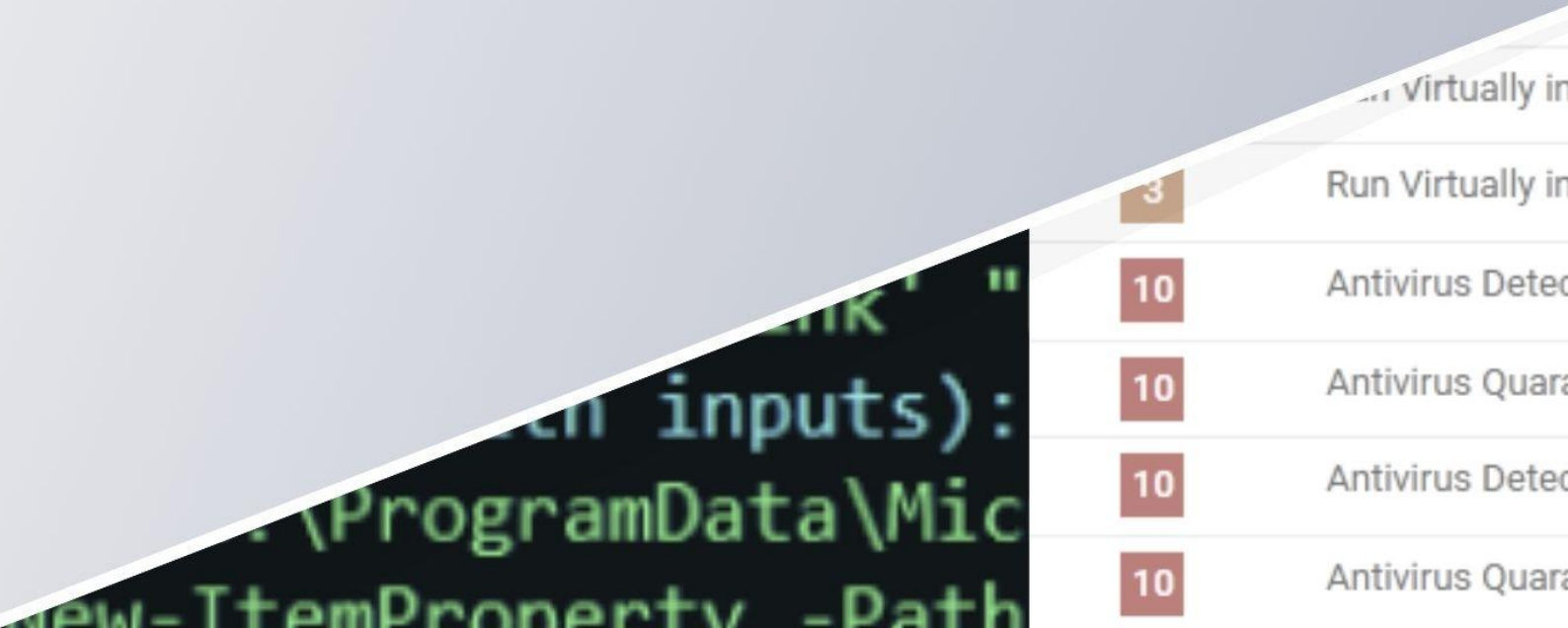
Crea un SOC GRATUITO

Ejecuta tácticas y técnicas de MITRE ATT&CK™

ATOMIC RED TEAM y OPEN EDR

OPEN EDR x



Contenido

Guía Paso a Paso para Configurar y Probar OpenEDR

Objetivo

El objetivo de esta guía es enseñar a los usuarios a instalar y configurar **OpenEDR** en una red de sistemas, realizando pruebas de seguridad utilizando técnicas del marco MITRE ATT&CK™ para validar la efectividad de la solución.

Paso 1: Registro y Creación de Cuenta en OpenEDR

1. **Acceder al Portal de OpenEDR**:
   - Dirígete al siguiente enlace para registrar tu cuenta: https://www.xcitium.com/free-edr/.
   - Haz clic en el botón **"GET STARTED"**.
2. **Registro de Cuenta**:
   - Rellena el formulario con los datos requeridos para crear una cuenta.
   - Una vez registrado, verás una página que te pedirá que omitas algunos pasos. Haz clic en **"Skip"**.
3. **Acceso a la Consola en la Nube**:
   - Después de completar el registro, recibirás un enlace de descarga para el agente de **Windows**. Copia ese enlace.
   - Haz clic en **"Download Windows Installer"** para descargar el instalador del agente **Windows**.

Paso 2: Instalación del Agente en Windows

1. **Descargar el Agente en PC01**:
   - En la máquina **PC01**, abre un navegador web e ingresa la URL proporcionada por OpenEDR para descargar el instalador del agente **Windows**.
2. **Ejecutar el Instalador**:
   - Una vez descargado el archivo, ejecuta el instalador de **OpenEDR** en **PC01**.
   - Durante la instalación, verás un icono verde en la bandeja de sistema, lo que indica que el agente está funcionando correctamente.
3. **Verificar el Agente en la Consola**:
   - Accede a la consola en la nube de OpenEDR y verifica que el equipo **PC01** esté correctamente enrolado en la sección **Endpoints**.

Paso 3: Instalación de Paquetes Adicionales en la Consola

1. **Acceder a la Consola**:
   - En la consola de OpenEDR, navega a la sección **"Endpoint"**.
2. **Instalar el Paquete EDR**:
   - En **"Total Devices"**, selecciona **PC01**.
   - Haz clic en **"Install or Manage Packages"**.
   - Marca la opción **"Install Xcitium Client - EDR"** y haz clic en **"Install"**.
3. **Reiniciar el Equipo**:
   - Después de la instalación, asegúrate de que el equipo se reinicie, lo cual puede hacerse de manera automática o manual.

4. **Verificar la Activación del EDR**:
    - Vuelve a la consola y ve a **"Total Devices"**.
    - Verifica que en la columna **"ACTIVE COMPONENTS"**, el agente **EDR** esté activo.

Paso 4: Habilitar la Ejecución de Scripts PowerShell

1. **Abrir PowerShell como Administrador**:
    - En **PC01**, abre **PowerShell** como administrador.
2. **Ejecutar el Comando**:
    - En PowerShell, ejecuta el siguiente comando para habilitar la ejecución de scripts no firmados:

      powershell
      Set-ExecutionPolicy Unrestricted

Paso 5: Verificar Alertas en OpenEDR

1. **Acceder a las Alertas**:
    - Ve a la consola de **OpenEDR** y navega a la pestaña **Security > EndPoint Zero Trust (EPP + EDR + ZD)**.
    - Haz clic en **Alerts** para ver las alertas generadas.
2. **Revisar las Alertas de EDR**:
    - En la lista de alertas, deberías ver una alerta correspondiente a la ejecución de PowerShell. Esta alerta será detectada por el **EDR**.

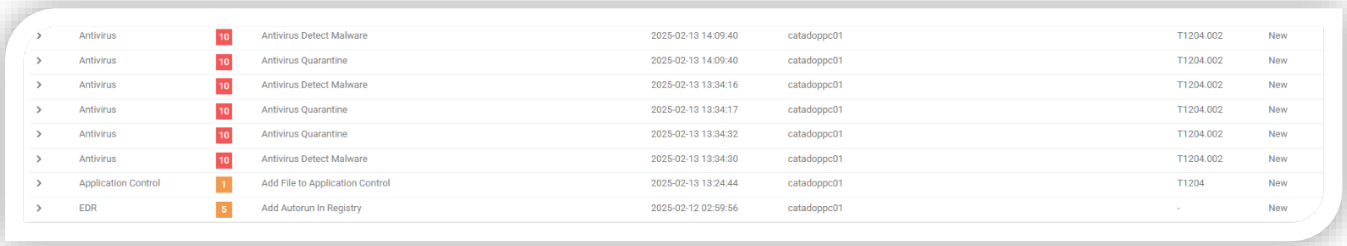
Paso 6: Ejecutar un Test de Seguridad con MITRE ATT&CK™

1. **Descargar el Framework Invoke-AtomicRedTeam**:
    - Abre **PowerShell** en **PC01** y ejecuta el siguiente comando para descargar el framework de **Red Canary**:
2. https://github.com/redcanaryco/atomic-red-team (tenéis tutoriales en youtube para su instalación)
3. **Verificar el Comportamiento en la Consola**:
    - Durante la ejecución del framework, la consola de **OpenEDR** debería empezar a registrar alertas relacionadas con las técnicas del MITRE ATT&CK™.

IMPORTANTE

*En el OPEN EDR, se deberá de crear una política en la cual notifiquen los ataques que se realizaran con **Atomic**. Ya que por su defecto, no las reconoce.*

- Las alertas mostrarán el **Mitre ID** correspondiente, como **T1204 ("User Execution")**, para cada técnica de ataque que se esté simulando.

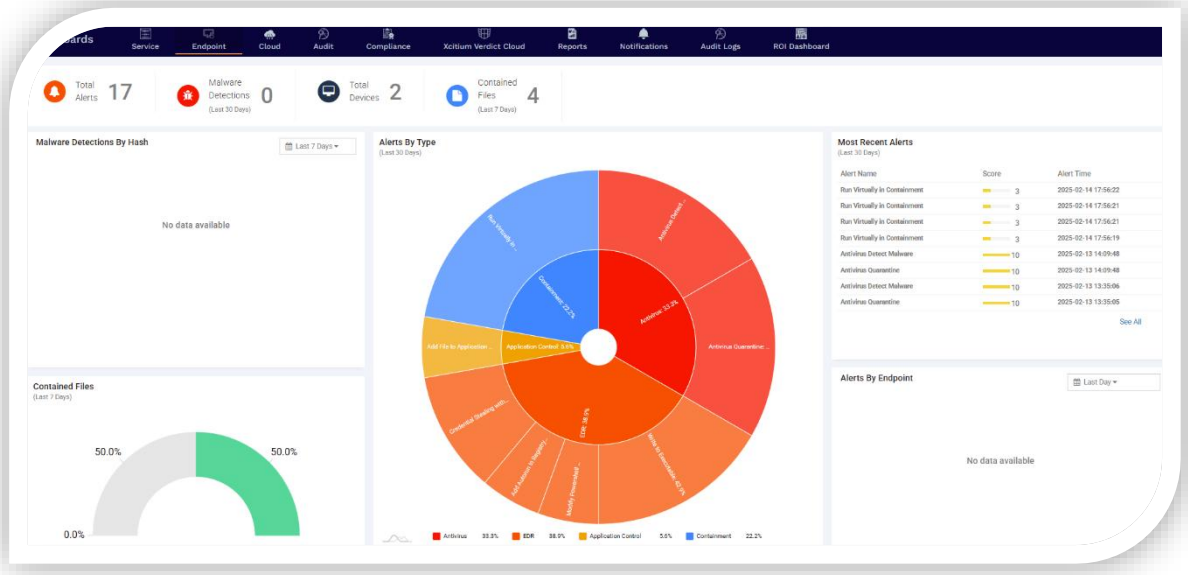


Antivirus	10	Antivirus Detect Malware	2025-02-13 14:09:40	catadoppc01		T1204.002	New
Antivirus	10	Antivirus Quarantine	2025-02-13 14:09:40	catadoppc01		T1204.002	New
Antivirus	10	Antivirus Detect Malware	2025-02-13 13:34:16	catadoppc01		T1204.002	New
Antivirus	10	Antivirus Quarantine	2025-02-13 13:34:17	catadoppc01		T1204.002	New
Antivirus	10	Antivirus Quarantine	2025-02-13 13:34:32	catadoppc01		T1204.002	New
Antivirus	10	Antivirus Detect Malware	2025-02-13 13:34:30	catadoppc01		T1204.002	New
Application Control	1	Add File to Application Control	2025-02-13 13:24:44	catadoppc01		T1204	New
EDR	5	Add Autorun In Registry	2025-02-12 02:59:56	catadoppc01		-	New

Paso 7: Análisis de las Alertas Generadas

1. **Revisar las Alertas en la Consola de OpenEDR**:
    - Vuelve a la consola de **OpenEDR** y verifica las alertas generadas en **Alerts**.
    - Para cada alerta, verifica que el **Mitre ID** corresponda a la técnica de MITRE ATT&CK™ que se ha ejecutado en **PC01**.
2. **Confirmar la Detección y Respuesta**:
    - Observa que las alertas estén correctamente identificadas por **OpenEDR** y que la respuesta haya sido la correcta, como el aislamiento de dispositivos o la detención de la ejecución de scripts maliciosos.

Como resultado debemos de ver lo siguiente:



Con esto podemos realizar pruebas y ver como se notifica en nuestro EDR.

Así mismo, realizar falsos positivos y ver cómo se comportan y cómo podemos analizarlos.