<!--MITIC / CERT-PY-->

# Administración de Logs {

<Por="Marcos Centurion"/>

}

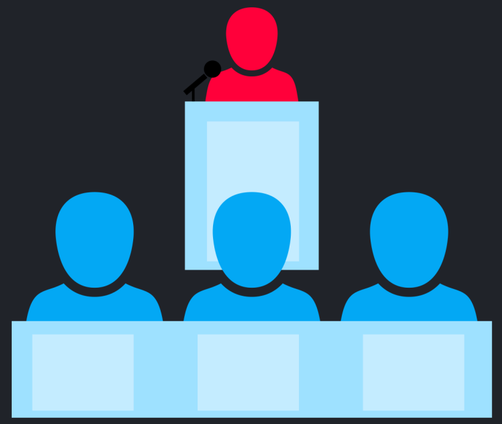
@LiquidIv4n

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY

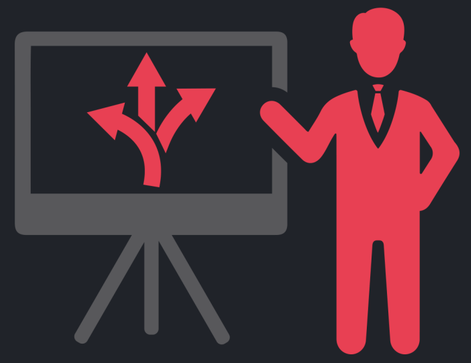
# Audiencia

Dirigido para el personal de seguridad informática y los administradores de programas; administradores de sistemas, redes y aplicaciones; equipos de respuesta a incidentes cibernéticos; y otros que sean responsables de realizar funciones relacionadas con la gestión de registros de sistemas Informáticos



# Contenidos

# Objetivos



## OBJETIVO GENERAL

RECONOCER COMO PROTEGERSE A SÍ MISMO Y A SU ORGANIZACIÓN A TRAVÉS DE LA RESPUESTA A INCIDENTES MEDIANTE LA ADMINISTRACIÓN Y EL ANÁLISIS DE REGISTROS

## OBJETIVOS ESPECÍFICOS

- DEFINIR LA GESTIÓN DE LOGS
- GUÍAS Y HERRAMIENTAS

# log

Un log es un registro de un evento que sucede dentro de los sistemas, dispositivos, redes de una organización

#Los registros se componen de:

- Identificadores
- Entradas de registro
- Información del evento
- Relacionado a un tipo de evento
- Motivo de creación o Disparador
- Origen - Destino del evento

# log

**Los registros/logs pueden contener una amplia variedad de información sobre los eventos que ocurren dentro de los sistemas y redes de la infraestruscta tecnológica:**

- Los registros relacionados a "**Software de Seguridad**" contienen principalmente información relacionada con la seguridad informática agrupados por lotes de activos o determinado conjunto de recursos de una organización.

- Los registros del "**Sistema Operativo**" y de "**Aplicación**" suelen contener una variedad de información, incluidos datos relacionados con la seguridad informática.

# Orígenes de los registros

### Software de Seguridad

### Sistema Operativo

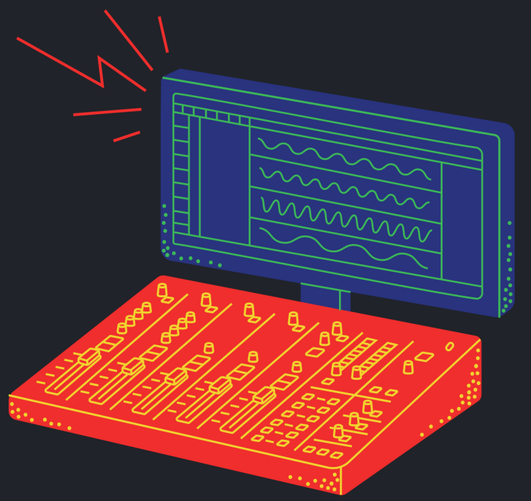
- Eventos del Sistema
- Registros de Auditoría

### Registros de Aplicación

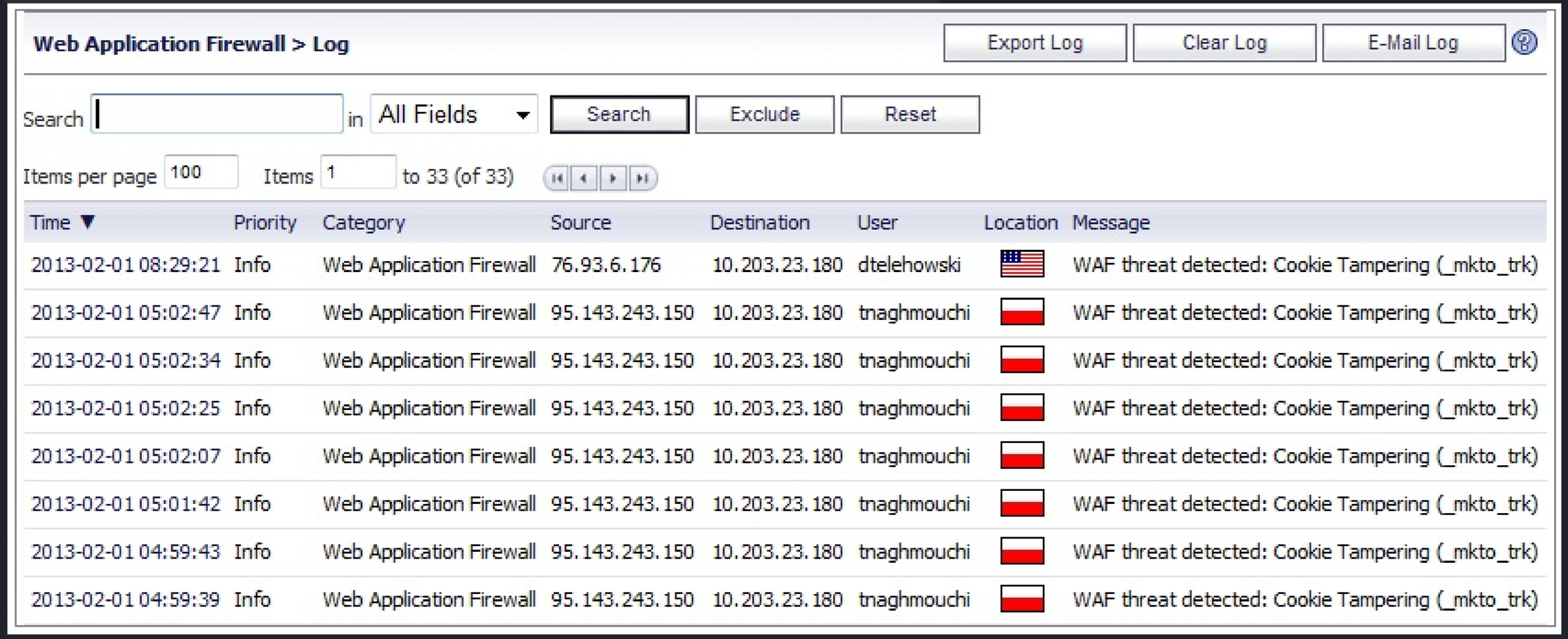
Solicitudes de cliente/servidor
Información de la cuenta
Información de uso
Acciones operativas significativas

Fuente / Orígen de registro:

- componente de software o hardware que genera datos de registro



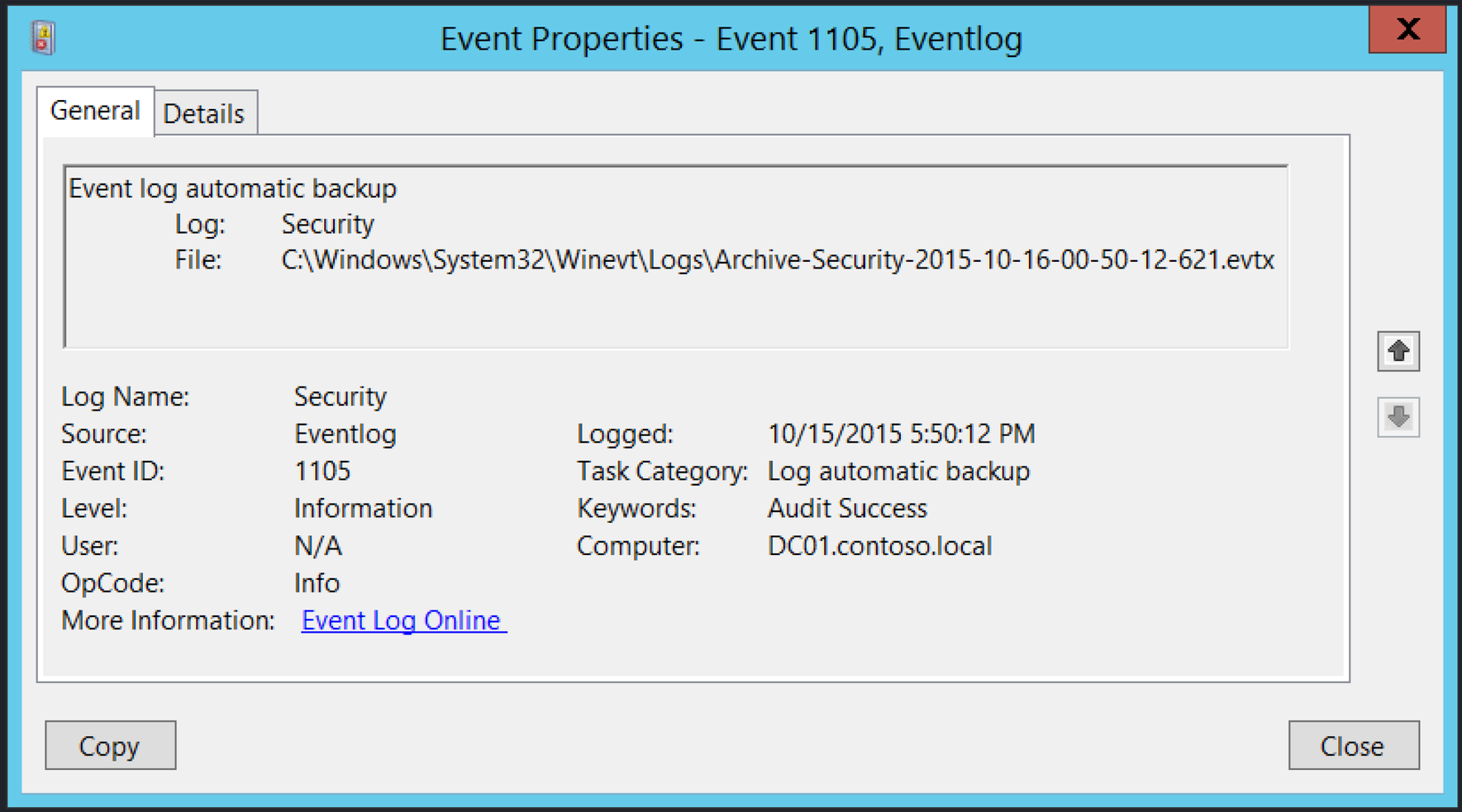
# log / Sofware de Seguridad




| Time ▼ | Priority | Category | Source | Destination | User | Location | Message |
|---|---|---|---|---|---|---|---|
| 2013-02-01 08:29:21 | Info | Web Application Firewall | 76.93.6.176 | 10.203.23.180 | dtelehowski | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 05:02:47 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 05:02:34 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 05:02:25 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 05:02:07 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 05:01:42 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 04:59:43 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |
| 2013-02-01 04:59:39 | Info | Web Application Firewall | 95.143.243.150 | 10.203.23.180 | tnaghmouchi | | WAF threat detected: Cookie Tampering (_mkto_trk) |

https://help.sonicwall.com/help/sw/eng/8112/8/0/0/content/WAF_Log.html

# log / Sistema Operativo - Evento de Sistema



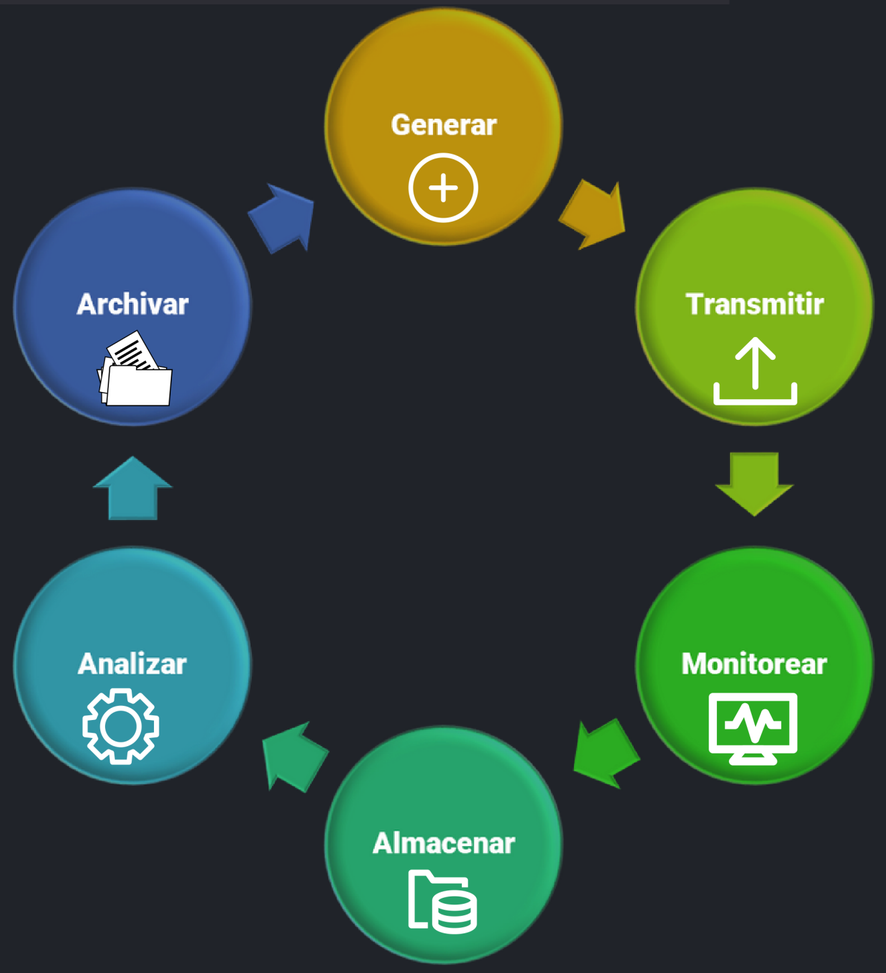

https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/event-1105

# log / Sistema Operativo - Servidor Web

```
254.32.63 - - [18/Aug/2016:08:38:00 -0400] "GET /blog HTTP/1.1" 301 5 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12.co.uk/bot.php?+)"
254.32.63 - - [18/Aug/2016:08:38:02 -0400] "GET /blog/ HTTP/1.1" 200 17013 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12.co.uk/bot.php?+)"
254.32.63 - - [18/Aug/2016:08:38:05 -0400] "GET /blog/feeds/atom/ HTTP/1.1" 200 81347 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12.co.uk/bot.p
+)"
249.79.144 - - [18/Aug/2016:08:45:45 -0400] "GET /blog/feeds/atom/ HTTP/1.1" 200 81347 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537
 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
.105.247.194 - - [18/Aug/2016:09:04:22 -0400] "GET / HTTP/1.1" 444 0 "-" "-"
.113.96.29 - - [18/Aug/2016:09:10:32 -0400] "GET /wp-login.php HTTP/1.1" 301 5 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1"
.113.96.29 - - [18/Aug/2016:09:10:32 -0400] "GET /wp-login.php/ HTTP/1.1" 404 6321 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1"
.211.62.84 - - [18/Aug/2016:09:51:11 -0400] "GET /blog/web-server-logs-seo-1/ HTTP/1.1" 200 5054 "-" "Mozilla/5.0 (compatible; +http://tweetedtimes.com)"
249.79.144 - - [18/Aug/2016:09:58:55 -0400] "GET /blog/ HTTP/1.1" 200 4627 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
.211.62.84 - - [18/Aug/2016:10:05:07 -0400] "GET /blog/feeds/rss/ HTTP/1.1" 200 81094 "-" "Mozilla/5.0 (compatible; +http://tweetedtimes.com)"
249.79.152 - - [18/Aug/2016:10:26:36 -0400] "GET /blog/http2-and-the-top-web-sites/ HTTP/1.1" 200 11761 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.goog
com/bot.html)"
172.183.60 - - [18/Aug/2016:10:56:06 -0400] "GET /blog/http2-and-the-top-web-sites/ HTTP/1.1" 200 11761 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:28.0) Ge
/20100101 Firefox/28.0 (FlipboardProxy/1.1; +http://flipboard.com/browserproxy)"
121.109.55 - - [18/Aug/2016:11:47:31 -0400] "GET /blog/fifty-shades-of-crawl/ HTTP/1.0" 200 15704 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12
.uk/bot.php?+)"
121.109.55 - - [18/Aug/2016:11:47:34 -0400] "GET /blog/http2-and-the-top-web-sites/ HTTP/1.0" 200 52543 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.maje
c12.co.uk/bot.php?+)"
249.79.152 - - [18/Aug/2016:13:01:54 -0400] "GET /blog/ HTTP/1.1" 200 4626 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
249.79.152 - - [18/Aug/2016:13:39:03 -0400] "GET /blog/http2-and-the-top-web-sites/ HTTP/1.1" 200 11761 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.goog
com/bot.html)"
197.202.83 - - [18/Aug/2016:13:53:24 -0400] "GET /blog/web-server-logs-seo-1/ HTTP/1.1" 200 5053 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:28.0) Gecko/201
01 Firefox/28.0 (FlipboardProxy/1.1; +http://flipboard.com/browserproxy)"
121.211.59 - - [18/Aug/2016:14:17:31 -0400] "GET /blog/feeds/rss/ HTTP/1.1" 200 81109 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12.co.uk/bot.p
+)"
121.211.59 - - [18/Aug/2016:14:17:33 -0400] "GET /blog/fifty-shades-of-crawl/ HTTP/1.1" 200 5680 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12.
uk/bot.php?+)"
121.211.59 - - [18/Aug/2016:14:17:35 -0400] "GET /contact/ HTTP/1.1" 200 2598 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.5; http://www.majestic12.co.uk/bot.php?+)"
```

https://www.searchdatalogy.com/blog/seo-web-server-log-files/

# Ciclo de vida del log

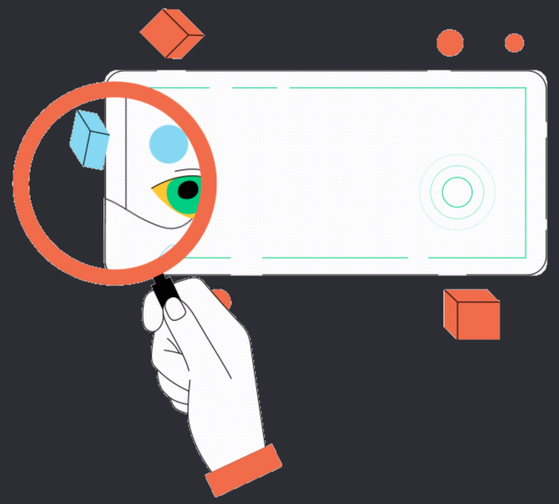



- Generar Logs
- Enviar/Transmitir
- Monitorear Logs
- Almacenar Logs
- Analizar Logs
- Archivar Logs

Adaptado de NIST SP 800-92

# Indicadores de Compromiso IoC

Un indicador de compromiso es una pista que se puede utilizar para indicar una intrusión o compromiso de un host en una red



#Un IoC pueden revelar

- Pista o artefacto forense
- TTP's
- Relevancia del incidente
- Path o ruta a mitigar
- Hashes

# Indicadores de Compromiso IoC

Los patrones y métodos de IoC se pueden usar para identificar a los atacantes, ya que cada grupo tiene un modus operandi que puede conducir a la atribución.

# ¿Por qué necesitamos gestionar los registros?

La gestión de registros de logs, beneficia a una organización de muchas maneras:

- Ayuda a garantizar la seguridad informática
- Análisis y revisiones de registros de rutina son vitales para identificar incidentes de seguridad, violaciones de políticas, actividades fraudulentas y problemas operativos
- Además de los beneficios inherentes de la gestión de registros, una serie de marcos de seguridad, obligan a las organizaciones a almacernar y revisar ciertos registros
- **Los registros también pueden ser útiles para realizar auditorías y análisis forenses**

# Los desafíos en la gestión de registros

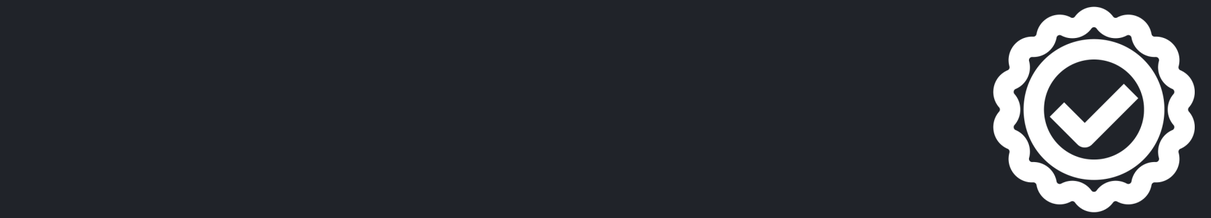
# Los desafíos en la gestión de registros

La mayoría de las organizaciones enfrentan desafíos similares relacionados con la administración de registros, que tienen el mismo problema subyacente: equilibrar efectivamente una cantidad limitada de recursos de administración de registros con un suministro cada vez mayor de datos de registro.

1. Problemas potenciales con la generación inicial de registros debido a su variedad y prevalencia
2. La confidencialidad, la integridad y la disponibilidad de los registros generados podrían violarse de manera inadvertida o intencional
3. Responsables de realizar el análisis de registros a menudo no cuentan con la preparación y el apoyo adecuados

# Prácticas recomendadas para enfrentar los principales desafíos en la gestión de registros

- Priorizar la gestión de registros de forma adecuada en toda la organización
- Establecer políticas y procedimientos para la gestión de registros.
- Crear y mantener una infraestructura de gestión de registros segura
- Proporcionar la formación adecuada a todo el personal con responsabilidades de gestión de registros.



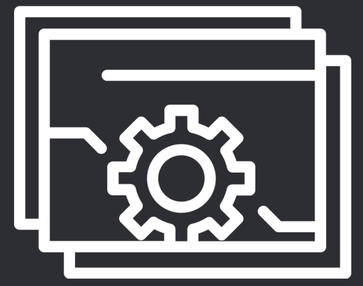
# Incidente

Incidente Cibernético de Seguridad ("Incidente"): es una violación o una amenaza inminente de violación a una política de seguridad de Ia información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad)/RESOLUCIÓN MITIC Nº 346-2020.pdf

Una ocurrencia que pone en peligro real o potencialmente la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite o que constituye una violación o amenaza inminente de violación de políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable/NIST (NIST SP 800-12 Rev. 1)

# Artefactos Sospechosos

## Artefactos Basados en Host



- Procesos corriendo
- Servicios en uso
- Hash de integridad de ejecutables en segundo plano
- Aplicaciones Instaladas
- Usuarios locales y de dominio
- Autenticaciones inusuales
- Nombres de usuario con formato no estándar
- Puertos de escucha y servicios asociados
- Configuración de resolución del sistema de nombres de dominio (DNS) y rutas estáticas
- Conexiones de red establecidas y recientes
- Ejecutar clave y otra persistencia de ejecución automática
- Tareas programadas
- Artefactos de ejecución (Prefetch y Shimcache)
- Registros de eventos
- Detecciones de antivirus

https://www.cisa.gov/uscert/ncas/alerts/aa20-245a

# Artefactos Sospechosos

## Información a revisar para el análisis del host

- Identifique cualquier proceso que no esté firmado y que se esté conectando a Internet
- Recopile todos los inicios de sesión de los usuarios y busque comportamientos atípicos
- Recopile todas las solicitudes de línea de comandos de PowerShell en busca de comandos codificados en Base64 para ayudar a identificar ataques maliciosos sin archivos.
- Busque procesos .RAR, 7zip o WinZip excesivos, especialmente con nombres de archivos sospechosos, para ayudar a descubrir la puesta en escena de exfiltración (los nombres de archivos sospechosos incluyen convenciones de nomenclatura como 1.zip, 2.zip, etc.).
- Archive el contenido de /var/log para todos los hosts.
- Archivo de salida de journald. Estos registros son prácticamente iguales a /var/log; sin embargo, proporcionan alguna verificación de integridad y no son tan fáciles de modificar.
- Módulos del kernel enumerados (lsmod) para detectar signos de un rootkit; La salida del comando dmesg puede mostrar signos de carga de rootkit y conexión del dispositivo, entre otras cosas.

https://www.cisa.gov/uscert/ncas/alerts/aa20-245a

# Artefactos Sospechosos

## Artefactos Basados en Red

- Tráfico y actividad de DNS anómalos, servidores de resolución de DNS inesperados, transferencias de zona DNS no autorizadas, exfiltración de datos a través de DNS y cambios en los archivos del host
- Protocolo de escritorio remoto (RDP), sesiones de red privada virtual (VPN), conexiones de terminal SSH y otras capacidades remotas para evaluar conexiones entrantes, herramientas de terceros no aprobadas, información de texto no cifrado y movimiento lateral no autorizado
- Protocolo de transferencia de hipertexto Capa de sockets seguros/seguros (HTTPS/SSL)
- Conexiones no autorizadas a indicadores de amenazas conocidas
- Telnet

https://www.cisa.gov/uscert/ncas/alerts/aa20-245a

# Artefactos Sospechosos

## Información a revisar para el análisis de red

- Busque nuevas conexiones en puertos no utilizados anteriormente
- Busque patrones de tráfico relacionados con el tiempo, la frecuencia y el recuento de bytes de las conexiones
- Conservar registros de proxy
- Deshabilite LLMNR en la red corporativa; si no se puede deshabilitar, recopile LLMNR (puerto UDP 5355) y NetBIOS-NS (puerto UDP 137)
- Revise los cambios en las tablas de enrutamiento, como la ponderación, las entradas estáticas, las puertas de enlace y las relaciones entre pares

https://www.cisa.gov/uscert/ncas/alerts/aa20-245a

# Herramientas para la gestión y el análisis de registros

01

## Scripts de Powershell

- Analizar a través de los registros
  - Get-WinEvent
  - Get-Eventlog
  - Search-UnifiedAuditlog

02

## Security Information and Event Management (SIEM)

- Sistema de Gestión Centralizado
  - Recolectar Logs
  - Normaliza(Parsear)
  - Correlación
  - Analiza
  - Priorización

03

## Full Packet Capture (FPCAP)

- Interceptar paquetes
  - Recolectar trazas de conexiones
  - examinar toda la conversación del paquete completo

04

## Bash Commands

Verificar archivos de logs en sistemas operativos Linux

# Herramientas para la gestión y el análisis de registros

01

## Scripts de Powershell

- **Get-EventLog Security | ?{$_.EventID -eq 4688} | Out-File C:\ ir_processcreated.txt**
- **Get-WinEvent -LogName 'Microsoft-Windows-PowerShell/Operational'**
- **Get-WinEvent -FilterHashtable @{LogName='system'} | Where-Object -FilterScript {($_.Level -eq 2) -or ($_.Level -eq 3)}**
- **Get-Process | Out-File c:\ ir_processes.txt**

https://4sysops.com/archives/search-the-event-log-with-the-get-winevent-powershell-cmdlet/

# Herramientas para la gestión y el análisis de registros

02

## Security Information and Event Management (SIEM)

- Sistema de Gestión Centralizado
  - ELK Stack & Security
  - WAZUH
  - Graylog
  - Beats & ELK

03

## Full Capture Packets (FPCAP)

- Interceptar paquetes
  - Packetbeat & ELK
  - Wireshark/TCPDUMP
  - PRTG

04

## Bash Commands

- less, more
- grep, zgrep
- find, locate, whereis
- last, w

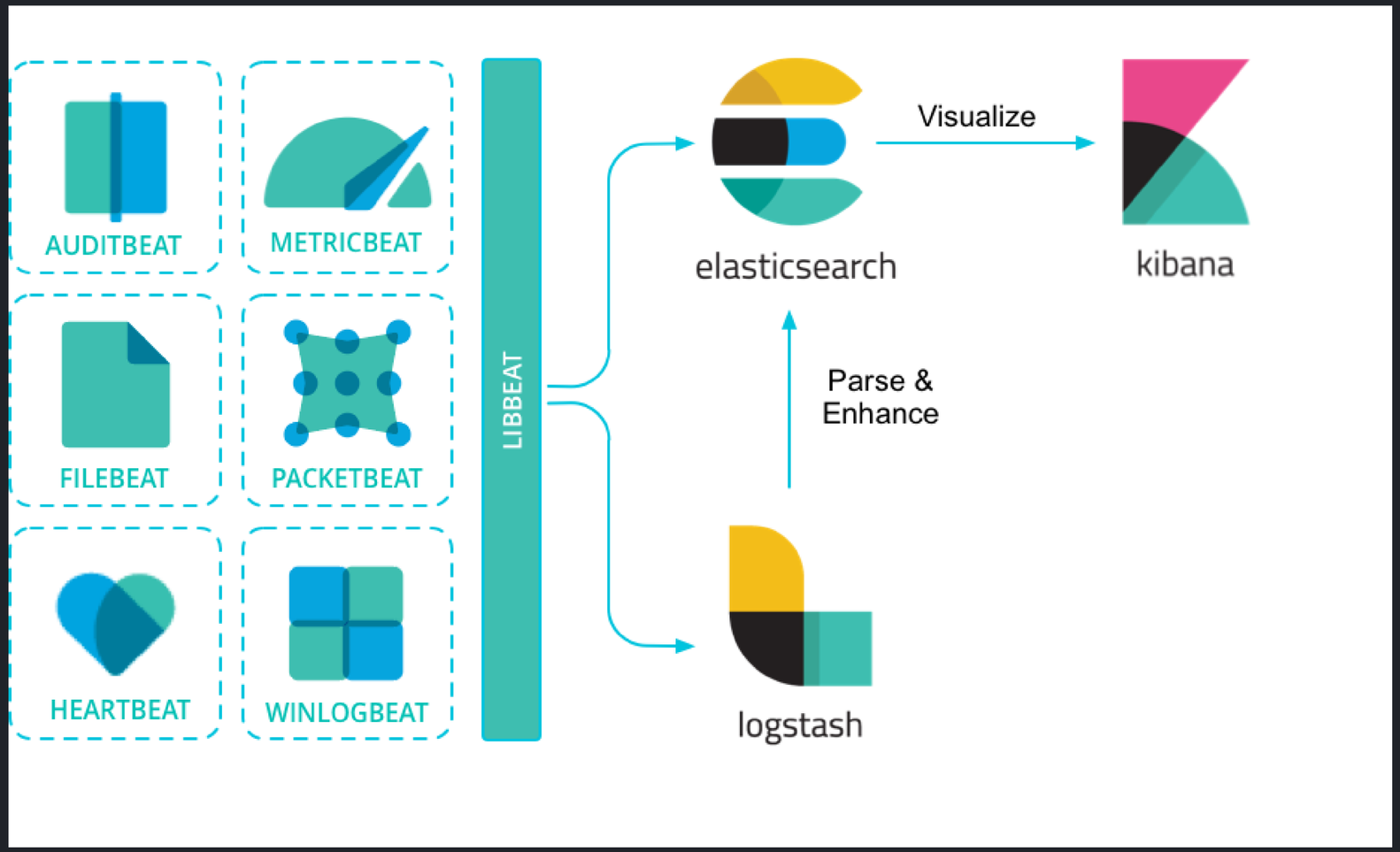
# Procesos operativos de gestión de registros

Los administradores de sistemas y de infraestructura deben seguir procesos estándar para administrar los registros de los que son responsables.

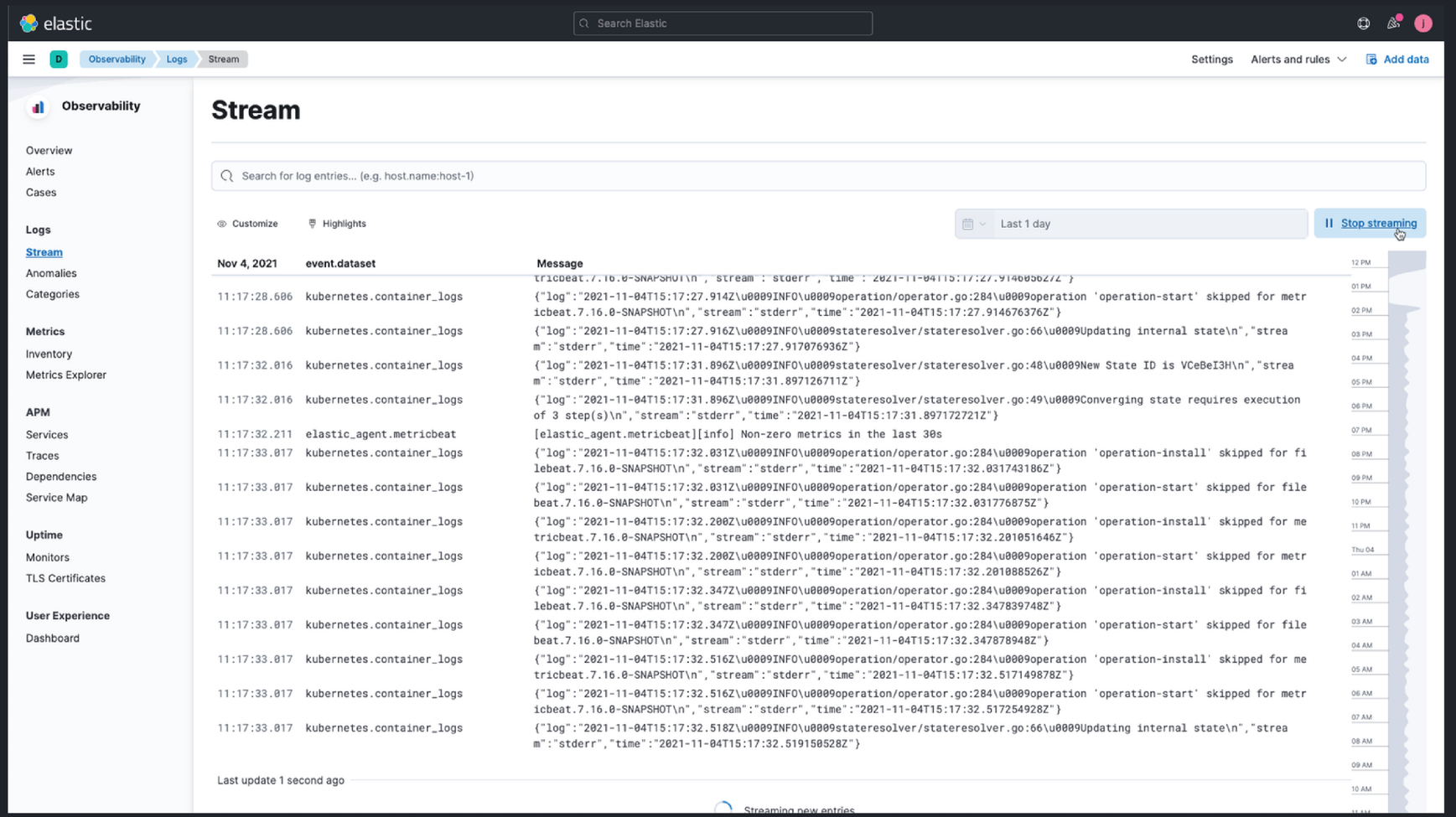
Los principales procesos operativos para la gestión de registros, que son los siguientes:

- Configure las fuentes de registro, incluida la generación de registros, el almacenamiento y la seguridad
- Realizar análisis de datos de registro
  - Comprender los registros(Necesidad de Contexto)
  - Priorización de registros
  - Comparar el análisis a nivel de sistema VS nivel Infraestructura
- Iniciar respuestas apropiadas a los eventos identificados
- Administre el almacenamiento a largo plazo de los datos de registro
- Proporcionar apoyo operativo
- Realizar pruebas y validaciones

# Centralizar Registros con herramientas Opensource



# Centralizar Registros con herramientas Opensource



# Casos de Estudio

1. Reportes públicos sobre Actores cibernéticos patrocinados por Estados Hostiles
2. Eventos Cibernéticos en Paraguay
    a. Sistemas Comprometidos
        i. Coincidencias

# Caso 1 - Actores Cibernéticos Patrocinados Explotan dispositivos de red vulnerables / CISA Alter (AA22-158A)

Actores cibernéticos, los cuales de acuerdo a reportes de nuestros pares, aparentan ser patrocinados por estados hostiles continúan explotando las vulnerabilidades conocidas públicamente para establecer una amplia red de infraestructura comprometida. Estos actores utilizan la red para explotar una amplia variedad de objetivos en todo el mundo, incluidas las organizaciones del sector público y privado.

Enfocándose en explotar vulnerabilidades presentes en dispositivos cibernéticos. Estos actores explotan vulnerabilidades para comprometer dispositivos de red sin parches, descuidados como routers, dispositivos de almacenamiento (NAS), que sirven como puntos de acceso adicionales para enrutar el tráfico de comando y control (C2) y actúan como puntos intermedios para realizar instrucciones en la red de otras entidades. En los últimos años, una serie de vulnerabilidades de alta gravedad para los dispositivos de infraestructura de red proporcionó a los actores la capacidad de explotar y obtener acceso a dispositivos vulnerables.

**Estos dispositivos a menudo son pasados por alto por los administradores al momento de aplicar parches y actualizaciones seguridad**

https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

https://attack.mitre.org/groups/

# Caso 1 - Actores Cibernéticos Patrocinados Explotan dispositivos de red vulnerables / CISA Alter (AA22-158A)

*Table 1: Top network device CVEs exploited by PRC state-sponsored cyber actors*

| Vendor | CVE | Vulnerability Type |
|---|---|---|
| Cisco | CVE-2018-0171 | Remote Code Execution |
| | CVE-2019-15271 | RCE |
| | CVE-2019-1652 | RCE |
| Citrix | CVE-2019-19781 | RCE |
| DrayTek | CVE-2020-8515 | RCE |
| D-Link | CVE-2019-16920 | RCE |
| Fortinet | CVE-2018-13382 | Authentication Bypass |
| MikroTik | CVE-2018-14847 | Authentication Bypass |
| Netgear | CVE-2017-6862 | RCE |
| Pulse | CVE-2019-11510 | Authentication Bypass |
| | CVE-2021-22893 | RCE |
| QNAP | CVE-2019-7192 | Privilege Elevation |
| | CVE-2019-7193 | Remote Inject |
| | CVE-2019-7194 | XML Routing Detour Attack |
| | CVE-2019-7195 | XML Routing Detour Attack |
| Zyxel | CVE-2020-29583 | Authentication Bypass |

https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

# Caso 1 - Actores Cibernéticos Patrocinados Explotan dispositivos de red vulnerables / CISA Alter (AA22-158A)

**Mitigaciones**

- Parchear los Sistemas(SO, Firmaware)
- Mover/Eliminar los dispositivos comprometidos de la red
- Segmentar las redes
- Deshabilite los servicios de red, puertos, protocolos y dispositivos no utilizados o innecesarios
- Habilitar la autenticación multifactor
- Mantener actualizados las copias de seguridad
- Aislar los servicios publicados hacia internet

- **Habilite el registro y la revisión de los accesos a la infraestructura de la red, los cambios de configuración y los servicios de infraestructura.**

https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

# Caso 2 - Eventos Cibernéticos en Paraguay / Respuesta a Incidentes

- Ataques de Ransomware
  - Casos de HIVE V4, V5
    - Human Operated
  - Globe Imposter 2.0
    - RaaS
  - Djavu
- Servidores Comprometidos
  - Servidores de Correo
  - Servidores web

Informe del estado de la Ciberseguridad

https://www.cert.gov.py/

# Caso 2 - Eventos Cibernéticos en Paraguay / Coincidencias?

- Equipos de red con vulnerabilidades presentes expuestos a internet
- Sistemas, Aplicaciones, sistemas operativos desactualizados
- Configuraciones por defecto en sistemas y aplicaciones
- Procedimientos de administración inseguros o malas prácticas de administración de sistemas(servicios expuestos, plugins con vulnerabilidades presentes)
- No prestar atención a los registros de logs
- Omisión de alertas de sistemas de seguridad

**Escuche atentamente a sus LOGS, ellos pueden advertirle sobre un ataque, con anticipación**

<!--Frase Célebre-->

# Marie Curie {

"Solo puede analizar los datos que tienes. Sé estratégico sobre que reunir y como almacenarlo"

}

# Preguntas?

<!--MITIC / CERT-PY-->

# Gracias!! {

<Por="Marcos Ivan Centurion Giles"/>

}

# Descargue la presentación

@LiquidIv4n

abuse@cert.gov.py

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY