Deloitte.

Febrero 2024

HackOn 2024

De la Proactividad a la Prevención: Explorando Threat Hunting y MDR

Agenda

1 **Introducción**
Ponentes

2 **Managed Detection and Response**
Modelo, herramientas, métricas

3 **Threat Hunting**
Modelo, sinergias

4 **Laboratorio**

5 **Comienza tu carrera**

Introducción

Ponentes

Sergio Rubia Martínez

- Ingeniero industrial, especializado en mecánica.
- Threat Hunter con experiencia en Respuesta ante Incidentes en Deloitte CyberSOC.

Gonzalo Frontela Hernández

- Ingeniero de telecomunicaciones, especializado en telemática.
- Analista de Nivel 3 en el equipo de MDR de Deloitte CyberSOC.

Servicio MDR

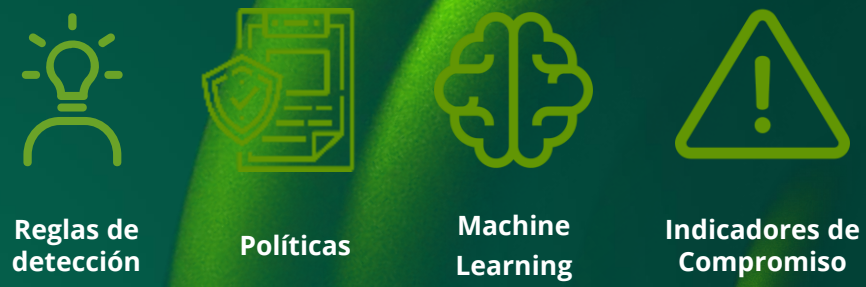
MDR (Managed Detection and Response)

Descripción del modelo

Enfoque Preventivo y Reactivo

Basa su planteamiento en:

- Detección y bloqueo de amenazas.
- Respuesta tras las alertas cuando algo no ha sido bloqueado.



 |

MDR (Managed Detection and Response)

Herramientas

Antivirus (AV)

Se basa en detectar firmas conocidas por su base de datos y políticas concretas.

EDR (Endpoint Detection and Response)

Antivirus de última generación, ofrece motores de detección de anomalías además de las capacidades de un AV tradicional. También da capacidades de respuesta sobre los agentes.

XDR (eXtended Detection and Response)

Permite ingestar logs de distintas fuentes en una misma plataforma ofreciendo motores de detección de anomalías mediante correlación cruzada, además de las capacidades de los EDR.

NDR (Network Detection and Response)

Ofrecen motores de detección de anomalías sobre los eventos de red, sin importar que vengan de máquinas monitorizadas o de cualquier otro elemento de la red.

ANTIVIRUS (AV)	EDR	XDR MINISTRY OF SECURITY
Focus Detects and removes known malware like viruses, worms, and Trojans.	**Focus** Monitors and responds to advanced threats on individual devices (endpoints).	**Focus** Provides cross-platform, holistic threat detection and response.
Method Uses signature-based detection to identify known threats.	**Method** Behavioral analysis, threat hunting, and real-time monitoring.	**Method** Integrates data from multiple security tools (e.g., AV, EDR, etc) to correlate and detect threats.
Purpose Provides baseline protection against common malware.	**Purpose** Offers enhanced security by identifying and mitigating unknown and targeted threats.	**Purpose** Offers comprehensive security by connecting the dots between different security layers.
Scope Focuses on detecting and blocking known malware and viruses.	**Scope** Monitors and responds to suspicious activities and threats on individual endpoints.	**Scope** Integrates data and threat intelligence from multiple security sources, covering a broader range of endpoints and networks.
Usage Traditional protection against common threats but may struggle with advancedor unknown attacks.	**Usage** Offers deeper visibility and control, ideal for threat hunting and investigating incidents.	**Usage** Provides a holistic, cross-environment view for threat detection, response, and better protection against complex attacks.

MDR (Managed Detection and Response)

Acciones de remediación

Escaneo de malware

Búsqueda de malware conocido y desconocido, este último mediante análisis estático y/o dinámico.

Aislamiento de equipos

Bloqueo de cualquier conexión de red de un equipo, excepto con la consola del EDR.

Eliminación de archivos

Se pueden configurar las políticas de modo que elimine los archivos que detecte como maliciosos.

Bloqueo de direcciones IP o Dominios

Bloqueo de conexiones a direcciones IP o dominios quese consideren anómalos o maliciosos, para prevenir conexiones C2 o phishing.

Detención de procesos

Monitoriza y detiene los procesos maliciosos/sospechosos para prevenir cualquier compromiso adicional.

Ejecución de scripts de remediación

Permiten ejecutar scripts sobre las máquinas para remediar el impacto causado por cualquier malware de manera rápida y efectiva.

La rapidez importa

MTTD vs MTTR

La rapidez importa

MTTR: Mean Time To React

Herramientas de Respuesta (EDR/XDR/NDR)

Estas herramientas permiten responder directamente ante las posibles detecciones del entorno.

Respuesta a Incidentes automática

Las soluciones SOAR (Security Orchestration, Automation, and Response) permiten automatizar flujos y tareas rutinarias, facilitando una respuesta mucho más rápida ante los tipos de incidentes más comunes.

Desarrollar y Documentar Protocolos de Respuesta

Se deben documentar planes de respuesta a incidentes para distintos tipos de amenazas. Estos deben contener los pasos específicos a seguir para contener, erradicar y recuperar.

Simulacros y Formaciones regulares

Realizar sesiones de formación habitualmente para que los analistas estén preparados para responder ante diferentes escenarios.

La rapidez importa

MTTD: Mean Time To Detect

Sistemas de detección avanzados (EDR/XDR/NDR)

Estas herramientas proveen de una muy buena capacidad de detección con un bajo tiempo medio para ello.

Threat Intelligence

Los Indicadores de Compromiso son muy volátiles, por eso es esencial tener buenas fuentes de inteligencia. Tener un equipo especializado y suscribirse a feeds e integrarlos en los protocolos de seguridad, permite estar al tanto de las últimas amenazas.

Monitorización Proactiva y Threat Hunting

Los EDR no detectan todo, por ello es muy importante tener una buena sinergia con un equipo de Threat Hunting, de cara a cubrir todos los ángulos y prevenir cualquier amenaza.

Concienciación y Formación en Ciberseguridad

Los usuarios son el principal vector de entrada de los ciberataques, por ello es muy importante que estén concienciados al respecto e informen de cualquier anomalía que detecten.

Servicio Threat Hunting

Threat Hunting

Descripción del modelo

Enfoque proactivo

Basa su planteamiento en la detección de amenazas mediante diferentes **modelos de Hunt**. Su objetivo es detectar comportamientos anómalos, no contemplados por las herramientas presentes.

Threat Hunting

Descripción del modelo

Tendencias de inteligencia

Relación con el equipo de CTI de Deloitte, en el que se realiza un estudio conjunto de las tendencias del mercado, en materia de malware, grupos de ransomware, APTs, vulnerabilidades activas, entre otras.

Amenazas desconocidas

Gracias al enfoque proactivo y ágil permite la extracción de TTPs asociadas a comportamiento sospechoso y vulnerabilidades que eluden los mecanismos más tradicionales. De este modo, se pueden detectar amenazas internas.

Mitigación y prevención

En base a las detecciones observadas y estudio realizado se proporcionan un listado de recomendaciones y medidas de mitigación acordes.

Soporte en incidentes

El equipo de Threat Hunting realiza acciones de búsqueda proactiva en incidentes, en el que presta soporte al equipo de Incident Response.

Sinergias TH y MDR

Generación de mecanismos de detección

De este estudio basado en hipótesis en las herramientas del cliente se proponen mecanismos de detección que los compañeros de MDR y TM, desplegarán en el

Alertas alta criticidad

En determinados casos de alertas de alta criticidad, nos alineamos con compañeros de MDR. En los que mediante la proporción de hipótesis previamente realizadas, podemos dar una respuesta más ágil a la alerta.

Estudio de actores de amenazas

Por otro lado, los compañeros de MDR proporcionan comportamientos para su estudio, a partir de cadenas de ejecución detectadas por el EDR, en los que la generación de una regla de detección no tiene cabida en un modelo de alertas, debido a su alta volumetría.

Laboratorio

 |

Laboratorio

Alerta vs Incidente

- Una alerta muestra una anomalía aislada.
- Un incidente nos cuenta “una historia”.

Selección de TTP: OS Credential Dumping: LSASS Memory (T1003.001)

- **Task Manager** realiza un dump del proceso lsass.exe (encargada de Servicio de Subsistema de Autoridad de Seguridad Local) (Alerta 114)
- **Procdump**, binario de la suite SysInternals (Alerta 115)
- Carga de DLL **comsvc.dll** por rundll32.exe renombrado. (Alerta 116)
- Carga de DLL **comsvc.dll** enmascarada

Laboratorio

Credential access

```
C:\Users\Administrator\Downloads\SysinternalsSuite>sigcheck.exe -accepteula C:\Users\Administrator\Downloads\testtt\pruebadll.dll

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\users\administrator\downloads\testtt\pruebadll.dll:
        Verified:       Signed
        Signing date:   10:37 PM 1/3/2024
        Publisher:      Microsoft Windows
        Company:        Microsoft Corporation
        Description:    COM+ Services
        Product:        Microsoft« Windows« Operating System
        Prod version:   10.0.20348.2110
        File version:   2001.12.10941.16384 (WinBuild.160101.0800)
        MachineType:    64-bit
```

```
PS C:\Windows\System32> .\rundll32.exe C:\Users\Administrator\Downloads\testtt\pruebadll.dll, MiniDump 816 C:\Temp
```

```
dataset = xdr_data
| filter event_sub_type = ENUM.LOAD_IMAGE_MODULE
| filter action_module_path contains "pruebadll.dll"
| fields action_module_path, actor_process_command_line, action_module_file_info
```

Query 1


```
{
  "company": "Microsoft Corporation",
  "description": "COM+ Services",
  "product_name": "Microsoft® Windows® Operating System",
  "product_version": "10.0.20348.2110",
  "file_version": "2001.12.10941.16384 (WinBuild.160101.0800)",
  "internal_name": "COMSVCS.DLL",
  "original_name": "COMSVCS.DLL",
  "legal_copyright": "© Microsoft Corporation. All rights reserved.",
  "entropy": "0.764279",
  "chisq_prob": "0.000000",
  "montepi_err": "0.134649"
}
```


```
dataset = xdr_data
| filter event_sub_type = ENUM.LOAD_IMAGE_MODULE
| alter action_module_internal_name = replace(json_extract(action_module_file_info,"$.internal_name"),"\"","")
| alter action_module_original_name = replace(json_extract(action_module_file_info,"$.original_name"),"\"","")
| filter action_module_internal_name = "COMSVCS.DLL" OR action_module_original_name = "COMSVCS.DLL"
| filter actor_process_command_line contains "MiniDump"
```

Query 2

 |

Comienza tu carrera

¿Te apuntas?

Make an Impact that matters

empleo.es.deloitte.com

Deloitte.

Muchas gracias.