centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1216

Procedimiento de empleo seguro
Trend Micro Deep Security

Mayo de 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.04.22 11:44:41 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-131-1

Fecha de Edición: abril de 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. Deep Security es la solución de Trend Micro que protege de amenazas, *malware* y cambios no autorizados, para proteger los despliegues de nube híbrido, en entornos físicos, virtuales, en la nube o en contenedores.
2. Permite proteger *workloads* nuevas y existentes frente a amenazas desconocidas con técnicas como el *machine learning* o la aplicación de parches virtuales.
3. Su agente ligero incorpora las siguientes funcionalidades para proporcionar seguridad, visibilidad y control:
   - EDR (con respuesta frente a amenazas conocidas, *zero-day*)
   - Reputación web
   - Control de aplicaciones
   - Supervisión de *logs*
   - Supervisión de Integridad (FIM)
   - *Firewall* de Host y Host IPS (que incorpora la tecnología de parcheado virtual[1])

[1] La tecnología de parcheado virtual previene de ataques frente a vulnerabilidades no parcheadas. Esto se consigue aplicando las reglas IPS necesarias para bloquear potenciales ataques frente a vulnerabilidades existentes en el sistema operativo y aplicaciones instaladas.

2. OBJETO Y ALCANCE

4. Esta guía ha sido elaborada para el producto **Deep Security versión 11** y subversiones contenidas dentro de la misma.
5. El producto se compone de una consola de gestión Deep Security Manager (DSM), la cual puede desplegarse on-*premise* o puede estar desplegada en modalidad SaaS y agentes *Deep Security Agent* (DSA) desplegados en los sistemas operativos a proteger.
6. Este producto ha sido cualificado e inclusión en el Catálogo de Productos y Servicios STIC (CPSTIC), en las familias 'EPP (*Endpoint Protection Platform*)' y 'EDR (*Endpoint Detection Response*).
7. La cualificación abarca los siguientes componentes: Deep Security Manager, Agente/Relay Linux y Windows. El *Virtual Appliance* ha sido excluido del alcance de la cualificación.

3. ORGANIZACIÓN DEL DOCUMENTO

8. El documento ha sido estructurado de la siguiente manera:

   a) **Apartado 4 y 5.** Fase de despliegue e instalación, describe todas las tareas necesarias para efectuar un despliegue seguro de Deep Security.

   b) **Apartado 6**. Fase de Configuración. Detalla las configuraciones a aplicar en el producto para que este opere de manera segura optimizando sus capacidades de protección y rendimiento.

   c) **Apartado 7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) **Apartado 8.** Listado de tareas a completar empleando la presente guía.

   e) **Apartado 9**. Referencias externas a este documento de recomendada revisión.

   f) **Apartado 10**. Abreviaturas empleadas en el documento.

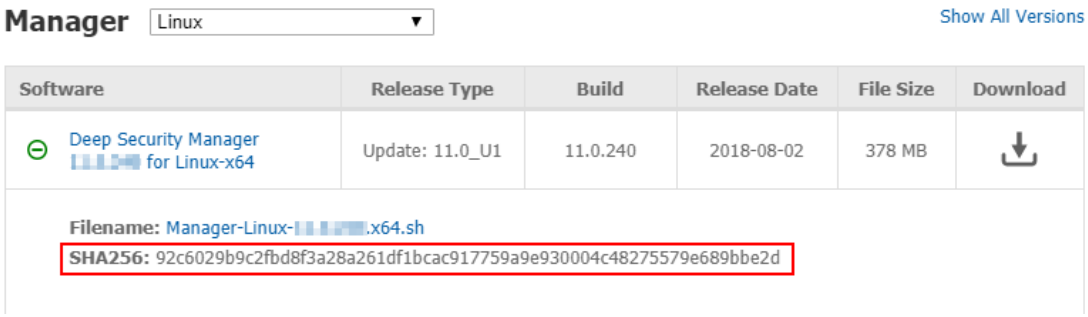
4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. La descarga del DSM y de los agentes DSA debe realizarse a través del siguiente enlace:

   https://help.deepsecurity.trendmicro.com/software-long-term-support.html

10. Todos los enlaces de descarga están acompañados de un hash SHA256 que permite validar que el fichero descargado no ha sido manipulado por terceros. **Se debe realizar esta comprobación de integridad.**



4.2 ENTORNO DE INSTALACIÓN SEGURO

11. La consola DSM será desplegada en una ubicación del CPD del cliente o bien en un servicio nube.

12. El DSM debe disponer de acceso exclusivamente a los puertos y servicios de Trend Micro así como a los dispositivos a proteger.

4.3 REGISTRO Y LICENCIAS

13. Durante el proceso de compra de licencias, el cliente recibirá un certificado de licenciamiento donde se listarán las claves de registro asociadas al producto.

14. El cliente deberá acceder al portal https://clp.trendmicro.com para registrarse y generar los correspondientes códigos de activación. Estos se generan al registrar los códigos de registro en dicho portal.

4.4 CONSIDERACIONES PREVIAS

15. Para disponer de un rendimiento óptimo, se recomienda dimensionar correctamente el entorno en base a los recursos que se prevé utilizar en base al número de agentes y periodos de retención. Este dimensionamiento se describe en el siguiente enlace:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Get-Started/sizing.html

16. En el caso de desplegar la consola DSM en un entorno virtual se recomienda aplicar las siguientes configuraciones:

a) Utilizar *vmxnet3* como *driver* de tarjeta virtual.

b) Utilizar *driver paravirtual SCSI* como controlador de disco virtual.

c) Aprovisionar disco en modo "*Thick Eager Zero Disk*".

17. Se recomienda desplegar, al menos 2 servidores DSM con balanceo de carga externo para garantizar la disponibilidad del servicio.
18. Se recomienda que exista resolución DNS entre los agentes, el DSM y viceversa.
19. Se recomienda que la BBDD se encuentre ubicada en un nodo o clúster separado del DSM y que estos se encuentren ubicados en la misma LAN con un ancho de banda disponible de 1Gb o superior.
20. A continuación, se describen algunas recomendaciones específicas para la base de datos SQL Server:
    a) Es requerido crear la BBDD de DSM antes de la instalación.
    b) Asegurar que la BBDD acepta conexiones TCP:

       http://msdn.microsoft.com/en-us/library/bb909712(v=vs.90).aspx

    c) La cuenta para conectar a la BBDD debe disponer de privilegios "*db_owner*" sobre la BBDD creada en SQL.
    d) En el caso de entornos *multitenant* se requiere disponer de privilegios "*db_owner*" para dicho usuario.
    e) Se recomienda activar el modo de recuperación simple en la BBDD: http://technet.microsoft.com/en-us/library/ms189272.aspx
21. A continuación, se describen algunas recomendaciones específicas para la base de datos SQL ORACLE:
    a) Asegurar que el servicio *listener* de Oracle está arrancado y acepta conexiones TCP.
    b) Crear el usuario *'*dms'*.
    c) Asignar privilegios *CONNECT*, *RESOURCE* y *tablespace* ilimitado a dicho usuario.
    d) Asignar privilegios *CREATE SEQUENCE*, *CREATE TABLE* y *UNLIMITED TABLESPACE* a dicho usuario.

5. FASE DE INSTALACIÓN

22. Se debe descargar la última versión de DSM disponible en el centro de descargas de Trend Micro (*https://downloadcenter.trendmicro.com*) verificando que el *checksum* de los ficheros se corresponde con el identificado en la web anterior.
23. Adicionalmente se recomienda descargar el *software* de agente correspondiente con los sistemas operativos a proteger (ej.: Windows 32 y 64bit y Linux) y depositarlos en el mismo directorio donde se lance la instalación del manager antes de ejecutar la instalación. De esta manera se importarán automáticamente en el inventario de DSM.
24. Una vez descargado, se debe realizar la instalación y seguir los pasos indicados en el siguiente KB:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/install-deep-security.html
25. Se recomienda desplegar una configuración *multi-nodo,* la cual aporte alta disponibilidad a los servicios de administración del producto.
26. Durante el proceso de instalación, el producto consultará si se quiere convertir el primer nodo de DSM en *relay*. Se debe marcar esa opción para que sea instalado.
27. Se recomienda habilitar, al menos, 2 *relay*. En el caso de una configuración con DSM *multi-nodo*, deberían ser los 2 DSM. Esta configuración puede llevarse a cabo siguiendo el siguiente KB:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Set-Up-Relays.html

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

28. **Se debe activar el modo de operación seguro del producto**. Deep Security permite la activación del modo FIPS. Los pasos se describen en:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/fips-140-2.html

6.2 AUTENTICACIÓN

29. El producto permite los siguientes métodos de autenticación.
    - Autenticación de usuarios locales definidos en la sección de administración.
    - Autenticación remota sincronizando con *Active Directory* local.
    - Autenticación SSO utilizando proveedor SAML:

      https://help.deepsecurity.trendmicro.com/11_0/on-premise/saml-single-sign-on-configuration.html
    - Se deben configurar todos los nodos DSM y de autenticación (AD, SAML, etc) para que utilicen el mismo servidor NTP.
30. El procedimiento de gestión de usuarios está descrito en el siguiente KB:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/user-management.html?redirected=true

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. El producto podrá gestionarse de manera local o remota y siempre a través de una GUI accesible vía web. Esta web será accesible únicamente mediante el protocolo HTTPS (no es accesible usando HTTP por no considerarse seguro) en el puerto 4119. Se recomienda limitar el acceso a dicho puerto únicamente a direcciones IP de confianza.
32. Se recomienda limitar el acceso RDP/SSH a los servidores de gestión a direcciones IP de confianza.
33. El producto se instala con un certificado SSL autofirmado. **Se debe sustituir dicho certificado por uno emitido por una entidad certificadora de confianza**. Los pasos para reemplazar dicho certificado se describen en el siguiente KB:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Reference/ref-ssl-cert.html?redirected=true

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

34. La gestión de privilegios se efectúa mediante una combinación de usuarios y roles. Por defecto el producto define los roles "*Full Access*" y "*Auditor*". También permite crear roles personalizados ajustándose a los requerimientos de funcionalidad y visibilidad requeridos.

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/ui-admin-roles.html

35. El producto permite forzar una política de contraseñas similar o más restrictiva a la descrita a continuación. Se deben aplicar los siguientes parámetros:

    - Longitud de la contraseña: **mínimo 12 caracteres**.
    - Complejidad:
        - Uno o más caracteres en **minúscula**.
        - Uno o más caracteres en **mayúscula**.
        - Uno o más **números**.
        - Uno o más caracteres **especiales**.
    - Cuando se cambia la contraseña, esta tendrá que diferir de la anterior en, al menos, 4 caracteres.
    - El cambio de contraseña debe realizarse, como máximo, **cada 60 días.**

36. Esta configuración se define en el siguiente enlace:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/security-settings.html

37. Se recomienda establecer también valores para los parámetros de sesión:

    - *Timeout* de autenticación (tiempo que permanece el usuario autenticado en la sesión, transcurrido el cual, el usuario debe volver a autenticarse).
    - *Timeout* de inactividad (tiempo que puede permanecer la sesión inactiva, trascurrido el cual, se producirá la desconexión automática). **Dicho parámetro, debe estar configurado, como máximo, a 5 minutos.**
    - Número máximo de sesiones concurrentes de un administrador.
    - Número de administradores que pueden acceder simultáneamente, que debe ser lo más reducido posible.
    - Número máximo de intentos fallidos de autenticación, y tiempo de espera tras superar un umbral. **El número máximo de intentos fallidos de acceso debe ser 3 y el tiempo de bloqueo mínimo 5 segundos.**

38. Esta configuración se describe en el siguiente KB:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/security-settings.html

39. Configuración del mensaje de aviso y consentimiento en el inicio de sesión (*login banner*). Configurable en la sección "*sign-in message*":

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/security-settings.html

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

40. El producto emplea unos puertos predefinidos para su operación:
    a) Consola de gestión: 4119.
    b) *Heartbeat* agentes: 4120.
    c) *Relay*: 4122
    d) Agente: 4118
41. Estos puertos pueden ser modificados, pero es conveniente mantenerlos, por motivos de estandarización y estabilidad de la plataforma.
42. Estos servicios deberán ser accesibles únicamente desde las direcciones IP de confianza, preferentemente aquellas donde accedan únicamente administradores autorizados. Esta configuración puede aplicarse empleando filtros *firewall* del propio producto:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Protection-Modules/Firewall/firewall-rule-action-priority.html

6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

43. Deep Security requiere de la utilización obligatoria del protocolo TLS 1.2 desde la versión 11.0 Update 1. Esto afecta a todos los componentes (DSM, DSA, DSRA, BBDD, etc) del producto.

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/tls-version.html#Enable

44. En el caso de la BBDD la configuración varía en función de la BBDD empleada:
    a) SQL Server. **Se debe configurar la comunicación para que específicamente utilice TLS1.2**. Su configuración se describe en el siguiente KB:

       https://support.microsoft.com/en-us/topic/kb3135244-tls-1-2-support-for-microsoft-sql-server-e4472ef8-90a9-13c1-e4d8-44aad198cdbe

    b) PostgreSQL emplea por defecto TLS 1.2.
    c) Oracle permite utilizar su método cifrado nativo. **Se debe configurar la comunicación para que específicamente utilice TLS1.2** Para ello:

       https://help.deepsecurity.trendmicro.com/11_1/aws/Manage-Components/dsm-db-encrypt.html

45. Se recomienda configurar comunicación bi-direccional cuando sea posible.
46. El siguiente KB detalla la configuración de la comunicación del agente, así como los algoritmos criptográficos empleados:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/communication-overview.html

6.6 GESTIÓN DE CERTIFICADOS

47. Por motivos de seguridad, **se debe sustituir el certificado SSL autofirmado** empleado por el DSM (procedimiento detallado):

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Reference/ref-ssl-cert.html?redirected=true

48. De cara a cumplir con los requisitos establecidos en la guía CC-STIC-807 el certificado cumplirá con los siguientes requisitos:
    - **RSA** con claves de, al menos, **3072 bits** de longitud.
    - **ECDSA** con curvas **P-256 o superior.**
    - **DSA** con claves de, al menos, **3072 bits** de longitud.
    - Funciones **Hash SHA-256** o superior.
49. El siguiente KB describe el procedimiento de importación de un certificado de CA:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Reference/ref-ssl-cert.html?redirected=true#Generate

50. El producto verificará la validez, autenticidad y FDQN asociados al certificado en las comunicaciones entre componentes. Otros parámetros adicionales podrán ser configurados en la fase de emisión del CSR (*Certificate Signing Request*):

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Reference/ref-ssl-cert.html#Generate2

6.7 SERVIDORES DE AUTENTICACIÓN

51. DSM permite efectuar autenticación empleando usuarios *Active Directory*:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/user-management.html#Synch?redirected=true

52. DSM permite efectuar autenticación SAML. Esta configuración queda descrita en el siguiente KB:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/saml-single-sign-on-configuration.html

53. Todas las comunicaciones emplean tráfico cifrado TLS.

6.8 SINCRONIZACIÓN

54. **Todos los componentes (DSM, DSRA, DSA, SGBD, etc) debe utilizar un servicio NTP de sincronización horaria**. Esta sincronización deberá efectuarse a nivel de sistema operativo y el producto tomará la hora del sistema como referencia.

6.9 ACTUALIZACIONES

55. **El producto debe estar actualizado** y contar con los parches de seguridad suministrados por el fabricante, junto con las firmas y reglas utilizadas para su funcionamiento. Se debe, por tanto, establecer un procedimiento de actualización que lo garantice.
56. El procedimiento de actualización del DSM es similar al de instalación y consiste en la descarga del instalador de manera segura y seguir los pasos indicados (ver apartado 5 FASE DE INSTALACIÓN)

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/install-deep-security.html?Highlight=upgrade%20dsm
57. El producto requiere de comunicación con los servicios en nube de Trend Micro para poder efectuar actualizaciones de firmas, reglas y distintas configuraciones. El siguiente KB detalla las URLs y puertos necesarios para la correcta operativa del producto:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/ports.html
58. **Se debe limitar el acceso únicamente a dichas URLs tanto a nivel de DSM como a nivel de agentes.**
59. Se recomienda emplear comunicaciones vía *proxy*. En el caso de utilizar el módulo *anti-malware*, si el agente DSA a proteger no dispone de conectividad directa a los servicios de Trend Micro, será necesario habilitar la configuración relativa a *"Network Setting for Census and Good File Reputation Service, and Predictive Machine Learning*". Estas configuraciones se describen en el siguiente KB:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/protecting-workloads-proxies.html

6.10 AUTO-CHEQUEOS

60. Deep Security en la fase de arranque de los servicios efectúa los siguientes chequeos:
    - Verificación de integridad de sus componentes (*checksum*).
    - Existencia de *relays* activos (componente requerido para actualizaciones).
    - Conectividad con servicios de actualización.
    - Validez de certificados empleados en la comunicación.

- Conectividad con BBDD.
- Disponibilidad del resto de nodos del grupo de balanceo.

61. En el caso de que alguno de estos chequeos sea erróneo o inválido, se generará el correspondiente mensaje en el log del servidor de aplicaciones o en el log del sistema. **Se debe, por tanto, revisar y analizar la información de logs para detectar errores en los auto-chequeos.**

6.11 SNMP

62. El producto permite el envío de eventos (alertas) utilizando el protocolo SNMPv2. Para obtener más información, se puede consultar el siguiente enlace:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/System-Settings/ui-admin-settings-snmp.html

6.12 ALTA DISPONIBILIDAD

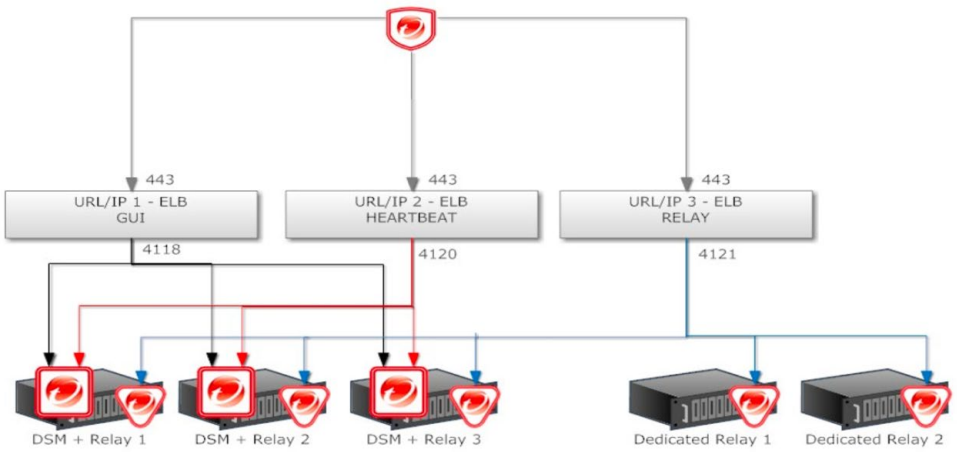
63. **Se debe desplegar el producto en alta disponibilidad si las necesidades de disponibilidad de la organización así lo requieren.**
64. Existen varios servicios que pueden disponer de alta disponibilidad:

    - DSM (consola):

      El DSM puede desplegarse en modo de alta disponibilidad. Este método garantiza la disponibilidad de la consola de gestión en el caso de fallo de uno de sus componentes. Para que esto sea posible es necesario que la BBDD esté configurada en un nodo externo preferiblemente en un clúster en modo HA.

      La configuración se describe a continuación:

      https://help.deepsecurity.trendmicro.com/11_0/on-premise/install-deep-security.html



Esta configuración no aplicaría si el modelo de consola fuera SaaS.

- Relays (DSRA):

Se recomienda disponer de, al menos, tantos *relays* como DSM existan.

Adicionalmente se recomienda desplegar un DSRA por cada ubicación (ej.: Madrid, Barcelona, etc) por motivos de optimización de ancho de banda y rendimiento. Se desaconseja la utilización de DSRAs en modalidad SaaS.

- SPS:

  Se recomienda desplegar, al menos 2 servidores SPS por cada ubicación.

6.13 AUDITORÍA

6.13.1 REGISTRO DE EVENTOS

65. El producto puede registrar tres (3) tipos de eventos:

    - Eventos del sistema (*System Events*):

      Relativos a actividades relacionadas con el funcionamiento del producto y tareas de auditoría (ej.: Acceso de usuarios, cambios de configuraciones en políticas, errores de actualización, etc).

    - Eventos de seguridad:

      Relativos a actividades registradas en los módulos de seguridad proporcionados por el producto (*Antimalware*, *Web Reputation*, *Application Control, Log Inspection, Integrity Monitoring, Firewall* e *IPS*). Ej.: Detección de *malware* por el módulo *antimalware*.

    - Alertas:

      Generadas en base a un evento o error del sistema.

      Ej.: Problemas de comunicaciones con servicios cloud de Trend Micro.

66. El siguiente KB describe los tipos de eventos que el producto puede generar:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/list-events-alerts.html

6.13.2 ALMACENAMIENTO LOCAL

67. Toda la información de eventos y configuraciones se almacena en la BBDD asociada al DSM. El dimensionamiento de la misma dependerá del volumen de clientes a proteger y del periodo de retención de eventos deseados. El siguiente KB define cómo efectuar dicha configuración, así como una estimación del tamaño de BBDD:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Get-Started/sizing.html

68. Una vez alcanzado el límite de retención, el producto comenzará a sobreescribir eventos antiguos.

69. **Se recomienda disponer de un método de almacenaje externo** (ej.: *syslog*), por ejemplo, para eventos más antiguos de 30 días.

    https://help.deepsecurity.trendmicro.com/10/0/Events-Alerts/Log-Event-Data-Storage.html

6.13.3 ALMACENAMIENTO REMOTO

70. Deep Security Manager permite el envío de eventos de sistema y seguridad a un sistema de almacenamiento remoto empleando el protocolo *syslog*.

71. **Se debe emplear la opción de cifrado de comunicaciones empleando el protocolo TLS.** Esta configuración se llevará a cabo especificando como modo de transporte el protocolo TLS:

72. Tal y como se indica detalladamente en el siguiente enlace:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/siem-syslog-forwarding-secure.html

6.14 *BACKUP*

73. Debe efectuarse una copia de seguridad de la BBDDs asociadas al producto DSM (creadas durante el procedimiento de instalación). **Estas copias deberán realizarse, al menos, con periodicidad diaria.**

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/update-database.html

74. En el caso de que los DSM estén ubicados en una infraestructura virtual, se recomienda efectuar una copia completa de dichas máquinas virtuales.

75. Se recomienda efectuar una copia de seguridad, al menos diaria, de los contenidos del directorio de instalación del DSM *(%programfiles%/Deep Security/*)

6.15 TAREAS PROGRAMADAS

76. DSM permite automatizar la programación de tareas con una ejecución periódica de las mismas. Se recomienda disponer de, al menos, las siguientes:

    - Actualizaciones de producto (firmas, patrones, etc). **Se debe programar la ejecución diaria** a partir de las 4AM CET.
    - *Scan for recommendation:*

      Se recomienda ejecución semanal, miércoles a partir de las 6AM CET aplicada a todo el parque de equipos.
    - *Scan for recommendation para máquinas nuevas:*

Crear tarea programada que ejecute un *scan for recommendation* en máquinas que nunca lo hayan ejecutado. Se recomienda ejecución diaria a partir de las 6AM CET.

77. Para más información, consultar el siguiente enlace:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/scheduled-tasks.html

6.16 SERVICIOS DE SEGURIDAD

78. Los servicios de seguridad proporcionados por Deep Security se dividen en los módulos descritos a continuación:

- Anti-Malware:

  Se recomienda aplicar la configuración a nivel de escaneo detallada en el siguiente enlace:

  Policies->Common Objects->Other->Malware Scan Configuration->ScanSettings

  Se recomienda **crear una configuración antimalware personalizada por cada tipología de entorno a configurar** (ej.: BBDD, Web, etc).

  La configuración recomendada para el **escaneo en tiempo real** es la siguiente:

Recommended Real-Time Scan Configuration	
General	Recommendation
Files to Scan	All Files
Directories to Scan	All directories
Actions	
Active Action	Disabled
Custom Actions:	Enabled
For Virus	Clean
For Trojans	Delete
For Packer	Quarantine
For Spyware	Quarantine
For Other Threats	Quarantine
Possible Malware upon Detection	ActiveAction
Options	
Enable Spyware / Grayware Scan	Enabled
Scan Compressed Files	Enabled
Maximum size of individual extracted files	Customized Size
Maximum Levels	2
Maximum number of files to extract	10
Scan Embedded Microsoft Office Objects	Enabled
Scan for Exploit Code in Microsoft Office Objects	Enabled
OLE Layers to Scan	3
Enable IntelliTrap*	Disabled
Enable Network Directory Scan	Enabled**
Scan Files When	Read/Write
Alert when …	Enabled

La configuración recomendada para el **escaneo programado** es la siguiente:

Recommended Scheduled Scan Configuration	
General	Recommendation
Files to Scan	All Files
Directories to Scan	All directories
Actions	
Active Action	Disabled
Custom Actions:	Enabled
For Virus	Clean
For Trojans	Delete
For Packer	Quarantine
For Spyware	Quarantine
For Cookie	Delete
For Other Threats	Quarantine
Possible Malware - Upon Detection	Quarantine
Options	
Enable Spyware / Grayware Scan	Enabled
Scan Compressed Files	Enabled
Maximum size of individual extracted files	Customized Size
Maximum Levels	3
Maximum number of files to extract	10
Scan Embedded Microsoft Office Objects	Enabled
Scan for Exploit Code in Microsoft Office Objects	Enabled
OLE Layers to Scan	3
CPU Usage	Medium
Alert when...	Enabled

La configuración recomendada para el **escaneo manual** es la siguiente:

Recommended Manual Scan Configuration	
General	Recommendation
Files to Scan	All Files
Directories to Scan	All directories
Actions	
Active Action	Disabled
Custom Actions:	Enabled
For Virus	Clean
For Trojans	Delete
For Packer	Quarantine
For Spyware	Quarantine
For Cookie	Delete
For Other Threats	Quarantine
Possible Malware - Upon Detection	Quarantine
Options	
Enable Spyware / Grayware Scan	Enabled
Scan Compressed Files	Enabled
Maximum size of individual extracted files	Customized Size
Maximum Levels	2
Maximum number of files to extract	10
Scan Embedded Microsoft Office Objects	Enabled
Scan for Exploit Code in Microsoft Office Objects	Enabled
OLE Layers to Scan	3
CPU Usage	High
Alert when...	Enabled

Adicionalmente se recomienda seguir las recomendaciones relativas a rendimiento descritas en la siguiente URL:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Performance-issues.html

Nota: Los motores antimalware avanzados (*Machine Learning* y *Behaviour Monitoring*), requieren que el servidor disponga de conectividad con las URLS públicas de Trend Micro descritas en el siguiente KB:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/ports.html

Si esta comunicación debe efectuarse vía *proxy*, será necesario efectuar la siguiente configuración específica en la política asignada:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Events-Alerts/census-good-file-reputation-predictive-machine-learning-alert.html

- *Web Reputation:*

  Se recomienda mantener el nivel de seguridad definido por defecto "*Medium*".

  Se desaconseja activar la opción "*lock pages that have not been tested by Trend Micro*" puesto que podría provocar falsos positivos.

  Salvo que exista algún problema de rendimiento o falso positivo, se desaconseja excluir direccionamientos y URLs conocidas de este motor.

- *Application Control:*

  Application Control elabora un inventario de todos ejecutables presentes en la máquina en el momento de su activación. Este *software* se agregará a lista blanca. **Se recomienda efectuar un escaneo completo *antimalware* antes de su activación**.

  Este módulo puede operar en modo permisivo (permite la ejecución de cualquier software salvo el bloqueado explícitamente) o restrictivo (solo permite la ejecución del software autorizado). **Se recomienda que, tras evaluar su viabilidad en un entorno de pruebas, se active en modo restrictivo.** Al ejecutarse en modo restrictivo bloqueará por defecto la ejecución de las siguientes extensiones:

  - *.class*
  - *.jar*
  - *.war*
  - *.ear*
  - *.php*
  - *.py*
  - *.pyc*
  - *.pyo*
  - *.pyz*

  Estas deberán permitirse manualmente en el caso de ser necesarias. Para más información sobre el control de aplicaciones, se puede consultar:

  https://help.deepsecurity.trendmicro.com/aws/application-control.html

- *Integrity Monitoring:*

  Se recomienda configurar una política sin reglas de monitorización y activar la opción "*Automatically Implement Integrity Monitoring Rule Recommendations (when possible)"* para que el sistema implemente aquellas reglas que apliquen en función del sistema operativo y aplicaciones instaladas. Una vez finalizada la configuración será necesario ejecutar un "*Scan For recommendations*" de manera manual o programada:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Policies/ug-rec-scan.html

Se recomienda activar la opción "*real-time*" supervisando la carga del sistema operativo para evitar problemas de rendimiento.

Una vez finalizada la configuración, se debe lanzar la primera reconstrucción de baseline:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/set-up-integrity-monitoring.html

Se recomienda que este *baseline* sea reconstruido tras un cambio significativo de configuración.

- *Log Inspection:*

  Se recomienda configurar una política sin reglas de monitorización y activar la opción "*Automatically Implement Log Inspection Rule Recommendations (when possible)*" para que el sistema implemente aquellas reglas que apliquen en función del sistema operativo y aplicaciones instaladas.

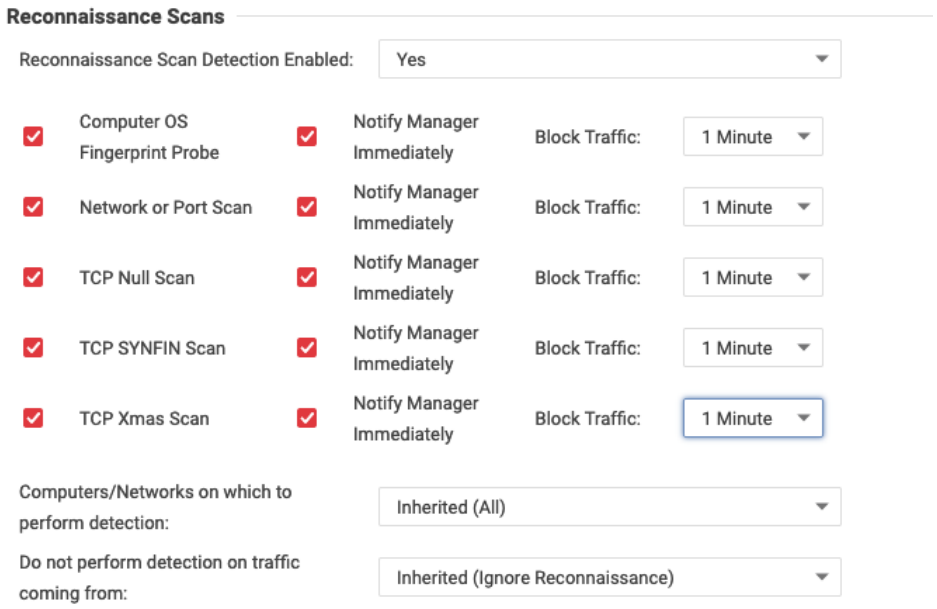
  Una vez finalizada la configuración será necesario ejecutar un "*Scan For recommendations*" de manera manual o programada:

  https://help.deepsecurity.trendmicro.com/11_0/on-premise/Policies/ug-rec-scan.html

- *Firewall:*

  El módulo permite establecer una configuración permisiva (con reglas de tipo "*deny*" que permiten cualquier tráfico no denegado) o (restrictiva con reglas tipo "*Allow*" que deniegan cualquier tráfico no permitido). Sin embargo, **se debe implementar una configuración restrictiva.** Se desaconseja activar el modo "*Tap*" pues afectaría tanto al motor IPS como firewall.

  Se recomienda activar la configuración "*Reconnaissance Scans*", estableciendo para todos los chequeos un bloqueo de 1 minuto.



Adicionalmente se podrán configurar direcciones IP desde las cuales se ignorarán escaneos.

https://help.deepsecurity.trendmicro.com/11_0/on-premise/set-up-firewall.html?redirected=true

– *IPS:*

El módulo IPS previene ataques de red tales como vulnerabilidades no parcheadas (*virtual patching*). Este módulo puede operar en modo "*Detect*" el cual solo detecta y registra ataques sin bloquearlos o en modo "*Prevent*" el cual previene cualquier ataque frente a vulnerabilidades no parcheadas.

Se recomienda activar inicialmente el modo "*detect*", revisar los logs generados durante un periodo temporal de 5 días para posteriormente activar el modo "*Prevent*" de manera definitiva.

Se recomienda configurar una política sin reglas de monitorización y activar la opción "*Automatically Implement IPS Rule Recommendations (when possible)*" para que el sistema implemente aquellas reglas que apliquen en función del sistema operativo y aplicaciones instaladas.

Una vez finalizada la configuración será necesario ejecutar un "*Scan For recommendations*" de manera manual o programada:

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Policies/ug-rec-scan.html

Los módulos de firewall e IPS utilizan el mismo *driver* de red a nivel de sistema. En el momento que se active cualquiera de los dos, el driver quedará activo y este podrá generar detecciones de eventos tanto en el módulo de firewall como IPS, independientemente de que dicho módulo esté desactivado.

- *Configuración general (aplica a todos los módulos):*

  Esta configuración se aplica dentro de la sección "*settings*" en una política o computer.

  - *Agent Self-Protection*: Se recomienda habilitar esta configuración con una *password* que impida la descarga y desinstalación de los módulos de seguridad del producto.

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/disable-agent-self-protection.html

  - *Limites asociados a la inspección de paquetes*:

    El driver de red (asociado a los módulos IPS/*firewall*) efectúa de manera automática inspección de paquetes descartando aquellos que estén malformados o representen un riesgo.

    La configuración por defecto es suficientemente permisiva para la mayoría de los usos, pero existen algunos parámetros que podrían ser necesarios modificar en función de las características del entorno. El parámetro *maximum TCP Connections* (valor por defecto 10.000), puede requerir ser ampliado para el correcto funcionamiento de servidores de BBDD y correo *smtp*.

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Policies/ui-editor-settings.html

7. FASE DE OPERACIÓN

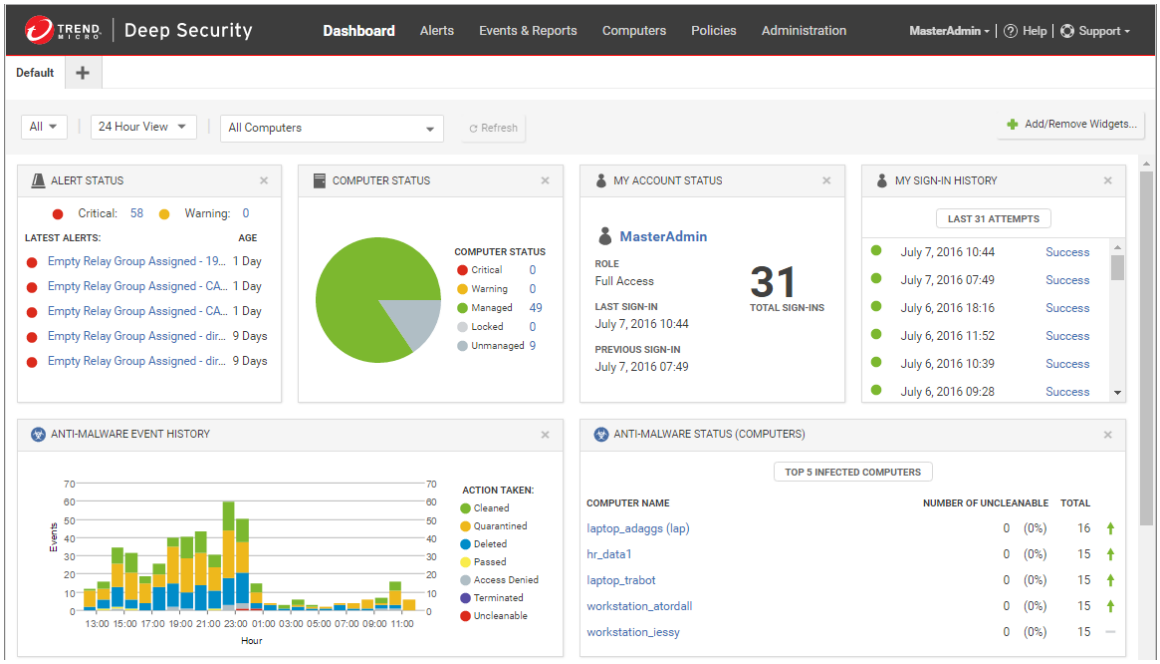
79. **Se debe activar el envío de alertas del producto a través de consola y correo electrónico**. De esta manera el producto notificará cualquier anomalía detectada (ej.: fallo en actualización) al administrador.

    https://help.deepsecurity.trendmicro.com/aws/alerts-configure.html

80. **Se debe revisar la descarga y actualización de firmas, reglas y paquetes.** Esto puede llevarse a cabo desde la siguiente consola:

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/Threat-Updates/ui-admin-updates-security.html

81. **Se debe configurar *dashboard* con la información relevante y revisarlo diariamente:**



82. Se recomienda mostrar los siguientes widgets:

    - *Computer Status.*
    - *Antimalware Event History.*
    - *Antimalware Status.*
    - *Web Reputation Event History.*
    - *Web Reputation Computer Activity.*
    - *Web Reputation URL Activity.*
    - *Integrity Monitoring Event History.*
    - *Integrity Monitoring Activity.*
    - *Integrity Monitoring Key Activity.*

- *Firewall Event History.*
- *Firewall Activity (Prevented)*
- *Firewall Activity (Detected).*
- *IPS Event History.*
- *IPS Activity (Prevented)*
- *IPS Activity (Detected).*

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/customize-dashboard.html

83. *Es debe prestar atención a los agentes con error y analizar las tendencias de detecciones* (*Activity* de cada módulo) durante los últimos 7 días identificando picos detecciones.
84. **Se deben revisar los eventos de sistema semanalmente identificando posibles fallos de comunicación de agentes u otros errores no críticos**.

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Events-Alerts/events.html
85. **Se deben revisar eventos de seguridad diariamente filtrando por aquellos cuya criticidad sea *high* o *critical*.**

    https://help.deepsecurity.trendmicro.com/11_0/on-premise/Events-Alerts/events.html
86. Revisar semanalmente sección "*computers*" filtrando por "*computer status*" y revisando aquellas que presenten errores y/o *warnings*.

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de licencia	☐	☐	
Consideraciones previas	☐	☐	
Instalación	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Configuración de Autenticación	☐	☐	
Configuración puertos accesibles	☐	☐	
Configuración Usuarios y Roles	☐	☐	
Configuración protocolos seguros	☐	☐	
Configuración de certificados	☐	☐	
Configuración NTP	☐	☐	
Configuración alertas	☐	☐	
Configuración Alta Disponibilidad	☐	☐	
Configuración Auditoría	☐	☐	
Configuración Almacenamiento	☐	☐	
Configuración *Backup*	☐	☐	
Configuración *Antimalware*	☐	☐	
Configuración *Web Reputation*	☐	☐	
Configuración *Application Control*	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración *Integrity Monitoring*	☐	☐	
Configuración *Log Inspection*	☐	☐	
Configuración *Firewall*	☐	☐	
Configuración IPS	☐	☐	
OPERACION			
FASE DE OPERACION			
Configuración del *dashboard*	☐	☐	
Configuración de alertas	☐	☐	

9. REFERENCIAS

Documentación Deep Security

https://help.deepsecurity.trendmicro.com/software-long-term-support.html

Deep Security Best Practices Guide

https://help.deepsecurity.trendmicro.com/11_0/on-premise/best-practice-guide.html

Portal licenciamiento Trend Micro

https://clp.trendmicro.com

Portal Web Reputation

https://global.sitesafety.trendmicro.com/

Portal de soporte de Trend Micro

https://success.trendmicro.com

10.ABREVIATURAS

CENSUS	BBDD de prevalencia de Trend Micro
CLP	*Customer Licensing Portal* (portal de licenciamiento de Trend Micro)
CSR	*Certificate Signing Request*
DSA	*Deep Security Agent*
DSM	*Deep Security Manager*
DSRA	*Deep Security Relay Agent*
ENS	Esquema Nacional de Seguridad.
GRID	BBDD de software legítimo (Lista Blanca) de Trend Micro
SGBD	Sistema Gestor de Base de Datos
SPN	*Smart Protection Network*
SPS	*Smart Protection Server*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL