OPTIMITI NETWORK

Aportamos valor tecnológico

Governance

Tomando el control de la ciberseguridad

InfoSecurity

ISEC INFOSECURITY TOUR 2016

Javier Rodríguez
Consultor de Seguridad

Leslie Pérez
Directora de Calidad Normativa
Auditor Líder ISO/IEC 27001:2013 / Operational Support and Analysis (OSA) / Service Offerings & Agreements (SOA) / Release, Control & Validation (RCV) /Planning, Protection and Optimization (PPO)

Lo valoras, Optimiti lo protege
Seguridad a otro nivel.

Ciberseguridad

El concepto no implica aspectos técnicos únicamente, requiere el conocimiento de la organización, definición de nuevos paradigmas en la asignación de actividades y responsabilidades.

Modelos de Gobierno de Seguridad de la Información

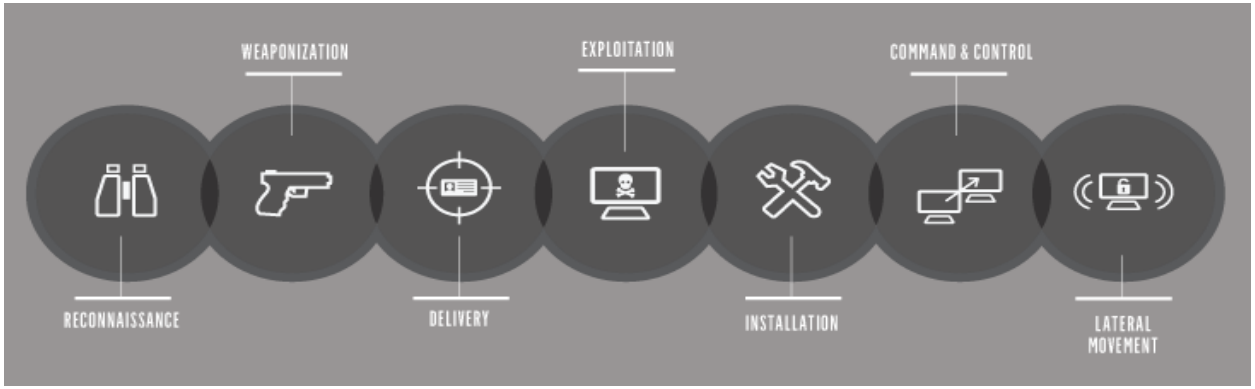
Amenazas Avanzadas

Inteligencia

Threat Intelligence

Advanced Persistent Threats (APT)

Campañas de gran sofisticación que no son detectados por soluciones de seguridad tradicionales, persistentes, y con objetivos muy concretos.

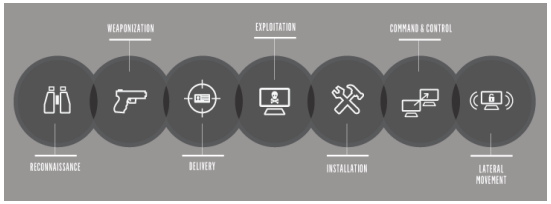


¿Que es Threat Intelligence?

"Incorporación, análisis, normalización y contextualización de datos procedentes de diversas fuentes externas e internas"

- Big Data Security
- Advanced Persistent Threats
- Security Analytics

→ Threat Intelligence



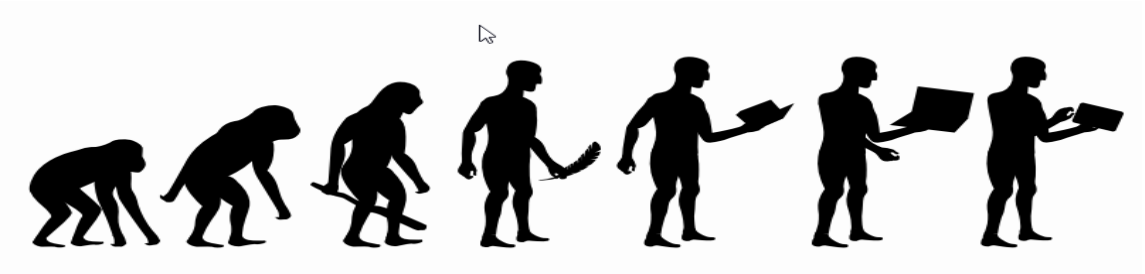
Información vs INTELIGENCIA

Información:

- Datos crudos, sin filtrar.
- La información obtenida no se evalúa
- Datos agregados desde múltiples fuentes sin correlación
- Los datos obtenidos no generan acciones

Inteligencia:

- Información ordenada y procesada
- Información evaluada por personal capacitado.
- Correlación de Información de fuentes especificas.
- Genera valor, favorece la toma de decisiones.



Cibermodelo de Seguridad

ESTRATEGICO

- Definición de Estrategia de Seguridad
- Habilitar Evaluación
- Habilitar Aseguramiento
- Definición de Roles y Responsabilidades
- Habilitar Comunicación

TACTICO

- Análisis de Impacto
- Identificación de Activos de Información clave e Infraestructuras Críticas
- Análisis de Riesgos

OPERATIVO

- Gestión de Incidentes de Ciberseguridad
- Defensa Proactiva

Threat Intelligence

- Investigar
- Analizar
- Difundir

REFLEXIONEMOS

DIRECCIÓN

EVALUACION y ASEGURAMIENTO

COMUNICACIÓN

¿Cuáles son los retos para elaborar un Modelo de Seguridad de la Información que refleje la interacción entre los procesos, los componentes tecnológicos y los roles en materia de seguridad de la información apuntalando a los objetivos de la organización?

¿El organigrama de la organización refleja los roles y las responsabilidades que realmente necesita la organización en materia de ciberseguridad?

¿Sus equipos tácticos y operativos se encuentran preparados para hacer frente a los nuevos retos de ciberseguridad?

¿La arquitectura de seguridad de su organización cuenta con mecanismos dedicados a la detección y mitigación de amenazas avanzadas?

¿Tenemos claro por que necesitamos habilitar un modelo de seguridad proactivo que apuntale al desarrollo de Threat Intelligence dentro de la organización ?

REFLEXIONEMOS

DIRECCIÓN

COMUNICACIÓN

EVALUACION y ASEGURAMIENTO

- ¿Las métricas en materia de seguridad de la información en tu organización, fueron diseñadas para conocer si los roles estén haciendo su trabajo asignado?

ó

- ¿Fueron diseñadas para dar visibilidad en el cumplimiento a las estrategias de seguridad de la información y disminución del nivel del riesgo?

Audiencia de las métricas

- ¿Te consideras juez y parte en materia de seguridad de la información dentro de tu organización? ¿Cuentas con el enfoque de revisiones de tercera parte?

REFLEXIONEMOS

DIRECCIÓN

COMUNICACIÓN

EVALUACION y ASEGURAMIENTO

- Después de una definición en materia de seguridad la información si el documento relacionado no es comunicado, ¿Crees que se este ejecutando el gobierno de seguridad de la información?

- ¿Concientización ó Educación Especializada?

Conclusiones

- Cambio del enfoque del modelo de seguridad actual, de un enfoque reactivo y tradicional a un enfoque proactivo y de generación de inteligencia en seguridad de la información.
- Se deben generar de estrategias de seguridad que incluyan controles tecnológicos enfocados a la detección de amenazas avanzadas, que permitan habilitar modelos de "Threat Intelligence" para combatir los ataques actuales y planificar futuros incidentes.
- Reducción de métricas que no generan valor.
- Mejora la comunicación en materia de seguridad de la información, entre los equipos operativos, tácticos y estratégicos así como con los terceros involucrados.
- Habilitar al personal en materia de ciberseguridad, reduciendo los costos asociados a la coordinación del equipo de respuesta a incidentes para la atención de múltiples alertas y falsos positivos.

Preguntas

GRACIAS

Leslie Pérez
leslie.perez@optimiti.com.mx
http://www.optimiti.com.mx/
OPTIMITI NETWORK, S.A. DE C.V.
Tel.:63943000
Cel.: 04455 43 88 08 74