Digital Security
Progress. Protected.

# EL MIEDO A UN CAMBIO NECESARIO

**Carlos Tortosa**
**Key Account Director**
ctortosa@eset.es

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Cryptolocker

Ransomware

Zero Days

Adware

DDOS

APT’s

Troyanos

Exploits

Fileless malware

Zero Trust

Digital Security
Progress. Protected.

- **EPP – Endpoint detection platform**
  - Protección esencial para cualquier tipo de dispositivos
- **EDR – Endpoint detection and response**
  - Herramienta de monitorización y análisis basada en procesos
- **XDR – Extended detection and response**
  - Herramienta que recopila y correlaciona datos de diferentes herramientas de protección
- **MDR – Endpoint detection and response managed**
  - Herramienta EDR gestionada por especialistas
- **Sandbox personalizada**
  - Herramienta de monitorización y análisis basada en archivos

Digital Security
Progress. Protected.

# Necesidades de las administraciones publicas

- Acceso a la mejor tecnología del mercado
- Uso de tecnologías certificadas
- Protección multicapa con visión de 360
- Actualización constante tecnológica
- Acceso a servicios de calidad
- Formación constante para usuarios

Digital Security
Progress. Protected.

# DISPOSICIONES GENERALES MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

## 7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

# Caso de estudio: situación actual

- Administracion publica de gobierno autonómico
- Sedes totales 8
- Mas de 3,000 dispositivos administrados
- Acceso limitado en alguna de las sedes
- Diferentes tecnologías administradas
- Solución de seguridad instalada

# Caso de estudio: Necesidades

- Elevar el nivel de protección de la actual solución de seguridad
- Acceder a tecnología actualizada con criterios de calidad predefinidos, y con certificaciones regladas
- Mejora del rendimiento de los equipos gestionados
- Gestión de los dispositivos móviles, no administrados con anterioridad
- Aplicación de políticas por:
  - Sedes
  - Perfiles de usuarios
  - Tipología del dispositivo
- Tiempo limitado para el despliegue
- Gestión desde una plataforma unificada
- Garantizar la formación del equipo de seguridad interno

# Caso de estudio: Propuestas

- Solución unificada: EPP+EDR ( ESET Protect Enterprise)
- Solución de seguridad basada en modulos + protección por comportamiento + herramienta basada en la nube (ESET Liveguard Advanced)
- Solución certificada como la de menor impacto en los recursos de los dispositivos (https://www.av-comparatives.org/reports/endpoint-prevention-response-epr-test-2021/)
- Gestión desde una consola centralizada para todas las soluciones propuestas
- Aplicación de políticas por (ESET Protect):
  - Sedes
  - Perfiles de usuarios
  - Tipología del dispositivo
- Despliegue realizado por técnicos de ESET España
- Gestión desde una plataforma unificada (ESET Protect)
- Formación continua realizada por técnicos certificados de ESET España

ESET
Digital Security
Progress. Protected.

# Empresa de ciberseguridad Nº1 en Europa

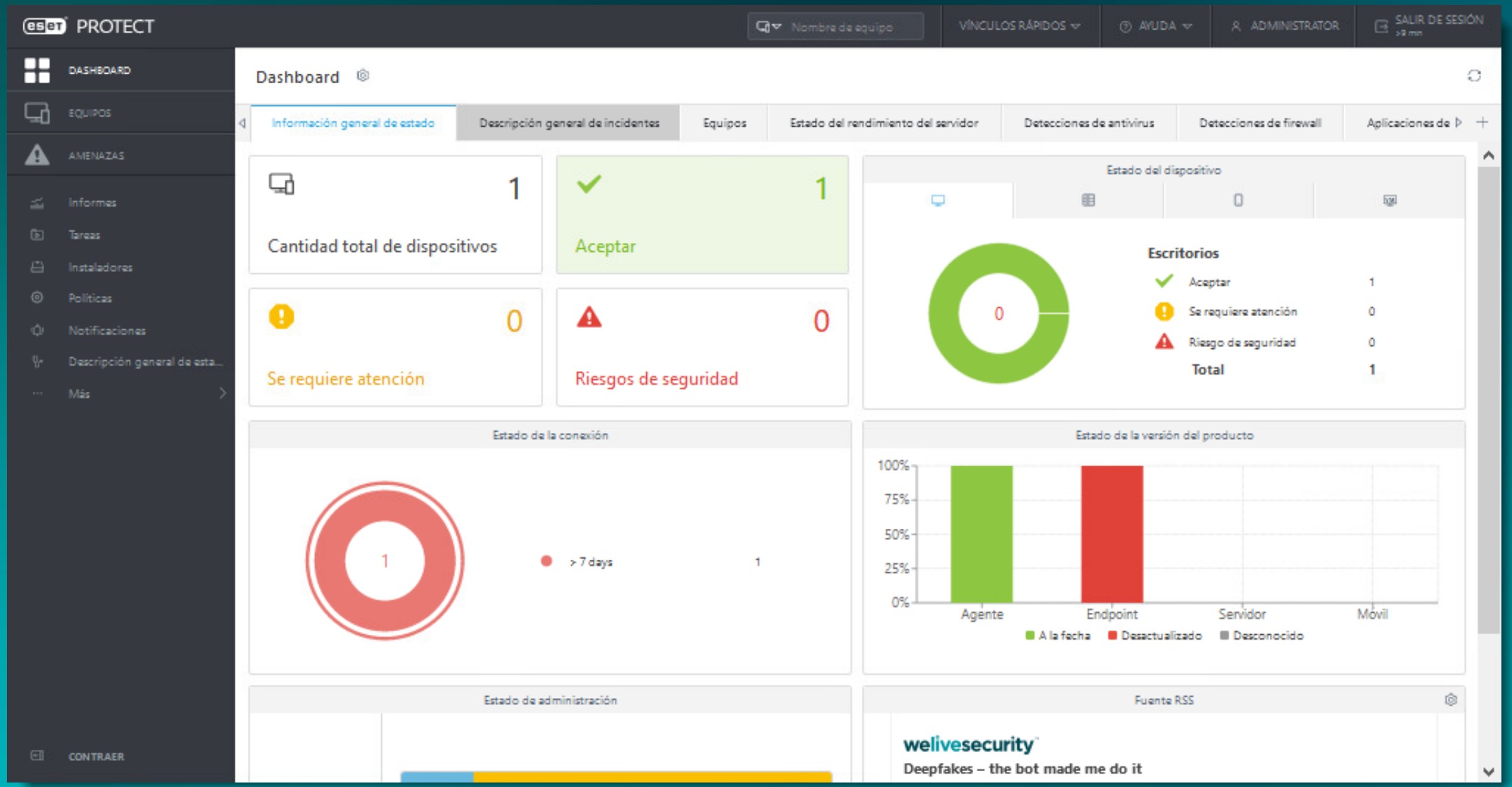
Digital Security
Progress. Protected.

# SOLUCIONES

PROTECT

Consola de administración unificada para todas las soluciones de seguridad de ESET

Digital Security
**Progress. Protected.**



Digital Security
Progress. Protected.

# SOLUCIONES

ENDPOINT SECURITY

SERVER SECURITY

**Plataforma de protección para prevenir ataques, detectar actividad maliciosa y capacidades de corrección instantánea.**

**Protección para SO: Windows/Windows Server – Linux/Linux Server – MAC – Android - IOS**

Digital Security
Progress. Protected.

# SOLUCIONES

## LIVEGUARD ADVANCED

**Detecta amenazas de día cero y nunca antes vistas**
**Tecnología de la sanbox basada en la nube**
**Detección basada en el comportamiento**

# SOLUCIONES

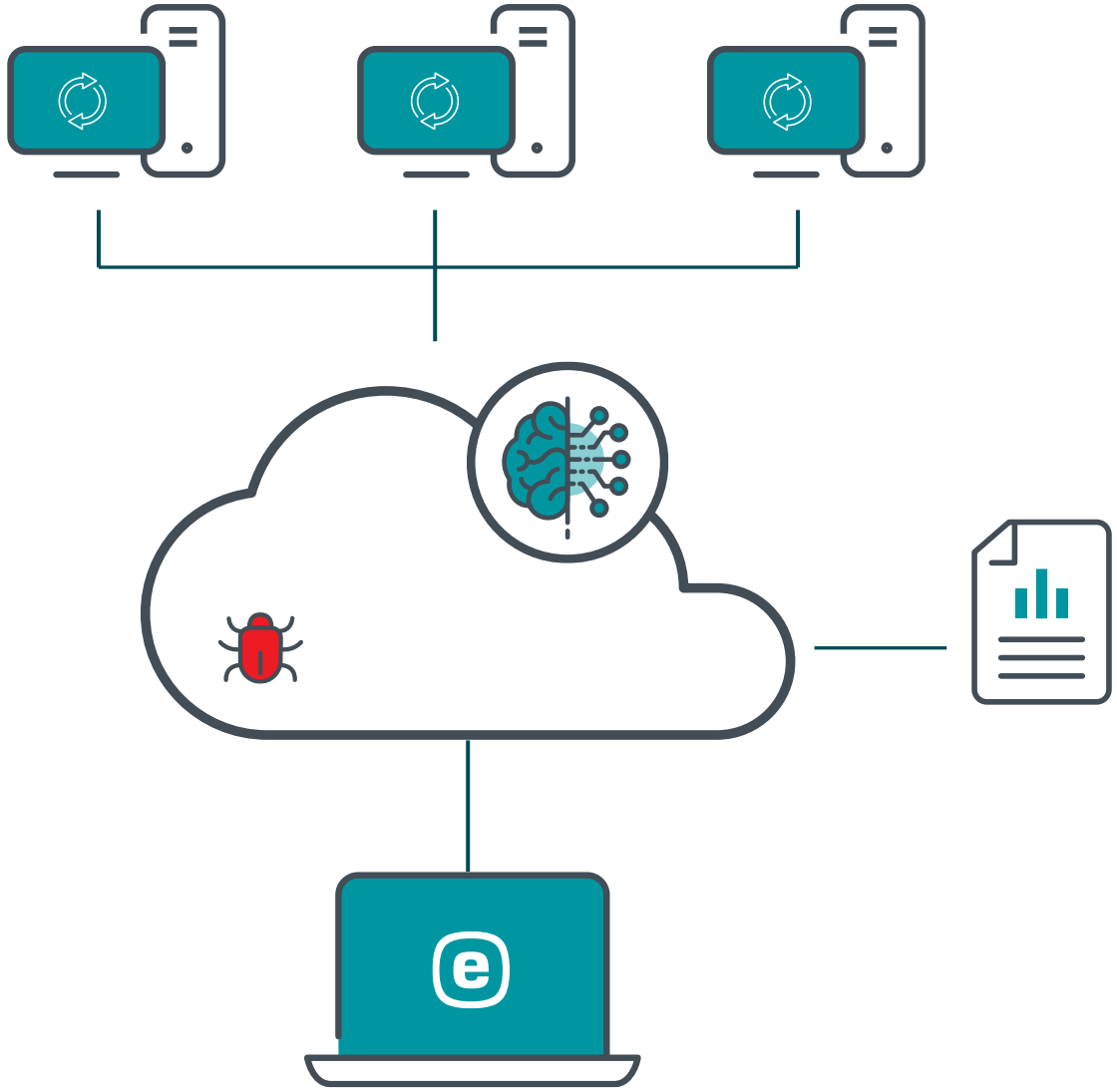
## ¿Qué hace ESET Liveguard?

**Sandbox en la nube**

**Utiliza machine learning**

**Añade protección a todos tus ordenadores de forma instantanea**

**Informe simple en cada analisis**



Digital Security
Progress. Protected.

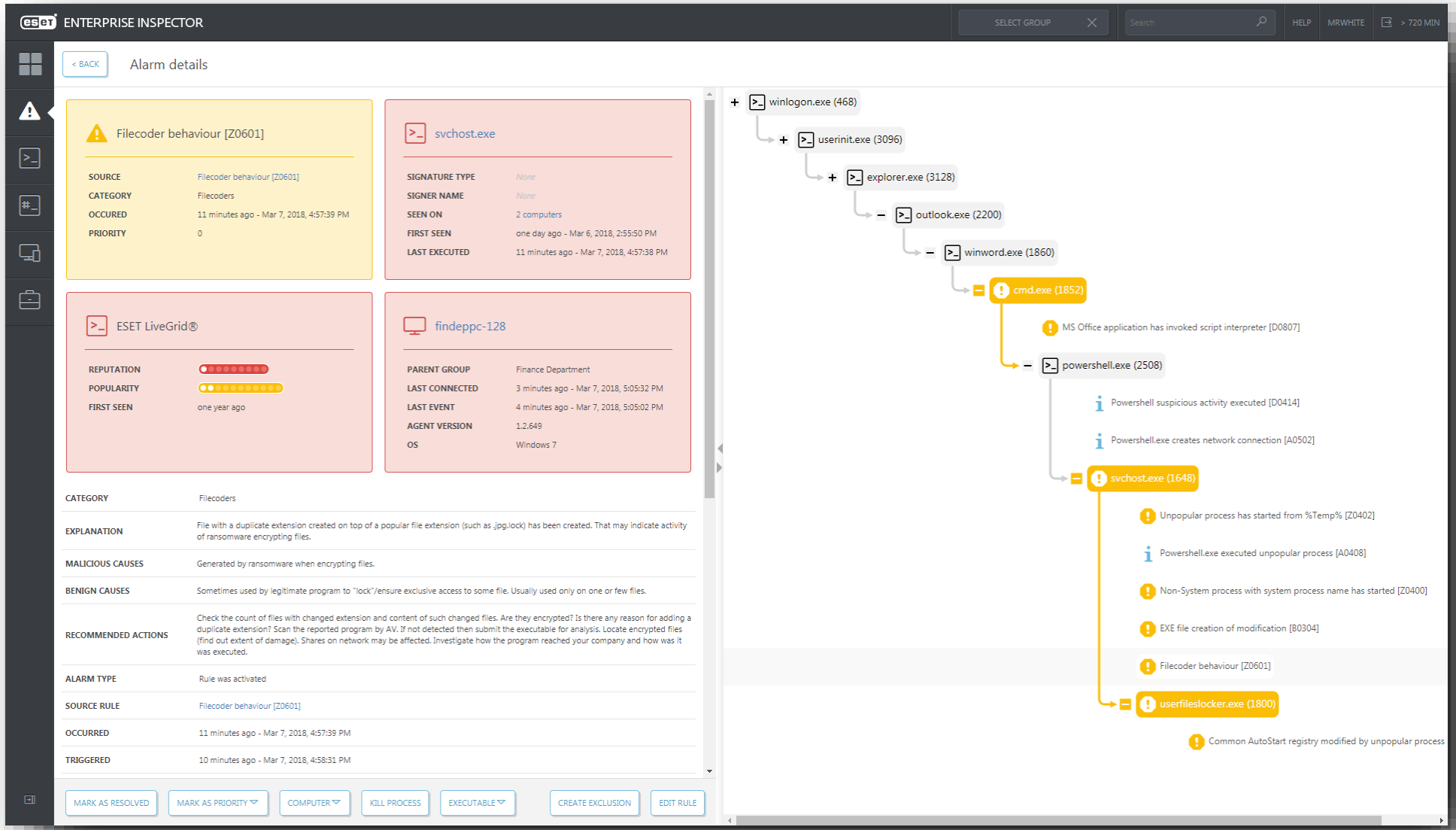
# SOLUCIONES

## ESET INSPECT

Herramienta de detección y respuesta de ESET frente a amenazas que permite la monitorización exhaustiva y continua de la actividad de los equipos en tiempo real, el análisis en profundidad de procesos sospechosos y la respuesta inmediata frente a incidentes y brechas de seguridad. En combinación con la plataforma ESET Endpoint Protection, ESET Inspect proporciona una prevención, detección y solución completa para:

- Detectar amenazas avanzadas persistentes
- Detener los ataques sin archivos
- Bloquear las amenazas zero-day
- Proteger contra el ransomware

# SOLUCIONES


ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
MRWHITE
> 720 MIN
< BACK
Alarm details
Filecoder behaviour [Z0601]
SOURCE Filecoder behaviour [Z0601]
CATEGORY Filecoders
OCCURED 11 minutes ago - Mar 7, 2018, 4:57:39 PM
PRIORITY 0
svchost.exe
SIGNATURE TYPE None
SIGNER NAME None
SEEN ON 2 computers
FIRST SEEN one day ago - Mar 6, 2018, 2:55:50 PM
LAST EXECUTED 11 minutes ago - Mar 7, 2018, 4:57:38 PM
ESET LiveGrid®
REPUTATION
POPULARITY
FIRST SEEN one year ago
findeppc-128
PARENT GROUP Finance Department
LAST CONNECTED 3 minutes ago - Mar 7, 2018, 5:05:32 PM
LAST EVENT 4 minutes ago - Mar 7, 2018, 5:05:02 PM
AGENT VERSION 1.2.649
OS Windows 7
CATEGORY Filecoders
EXPLANATION File with a duplicate extension created on top of a popular file extension (such as .jpg.lock) has been created. That may indicate activity of ransomware encrypting files.
MALICIOUS CAUSES Generated by ransomware when encrypting files.
BENIGN CAUSES Sometimes used by legitimate program to "lock"/ensure exclusive access to some file. Usually used only on one or few files.
RECOMMENDED ACTIONS Check the count of files with changed extension and content of such changed files. Are they encrypted? Is there any reason for adding a duplicate extension? Scan the reported program by AV. If not detected then submit the executable for analysis. Locate encrypted files (find out extent of damage). Shares on network may be affected. Investigate how the program reached your company and how was it was executed.
ALARM TYPE Rule was activated
SOURCE RULE Filecoder behaviour [Z0601]
OCCURRED 11 minutes ago - Mar 7, 2018, 4:57:39 PM
TRIGGERED 10 minutes ago - Mar 7, 2018, 4:58:31 PM
MARK AS RESOLVED
MARK AS PRIORITY
COMPUTER
KILL PROCESS
EXECUTABLE
CREATE EXCLUSION
EDIT RULE
winlogon.exe (468)
userinit.exe (3096)
explorer.exe (3128)
outlook.exe (2200)
winword.exe (1860)
cmd.exe (1852)
MS Office application has invoked script interpreter [D0807]
powershell.exe (2508)
Powershell suspicious activity executed [D0414]
Powershell.exe creates network connection [A0502]
svchost.exe (1648)
Unpopular process has started from %Temp% [Z0402]
Powershell.exe executed unpopular process [A0408]
Non-System process with system process name has started [Z0400]
EXE file creation of modification [B0304]
Filecoder behaviour [Z0601]
userfileslocker.exe (1800)
Common AutoStart registry modified by unpopular process

Digital Security
Progress. Protected.

# SOLUCIONES

## SERVICIOS PROFESIONALES

- APOYO PREMIUM ESENCIAL
- SOPORTE PREMIUM AVANZADO
- IMPLEMENTACIÓN Y ACTUALIZACIÓN
- MONITORIZACIÓN

## SERVICIOS DE SEGURIDAD

- DETECCIÓN Y RESPUESTA ESENCIAL
- DETECCIÓN Y RESPUESTA AVANZADA
- DETECCIÓN Y RESPUESTA PREMIUM

# Conclusiones

- Cambio de todo el parque tecnológico en un tiempo máximo de 4 semanas
- Implementación de la nueva solución al máximo rendimiento
- Formación continua del equipo IT del la AAPP
- Evolución de una solución “tradicional” a una protección con diferentes tecnologías integradas

Digital Security
Progress. Protected.

# Conclusion final

**El miedo al cambio no debe ser motivo para no acceder a la mejor tecnología posible**

Digital Security
Progress. Protected.

# Gracias

**Carlos Tortosa**
**Key Account Director**
ctortosa@eset.es
linkedin.com/in/J-Carlos-Tortosa