Comunicación de Eventos de Seguridad orientada al Análisis de Riesgos Dinámico

David López[1,2], Oscar Pastor[2], Luis Javier García Villalba[1]

[1] Grupo de Análisis, Seguridad y Sistemas (GASS)
Dto. de Ingeniería del Software e Inteligencia Artificial (DISIA)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n
Ciudad Universitaria, 28040 Madrid
Email: {dlcuenca, javiergv@fdi.ucm.es}

[2] Ingeniería de Sistemas para la Defensa de España S.A. (ISDEFE)
Dir. Defensa y Seguridad
Email: {dlcuenca, opastor@isdefe.es}

***Abstract*—Bajo el concepto de Análisis de Riesgo Dinámico, se enmarca un proceso de actualización incesante de los parámetros que intervienen en el cálculo del riesgo, para la optimización de su tratamiento posterior. En este trabajo se propone una extensión al modelo de datos IODEF orientada al Análisis de Riesgos Dinámico (IODEF-DRA). Este modelo tiene por objetivo facilitar una visión global del riesgo, a través de la integración en tiempo real y mediante comunicaciones basadas en él, de un amplio abanico de sistemas de seguridad con herramientas de Análisis de Riesgos (basadas en metodologías reconocidas). La utilidad de esta integración se refleja en el escenario presentado como prueba de concepto, donde se evidencian las posibles mejoras en los resultados del Análisis de Riesgos.**

I. Introducción

La realización de un Análisis de Riesgos (AARR) para los Sistemas de Información (SSII) de una Organización es un trabajo que requiere un esfuerzo sustancial, y que incluye la recopilación de una importante cantidad de datos sobre la estructura y activos de la información, sus interrelaciones y las amenazas que los acechan [1]–[7]. Hasta el momento, esta inversión de trabajo tiende a utilizarse puntualmente como el punto de partida para la definición de un Plan de Mitigación de Riesgos a diferentes plazos, renovándose el resultado del AARR periódicamente, en el mejor de los casos transcurrido un lapso de tiempo considerable.

Puesto que los SSII, y del mismo modo los riesgos sobre éstos, evolucionan a gran velocidad el anterior planteamiento implica que el esfuerzo invertido puede quedar desfasado, sin un adecuado seguimiento y actualización continuada del AARR. Este concepto comúnmente se enmarca bajo la denominación de Análisis de Riesgos Dinámico [8], o DRA por sus siglas en inglés. El ejemplo más extremo en este sentido, ocurre durante la materialización de una amenaza en lo que catalogaríamos como evento o incidente de seguridad. En estos casos, puntualmente o durante un periodo de tiempo según evolucione el incidente, se altera por completo el panorama del riesgo desvirtuando los resultados de AARR previos.

En la Sección II se recogen los esfuerzos hasta el momento en torno a la comunicación de eventos de seguridad, así como el modelo propuesto específicamente para la comunicación de éstos a las herramientas de AARR, enfocadas al DRA. En la Sección III se presenta una prueba de concepto de estas comunicaciones basadas en el modelo propuesto (IODEF-DRA) para un escenario predefinido. En la Sección IV se recogen las conclusiones y propuestas de trabajo futuro.

II. Modelos de Datos para Comunicación de Eventos de Seguridad

A. Antecedentes

Este campo se encuentra aún en estado de evolución, pese a haber sido foco de atención por parte de organismos de estandarización como el Internet Engineering Task Force (IETF), quién a través de su Grupo de Trabajo Extended Incident Handling (INCH WG) han realizado esfuerzos para estandarizar los flujos de información en relación a incidentes de seguridad. Estos intentos por estandarizar la manera de intercambiar información relativa a incidentes de seguridad, se han enfocado en primer lugar, al intercambio de información sobre intrusiones en SSII a través del protocolo experimental IDMEF [9], para ampliarse posteriormente hacia un formato para el intercambio de información sobre incidentes bajo el nombre de IODEF [10], fundamentalmente orientado a la cooperación entre equipos de respuesta frente a incidentes de seguridad (más conocidos como CERT o CSIRT).

Pese a ello, los intentos por estandarizar modelos de datos, orientados al intercambio de información sobre eventos de seguridad en SSII, se han mostrado fallidos debido a la complejidad y al enfoque prioritario como instrumento de uso de los CERTs [11], que ha derivado en una baja aceptación por

parte de los productos comerciales, limitándose mayoritariamente a productos de desarrollo ad-hoc para estos organismos.

B. Definición del Modelo IODEF-DRA

Aprovechando el esfuerzo acometido para llevar el modelo IODEF a un estado de madurez considerable, y de la ambición de establecerse como estándar para comunicación de incidentes de seguridad, se toma como referente, para el desarrollo de un modelo de datos específico para la transmisión de información relevante de cara al uso por sistemas de AARR metodológicos desplegados en una Organización.

La extensión propuesta toma en consideración la obligatoriedad de completar las clases que IODEF dispone como imprescindibles, estableciendo nuevas clases a contemplar en la estructura de datos. El resto de clases definidas por IODEF podrán ser opcionalmente completadas, si bien, no serían un requisito para el correcto tratamiento por parte de interfaces de AARR que se adhirieran al modelo presentado. Conforme a [12], se considerará el incidente de seguridad como un evento o conjunto de éstos (susceptibles de ser notificados a la herramienta de AARR), contrastados por los sistemas de seguridad desplegados y que inciden en la probabilidad de comprometer la seguridad de la información y las operaciones.

El formato extendido propuesto conforme las especificaciones que se detallan a continuación, se reflejaría en la Fig. 1, obviando las clases opcionales del formato IODEF, que no son extendidas por el nuevo formato.

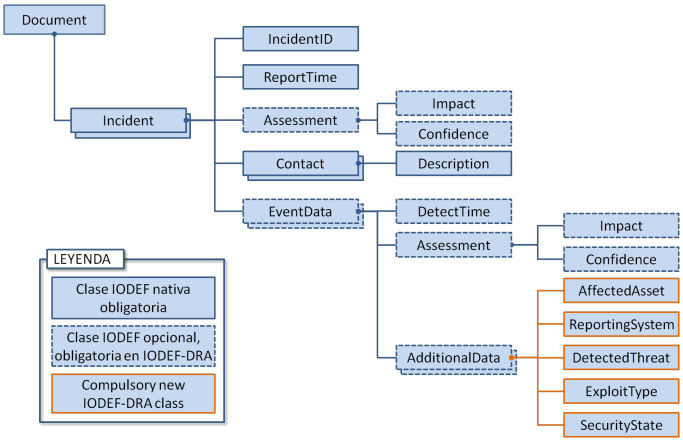

Fig. 1. Modelo IODEF extendido para AARR Dinámico (IODEF-DRA)

Como parte del evento de seguridad, se ven involucrados los siguientes factores que afectan a la evolución del riesgo, conforme a las metodologías de AARR revisadas:

- Activo afectado (**AffectedAsset**): Sería un nuevo atributo encargado de identificar el activo, de entre aquellos contemplados en el AARR, sobre el que impactaría en primera instancia el incidente de seguridad. A través de este atributo podrían identificarse mediante código alfanumérico compartido con la herramienta de AARR, aquellos activos susceptibles de sufrir un ataque.
- Amenaza detectada (**DetectedThreat**): Sería un nuevo atributo que reflejaría el tipo de amenaza relacionada con el ataque observado, en caso de que el sistema que notifique el evento sea capaz de establecer una relación entre ambos. Las amenazas a considerar podrían partir de un catálogo común con la herramienta de AARR.
- Vulnerabilidad explotada (**ExploitType**). Nuevo atributo que dependiendo del ámbito de vulnerabilidades contempladas se podría recurrir a formatos estándar, tales como CVE, NVD, OVAL, etc. en el caso de las propias de SSII.
- Estado de seguridad (**SecurityState**): Sería un nuevo atributo para definir la situación de avance en la que se encuentra el ataque o evento de seguridad, con la finalidad básica de conocer si el sistema de seguridad ha sido superado o aún mantiene al atacante bajo control, pese a que el ataque haya tenido éxito en cierta medida.
- Sistema notificador (**ReportingSystem**): Sería un nuevo atributo que identificaría el tipo de sistema que notifica el evento. Dependiendo del ámbito elegido, este podría ir desde IDs a sistemas de detección de intrusión física o CERTs colaboradores.
- Evaluación (**Assessment**): Esta clase nativa de IODEF pasaría a ser obligatoria, recogería la evaluación general del evento a través de sus componentes relativos al impacto y certidumbre, identificados a continuación.
- Impacto provocado (**Impact**): Esta clase nativa de IODEF pasaría a ser obligatoria, colgando de la clase Assessment que también debería aparecer como atributo asociado al evento. Permitiría definir a través de sus atributos asociados la severidad y estado de consumación del ataque, estimados por el sistema de seguridad que detectó y transmitió el evento.
- Nivel de certidumbre (**Confidence**): Esta clase nativa de IODEF también dependiente de Assessment, pasaría a ser igualmente obligatoria. El sistema de seguridad facilitaría una evaluación relativa a la probabilidad de que la notificación sea debida a un falso positivo. En caso de no disponer de capacidad para determinarla se debería especificar por defecto con un valor de certidumbre que no provoque su descarte por parte de la herramienta de AARR. En caso de observarse un encadenamiento de eventos de seguridad el nivel de certidumbre de las nuevas notificaciones sería consecuentemente mayor.
- Tiempo de detección (**DetectTime**): Esta clase nativa de IODEF dependiente de EventData, pasaría a ser obligatoria. Permitiría establecer en formato unificado el instante de tiempo en que se detectó el evento. El incidente de seguridad, considerado por IODEF como la clase superior que recogería múltiples eventos, haría referencia a los siguientes factores (además del mencionado Assessment):
- Identificador del incidente (**IncidentID**): Esta clase nativa de IODEF obligatoria por defecto, permitiría identificar unívocamente el incidente de seguridad.
- Tiempo de notificación (**ReportTime**): Esta clase nativa de IODEF obligatoria por defecto, permitiría establecer en formato unificado el instante de tiempo en que se notificó el incidente por parte del sistema correspondiente.
- Evaluación (**Assessment**): Esta clase nativa de IODEF

obligatoria por defecto, recogería la evaluación general del incidente de manera semejante a lo definido para los eventos individualizados. En caso de notificarse un único evento como parte del incidente, la evaluación sería idéntica a la del evento, para los atributos de impacto y certidumbre.
- Información de contacto (**Contact**): Esta clase nativa de IODEF obligatoria por defecto, recogería los datos de contacto del administrador del sistema de seguridad notificador.
- Datos de evento (**EventData**): Esta clase nativa de IODEF opcional por defecto pasaría a ser obligatoria, integrado por uno o una lista de eventos de seguridad conteniendo la información definida previamente.

El diseño de las clases del formato nativo IODEF, involucradas en este modelo, se definen a lo largo de [10]. A continuación, se adjunta el diseño de las nuevas clases contempladas como parte de la extensión para el modelo IODEF-DRA:

- Clase AFFECTED ASSET
  - STRING type: sería opcional e identificaría la naturaleza del activo afectado.
  - STRING assetID: sería obligatorio y recogería el identificador unívoco correspondiente al activo particular protegido por el sistema de seguridad y afectado por el evento a notificar.
- Clase REPORTING SYSTEM
  - STRING type: sería obligatorio e identificaría la naturaleza del sistema que detectó el evento de seguridad.
  - STRING systemID: también obligatorio, recogería el identificador unívoco correspondiente al sistema, de modo que se puedan conocer las características de éste, sus niveles históricos de falsos positivos, e incluso las salvaguardas que pudiera ofrecer, en caso de un desarrollo ulterior de posibles respuestas automatizadas.
- Clase DETECTED THREAT
  - STRING type: sería obligatorio e identificaría genéricamente la naturaleza de la amenaza detectada por el sistema de seguridad.
  - STRING threatID: también obligatorio, recogería el identificador unívoco correspondiente a la amenaza que facilitaría el seguimiento en el árbol de ataque del avance de éste y por tanto permitiría el recálculo del riesgo.
- Clase EXPLOIT TYPE
  - STRING vulnerabilityID: sería obligatorio y recogería el identificador unívoco correspondiente a la vulnerabilidad, si bien en caso de desconocerse podría tratarse como unknown.
- Clase SECURITY STATE
  - STRING state: sería obligatorio e identificaría la medida adoptada por el sistema que detectó el evento de seguridad, frente a éste.

C. Implementación del Modelo IODEF-DRA

La aplicación efectiva de este modelo, impondría una serie de requisitos para los sistemas involucrados en la comunicación, en particular:

- Las herramientas de seguridad deberían ser capaces, o proveer mecanismos para poder:
  - Configurar el activo protegido en consonancia con los contemplados en el AARR.
  - Detectar el incidente y generar la correspondiente alerta cuando exista un nivel de certitud umbral que descarte los falsos positivos, en paralelo con las restantes funcionalidades propias de la herramienta.
  - Exportar información en el formato aquí expuesto (IODEF-DRA).
  - Comunicarse con la herramienta de AARR para enviarle los datos exportados en el formato (la comunicación debería producirse preferiblemente bajo condiciones adecuadas de seguridad como las identificadas).
- Por su parte, la herramienta de AARR requeriría:
  - Capacidad de catalogar e identificar unívocamente los activos con códigos compatibles con los aquí referenciados.
  - Recibir comunicaciones en tiempo real (configuración modo push), o constatar de manera continua la existencia de notificaciones de algún repositorio al efecto (configuración modo pull).
  - Importar los datos conforme al modelo IODEF extendido (IODEF-DRA).
  - Bajo condiciones ideales de seguridad, verificar la autenticidad (en relación al sistema que generó la alerta) e integridad de los datos procesados.
  - Validar que los datos relativos a la identificación de activos son correctos y corresponden con los configurados en la herramienta. Adicionalmente, sería relevante que existiera un mapeo similar en relación al identificador de la amenaza detectada.
  - Revaluar el riesgo bajo las nuevas condiciones de seguridad.
  - Mostrar el nuevo mapa de riesgo, considerando la fiabilidad relativa (caracterizada mediante el atributo Confidence) de la información procesada.

III. Prueba de Concepto de un Análisis de Riesgo Dinámico Mediante el Modelo IODEF-DRA

A. Escenario de Integración del Modelo IODEF-DRA

Partiendo del AARR sobre un Sistema de Información (en adelante SI) sencillo, compuesto por un conjunto limitado de activos que incluyen: personal, sala de equipos en una instalación remota, equipos y datos, se generaría un árbol de ataque (ver Fig. 2) que contemplase el nivel de riesgo asociado a la materialización de las amenazas, en el estado inicial para cada nodo. Este sería el equivalente a un AARR estático, realizado con la herramienta de AARR en base a la metodología que aplique. Para este cálculo se tendrían en

consideración las circunstancias que concurren a nivel de la organización, tanto organizativas, como técnicas y humanas.

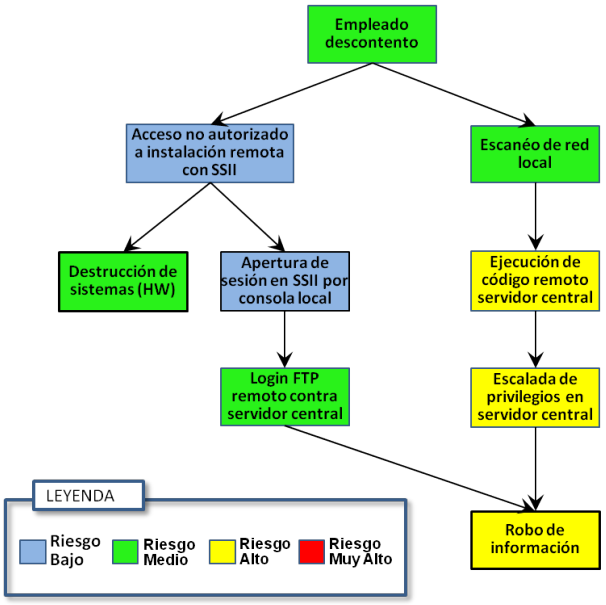

Fig. 2. Árbol de ataque inicial para prueba de concepto de IODEF-DRA

El proceso de AARR a desarrollar para llegar a dichos cálculos no es el foco de interés de este estudio, por lo que se simplificará. Un código de colores muestra el nivel de riesgo de partida para cada nodo como resultado del análisis de riesgos inicial. En el árbol de ataque tomado como ejemplo, un empleado disconforme con la compañía pudiendo causarle daños por dos vías. Por un lado, podría realizar un escaneo de red y lanzar un ataque contra un servidor de datos central. Por el otro podría forzar la entrada a una instalación remota y desatendida, para a continuación, dañar físicamente los equipos o utilizarlos para lanzar un ataque informático desde un segmento de red menos protegido. El objetivo más crítico (mayor riesgo) sería el robo de información, y el camino más plausible la ejecución de código remoto en el servidor desde un equipo de usuario y posterior escalada de privilegios. Las ventajas que ofrecería la integración de sistemas de seguridad con una herramienta de Análisis de Riesgos Dinámico (aplicación que implementa una metodología reconocida, y se adhiere al formato IODEF-DRA) en est escenario, serían:

- Una herramienta DRA basada en un adecuado enfoque metodológico podría tener el conocimiento de aquellos datos considerados críticos dentro del SI, y de los servidores que los alojan, en tanto que un sistema de seguridad a más bajo nivel podría ser ignorante de esta información.
- El administrador de un sistema de seguridad del SI probablemente no tendrá acceso a la información sobre la seguridad física en las instalaciones, mientras que la herramienta DRA estaría capacitada para establecer una relación con los sistemas de seguridad física en la instalación remota, permitiéndole establecer la cadena de eventos que conducen al robo de información o a la destrucción de sistemas más o menos críticos.
- La herramienta DRA tendría conocimiento de las medidas de autenticación o los procedimientos relacionados con conexiones FTP desde equipos remotes y los flujos de información entre ellos, lo que sería de gran utilidad para el análisis del riesgo durante el ataque.

En base a la integración de los sistemas de seguridad (tanto lógica como física en torno al SI representada en la Fig. 3, la herramienta de AARR se mantiene a la espera activa de mensajes sobre eventos de seguridad que aquellos le notifiquen.

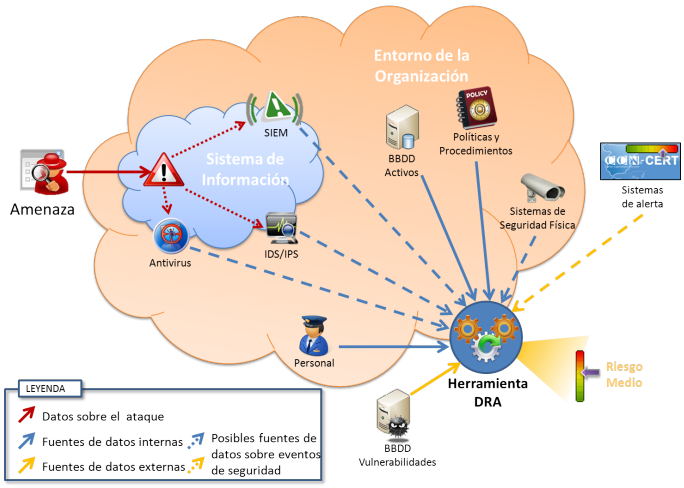

Fig. 3. Evaluación Dinámica del Riesgo integrando sistemas de seguridad

B. Desarrollo del Análisis de Riesgos Dinámico

La cadena de eventos e interacciones con la herramienta DRA, a lo largo del incidente de seguridad, sería la siguiente:

1) Un sistema de seguridad física detecta en primera instancia una intrusión en la sala de equipos. Al tratarse de una instalación remota la reacción por parte de un equipo de seguridad se vería obstaculizada. A través de la centralita del sistema anti-intrusión la alarma llega a la consola de monitorización de vigilancia, capaz de notificar mediante un mensaje IODEF-DRA como el ilustrado a continuación, a la herramienta de AARR.

```
<?xml version="1.0" encoding="UTF-8"?>
<Incident purpose="reporting">
<IncidentID name="physicalAlert">00001</IncidentID>
<ReportTime>2012-03-10T20:13:05+00:00</ReportTime>
<Assessment>
<Impact severity="medium" completion="succeeded"/>
<Confidence rating="high"/>
</Assessment>
<Contact role="admin" type="person">
<Description>Security Staff on site</Description>
</Contact>
<EventData>
<DetectTime>2012-03-10T20:13:02+00:00</DetectTime>
<Assessment>
<Impact severity="medium" completion="succeeded"/>
<Confidence rating="high"/>
</Assessment>
<AdditionalData>
```

```
<AffectedAsset type="site" assetID="remote-site"/>
<ReportingSystem type="physicalSecurityConsole"
systemID="console01"/>
<DetectedThreat type="unauthorized access" threatID=
"Breakin"/>
<ExploitType vulnerabilityID="unknown"/>
<SecurityState state="supervised"/>
</AdditionalData>
</EventData>
</Incident>
</IODEF-Document>
```

2) La herramienta DRA recalcula el riesgo en tiempo real, estimándose los nuevos valores del riesgo, para los nodos susceptibles de ser afectados (ver Fig. 4-A).
3) El atacante logra conectar localmente a la consola de uno de los equipos alojados en la instalación remota, tras varios intentos fallidos detectados por el HIDS (Host-based IDS) instalado. Éste reacciona, notificando a la herramienta DRA el evento de intentos fallidos de login mediante un mensaje IODEF-DRA específico.

```
<?xml version="1.0" encoding="UTF-8"?>
<Incident purpose="reporting">
<IncidentID name="HostIDSAlert">00015</IncidentID>
<ReportTime>2012-03-10T20:18:33+00:00</ReportTime>
<Assessment>
<Impact severity="low" completion="succeeded"/>
<Confidence rating="high"/>
</Assessment>
<Contact role="admin" type="person">
<Description>Network administrator</Description>
</Contact>
<EventData>
<DetectTime>2012-03-10T20:18:25+00:00</DetectTime>
<Assessment>
<Impact severity="low" completion="succeeded"/>
<Confidence rating="high"/>
</Assessment>
<AdditionalData>
<AffectedAsset type="host" assetID="Remoteserver"/>
<ReportingSystem type="HIDS" systemID="HIDS08"/>
<DetectedThreat type="Local console login failure"
threatID="FailedLoginAttempts"/>
<ExploitType vulnerabilityID="unknown"/>
<SecurityState state="supervised"/>
</AdditionalData>
</EventData>
</Incident>
</IODEF-Document>
```

4) La herramienta DRA procesa el mensaje y reevalúa el nivel de riesgo en los nodos de nuevo (ver Fig. 4-B). En el contexto actual, la herramienta DRA juzga que el nodo que representa el robo de información pasa a ser fácilmente alcanzable por el atacante, al estar al tanto de que las conexiones FTP desde los servidores remotos no son bloqueadas debido a requisitos de negocio, conforme a la política de seguridad. Por tanto, el nivel de riesgo del nodo, aumenta al nivel más elevado.
5) El siguiente paso del atacante es lanzar un login remoto vía FTP contra uno de los servidores de la organización. En este caso, un NIDS (Network IDS) monitorizando la red detectaría esta actividad que no se ajustaría a los patrones normales de comunicación de datos al servidor central, siendo capaz de notificar mediante otro mensaje IODEF-DRA a la herramienta DRA.

```
<?xml version="1.0" encoding="UTF-8"?>
<Incident purpose="reporting">
<IncidentID name="NetworkIDSAlert">00059</IncidentID>
<ReportTime>2012-03-10T20:21:18+00:00</ReportTime>
<Assessment>
<Impact severity="low" completion="succeeded"/>
<Confidence rating="medium"/>
</Assessment>
<Contact role="admin" type="person">
<Description>Network administrator</Description>
</Contact>
<EventData>
<DetectTime>2012-03-10T20:21:13+00:00</DetectTime>
<Assessment>
<Impact severity="low" completion="succeeded"/>
<Confidence rating="medium"/>
</Assessment>
<AdditionalData>
<AffectedAsset type="host" assetID="Fileserver"/>
<ReportingSystem type="NIDS" systemID="NIDS01"/>
<DetectedThreat type="Remote FTP connexion" threatID=
"RemoteFTP"/>
<ExploitType vulnerabilityID="unknown"/>
<SecurityState state="supervised"/>
</AdditionalData>
</EventData>
</Incident>
</IODEF-Document>
```

6) La certitud de que la conexión FTP se deba a un evento de seguridad sería menor, al poder tratarse de una excepción en la operativa del sistema. Sin embargo, la herramienta DRA estaría al tanto de la cadena de eventos previa, y afianzaría la evaluación del alto riesgo relacionado con el robo de la información (ver Fig. 4-C).
7) El atacante habría pasado a estar conectado al servidor de datos central, pudiendo a continuación buscar la información crítica que llevarse consigo.

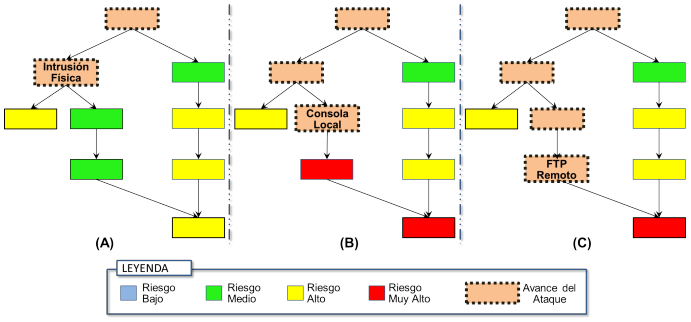

Fig. 4. Evolución del riesgo en base al árbol de ataque inicial usando DRA

El cálculo del riesgo en tiempo real, refleja a lo largo del ataque el aumento del riesgo en el nodo final, que representa la captura de la información sensible. De este modo la visión de conjunto proporcionada por una metodología de AARR unida a la actualización del nivel de riesgo conforme al avance del atacante podría haber permitido frustrar mediante una intervención preventiva, el hecho de que el usuario alcanzara la información sensible a proteger. Si nadie estableciera la relación entre los diferentes eventos acaecidos, la información

crítica podría ser sustraída a través de la conexión FTP antes de que el personal de seguridad se personara en la instalación remota en respuesta a la alarma del sistema de seguridad física. Por el contrario, monitorizar el riesgo mediante la herramienta DRA ayudaría a la toma de decisiones, como el cierre de las conexiones FTP remotas desde el sistema en la instalación remota afectado por el ataque. El negocio podría resultar afectado, si bien la evaluación por parte de la herramienta reflejaría que el robo de información sería aún más grave.

IV. Conclusiones y Trabajo Futuro

Son múltiples las soluciones que han contemplado en alguna medida los retos que plantea el AARR Dinámico, cubriendo algunos de los aspectos fundamentales. El desarrollo de métodos y tecnologías que abordan problemáticas particulares, dentro del conjunto de variables que influyen en la evaluación del riesgo, permite encarar desde diferentes ángulos esta tarea. Esta multiplicidad de planteamientos no facilita un enfoque cooperativo e integrador, que aporte una visión más completa. Por el contrario, las soluciones tienden a centrarse en un ámbito que con mayor o menor eficacia puede contemplar los cambios surgidos en él (nuevas vulnerabilidades, detección de ataques) pero no alcanzan una visión de conjunto, que abarque los múltiples cambios que podrían afectar al riesgo.

A través del modelo IODEF-DRA presentado, se pretende englobar la visión de conjunto a través de herramientas de AARR basadas en metodologías reconocidas que puedan recibir información de múltiples fuentes sobre eventos de seguridad, en un formato que les permita su integración y análisis en tiempo real. La aplicación efectiva de estas comunicaciones, basada en este esquema de datos, entre los sistemas de seguridad de la Organización, u otras fuentes externas de confianza tales como CERTs, y las herramientas de AARR, repercutiría en los siguientes beneficios:

- Capacidad para actualizar los procesos de AARR en tiempo real, ofreciendo la posibilidad de una monitorización continuada de su evolución, que permita una percepción instantánea del riesgo sobre los objetivos del negocio, así como una respuesta más rápida.
- Aplicación de un enfoque metodológico del AARR, de utilidad tanto a nivel técnico como a alto nivel. Este enfoque conduciría a una visión homogénea del riesgo en la Organización, que aportaría una respuesta ante los incidentes mejor alineada con las políticas de seguridad.
- Posibilidad de tener en consideración activos de nivel superior de la Organización, tales como componentes de seguridad, políticas u otros factores organizativos más allá de la mera arquitectura del SI. La integración de los sistemas de seguridad con el AARR metodológico expandiría el dominio evaluado al propio SI y su entorno.

El escenario recogido en la prueba de concepto muestra cómo la integración propuesta mediante el uso de IODEF-DRA, evidencia las mencionadas ventajas. Primero permitió monitorizar y detectar el aumento del riesgo, teniendo en cuenta el impacto de los activos en los objetivos del negocio. Proporcionó una visión unificada del riesgo, desde el punto de vista técnico y del de gestión, facilitando la toma de decisiones. Finalmente, integró la seguridad física en torno al SI, y tuvo en cuenta aspectos relacionados con las políticas de seguridad para evaluar el riesgo en tiempo real.

El planteamiento de trabajo futuro se orienta a la evolución del proceso de captura de datos, orientados al AARR Dinámico, que permitiría mejorar la calidad y fiabilidad de los AARR. Para ello, se seguirán dos líneas de acción principalmente: la primera orientada a un mayor desarrollo y promoción del uso del modelo IODEF-DRA; y la segunda, la adopción de otras fuentes de información que diversifiquen el input que reciben las herramientas DRA, para obtener una base de conocimiento en tiempo real más completa que optimice la evaluación del riesgo.

Agradecimientos

Los autores agradecen la financiación que les brinda el Subprograma AVANZA COMPETITIVIDAD I+D+I del Ministerio de Industria, Turismo y Comercio (MITyC) a través del Proyecto TSI-020100-2011-165. Asimismo, los autores agradecen la financiación que les brinda el Programa de Cooperación Interuniversitaria de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), Programa PCI-AECID, a través de la Acción Integrada MAEC-AECID MEDITERRÁNEO A1/037528/11.

Referencias

[1] ISO/IEC 27005:2008, *Information technology - Security techniques - Information security risk management*, 2008.

[2] MAGERIT versión 2, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I Método*, Ministerio de Administraciones Públicas (MAP), España, 2006.

[3] C. Alberts, and A. Dorofee "Managing Information Security Risk. The OCTAVE Approach", in Addison Wesley, 2005.

[4] Siemens - Insight Consulting, *The Logic behind CRAMMs Assessment of Measures of Risk and Determination of Appropriate Countermeasures*, Siemens, 2005.

[5] EBIOS v2: *Méthode pour lExpression des Besoins et lIdentification des Objectifs de Sécurité*, Direction Centrale de la Sécurité des Systèmes dInformation (DCSSI), France, 2004.

[6] BSI *IT Baseline Protection Manual Bundesamt fr Sicherheit in der Informationstechnik* Federal Office for Information Security (BSI), Deutschland, 2000.

[7] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems", in *NIST Special Publication 800-30*, 2002.

[8] D. López, O. Pastor, and L.J. García Villalba, "Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información", in *Actas de la XII Reunión Española de Criptología y Seguridad de la Información (RECSI 2012)*, Donostia-San Sebastián, España, Sep. 2012

[9] H. Debar, D. Curry, and B. Feinstein, "Intrusion Detection Message Exchange Format (IDMEF)", Internet Engineering Task Force (IETF), RFC-4765, Mar. 2007. [Online]. Available: http://datatracker.ietf.org/doc/rfc4765/

[10] R. Danyliw, J. Meijer, and Y. Demchenko, "Incident Object Description and Exchange Format (IODEF)", Internet Engineering Task Force (IETF), RFC-5070, Dec. 2007. [Online]. Available: http://datatracker.ietf.org/doc/rfc5070/

[11] K. Gorzelak, T. Grudziecki, P. Jacewicz, P. Jaroszewski, L. Juszczyk, and P. Kijewski, *Proactive Detection of Network Security Incidents*, European Network and Information Security Agency (ENISA), Report Deliverable 2011-12-07, pp.114-116, 2011.

[12] ISO/IEC 27035:2011, *Information technology - Security techniques - Information security incident management*, 2011.