Recogida de eventos de diferentes fuentes

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*

Rafael Calzada Pradas

@CertUC3M

Objetivo/Agenda

- Fuentes de inforormación interna
  - Cortafuegos perimetral e interno
  - Encaminadores
  - Servidores de autenticación
  - Accesos a servicios Web
- Recolección de la Información
- Elastalert
- Información de uso

Cortafuegos perimetral

- Flujos:
  - Hora de inicio, fin, aplicación, IP origen y destino, bytes transmitidos, tamaño medio de paquete, ¿usuario?
- Amenazas y ataques detectados
  - IP origen, tipo de ataque/amenaza

Encaminadores

- Flujos:
  - Hora de inicio, fin, IP origen y destino, bytes transmitidos, puertos y protocolo L4
- Ataques detectados:
  - DoS y DDoS
  - Escaneos de detección
  - Equipos internos comprometidos

Servidores de autenticación

SSO

Eduroam

VPN

LDAP

Servicios Web Legacy

- Usuario, IP origen

Clientes (Windows y Linux)

Ataques detectados:

- Fuerza bruta
- ¿Ubicuidad?

- Accesos a la plataforma
  - Correctos:
    - Usuario, IP origen, Objeto accedido, tiempo de respuesta, bytes entregados, User-Agent → analítica
  - Incorrectos:
    - IP origen, Objeto accedido, referer → Pentesting, enlaces erróneos

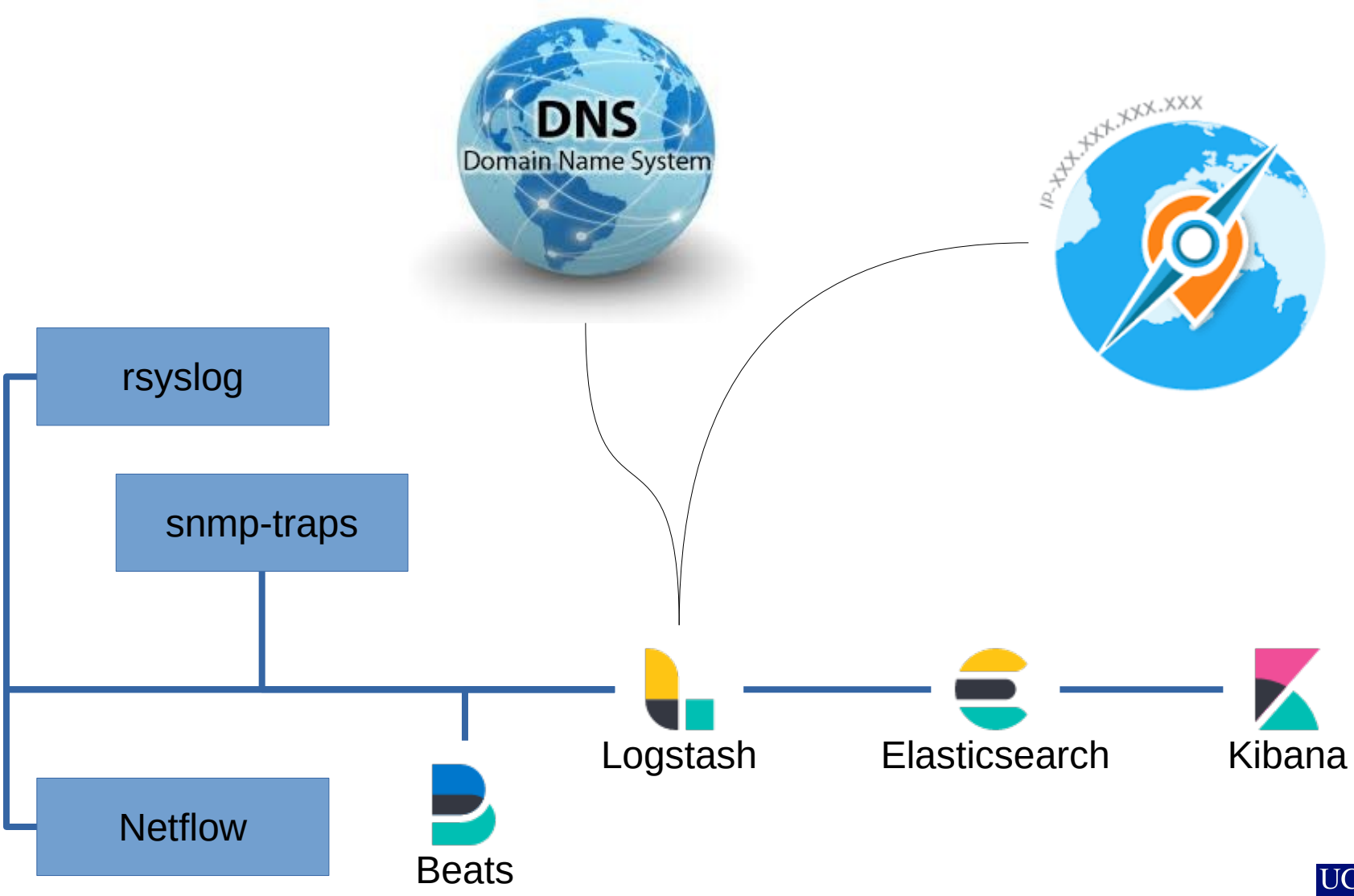
Accesos HTTP:

- C&C
- Ataques detectados
  (Similar a Cortafuegos de nueva generación):
  - Equipos internos comprometidos
  - Servidores internos *atacados*

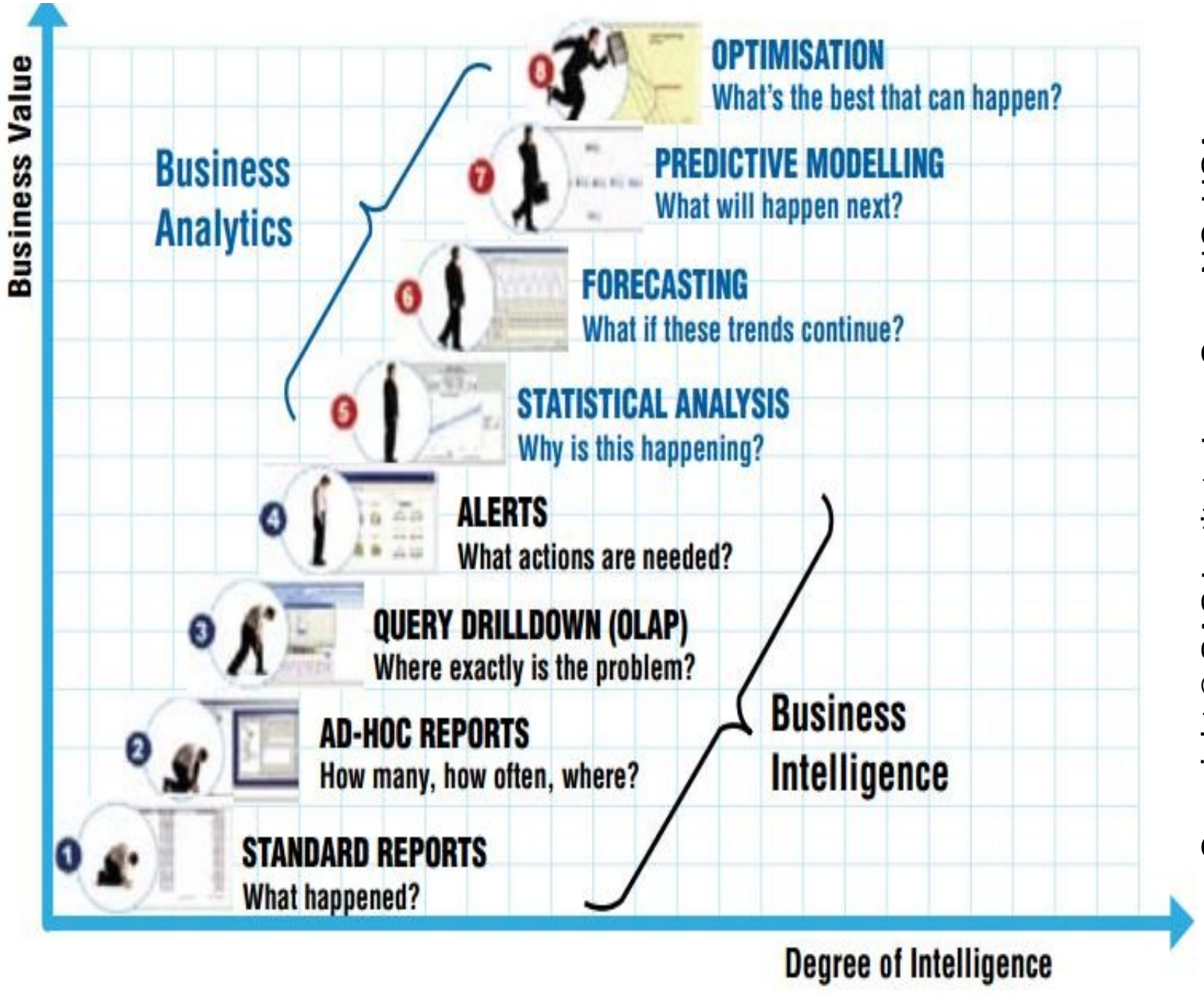
Consultas DNS:

- Complementa información Flujos

Recolección de la información



¿Dónde estamos?
¿Hacia donde vamos?



Retos

- Eventos:
  - Muchos
  - De muchas fuentes
  - Cuidado con RGPD y LOPDyGDD
  - ¿Plazo de conservación?
- Infraestructura
  - Capacidad de proceso/almacenamiento
  - Visión 360º. No sólo para seguridad
- Salida
  - IPs con mala reputación, URLs a bloquear
  - ¿Qué es un ataque?
  - Cuidado con los falsos positivos…
- MANTENER INFORMADOS A LOS USUARIOS → AUTOSERVICIO

Plugin de Kibana

Permite generar alertas en base a consultas sobre los datos en Elasticsearch

https://github.com/Yelp/elastalert

- Email
- JIRA
- OpsGenie
- **Commands**
- HipChat
- MS Teams
- Slack
- Telegram
- GoogleChat
- AWS SNS
- VictorOps
- PagerDuty
- Exotel
- Twilio
- Gitter

Configuración de alertas:

https://elastalert.readthedocs.io/en/latest/ruletypes.html

Ejemplo de alerta

```
# Alert when some field changes between documents
# This rule would alert on documents similar to the following:
# {'username': 'bob', 'country_name': 'USA', '@timestamp': '2014-10-15T00:00:00'}
# {'username': 'bob', 'country_name': 'Russia', '@timestamp': '2014-10-15T05:00:00'}
# Because the user (query_key) bob logged in from different countries (compare_key) in the same day (timeframe)

# (Optional)
# Elasticsearch host
# es_host: elasticsearch.example.com

# (Optional)
# Elasticsearch port
# es_port: 14900

# (Optional) Connect with SSL to Elasticsearch
#use_ssl: True

# (Optional) basic-auth username and password for elasticsearch
#es_username: someusername
#es_password: somepassword

# (Required)
# Rule name, must be unique
name: New country login

# (Required)
# Type of alert.
# the change rule will alert when a certain field changes in two documents within a timeframe
type: change

# (Required)
# Index to search, wildcard supported
index: logstash-*
```

Ejemplo de alerta

```
# (Required, change specific)
# The field to look for changes in
compare_key: country_name

# (Required, change specific)
# Ignore documents without the compare_key (country_name) field
ignore_null: true

# (Required, change specific)
# The change must occur in two documents with the same query_key
query_key: username

# (Required, change specific)
# The value of compare_key must change in two events that are less than timeframe apart to trigger an alert
timeframe:
  days: 1

# (Required)
# A list of Elasticsearch filters used for find events
# These filters are joined with AND and nested in a filtered query
# For more info: http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/query-dsl.html
filter:
- query:
    query_string:
      query: "document_type: login"

# (Required)
# The alert is use when a match is found
alert:
- "email"

# (required, email specific)
# a list of email addresses to send alerts to
email:
- "elastalert@example.com"
```

Uso de listas públicas

- 1, AlienVault Reputation, https://www.alienvault.com/open-threat-exchange/ip/IPADDRESS
- 2, Block List DE, http://www.blocklist.de/en/index.html, https://lists.blocklist.de/lists/all.txt
- 3, Brute Force Blocker, http://danger.rulez.sk/index.php/bruteforceblocker/
- 4, Dshield Block List, https://www.dshield.org/xml.html, https://www.dshield.org/block.txt
- 5, Emerging Threats, https://www.proofpoint.com/us/threat-intelligence-overview
- 6, Malware Domain List, https://www.malwaredomainlist.com/
- 7, OpenBL Base, http://www.openbl.org/
- 8, Ransomware Tracker CW C2 DOMBL, https://ransomwaretracker.abuse.ch
- 9, Ransomware Tracker CW C2 URLBL, https://ransomwaretracker.abuse.ch
- 10, Ransomware Tracker CW PS DOMBL, https://ransomwaretracker.abuse.ch
- 11, SPAMHAUS Drop, https://www.spamhaus.org
- 12, SPAMHAUS Edrop, https://www.spamhaus.org
- 13, SSL Abuse, https://sslbl.abuse.ch/blacklist

Interfaz de consulta

uc3m | Universidad Carlos III de Madrid

CONSULTA LISTAS DE REPUTACIÓN

La Universidad Carlos III utiliza listas de reputación negativa para bloquear las conexiones hacia sitios potencialmente peligrosos.

Desde esta página puede consultarse si un determinado sitio web o una determinada dirección IP se encuentra incluida en alguna de dichas listas de reputación negativa.

En caso de que el sitio web o la dirección aparezcan, se proporciona información para que el administrador del sitio pueda solicitar la baja de la lista en la que se encuentre.

Introduzca el nombre del sitio o la dirección IP:

Lookup

Buscando información sobre: **218.4.168.82**

Información sobre la dirección: **218.4.168.82**

Nombre de la lista: Brute Force Blocker

Más información de la lista: Página informativa de la lista

URL: Descarga de la lista completa

Información adicional: 218.4.168.82 # 2018-11-20 15:30:57 3 1539345

Referencias del ponente

- Explotación de logs con ELK
  (Grupo de Usuarios PaloAlto)
  - https://www.youtube.com/watch?v=0fhVNu_egCo
- Gestores de Log
  (Grupos de Trabajo de RedIRIS 2015)
  - http://tv.rediris.es/es/jt2015/492/file/459.html
- Visualización y Analitica de Logs
  (Jornadas Técnicas de RedIRIS 2015)
  - http://tv.rediris.es/es/jt2015/486/file/504.html
- Taller de ELK (Jornadas Técnicas de RedIRIS 2016)
  - https://tv.rediris.es/es/jt2016/642/file/579.html

Referencias externas

- Elastic WebSite
  - http://www.elastic.co
- SearchGuard
  - https://search-guard.com
- Data driven security (libro)
  - http://datadrivensecurity.info/
- “Enhancing Intrusion Analysis through Data Visualization”, Wylie Shanks, 2015. (Artículo)
  - https://www.sans.org/reading-room/whitepapers/detection/enhancing-intrusion-analysis-data-visualization-35757
- Managing events @1M events/s using Elasticsearch (presentación)
  - https://speakerdeck.com/joealex/managing-security-at-1m-events-a-second-using-elasticsearch


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

UC3M
SDIC

Universidad
Carlos III de Madrid
www.uc3m.es

web: sdic.uc3m.es
twitter: @CertUC3M
Mail: rafael.calzada@uc3m.es/cert@uc3m.es