seguro		Troubleshooting
	Terminal seguro - Los registros orbitales		Documentation

	se llenan de errores - CSCwh73163	
	Secure Endpoint on AWS Workspaces - Scripts de inicio y configuración para Golden Images	Configuration
	Información de instantánea de diagnóstico de terminal seguro	Configuration
	Revisar análisis de Windows de terminales seguros (CSE)	Documentation
Conector para Android	Obtener datos de solución de problemas en un dispositivo Android para un terminal seguro	Troubleshooting
	Compatibilidad con SO de conector de Android de terminal seguro	Documentation
Claridad de iOS	Compatibilidad con Cisco Security Connector para Apple iOS	Documentation
	Creación de informes de problemas/datos de diagnóstico desde el terminal seguro Cisco Security Connector	Troubleshooting
	¿Cómo se supervisa un dispositivo iOS para utilizarlo con Cisco Security Connector (CSC)?	Troubleshooting
Conector de Windows	Recopilación de datos de diagnóstico de un conector de terminal seguro que se ejecuta en Windows	Troubleshooting
	Compatibilidad con SO de conector de Windows de terminal seguro	Documentation
	Requisitos de reinicio de actualización de conector de Windows de terminal seguro	Documentation
	Anuncio de fin de soporte para las versiones de Secure Endpoint Connector	Documentation
	Anuncio de fin de soporte técnico para Windows XP, Windows Vista y Windows 2003 para Secure Endpoint Connector	Documentation
	Preguntas frecuentes para clientes existentes a fecha de 8 de enero de 2020 sobre nuevos paquetes de terminales	Documentation

	seguros		
	Configurar la directiva de Windows en un terminal seguro	Video	Configuration
	[External] - Instalador de switches de línea de comandos para conector de terminal seguro		Configuration
	Switches de línea de comandos de terminales seguros		Configuration
	Forzar Manualmente la Actualización de Definiciones de TETRA - Terminal Seguro	Video	Troubleshooting
	Pasos de configuración de Secure Endpoint Update Server		Configuration
	Cómo recopilar registros de ProcMon para solucionar problemas de Secure Endpoint al inicio		Troubleshooting
	Crear una lista de detección personalizada avanzada en Cisco Secure Endpoint		Troubleshooting
	Analice Secure Endpoint Diagnostic Bundle para una CPU alta		Troubleshooting
	Cómo desinstalar Secure Endpoint Windows Connector con modo seguro		Troubleshooting
	Procedimiento para desinstalar el conector de terminal seguro si se olvida la contraseña		Troubleshooting
	El proceso de Windows se inicia antes de Secure Endpoint Connector Solución alternativa: Secure Endpoint		Configuration
	Compatibilidad de Secure Endpoint Exploit Prevention Engine con EMET		Configuration
	Prevención de vulnerabilidades		Documentation
	Guía de Cisco Secure Endpoint sobre la persistencia de la identidad		Configuration
	Lista de certificados raíz necesarios para la instalación segura de terminales en Windows		Troubleshooting

	Códigos de salida del instalador del conector de Windows de terminal seguro		Documentation
	Solucionar problemas de protección de scripts en un terminal seguro		Troubleshooting
	Limitaciones del control de dispositivos en entornos VMWare		Troubleshooting
	Resolución de Problemas de Actualización de Definiciones TETRA con Error 3000		Troubleshooting
	Configurar detecciones personalizadas - Avanzado con ClamAV SIGTOOL.EXE en Windows		Configuration
	Solución de problemas de instalación del Asistente de instalación de red|Secure Client Full		Troubleshooting
Conector de Linux	Recopilación de datos de diagnóstico del conector de Linux de terminal seguro		Troubleshooting
	Compatibilidad con SO de conector de Linux de terminal seguro		Documentation
	Requisitos de reinicio para la actualización del conector de Secure Endpoint Linux		Documentation
	Instalación de Secure Endpoint Linux Connector	Video	Configuration
	Opciones de definición de virus Secure Endpoint ClamAV en Linux		Configuration
	CLI de Cisco Secure Endpoint para Mac/Linux		Configuration
	Errores del conector de Secure Endpoint Linux		Troubleshooting
	Guía básica de solución de problemas para Secure Endpoint Linux Connector		Troubleshooting
	Secure Endpoint Linux Primer		Documentation
	Conector de Linux de terminal seguro en Ubuntu		Configuration
	Asesor para Secure Endpoint Linux Connector 1.15.0 en Ubuntu 20.04.0 LTS y Ubuntu 20.04.1 LTS		Documentation

	Falla de Linux Kernel-Devel	Troubleshooting
	Compatibilidad a largo plazo con conector de Linux de terminal seguro	Documentation
	Troubleshooting de Secure Endpoint Linux Connector Fault 18	Troubleshooting
Conector Mac	Secure Endpoint Connector para Mac Diagnostic Data Collection	Troubleshooting
	Compatibilidad con SO de conector de Mac de terminal seguro	Documentation
	Analice macOS Secure Endpoint Diagnostic Bundle para una CPU alta	Troubleshooting
	Exclusiones de procesos de terminales seguros en macOS y Linux	Configuration
	Guía de ajuste del rendimiento del conector Mac de terminal seguro	Troubleshooting
	Acceso al núcleo MAC y al disco completo en la consola: terminal seguro	Troubleshooting
	Procedimiento de desinstalación manual para el conector Mac de terminal seguro	Configuration
	Asesor para Secure Endpoint Mac Connector 1.14 en macOS 11 (Big Sur), macOS 10.15 (Catalina) y macOS 10.14 (Mojave)	Configuration
	Fallos del conector Mac de terminal seguro	Troubleshooting
Nube privada	Documentación general	Documentation
	Política de compatibilidad con la nube privada de terminales seguros	Documentation
	Instalación y configuración de la nube privada virtual de terminal seguro	Documentation
	Volver a crear una imagen del terminal seguro de la nube privada PC3000 y restaurar la copia de seguridad	Configuration
	Generar y agregar certificados necesarios para la instalación de Secure Endpoint Private Cloud 3.x en adelante	Configuration

	Procedimiento de actualización para AirGapped Secure Endpoint Private Cloud (virtual y dispositivo)	Configuration
	Generar instantánea de compatibilidad con la nube privada de terminal seguro y habilitar la sesión de asistencia en directo	Troubleshooting
	Acceso a la CLI de Secure Endpoint Private Cloud mediante SSH y transferencia de archivos mediante SCP	Configuration
	Procedimiento de actualización de Secure Endpoint Private Cloud 3.0.1	Documentation
	Actualización a Secure Endpoint Private Cloud 3.1.1: espacio en disco y memoria adicionales	Documentation
	Anuncio de EOS para las versiones de Secure Endpoint Private Cloud	Documentation
Eficacia/remediación/conformidad	Brotes/infecciones (respuesta ante incidentes)	Documentation

Dispositivo de análisis de malware seguro de Cisco

Portales de productos	Artículos relacionados	Etiquetas
Dispositivo de análisis de malware seguro de Cisco	Guías de Configuración	Documentation
	Guías de instalación y actualización	Documentation
	Versión del sistema de Secure Malware Analytics Appliance	Documentation
	Anuncio de fin de venta y fin del ciclo de vida	Documentation
	Configuración de Secure Malware Analytics Appliance para operaciones de clúster	Configuration
	Genere una instantánea de soporte de Secure Malware Analytics y habilite la sesión de soporte en directo	Troubleshooting
	Configuración del cliente SSH para Cisco Secure Malware Analytics Appliance	Configuration

	Actualizar el modo Air-Gap de Secure Malware Analytics Appliance	Configuration
	Genere una instantánea de soporte de Secure Malware Analytics y habilite la sesión de soporte en directo	Configuration
	Configuración de Secure Malware Analytics Appliance con Prometheus Monitoring Software	Configuration
	Cómo iniciar Secure Malware Analytics Appliance en modo de recuperación con EFI Shell y agregar modo de recuperación a las opciones de arranque	Configuration
	Actualizar el modo Air-Gap de Secure Malware Analytics Appliance	Configuration
	Configuración de Secure Malware Analytics RADIUS sobre autenticación DTLS para la consola y el portal OPadmin	Configuration
	Configurar integraciones de terceros de Secure Malware Analytics Appliance	Configuration
	Resolución de problemas de muestras y dispositivos no presentes en el panel de Secure Malware Analytics Appliance	Configuration
	Resolución de problemas de integración de Secure Malware Analytics Appliance con FMC	Configuration
	Lista de reproducción de vídeo de Secure Malware Analytics	Video

Cisco SecureX

Portales de productos	Artículos relacionados	Etiquetas
Cisco SecureX Nube de Estados Unidos Nube de UE Nube APJC	Guías de Configuración	Documentation
	Guía de referencia de SecureX	Configuration
	Blogs de SecureX	Documentation
	Preguntas frecuentes sobre SecureX	Documentation

Biblioteca a demanda de Cisco Live

		Video
	Lista de reproducción de vídeo de Cisco SecureX	Video
Respuesta ante amenazas de SecureX [anteriormente Cisco Threat Response (CTR)] Nube de Estados Unidos Nube de UE Nube APJC	Integre CTR y Secure Malware Analytics	Configuration
	Integre Cisco Threat Response y Firepower	Configuration
	Resolución de problemas en la integración de FMC y CTR	Configuration
	Integración de Cisco Threat Response (CTR) y ESA — Video	Configuration
	ESA: Reputación y análisis de archivos	Configuration
	Integración de WSA con CTR	Configuration
	Preguntas frecuentes de CTR	Configuration
	Tutoriales de configuración de Cisco Threat Response	Configuration
	Lista de reproducción de vídeo de Cisco Threat Response	Video
SecureX Orchestrator Nube de Estados Unidos Nube de UE Nube APJC	Tutorial de SecureX Orchestration	Documentation
	Reflexiones sobre automatizaciones - Comunidad de Cisco	Configuration Troubleshooting
	ActionOrchestratorContent - Github	Documentation

Artículos relacionados con integraciones

Portales de productos	Artículos relacionados	Etiquetas
Cisco Secure Endpoint Nube de Estados Unidos Nube de UE Nube APJC	Integración de un terminal seguro con FMC	Configuration
	Instalación y configuración del módulo AMP mediante AnyConnect 4.x y el habilitador AMP	Configuration
	ESA/CES: procedimiento para registrar dispositivos agrupados en clúster en un terminal seguro	Configuration
	Integre terminales seguros y análisis de malware seguro con WSA	Configuration
Cisco Secure Malware Analytics Nube de Estados Unidos Nube de UE	Integración de análisis de malware seguro y global	Configuration
	ID de cliente de análisis de archivos en dispositivos de seguridad de contenido (ESA, SMA, WSA) y DC/FMC	Troubleshooting
Cognitive Threat Analytics / Alertas de amenazas globales (CTA)	Demostración de CTA con terminal seguro	Configuration
	Preguntas frecuentes sobre el fin de servicio de Secure Endpoint Global Threat Alerts (GTA)	Documentation

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).