Visualización y analítica de los logs del cortafuegos

Nuria Prieto/Rafael Calzada
cert@uc3m.es @CertUC3M

Universidad Carlos III de Madrid
www.uc3m.es

It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.
Arthur Conan Doyle (1891) *A Scandal in Bohemia*

Servicio de Informática y Comunicaciones

web: sdic.uc3m.es
twitter: @sdic_uc3m

Agenda

- Gestión de eventos, visualización de datos
- Cómo lo hemos montado
- Información que se recoge
- Casos de uso
- Ideas de futuro

Gestión de eventos: ¿Qué es un evento?

- Evento: Algo que sucede, detectado en uno o más sistemas y puede estar relacionado con otros eventos
- Por ejemplo, una conexión desde una IP de eduroam….
  - Tiene una validación previa en **RADIUS**, una asignación de IP mediante **DHCP**
  - Puede tener una consulta **DNS** asociada
  - **Empieza** en un momento dado e intervienen unos actores (**origen, destino, puertos, protocolo**)
  - Se recoge como un flujo en los **routers** implicados (bytes enviados/recibidos)
  - Se recoge como una sesión en el **cortafuegos**
    - Que tiene asociada una **aplicación**, puede suponer una **amenaza**, se le aplica una **política**
  - Tiene un **final**

Visualización de datos

"Una imagen vale más de que mil palabras"

- Debe responder a una pregunta
  - ¿Qué servidores SSH tenemos activos en nuestra red?
- Puede dar lugar a otras nuevas
  - ¿Desde que países las sesiones transfieren menos de 10 KB?
- Permiten explorar y descubrir
  - Voy a echar un vistazo a lo que está haciendo el cortafuegos

Visualización de datos

"Una imagen vale más de que mil palabras"

- Sustenta decisiones
  - Cortamos el acceso SSH desde China y aledaños
- Transmite información
  - El cerebro asimila más fácilmente los gráficos que las tablas/números
- Aumenta la eficiencia
  - Ya que no es necesario conocer a fondo las diferentes plataformas que tenemos desplegadas

Como lo hemos montado - Hardware

Reciclando....

- Hardware: Servidor HP DL580-G5, adquirido en 2010
- Cuatro procesadores E7450@2.40GHz (6 core/procesador) → 24 cores
- 8+64 GB de RAM (DDR2 667MHz)
- Cabina de almacenamiento HP MSA, reutilizada de audiovisuales
  - 11 TB de almacenamiento útil
  - Accedido mediante 3 tarjetas SmartArray
  - 10 slots libres para añadir disco en la cabina.
  - Sistemas RAID5 y 4 discos spare por si acaso
- SOLO HEMOS INVERTIDO 1300€ + IVA!!!!!

Como lo hemos montado - Software

ELK + Redis

- ElasticSearch 1.7.1
  - Almacenamiento e indexación
- Logstash 1.5.1
  - Recolección
  - Análisis, filtrado e inserción de ElasticSearch
- Kibana 4.1.1
  - Visualización
- Redis 2.8
  - Sistema de colas

Como lo hemos montado - RRHH

Nuria

- Mantenimiento del servidor
- Instalación de ELK+Redis
- Control de accesos
- Patrones de Logstash

Rafa

- Diseño Paneles
- Configuración en Zabbix
- RRPP

- Leer, leer y buscar en Google
- Análisis de rendimiento y ajuste del sistema

Información que se recoge

La información proviene del cortafuegos **PaloAlto 5050**

- Gestión de las sesiones, incluyendo información de Aplicaciones.
- Amenazas
- Acciones de los perfiles de seguridad
  - Antivirus/malware
  - Antispyware
  - Bloqueo de URLs
- En un día *tranquilo* 60M eventos
- Con días de 110M eventos

Ejemplo 1: Problemas en una subred

Martes 17/11/2015, 10:00 AM

- Se detectan problemas de conexión con Internet en una subred de laboratorios.
- ¿Será el cortafuegos?....
- Vamos a ver que está pasando en la última hora....

Ejemplo 1: Problemas en una subred

- No es el cortafuegos, pero ahora sabemos lo que pasa y como solucionarlo....
- El equipo tiene un proxy instalado en el puerto 80
  - Muy probablemente se ha activado el módulo proxy de Apache
  - Esta siendo accedido desde el extranjero:
    - US, CN, GB, RU, ID

Ejemplo 2: Carga elevada en el cortafuegos

Sábado 21/11/2015, 19:30

- La carga del cortafuegos ha pasado del 50%
  - El número de sesiones no ha sido muy elevado
  - ¿Posible escaneo desde multiples orígenes?

Ejemplo 2: Carga elevada en el cortafuegos

- Confirmado:
  - Múltiples orígenes
  - Con destino a una subred no asignada
  - La carga se debe a que está activado el log de los bloqueos

Ejemplo 3: Accesos remotos

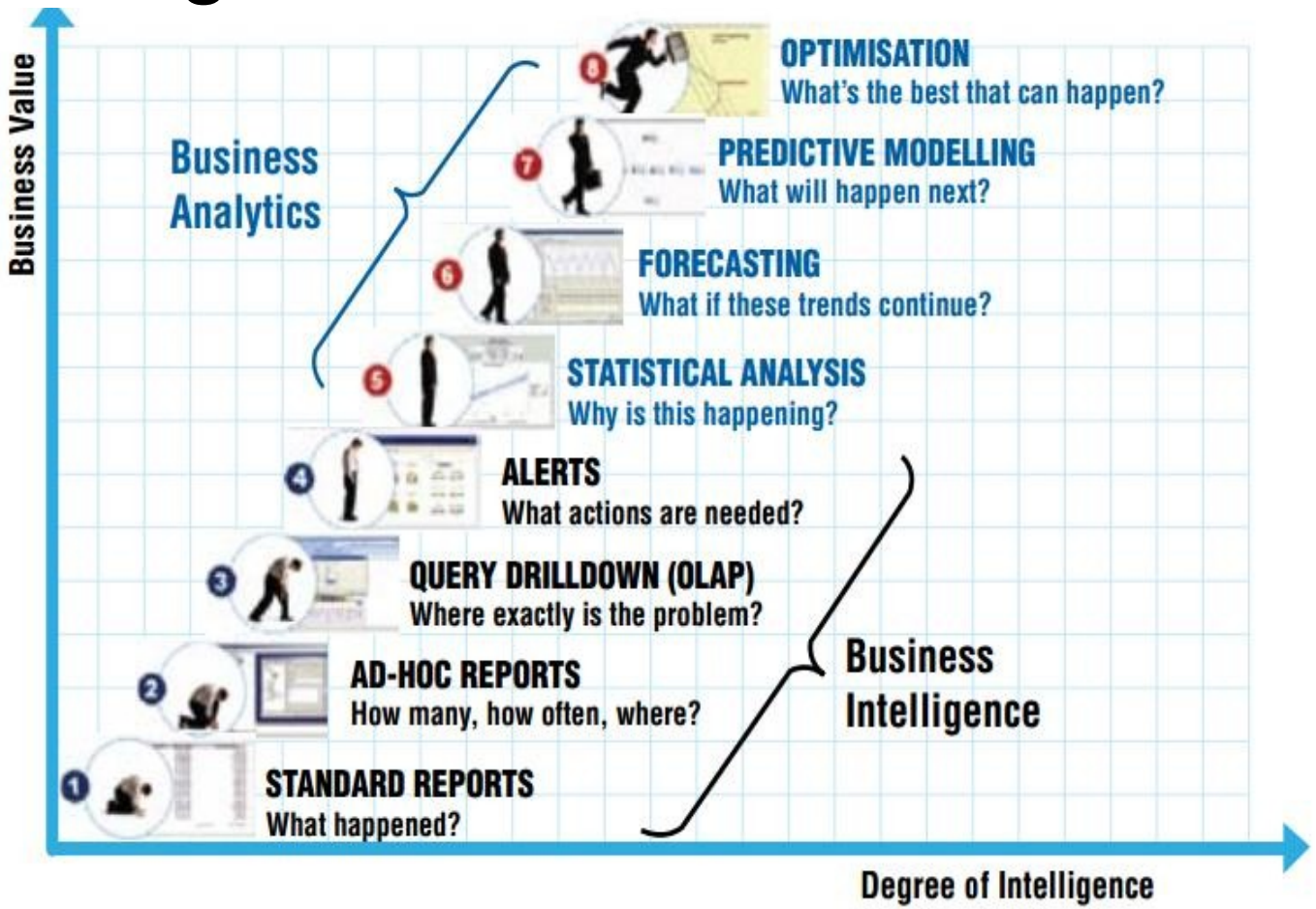
- Nos gustaría saber, si nuestros usuarios acceden a los sistemas red interna mediante SSH, Terminal Server, VNC, etc
- Podemos utilizar los bytes recibidos/enviados para determinar si la conexión ha tenido éxito o no
- Vamos a ver que pasó el 20/11/2015

Ejemplo 4: Paseo por otros Paneles

- ELK permite visualizar la información del funcionamiento del cortafuegos PaloAlto y agregarla a nuestro gusto
  - Y consultarla no supone un aumento en la carga del cortafuegos....

Modelo de Madurez

Hemos llegado al nivel 3 ó 5



Ideas de futuro

- Recopilar información para agilizar la respuesta a incidentes:
  - Inicios de sesión, en cualquier sistema
  - Consultas DNS
    - Para botnets, y descarga de malware
  - Antivirus
  - Accesos a aplicaciones
- Mejorar la infraestructura:
  - Pasar a 3 nodos

Ideas de futuro

- Pero sobretodo
  - Ofrecerlo como servicio para otras áreas:
    - Para saltar al nivel 5


grazie
dakujem
gràcies
merci
thanks
gracias
ありがとう
спасибо
hvala
obrigado
spas
mochchakkeram
bedankt
danke
bakka bér
شكراً
díky
thank you
gracias
ačiū
Salamat
grazas
Arigatō
감사합니다
Tak
gràcies
eskerrik asko
merci
grazie
aitäh
asante
dzięki
obrigado
dankon
köszönöm
dank
kiitos
ngiyabonga
terima kasih
tack
dankie
Շնորհակալություն

UC3M
SDIC

Universidad
Carlos III de Madrid
www.uc3m.es

Servicio de Informática y Comunicaciones

web: sdic.uc3m.es
twitter: @sdic_uc3m