UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

CONSOLIDADO DE SUBSANACIONES A LA EVALUACIÓN INICIAL AL PLIEGO DE CONDICIONES CONVOCATORIA No 007 DE 2026 "ADQUIRIR UNA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA ANTE CIBERAMENAZAS A NIVEL DE RED, QUE GARANTICE LA ADMINISTRACIÓN Y ANALÍTICA DE TRÁFICO CENTRALIZADA, INTEGRACIÓN CON LA INFRAESTRUCTURA DE SEGURIDAD ACTUAL DE LA UNIVERSIDAD, CAPACIDADES DE VISIBILIDAD, MONITOREO Y CORRELACIÓN DE EVENTOS PARA ENDPOINTS ESTRATÉGICOS, INCLUYENDO LOS COMPONENTES DE HARDWARE Y SOFTWARE NECESARIOS PARA SU IMPLEMENTACIÓN, CONFIGURACIÓN Y OPERACIÓN ON PREMISE, SOPORTE TÉCNICO ESPECIALIZADO 7X24 Y GARANTÍA".

OBSERVACIONES REALIZADAS POR LA EMPRESA HEIMCORE SAS NIT: 900.425.697-2 DIRECCIÓN: CALLE 98 NO. 70 - 91 OF 202 EDIFICIO VARDI CORREO ELECTRÓNICO: info@heimcore.com.co NÚMERO DE TELÉFONO: 300 3764569 / 300 8025736 / 601 5804352 / 3186267462

OBSERVACIÓN No. 1

1. **Ítem 6. La solución deberá permitir el almacenamiento y consulta de eventos, alertas, registros y telemetría histórica por un periodo mínimo de noventa (90) días, conforme a la arquitectura ofertada.**

   Respuesta Heimcore: *CUMPLE. XDR for Networks, p. 2 · DDD, pp. 419–421*

   Cómo cumple: *Se configura una política de conservación mínima de 90 días para eventos, alertas y telemetría en Deep Discovery Director, con el almacenamiento dimensionado en las máquinas virtuales de la solución.*

   Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

   Subsanación Heimcore:
   Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) (ambos incluidos en la oferta inicial) son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

   Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

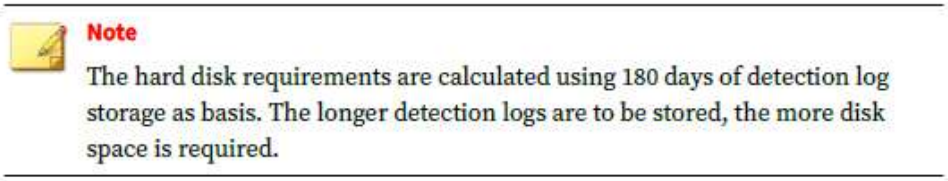
   Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona

   Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia

múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "Se configura una política de conservación mínima de 90 días para eventos, alertas y telemetría en Deep Discovery Director, con el almacenamiento dimensionado en las máquinas virtuales de la solución."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que el cálculo de retención de telemetría son 180 días. Página 2-4



Note

The hard disk requirements are calculated using 180 days of detection log storage as basis. The longer detection logs are to be stored, the more disk space is required.

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. HEIMCORE aclaró la inquietud de la Universidad según la cual "se ofertó la versión 7.0 para *Deep Discovery Inspector (DDI)* y se anexó documentación de la versión 5.5 para *Deep Discovery Director (DDD) v5.5 patch 2*", porque Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) son productos diferentes con ciclos y numeraciones independientes. Sin embargo, al revisar la página oficial de Trend Micro sobre las últimas versiones de Depp Discovery Director, se evidencia que la última versión lanzada y estable es la Deep Discovery Director 5.6. (https://docs.trendmicro.com/en-us/documentation/deep-discovery-director/)

Por otra parte, el punto 1 de la Adenda No. 1 de la Convocatoria Pública Nro. 007-2026, indica que el software ofertado no debe tener estado de fin de vida (EOL) ni fin de soporte (EOS) inferior a (2) años, sin embargo, el Deep Discovery Director versión 5.5 se encuentra en estado "End-of-Sale" y fin de vida para el "31 de julio del 2027" (https://success.trendmicro.com/en-US/solution/KA-0004690?utm_source=chatgpt.com), situación que no cumple con el requerimiento de la universidad.

El requerimiento se cumple en *Deep Discovery Director (DDD) 5.5*, sin embargo, esta versión no cumple con el requerimiento de periodo de estado de fin de vida (EOL) y fin de soporte (EOS) solicitado por la universidad.

OBSERVACIÓN No. 2

2. **Ítem 13. La solución deberá permitir configuraciones orientadas a garantizar que la información analizada y los eventos de seguridad permanezcan bajo control y administración de la Universidad, conforme a las políticas institucionales de seguridad de la información.**

Respuesta Heimcore: *CUMPLE. DDI Datasheet, pp. 1–2 · DDD, pp. 25–29*

Cómo cumple: La inspección NDR, configuración y administración se ejecutan en los appliances y VMs controlados por la Universidad; los servicios XDR/Sandbox se conectan mediante canales seguros y políticas institucionales de tratamiento de datos.

Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

Subsanación Heimcore:
Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) (ambos incluidos en la oferta inicial) son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "La inspección NDR, configuración y administración se ejecutan en los appliances y VMs controlados por la Universidad; los servicios XDR/Sandbox se conectan mediante canales seguros y políticas institucionales de tratamiento de datos."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución NDR ofertada permanece bajo control de la Universidad. Página 9-30

On-Premises Specific Screens

The following configuration screens display on the management console when Deep Discovery Director (Consolidated Mode) is integrated with a Deep Discovery Director (Internal Network Analytics Version) server operating in Deep Discovery Director (Standalone Network Analytics Mode).

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD:
No se acepta la observación. HEIMCORE aclaró la inquietud de la Universidad según la cual "se ofertó la versión 7.0 para *Deep Discovery Inspector (DDI)* y se anexó documentación de la versión 5.5 para *Deep Discovery Director (DDD) v5.5 patch 2*", porque Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) son productos diferentes con ciclos y numeraciones independientes. Sin embargo, al revisar la página oficial de Trend Micro sobre las ultimas versiones de Depp Discovery Director, se evidencia que la última versión lanzada y estable es la Deep Discovery Director 5.6. (https://docs.trendmicro.com/en-us/documentation/deep-discovery-director/)

Por otra parte, el punto 1 de la Adenda No. 1 de la Convocatoria Pública Nro. 007-2026, indica que el software ofertado no debe tener estado de fin de vida (EOL) ni fin de soporte (EOS) inferior a (2) años, sin embargo, el Deep Discovery Director versión 5.5 se encuentra en estado "End-of-Sale" y fin de vida para el "31 de julio del 2027" (https://success.trendmicro.com/en-US/solution/KA-0004690?utm_source=chatgpt.com), situación que no cumple con el requerimiento de la universidad.

Además, el requerimiento no se cumple, la documentación aportada evidencia la existencia de componentes on premise, pero no demuestra de forma integral que la información analizada, los eventos de seguridad y la telemetría utilizada por todas las capacidades obligatorias permanezcan bajo control y administración de la Universidad. Esto teniendo en cuenta que la solución ofertada utiliza servicios *SaaS/Vision One*.

OBSERVACIÓN No. 3

3. **Ítem 17. La solución debe contar con capacidades centralizadas de investigación y correlación de eventos que permitan analizar la telemetría de red y la información asociada a los activos monitoreados por la solución, incluyendo el análisis del tráfico de red relacionado con protocolos de correo electrónico cuando este sea visible a nivel de red.**

   CUMPLE. DDD, pp. 27–29 y 171–173 · XDR for Networks, pp. 1–2

   Cómo cumple: *Deep Discovery Director consolida detecciones, telemetría de red, activos y protocolos visibles, incluidos los asociados al correo electrónico.*

   Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

   Subsanación Heimcore:

Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) (ambos incluidos en la oferta inicial) son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "Deep Discovery Director consolida detecciones, telemetría de red, activos y protocolos visibles, incluidos los asociados al correo electrónico."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución cuenta con capacidades de investigación y correlación de eventos para analizar la telemetría de red, incluso con protocolos de correo electrónico Página 1-2

About Deep Discovery Director (Consolidated Mode)

Trend Micro Deep Discovery Director is a management solution that enables the following:

- Centralized deployment of hotfixes, critical patches, firmware, and Virtual Analyzer images
- Configuration replication
- Log aggregation
- Realtime threat detection monitoring and correlation
- Threat intelligence management and sharing

To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options.

Deep Discovery Director also supports out-of-the-box integration with Deep Discovery Analyzer, Deep Discovery Email Inspector, Deep Discovery Inspector, Deep Discovery Web Inspector, and Deep Discovery Director - Network Analytics.

Deep Discovery Inspector log aggregation	Deep Discovery Director (Consolidated Mode) aggregates Deep Discovery Inspector detection logs. Using the same intuitive multi-level format, the Deep Discovery Director (Consolidated Mode) management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.
Deep Discovery Email Inspector log aggregation	Deep Discovery Director (Consolidated Mode) aggregates Deep Discovery Email Inspector detection, email message tracking and MTA logs. Using the same intuitive multi-level format that Deep Discovery Email Inspector users are accustomed to, the Deep Discovery Director (Consolidated Mode) management console provides real-time threat visibility and analysis.

Appliance logs	The **Logs** screen where users can find Deep Discovery appliance related logs such as **Email Message Tracking**, **MTA**, and **Message Queue** logs.
Syslog	The **Syslog** screen allows Deep Discovery Director (Consolidated Mode) to send suspicious objects lists and detection and appliance related logs in CEF and LEEF to up to three **Syslog** servers.
System alerts	Administrators can view the details of triggered alerts directly on the management console. Custom rules can be created to be alerted of specific threats.
Reports	Deep Discovery Director (Consolidated Mode) can generate scheduled and on-demand **Network Security** and **Email Security** reports.
Simple Network Management Protocol	Deep Discovery Director (Consolidated Mode) supports Simple Network Management Protocol (SNMP) and can use it to send SNMP trap messages to notify administrators about events that require attention, and to listen to SNMP manager requests for system information and status updates.

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Si bien se evidencia que *Deep Discovery Director (DDD)* es el componente de administración y centralización de la solución, con capacidades de despliegue centralizado, replicación de configuraciones, agregación de logs, monitoreo y correlación de detecciones en tiempo real, así como gestión de inteligencia de amenazas. La versión de *Deep Discovery Director (DDD)* ofertada no cumple con el requerimiento de estado de fin de vida (EOL) y fin de soporte (EOS) requeridos por la universidad.

OBSERVACIÓN No. 4

4. **Ítem 17. La solución debe contar con capacidades centralizadas de investigación y correlación de eventos que permitan analizar la telemetría de red y la información asociada a los activos monitoreados por la solución, incluyendo el análisis del tráfico de red relacionado con protocolos de correo electrónico cuando este sea visible a nivel de red.**

Respuesta Heimcore: *CUMPLE. DDD, pp. 27–29 · Conexión directa DDI*

Cómo cumple: *Dos instancias virtuales de Deep Discovery Director se implementan en HA y consolidan lógicamente la administración y el análisis de los DDI de Calle 40 y Bosa Porvenir.*
Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

Subsanación Heimcore:
Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) (ambos incluidos en la oferta) son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "Dos instancias virtuales de Deep Discovery Director se implementan en HA y consolidan lógicamente la administración y el análisis de los DDI de Calle 40 y Bosa Porvenir.."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución cuenta con capacidades de investigación y correlación de eventos para analizar la telemetría de red, incluso con protocolos de correo electrónico Página 1-2.

About Deep Discovery Director (Consolidated Mode)

Trend Micro Deep Discovery Director is a management solution that enables the following:

- Centralized deployment of hotfixes, critical patches, firmware, and Virtual Analyzer images
- Configuration replication
- Log aggregation
- Realtime threat detection monitoring and correlation
- Threat intelligence management and sharing

To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options.

Deep Discovery Director also supports out-of-the-box integration with Deep Discovery Analyzer, Deep Discovery Email Inspector, Deep Discovery Inspector, Deep Discovery Web Inspector, and Deep Discovery Director - Network Analytics.

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Si bien se evidencia que *Deep Discovery Director (DDD)* es el componente de administración y centralización de la solución, con capacidades de despliegue centralizado, replicación de configuraciones, agregación de logs, monitoreo y correlación de detecciones en tiempo real, así como gestión de inteligencia de amenazas. La versión de *Deep Discovery Director (DDD)* ofertada no cumple con el requerimiento de estado de fin de vida (EOL) y fin de soporte (EOS) requeridos por la universidad.

OBSERVACIÓN No. 5

5. **Ítem 20. La solución deberá permitir esquemas de alta disponibilidad (HA) para los componentes críticos de administración, análisis y procesamiento, incorporando mecanismos de redundancia, failover y continuidad operativa que minimicen la interrupción del servicio ante fallos de hardware o software**

CUMPLE. DDI Datasheet, p. 2 · Deep Discovery Director, pp. 25–29 y 426–427

Cómo cumple: *La administración central se despliega con Deep Discovery Director virtual en HA. Los appliances incorporan RAID y fuentes redundantes, y se configuran respaldo, restauración y procedimiento documentado de continuidad operativa.*

Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

Subsanación Heimcore:
*Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) (**ambos incluidos en la oferta inicial**) son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.*

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "La administración central se despliega con Deep Discovery Director virtual en HA. Los appliances incorporan RAID y fuentes redundantes, y se configuran respaldo, restauración y procedimiento documentado de continuidad operativa."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución cuenta con capacidades de investigación y correlación de eventos para analizar la telemetría de red, incluso con protocolos de correo electrónico Página 6-4

TABLE 6-1. Directory Object Types

OBJECT	DISPLAYED INFORMATION
Appliances	• **Plan**: Plans that were or will be deployed to the appliance • **Appliance**: Identifiers such as IP address, virtual IP address, host name and display name, threat intelligence sync times, file password sync time, and other information **Note** For Deep Discovery Analyzer clusters, Deep Discovery Director (Consolidated Mode) also displays the following: • **Active primary appliance**: Information on the active primary appliance (high availability cluster and load balancing cluster) • **Passive primary appliance**: Information on the passive primary appliance (high availability cluster) • **Secondary appliances**: Information on the secondary appliance (load balancing cluster)

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. HEIMCORE aclaró la inquietud de la universidad según la cual "se ofertó la versión 7.0 para *Deep Discovery Inspector (DDI)* y se anexó documentación de la versión 5.5 para *Deep Discovery Director (DDD) v5.5 patch 2*", porque Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) son productos diferentes con ciclos y numeraciones independientes. Sin embargo, al revisar la pagina oficial de Trend Micro sobre las ultimas versiones de Depp Discovery Director, se evidencia que la última versión lanzada y estable es la Deep Discovery Director 5.6. (https://docs.trendmicro.com/en-us/documentation/deep-discovery-director/).

Por otra parte, el punto 1 de la Adenda No. 1 de la Convocatoria Pública Nro. 007-2026, indica que el software ofertado no debe tener estado de fin de vida (EOL) ni fin de soporte (EOS) inferior a (2) años, sin embargo, el Deep Discovery Director versión 5.5 se encuentra en estado "End-of-Sale" y fin de vida para el "31 de julio del 2027" (https://success.trendmicro.com/en-US/solution/KA-0004690?utm_source=chatgpt.com), situación que no cumple con el requerimiento de la universidad.

Finalmente, la subsanación acredita HA para *Deep Discovery Director (DDD)*, así como mecanismos de redundancia de hardware, respaldo y restauración; sin embargo, estos elementos no demuestran el *failover* del servicio de análisis y procesamiento hacia un nodo alterno. Adicionalmente, la evidencia presentada sobre *Active Primary/Passive Primary* corresponde a *Deep Discovery Analyzer* y no acredita HA para *Deep Discovery Inspector (DDI)* ni para los demás componentes ofertados.

OBSERVACIÓN No. 6

6. **Ítem 24. La solución deberá permitir la administración centralizada de políticas, eventos, tareas y reportes mediante una consola unificada de gestión.**

Respuesta Heimcore: *CUMPLE. DDD, pp. 27–29 y 257–263 · Conexión directa DDI*

Cómo cumple: *Deep Discovery Director centraliza appliances, políticas, eventos, tareas y reportes; unifica la investigación XDR de red y endpoint.*

Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

Subsanación Heimcore:
Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) ambos incluidos en la oferta inicial, son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "Deep Discovery Director centraliza appliances, políticas, eventos, tareas y reportes; unifica la investigación XDR de red y endpoint."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución cuenta con capacidades de administración centralizada y una única consola Página 4 y 1-2

automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

About Deep Discovery Director (Consolidated Mode)

Trend Micro Deep Discovery Director is a management solution that enables the following:

- Centralized deployment of hotfixes, critical patches, firmware, and Virtual Analyzer images
- Configuration replication
- Log aggregation
- Realtime threat detection monitoring and correlation
- Threat intelligence management and sharing

To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options.

Deep Discovery Director also supports out-of-the-box integration with Deep Discovery Analyzer, Deep Discovery Email Inspector, Deep Discovery Inspector, Deep Discovery Web Inspector, and Deep Discovery Director - Network Analytics.

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La subsanación permite verificar que *Deep Discovery Director (DDD)* proporciona una consola centralizada para la administración de los componentes de la solución, incluyendo la gestión de configuraciones, eventos, tareas, detecciones y reportes. Sin embargo, la versión de *Deep Discovery Director (DDD)* ofertada no cumple con el requerimiento de estado de fin de vida (EOL) y fin de soporte (EOS) requeridos por la universidad.

OBSERVACIÓN No. 7

7. **Ítem 34. La solución debe permitir el acceso a plataformas analíticas de inteligencia de amenazas que proporcionen contexto ampliado sobre indicadores, infraestructura asociada y relaciones entre objetos.**

Respuesta Heimcore: *CUMPLE. DDD, pp. 171–173 y 214–215*

Cómo cumple: *Deep Discovery Director ofrece gráficos de correlación e Intelligence Reports para consultar relaciones entre indicadores, infraestructura y objetos.*

Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

Subsanación Heimcore:
Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) ambos incluidos en la oferta inicial, son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS). Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "Deep Discovery Director ofrece gráficos de correlación e Intelligence Reports para consultar relaciones entre indicadores, infraestructura y objetos."

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución cuenta con gráficos de correlación llamados Intelligence Reports para consultar relaciones entre indicadores, infraestructura y objetos Página 1-6 y A-4

Web API access	Deep Discovery Director (Consolidated Mode) now allows the creation of user accounts that are only allowed system access via web API. Web API can be used to automate certain threat intelligence related tasks.

SERVICE	DESCRIPTION	ADDRESS AND PORT	NOTES
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the TrendAI™ Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.	ddd55.threatconnect.trendmicro.com:443	Related to product version

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La subsanación permite verificar que *Deep Discovery Director (DDD)* cuenta con capacidades de inteligencia de amenazas mediante la correlación de objetos sospechosos y datos de amenazas, generando *Intelligence Reports* que permiten ampliar el contexto y analizar las relaciones entre indicadores, infraestructura y objetos. Sin embargo, la versión de *Deep Discovery Director (DDD)* ofertada no cumple con el requerimiento de estado de fin de vida (EOL) y fin de soporte (EOS) requeridos por la universidad.

OBSERVACIÓN No. 8

8. **Ítem 40. La solución deberá contar con la capacidad de integrarse con las herramientas de seguridad existentes en la Universidad Distrital, incluyendo el firewall de Palo Alto Networks (NGFW 3420), el EDR de Kaspersky y la plataforma de monitoreo y gestión de eventos SolarWinds Security Event Manager (SEM).**

CUMPLE. DDI AG, pp. 326–327 · DDI AG, pp. 343–345

Cómo cumple: *Palo Alto se integra de forma nativa para respuesta; SolarWinds SEM recibe CEF/LEEF; Kaspersky convive con Endpoint Sensor y su interoperabilidad se valida mediante piloto y matriz de exclusiones.*

Evaluación Universidad: *De acuerdo con el ítem 50, la convivencia del agente EDR Kaspersky con el endpoint ofrecido no demuestra por sí sola una integración funcional entre ambas plataformas, ya que esta debería ser validada mediante pruebas piloto.*

Subsanación Heimcore:

Heimcore se permite aclarar que, aparte de la manera mencionada en la respuesta del Anexo Técnico, la solución ofertada se integra con la herramienta EDR de Kaspersky mediante diferentes evidencias verificables.

Por un lado, desde el punto de vista del fabricante Kaspersky, en su documentación oficial, indica que sus soluciones de Endpoint se integran con Trend Micro, lo cual se puede verificar en el siguiente enlace https://support.kaspersky.com/kes-for-windows/12.8/257253

- **Trend Micro**

  EDR Agent is compatible with Trend Micro Apex One version 14.0.12994 or later (including Security Agent).

  EDR Agent is compatible with Trend Micro Deep Security version 20.0.1 or later (including Security Agent).

Por otro lado, desde la perspectiva del fabricante ofertado Trend Micro, se puede verificar mediante dos enlaces públicos la compatibilidad probada y homologada que exige el pliego de condiciones https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-security-solutions-auto-uninstall#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-smlyef

- Kaspersky Endpoint Security 10 for Windows 10.1.0.867 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.1.23 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.1.23 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.1.23 x86
- Kaspersky Endpoint Security 10 for Windows 10.2.2.10535 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.2.10535 x86
- Kaspersky Endpoint Security 10 for Windows Server 10.0.0.486 x64
- Kaspersky Endpoint Security 10 for Windows x64
- Kaspersky Endpoint Security 10 for Windows x64
- Kaspersky Endpoint Security 10 for Windows x86
- Kaspersky Endpoint Security 10.3.0.6294 x86 x64
- Kaspersky Endpoint Security 11 for Windows 11.0.0.6499 x64

- Kaspersky Internet Security 2013 13.0.1.4190
- Kaspersky Lab Network Agent 8.0.2177
- Kaspersky Network Agent 10.1.249
- Kaspersky Network Agent 6.0.1405
- Kaspersky Network Agent 6.0.1591

Por último, compartimos otro enlace donde indica cuales son los terceros sobre los cuales la solución puede integrarse para colección de logs, que en efecto, es lo que requiere el pliego de condiciones y Anexo Técnico https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-__log-vendors-products-2

Third-Party Log Collection supported vendors and products

View a partial list of the supported vendors and products for third-party log ingestion.

Logs from any product that can send logs in Syslog format (including CEF and LEEF formats) can be ingested into TrendAI Vision One™ via **collectors** connected to **log repositories** in **Third-Party Log Collection**. To ingest log data from products that do not support Syslog format or do not have dedicated connectors or integrations in TrendAI Vision One™, you must first convert the logs to Syslog format before forwarding the data to TrendAI Vision One™.

Vendor	Product
Kaspersky	• AV • Endpoint

Para Kaspersky se integra tanto con la solución de Antivirus como con la de EDR.

Por otro lado, es importante aclarar que, el agente ofertado se despliega en la configuración "Endpoint Sensor only" (XDR for Endpoints / EDR) de Endpoint Security. En esta configuración, el agente no instala ni habilita motor de Anti-Malware, Web Reputation, Intrusion Prevention, Application Control, Device Control, Firewall, Integrity Monitoring ni Log Inspection.

Por lo tanto, no existe duplicidad de funciones de prevención en tiempo real con Kaspersky Endpoint Security (EPP), y consecuentemente no se produce el conflicto típico de dos motores antimalware compitiendo por el mismo punto de interceptación del sistema de archivos.

El modelo de operación del sensor es de telemetría y observación: recolecta eventos de proceso, archivo, registro, red, sesión y línea de comandos, y los envía a la plataforma para correlación XDR. No compite por la cadena de decisión de bloqueo, que sigue siendo responsabilidad exclusiva de Kaspersky EPP.

Por esta razón, aclarando que la solución se integra mediante soluciones validadas por cada fabricante, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. La subsanación permite verificar que el agente ofertado puede operar en modalidad *Sensor Only*, orientada a la recolección de telemetría y visibilidad, sin habilitar funciones de protección que puedan generar duplicidad con el *Kaspersky Endpoint Security* instalado en los equipos de la Universidad Distrital. Adicionalmente, se aporta documentación de los fabricantes que evidencia la compatibilidad entre las soluciones.

OBSERVACIÓN No. 9

9. **Ítem 50. Los mecanismos utilizados para la recolección de telemetría y visibilidad sobre los endpoints no deberán interferir ni generar conflictos con las soluciones de seguridad existentes en la infraestructura institucional, incluyendo antivirus, EDR u otras herramientas de protección de endpoints, garantizando la convivencia operativa sobre los equipos monitoreados.**

CUMPLE. Endpoint Security, pp. 2–3

Cómo cumple: *Se ejecuta un piloto de convivencia con Kaspersky EDR, se definen exclusiones mutuas y se despliega progresivamente el Endpoint Sensor sin desactivar la protección institucional.*

Evaluación Universidad: Aunque un piloto puede ser adecuado, este no constituye por sí mismo evidencia verificable de que el requisito se cumpla al momento de la evaluación, por lo que no permite determinar de manera objetiva si, a futuro, existirá una adecuada coexistencia y compatibilidad entre el EDR Kaspersky actualmente implementado y la solución ofrecida.

Adicionalmente, debido al cronograma del proceso, no resulta viable la ejecución de pilotos durante la etapa de evaluación, teniendo en cuenta que, una vez adjudicado el contrato, se dará inicio al proceso de implementación y no de pruebas.

Subsanación Heimcore:
Heimcore se permite aclarar que, aparte de la manera mencionada en la respuesta del Anexo Técnico, la solución ofertada se integra con la herramienta EDR de Kaspersky mediante diferentes evidencias verificables.

Por un lado, desde el punto de vista del fabricante Kaspersky, en su documentación oficial, indica que sus soluciones de Endpoint se integran con Trend Micro, lo cual se puede verificar en el siguiente enlace https://support.kaspersky.com/kes-for-windows/12.8/257253

- **Trend Micro**

  EDR Agent is compatible with Trend Micro Apex One version 14.0.12994 or later (including Security Agent).

  EDR Agent is compatible with Trend Micro Deep Security version 20.0.1 or later (including Security Agent).

Por otro lado, desde la perspectiva del fabricante ofertado Trend Micro, se puede verificar mediante dos enlaces públicos la compatibilidad probada y homologada que exige el pliego de condiciones

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-security-solutions-auto-uninstall#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-smlyef

- Kaspersky Endpoint Security 10 for Windows 10.1.0.867 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.1.23 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.1.23 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.1.23 x86
- Kaspersky Endpoint Security 10 for Windows 10.2.2.10535 x64
- Kaspersky Endpoint Security 10 for Windows 10.2.2.10535 x86
- Kaspersky Endpoint Security 10 for Windows Server 10.0.0.486 x64
- Kaspersky Endpoint Security 10 for Windows x64
- Kaspersky Endpoint Security 10 for Windows x64
- Kaspersky Endpoint Security 10 for Windows x86
- Kaspersky Endpoint Security 10.3.0.6294 x86 x64
- Kaspersky Endpoint Security 11 for Windows 11.0.0.6499 x64
- Kaspersky Internet Security 2013 13.0.1.4190
- Kaspersky Lab Network Agent 8.0.2177
- Kaspersky Network Agent 10.1.249
- Kaspersky Network Agent 6.0.1405
- Kaspersky Network Agent 6.0.1591

Por último, compartimos otro enlace donde indica cuales son los terceros sobre los cuales la solución puede integrarse para colección de logs que, en efecto, es lo que requiere el pliego de condiciones y Anexo Técnico https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-__log-vendors-products-2

Third-Party Log Collection supported vendors and products

View a partial list of the supported vendors and products for third-party log ingestion.

Logs from any product that can send logs in Syslog format (including CEF and LEEF formats) can be ingested into TrendAI Vision One™ via **collectors** connected to **log repositories** in **Third-Party Log Collection**. To ingest log data from products that do not support Syslog format or do not have dedicated connectors or integrations in TrendAI Vision One™, you must first convert the logs to Syslog format before forwarding the data to TrendAI Vision One™.

Vendor	Product
Kaspersky	• AV • Endpoint

Para Kaspersky se integra tanto con la solución de Antivirus como con la de EDR.

Adicionalmente, es importante aclarar que, el agente ofertado se despliega en la configuración "Endpoint Sensor only" (XDR for Endpoints / EDR) de Endpoint Security. En esta configuración, el agente no instala ni habilita motor de Anti-Malware, Web Reputation, Intrusion Prevention, Application Control, Device Control, Firewall, Integrity Monitoring ni Log Inspection.

Por lo tanto, no existe duplicidad de funciones de prevención en tiempo real con Kaspersky Endpoint Security (EPP), y consecuentemente no se produce el conflicto típico de dos motores antimalware compitiendo por el mismo punto de interceptación del sistema de archivos.

El modelo de operación del sensor es de telemetría y observación: recolecta eventos de proceso, archivo, registro, red, sesión y línea de comandos, y los envía a la plataforma para correlación XDR. No compite por la cadena de decisión de bloqueo, que sigue siendo responsabilidad exclusiva de Kaspersky EPP.

Por esta razón, aclarando que la solución se integra mediante soluciones validadas y evidencias verificables por cada fabricante, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. La subsanación permite verificar que el agente ofertado puede operar en modalidad *Sensor Only*, orientada a la recolección de telemetría y visibilidad, sin habilitar funciones de protección que puedan generar duplicidad con el *Kaspersky Endpoint Security* instalado en los equipos de la Universidad Distrital. Adicionalmente, se aporta documentación de los fabricantes que evidencia la compatibilidad entre las soluciones.

OBSERVACIÓN No. 10

10. **Ítem 80. La solución debe ser capaz de recibir entradas para indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA) para clasificar y analizar eventos**.

Respuesta Heimcore: *CUMPLE. DDD, pp. 214–215 · DDI AG, pp. 263–264 · Conexión directa DDI*

Cómo cumple: *Los IoC se ingresan mediante objetos sospechosos/STIXTAXII y los IOA se aplican desde las capacidades analíticas XDR para clasificar y correlacionar eventos.*

Evaluación Universidad: *El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.*

Subsanación Heimcore:
Heimcore se permite aclarar que Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) ambos incluidos en la oferta inicial, son dos productos diferentes, independientes y complementarios, que cumplen funciones distintas dentro de la arquitectura de detección de amenazas avanzadas de Trend Micro.

Deep Discovery Inspector (DDI) v7.0 es el appliance sensor de inspección de red. Se despliega out-of-band (fuera de línea, mediante puerto espejo/SPAN o TAP), por lo que no interrumpe el tráfico. Analiza tráfico este-oeste y norte-sur para detectar amenazas avanzadas, APTs y ataques dirigidos, incluye motor de análisis Virtual Analyzer (sandbox) y genera detecciones, alertas y reportes. Es el componente que detecta.

Deep Discovery Director (DDD) v5.5 patch 2 es la consola de gestión y orquestación centralizada de la familia Deep Discovery. No inspecciona tráfico por sí mismo; su función es administrar múltiples appliances (DDI, Deep Discovery Analyzer, Deep Discovery Email Inspector), ejecutando: despliegue centralizado de hotfixes, critical patches y firmware; replicación de configuraciones entre appliances; consolidación de detecciones, dashboards y reportes; y gestión y distribución de inteligencia de amenazas (objetos sospechosos, feeds STIX/TAXII 1.x, 2.0/2.1, OpenDXL y Web Service HTTP/HTTPS).

Es el componente que gestiona y correlaciona.

Por tratarse de productos con líneas de desarrollo independientes, cada uno mantiene su propia numeración de versión y su propio calendario de liberación. DDD está diseñado con compatibilidad hacia múltiples versiones de los appliances gestionados de forma simultánea (por ejemplo, puede administrar appliances DDI de distintas versiones al mismo tiempo). Por lo tanto, DDD v5.5 patch 2 y DDI v7.0 son las versiones vigentes de cada producto respectivamente y operan de forma integrada.

En conclusión, por parte de Heimcore aclaramos que, en el ítem 12 incluimos la última versión de Deep Discovery Inspector (DDI) v7.0 y, mediante aclaración, indicamos que la última versión estable de Deep Discovery Director (DDD) el cual también fue ofertado tanto en el ítem 12 como en la respuesta del ítem 6 calificado inicialmente como "no cumple" es la v5.5 patch 2, de la cual nos permitimos adjuntar nuevamente la documentación correspondiente y la manera en la que cumple es la misma que indicamos en el Anexo Técnico. "Los IoC se ingresan mediante objetos sospechosos/STIXTAXII y los IOA se aplican desde las capacidades analíticas XDR para clasificar y correlacionar eventos." Sin embargo, como se indica en la respuesta inicial, los IOA se aplican desde las capacidades analíticas XDR para clasificar y correlacionar eventos, es decir desde otra solución que no es DDD, la cual también está incluida en la oferta.

Por último, nos permitimos añadir otra página del mismo documento donde se indica que que la solución cuenta con gestión de Indicadores de Compromiso e indicadores de ataque (Attack Patterns) Página 4-127

Analysis Using the Transaction and IOC Details

The **Transaction and IOC Details** section provides information about transactions and IOCs from the **Correlation Graph** section.

The oldest transactions are listed first. IOCs are listed by highest risk level first and then by first seen time.

Procedure

- Scroll through the **Transactions** and **IOCs** lists to identify information useful for analysis.
- Click on a correlation line in the **Correlation Graph** section to display a summary and to filter and limit the transactions and IOCs that are displayed in the **Transaction and IOC Details** section to ones that are directly related to the selected correlation line.

Tip
Click on an empty space in the **Correlation Graph** section to remove the filter.

- Click on an internal host, external server, or email sender in the **Correlation Graph** section to display details about the selected internal host, external server, or email sender in the **Transaction and IOC Details** section.

Tip
Click on an empty space in the **Correlation Graph** section to revert the **Transaction and IOC Details** section back to normal.

- Perform one of the following actions on **Transaction and IOC Details** section items:

3. Use the following sections for advanced analysis of malicious activity:
   - **Summary**

     Displays the severity, the number of detected internal hosts and Indicators of Compromise (IOCs), the assigned attack patterns, and provides a high-level overview of the malicious activity of the correlation data.

Por esta razón, entendiendo que es un tema de interpretación de dos diferentes productos, solicitamos muy amablemente se evalúe nuestra oferta como Cumple Técnicamente.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. HEIMCORE logra aclarar la inquietud de la Universidad según la cual "se ofertó la versión 7.0 para *Deep Discovery Inspector (DDI)* y se anexó documentación de la versión 5.5 para *Deep Discovery Director (DDD) v5.5 patch 2*", porque Deep Discovery Inspector (DDI) y Deep Discovery Director (DDD) son productos diferentes con ciclos y numeraciones independientes. Sin embargo, al revisar la pagina oficial de Trend Micro sobre las ultimas versiones de Depp Discovery Director, se evidencia que la última versión lanzada y estable es la Deep Discovery Director 5.6. (https://docs.trendmicro.com/en-us/documentation/deep-discovery-director/)

Por otra parte, el punto 1 de la Adenda No. 1 de la Convocatoria Pública Nro. 007-2026, indica que el software ofertado no debe tener estado de fin de vida (EOL) ni fin de soporte (EOS) inferior a (2) años, sin embargo, el Deep Discovery Director versión 5.5 se encuentra en estado "End-of-Sale" y fin de vida para el "31 de julio del 2027" (https://success.trendmicro.com/en-US/solution/KA-0004690?utm_source=chatgpt.com), situación que no cumple con el requerimiento de la universidad.

Al revisar nuevamente el requerimiento, se confirma que no se cumple, la evidencia presentada describe el análisis y gestión de IoC e indicadores de ataque, pero no demuestra la capacidad de crear o importar indicadores de ataque (IOA) personalizados como entradas para la clasificación y análisis de eventos, que es lo requerido en el ítem.

OBSERVACIONES REALIZADAS POR LA EMPRESA GRUPO MICROSISTEMAS COLOMBIA S.A.S. NIT: 900.418.656-1 DIRECCIÓN: TRANSVERSAL 22 # 98 - 82, OFICINA 501-502 CORREO ELECTRÓNICO: adriana.alfonso@gmsseguridad.com NÚMERO DE TELÉFONO: 6017433559

OBSERVACIÓN 1:

1. **ÍTEM 10: Especificaciones técnicas - Patch cord dúplex de fibra óptica LC/LC:**
   - **Debe contar con las siguientes características:**
     - **OM4 u OM5.**
     - **Longitud de Onda mínimo de 850/1300 nm.**
     - **Longitud 2.0 metros con conector LC-LC**
     - **Tipo: Uniboot ó Zip-cord**
     - **Cincuenta y Ciento Veinticinco micrones (50/125) µm.**
     - **Soportar 10G hasta 550 metros y 1Gbps hasta 1100 metros, certificados según el estándar IEEE 802.3ae.**
   - **Los conectores deben cumplir con los estándares de cableado como lo estipula la norma ANSI/TIA-568- 3-D**
   - **Deben ser probados para soportar velocidades de transmisión hasta de 10 Gb/s para enlaces de hasta 550m con una fuente de 850nm según los estándares IEEE 802.3ae 10 GbE.**
   - **Deben estar garantizado mínimo por 25 años.**
   - **El cable debe tener un retardante de fuego de alta calidad, libre de halógenos, no producir gases tóxicos, la chaqueta de la fibra debe ser del tipo (LSZH ó LSZH-3).**
   - **Estos deben ser elaborados por el mismo fabricante.**

- **Deben ser originales de fábrica y precertificados por el fabricante como estipula la ANSI/TIA 568.3-D, deben venir en su bolsa original de empaque tal como salen de la fábrica.**
- **Los elementos estarán identificados individualmente con el correspondiente logo de la prueba de laboratorio, de forma permanente. Serán certificados por UL ó CSA ó ETL, para garantizar que los elementos ofrecidos han sido avalados por estos laboratorios. Adicionalmente puede estár marcado con el número de la prueba de flamabilidad.**
- **Debe tener ficha técnica del fabricante del producto, con número de parte donde se pueda verificar las especificaciones y parámetros de desempeño, a través de la página web del fabricante.**

Subsanación GMS:

Mediante la presente y de conformidad con la evaluación publicada por la entidad, nos permitimos aclarar lo siguiente:

El documento punto a punto fue aceptado y firmado por el representante legal, cumpliendo con todos los requerimientos técnicos del proceso.

Nos permitimos aclarar y entregar los enlaces de los dos ítems que la entidad indico que no se cumplían:

SFP+:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html#CiscoSFP10GSRmodule.

Patch Core Siemon FJ2-LCLC5V-05AH
https://files.siemon.com/en/specsheet/siemon-xglo-and-lightsystem-jumper-and-pigtails_spec-sheet.pdf

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación.
Considerando la Nota 4 del anexo 10 del pliego de condiciones que indica "*La información suministrada por el oferente deberá ser clara, verificable y corresponder a documentación oficial del fabricante (fichas técnicas, datasheets, manuales o enlaces oficiales). No se aceptarán documentos elaborados por el oferente que no cuenten con respaldo del fabricante.*" El oferente no adjuntó la ficha técnica el fabricante en la entrega de la oferta, por lo tanto, no se puede validar una ficha técnica entregada después de la entrega de la oferta.

OBSERVACIÓN 2:

2. **ÍTEM 10: Especificaciones técnicas - SFP +**
    - **Fabricante: Cisco – Se solicita de este fabricante teniendo en cuenta que el Switch Core es de esta marca y uno diferente podría traer complicaciones en la garantía del Switch Core.**
    - **Formato: SFP-10G-SR**
    - **Velocidad: 10 Gbps**
    - **Tipo de enlace: Ethernet 10 Gigabit (10GBASE-SR)**

- **Fibra: Multimodo (MMF)**
- **Conector: LC dúplex**
- **Longitud de onda: 850 nm**
- **Alcance típico: Hasta 400 m (OM4)**

Subsanación GMS:

Mediante la presente y de conformidad con la evaluación publicada por la entidad, nos permitimos aclarar lo siguiente:

El documento punto a punto fue aceptado y firmado por el representante legal, cumpliendo con todos los requerimientos técnicos del proceso.

Nos permitimos aclarar y entregar los enlaces de los dos ítems que la entidad indico que no se cumplían:

SFP+:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html#CiscoSFP10GSRmodule.

Patch Core Siemon FJ2-LCLC5V-05AH
https://files.siemon.com/en/specsheet/siemon-xglo-and-lightsystem-jumper-and-pigtails_spec-sheet.pdf

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación.
Considerando la Nota 4 del anexo 10 del pliego de condiciones que indica "*La información suministrada por el oferente deberá ser clara, verificable y corresponder a documentación oficial del fabricante (fichas técnicas, datasheets, manuales o enlaces oficiales). No se aceptarán documentos elaborados por el oferente que no cuenten con respaldo del fabricante.*" El oferente no adjuntó la ficha técnica el fabricante en la entrega de la oferta, por lo tanto, no se puede validar una ficha técnica entregada después de la entrega de la oferta.

COMITÉ ASESOR DE CONTRATACIÓN