Ciberseguridad: perspectivas y desafíos para la sociedad

Dr. Ing. Gustavo Betarte

Profesor Titular, Grado 5
Grupo de Seguridad Informática
InCo, Facultad de Ingeniería, UDELAR

Mesa Redonda Ciberseguridad
Academia Nacional de Ingeniería

Montevideo, noviembre 2015

Plan

Plan

Plan

Plan

Plan

Activos y Riesgos

Activos y Riesgos

De los activos . . .

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

- Pérdida de propiedad Intelectual

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

- Pérdida de propiedad Intelectual
- Destrucción o alteración de los datos

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

- Pérdida de propiedad Intelectual
- Destrucción o alteración de los datos
- Daño a la reputación

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

- Pérdida de propiedad Intelectual
- Destrucción o alteración de los datos
- Daño a la reputación
- Fallo de infraestructura crítica

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

- Pérdida de propiedad Intelectual
- Destrucción o alteración de los datos
- Daño a la reputación
- Fallo de infraestructura crítica
- Sanciones legales y/o regulatorias

Activos y Riesgos

De los activos . . .

- En los últimos 20 años la naturaleza de los activos de las organizaciones/empresas ha cambiado significativamente, pasando de lo físico a lo virtual
- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos

. . . a los riesgos actuales

- Pérdida de propiedad Intelectual
- Destrucción o alteración de los datos
- Daño a la reputación
- Fallo de infraestructura crítica
- Sanciones legales y/o regulatorias
- . . .

Criticidad de los ciber-ataques

Criticidad de los ciber-ataques

- Ciber-ataques y fallos en sistemas de las infraestructuras críticas se encuentran en el Top 5 de riesgos globales según el WEF (World Economic Forum)

Criticidad de los ciber-ataques

- Ciber-ataques y fallos en sistemas de las infraestructuras críticas se encuentran en el Top 5 de riesgos globales según el WEF (World Economic Forum)
- En últimos 5 años el número de amenazas cibernéticas se ha multiplicado de manera exponencial

Criticidad de los ciber-ataques

- Ciber-ataques y fallos en sistemas de las infraestructuras críticas se encuentran en el Top 5 de riesgos globales según el WEF (World Economic Forum)
- En últimos 5 años el número de amenazas cibernéticas se ha multiplicado de manera exponencial
- Algunas estimaciones predicen que entre 9 y 21 billones de USD de valor económico global podrían estar en riesgo si los gobiernos y las empresas no son capaces de combatir las ciber-amenazas

Escenarios tecnológicos

Escenarios tecnológicos

Convergencia

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos
- Interdependencia con sistemas externos

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos
- Interdependencia con sistemas externos
- Consolidación hacia estándares de comunicación (IP)

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos
- Interdependencia con sistemas externos
- Consolidación hacia estándares de comunicación (IP)

Algunas consecuencias

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos
- Interdependencia con sistemas externos
- Consolidación hacia estándares de comunicación (IP)

Algunas consecuencias

- Exposición de los sistemas (de infraestructuras críticas) a potenciales ataques sobre Internet

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos
- Interdependencia con sistemas externos
- Consolidación hacia estándares de comunicación (IP)

Algunas consecuencias

- Exposición de los sistemas (de infraestructuras críticas) a potenciales ataques sobre Internet
- Nuevos riesgos: conexiones wireless, mantenimiento remoto por terceros, BYOD

Escenarios tecnológicos

Convergencia

- Interconexión de sistemas internos
- Interdependencia con sistemas externos
- Consolidación hacia estándares de comunicación (IP)

Algunas consecuencias

- Exposición de los sistemas (de infraestructuras críticas) a potenciales ataques sobre Internet
- Nuevos riesgos: conexiones wireless, mantenimiento remoto por terceros, BYOD
- Ataques pueden ocasionar daños cuyo valor supere el de la organización o compañía, con consecuencias significativas

Tipos de ataques

Tipos de ataques

- Aplicaciones Web

Tipos de ataques

- Aplicaciones Web
- Dispositivos móviles inteligentes

Tipos de ataques

- Aplicaciones Web
- Dispositivos móviles inteligentes
- Medios sociales

Tipos de ataques

- Aplicaciones Web
- Dispositivos móviles inteligentes
- Medios sociales
- Infraestructuras críticas

Tipos de ataques

- Aplicaciones Web
- Dispositivos móviles inteligentes
- Medios sociales
- Infraestructuras críticas
- Ciber-espionaje

Objetivos de los ataques

Objetivos de los ataques

Porte de la organización/empresa

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio
- Contratos con clientes, proveedores, distribuidores

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio
- Contratos con clientes, proveedores, distribuidores
- Credenciales de login de empleados

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio
- Contratos con clientes, proveedores, distribuidores
- Credenciales de login de empleados
- Información de activos de la organización

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio
- Contratos con clientes, proveedores, distribuidores
- Credenciales de login de empleados
- Información de activos de la organización
- Diseño de productos

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio
- Contratos con clientes, proveedores, distribuidores
- Credenciales de login de empleados
- Información de activos de la organización
- Diseño de productos
- Código fuente

Objetivos de los ataques

Porte de la organización/empresa

- No es relevante
- Los ciber-criminales atacan a organizaciones de todos los tamaños y de cualquier vertical

Valores buscados

- Planes de negocio
- Contratos con clientes, proveedores, distribuidores
- Credenciales de login de empleados
- Información de activos de la organización
- Diseño de productos
- Código fuente
- Datos de empleados, proveedores, distribuidores, clientes

Un escenario que evoluciona muy rápidamente

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Advanced Persistent Threats (APT)

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Advanced Persistent Threats (APT)

- Secuencia de intrusiones guiadas por fallas y éxitos

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Advanced Persistent Threats (APT)

- Secuencia de intrusiones guiadas por fallas y éxitos
- Explotación de diferentes vulnerabilidades y combinación de ataques

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Advanced Persistent Threats (APT)

- Secuencia de intrusiones guiadas por fallas y éxitos
- Explotación de diferentes vulnerabilidades y combinación de ataques
- Tienden a persistir dentro de la infraestructura de la organización

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Advanced Persistent Threats (APT)

- Secuencia de intrusiones guiadas por fallas y éxitos
- Explotación de diferentes vulnerabilidades y combinación de ataques
- Tienden a persistir dentro de la infraestructura de la organización
- Los afectados raramente saben que son objetivo de ataque y desconocen origen del mismo

Un escenario que evoluciona muy rápidamente

Cambio en la naturaleza de las amenazas

- de amenazas conocidas, puntuales y dispersas,
- a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos

Advanced Persistent Threats (APT)

- Secuencia de intrusiones guiadas por fallas y éxitos
- Explotación de diferentes vulnerabilidades y combinación de ataques
- Tienden a persistir dentro de la infraestructura de la organización
- Los afectados raramente saben que son objetivo de ataque y desconocen origen del mismo
- Defensa no puede ser (sólo) reactiva

Kill chain

Kill chain

Kill chain

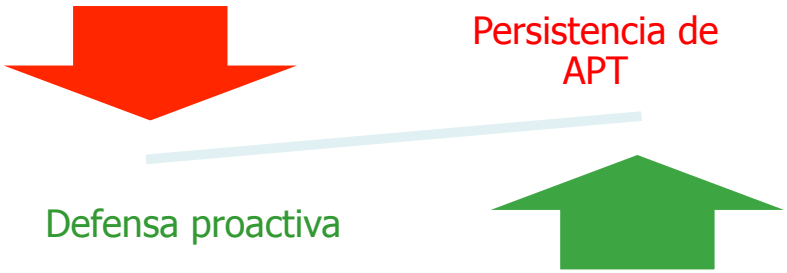
- Modus operandi de los APT actuales

Kill chain

- Modus operandi de los APT actuales
- Amenazas persistentes vs. Defensa proactiva

Kill chain

- Modus operandi de los APT actuales
- Amenazas persistentes vs. Defensa proactiva



Threat intelligence

Threat intelligence

Busca entender ...

Threat intelligence

Busca entender ...

- Qué tipo de ataques han ocurrido y pueden ocurrir

Threat intelligence

Busca entender . . .

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos

Threat intelligence

Busca entender ...

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos
- Cómo pueden ser mitigados

Threat intelligence

Busca entender . . .

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos
- Cómo pueden ser mitigados

. . . y caracterizar

Threat intelligence

Busca entender . . .

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos
- Cómo pueden ser mitigados

. . . y caracterizar

- Cuáles son los actores maliciosos relevantes

Threat intelligence

Busca entender . . .

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos
- Cómo pueden ser mitigados

. . . y caracterizar

- Cuáles son los actores maliciosos relevantes
- Cuáles son sus objetivos y sus capacidades (TTP)

Threat intelligence

Busca entender . . .

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos
- Cómo pueden ser mitigados

. . . y caracterizar

- Cuáles son los actores maliciosos relevantes
- Cuáles son sus objetivos y sus capacidades (TTP)
- Qué vulnerabilidades, configuraciones incorrectas o debilidades son sus más probables objetivos

Threat intelligence

Busca entender . . .

- Qué tipo de ataques han ocurrido y pueden ocurrir
- Cómo esos ataques pueden ser detectados y reconocidos
- Cómo pueden ser mitigados

. . . y caracterizar

- Cuáles son los actores maliciosos relevantes
- Cuáles son sus objetivos y sus capacidades (TTP)
- Qué vulnerabilidades, configuraciones incorrectas o debilidades son sus más probables objetivos
- Qué acciones han tomado en el pasado

Trabajo en curso

Trabajo en curso

- Análisis de seguridad basado en procesos automatizados

Trabajo en curso

- Análisis de seguridad basado en procesos automatizados
- Reconocimiento y prevención de ataques en aplicaciones web

Análisis de seguridad automatizado

Proyecto STIC-AMSUD *AKD*

Objetivos

Análisis de seguridad automatizado

Proyecto STIC-AMSUD *AKD*

Objetivos

- Detección de compromisos informáticos usando base de conocimiento de indicadores de compromiso definidos en (STIX) y (CybOX) (MITRE - NIST)

Análisis de seguridad automatizado

Proyecto STIC-AMSUD *AKD*

Objetivos

- Detección de compromisos informáticos usando base de conocimiento de indicadores de compromiso definidos en (STIX) y (CybOX) (MITRE - NIST)
- Derivación de indicadores a partir de hallazgos encontrados

Análisis de seguridad automatizado

Proyecto STIC-AMSUD *AKD*

Objetivos

- Detección de compromisos informáticos usando base de conocimiento de indicadores de compromiso definidos en (STIX) y (CybOX) (MITRE - NIST)
- Derivación de indicadores a partir de hallazgos encontrados
- Recolección de evidencia definida en los indicadores derivados.

Análisis de seguridad automatizado

Proyecto STIC-AMSUD *AKD*

Objetivos

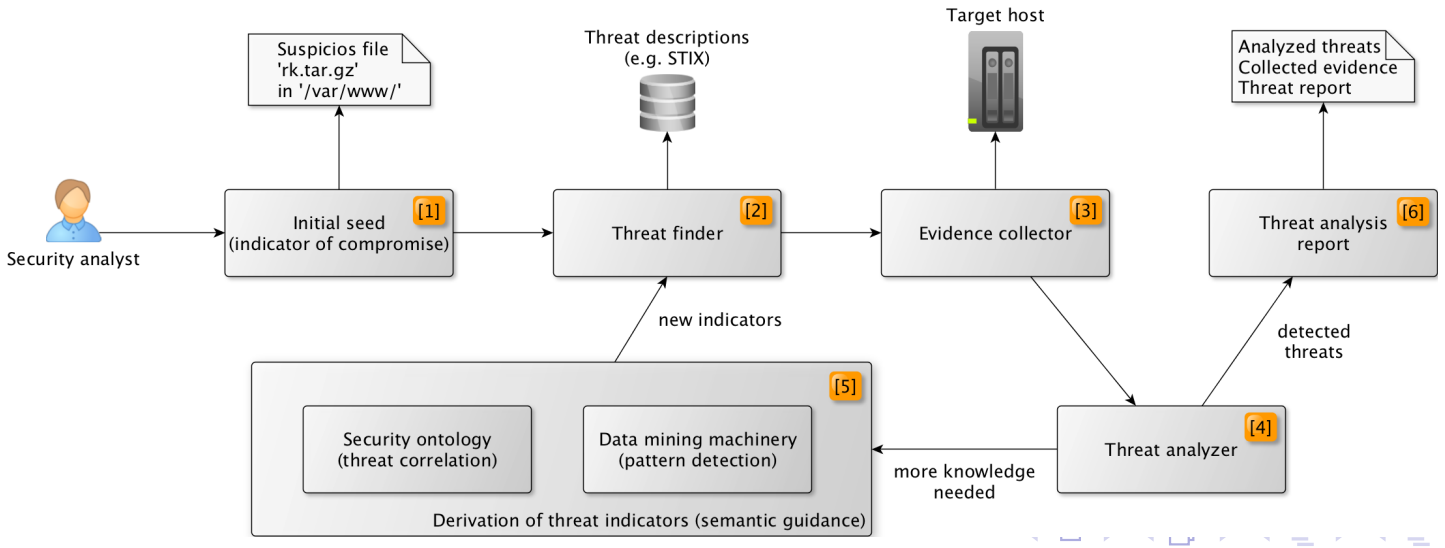
- Detección de compromisos informáticos usando base de conocimiento de indicadores de compromiso definidos en (STIX) y (CybOX) (MITRE - NIST)
- Derivación de indicadores a partir de hallazgos encontrados
- Recolección de evidencia definida en los indicadores derivados.
- Evaluación de compromiso verificando que la evidencia obtenida determina la existencia de un ataque.

Análisis de seguridad automatizado

Proyecto STIC-AMSUD *AKD*

Objetivos

- Detección de compromisos informáticos usando base de conocimiento de indicadores de compromiso definidos en (STIX) y (CybOX) (MITRE - NIST)
- Derivación de indicadores a partir de hallazgos encontrados
- Recolección de evidencia definida en los indicadores derivados.
- Evaluación de compromiso verificando que la evidencia obtenida determina la existencia de un ataque.



Prevención de ataques en aplicaciones web

Proyecto ICT4V *WAFINTL*

Prevención de ataques en aplicaciones web

Proyecto ICT4V *WAFINTL*

Objetivos

Prevención de ataques en aplicaciones web

Proyecto ICT4V *WAFINTL*

Objetivos

- Técnicas de detección y determinación de perfiles de atacantes usando aprendizaje automático

Prevención de ataques en aplicaciones web

Proyecto ICT4V *WAFINTL*

Objetivos

- Técnicas de detección y determinación de perfiles de atacantes usando aprendizaje automático
- Honeypots de alto nivel de interacción para el registro y análisis de ataques

Prevención de ataques en aplicaciones web

Proyecto ICT4V *WAFINTL*

Objetivos

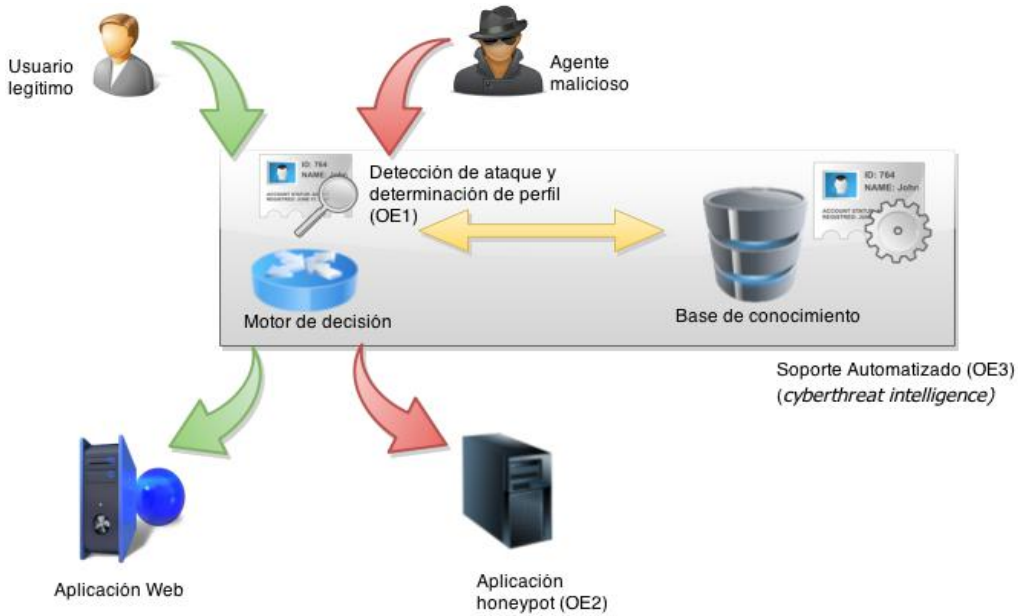
- Técnicas de detección y determinación de perfiles de atacantes usando aprendizaje automático
- Honeypots de alto nivel de interacción para el registro y análisis de ataques
- Técnicas y herramientas para inteligencia de amenazas basados en KD

Prevención de ataques en aplicaciones web

Proyecto ICT4V *WAFINTL*

Objetivos

- Técnicas de detección y determinación de perfiles de atacantes usando aprendizaje automático
- Honeypots de alto nivel de interacción para el registro y análisis de ataques
- Técnicas y herramientas para inteligencia de amenazas basados en KD



Referencias

G. Barthe; G. Betarte; J.D. Campo; C. Luna; D. Pichardie

System-level non-interference for constant-time cryptography.
En Proceedings of CCS 2014: 21st ACM Conference on Computer and Communications Security, Arizona, USA, November 2014.

M. Barrère; G. Betarte et al.

Machine-assisted Cyber Threat Analysis using Conceptual Knowledge Discovery.
En Proceedings of FCA4AI: 4th International Workshop "What can FCA do for Artificial Intelligence?", 2015, co-located with the International Joint Conference on Artificial Intelligence (IJCAI 2015), Buenos Aires, Argentina, July 2015.

M. Barrère; G. Betarte; M. Rodríguez

Towards machine-assisted formal Procedures for the Collection of Digital Evidence.
En Proceedings of IEEE Symposium on Privacy, Security and Trust (PST 2011), Montreal, Canada, July 2011.

Grupo de Seguridad Informática

Referencias


The Mitre Corporation.
Open Vulnerability and Assessment Language (OVAL).
http://oval.mitre.org/ (Última visita: 27 de febrero de 2014).


The Mitre Corporation.
Common Attack Pattern Enumeration and Classification (CAPEC).
http://capec.mitre.org/ (Última visita: 30 de octubre de 2012).


The Mitre Corporation.
Cyber Observable eXpression (CybOX).
http://cybox.mitre.org/ (Última visita: 27 de febrero de 2014).


The Mitre Corporation.
Structured Threat Information eXpression (STIX).
http://stix.mitre.org/ (Última visita: 27 de febrero de 2014).