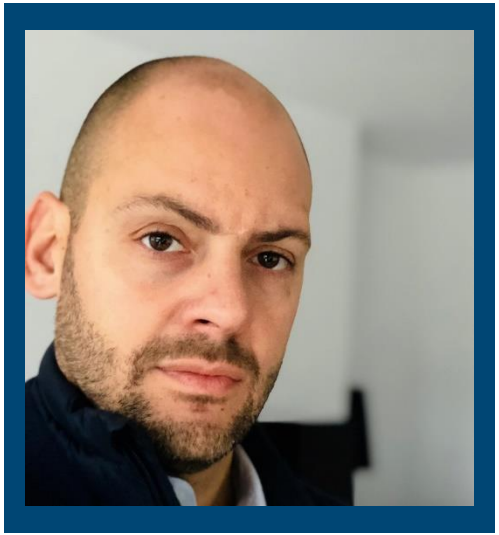
XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

Dealing with infected “anonymous” endpoints

CCN-CERT
centro criptológico nacional



- Xavier Panadero Lleonart
- Centre de Seguretat de la Informació de Catalunya
- xpanadero@cesicat.cat

Índice

CESICAT

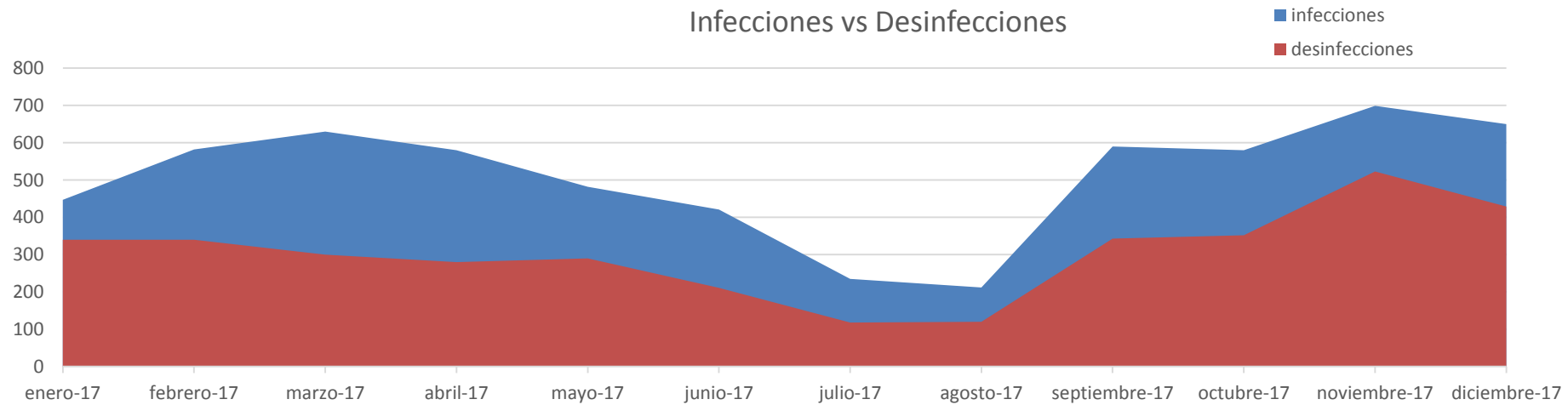
Centro de Seguridad de la Información de Catalunya

El Centro de Seguridad de la Información de Catalunya – CESICAT - es por acuerdo de gobierno GOV/103/2012, el encargado del gobierno y la gestión de la ciberseguridad en la Generalitat de Catalunya y su sector público.

Problemática

Un titular para invitar a la reflexión

Aproximadamente el 50% de los incidentes de seguridad por código malicioso son altamente complejos de resolver **por no poder identificar** los sistemas afectados.



Problemática

Un titular para invitar a la reflexión

Aproximadamente el 50% de los incidentes de seguridad por código malicioso son altamente complejos de resolver **por no poder identificar** los sistemas afectados.

Infected “anonymous” endpoints

Origen del problema

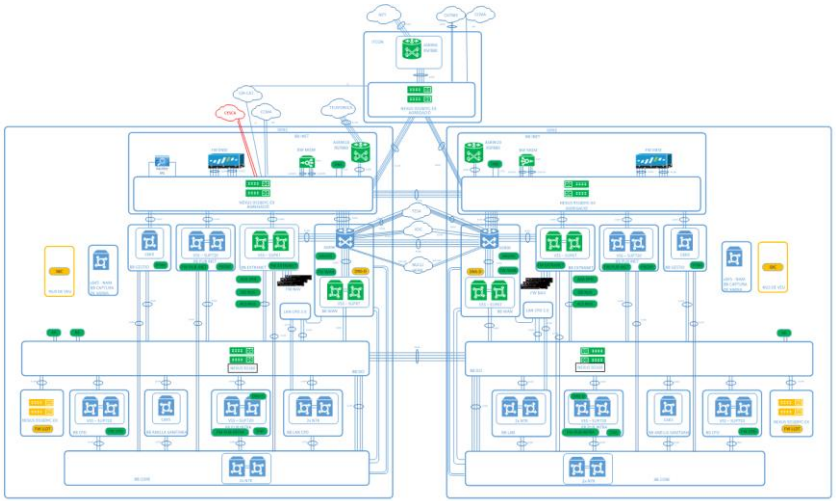
Puesto de trabajo

- **Elevado numero de usuarios**
- **Gran numero de sedes**
- Entorno **NO TRANSFORMADO**
- **Inventarios desactualizados**
- **Complejidad** de los diferentes departamentos

Origen del problema

Red

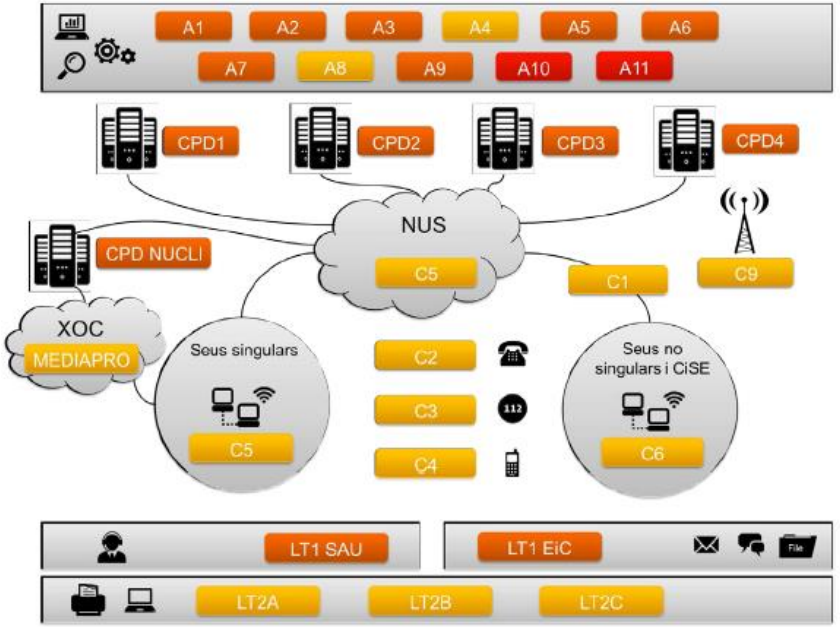
- Acceso a la red **sin autenticación**
- **Asignación dinámica de IP's**
- **Arquitecturas diferentes** según entorno productivo (NAT / Proxies)
- **Inventarios desactualizados** y con falta de información.
- **Red de invitados y de proveedores**



Origen del problema

Entorno multiproveedor

- **Tres proveedores** de puesto de trabajo
- **Diferentes niveles de madurez** en la gestión del puesto de trabajo



Consecuencias

La **imposibilidad de detectar el origen** provoca graves consecuencias

- Riesgo de **propagación**
- **Impacto** en la red
- **Alteración del nivel de protección**
- **Dificultad en determinar** el nivel real de **impacto** real al negocio
- **Elevada dedicación** en el intento de identificar las maquinas

Posibles soluciones

1ª Aproximación - **Cabeceras HTTP**

- Cabecera X-Forwarded-For
- Custom Headers

```
Hypertext Transfer Protocol
> HEAD / HTTP/1.1\r\n
  Host: [redacted].com\r\n
  User-Agent: curl/7.51.0\r\n
  Accept: */*\r\n
  X-Forwarded-For: 10.0.11.209\r\n
  X-Forwarded-For-Port: 49832\r\n
  NewHeader: 10.0.11.209\r\n
  \r\n
  [Full request URI: http://[redacted].com/]
  [HTTP request 1/1]
  [Response in frame: 22]
```

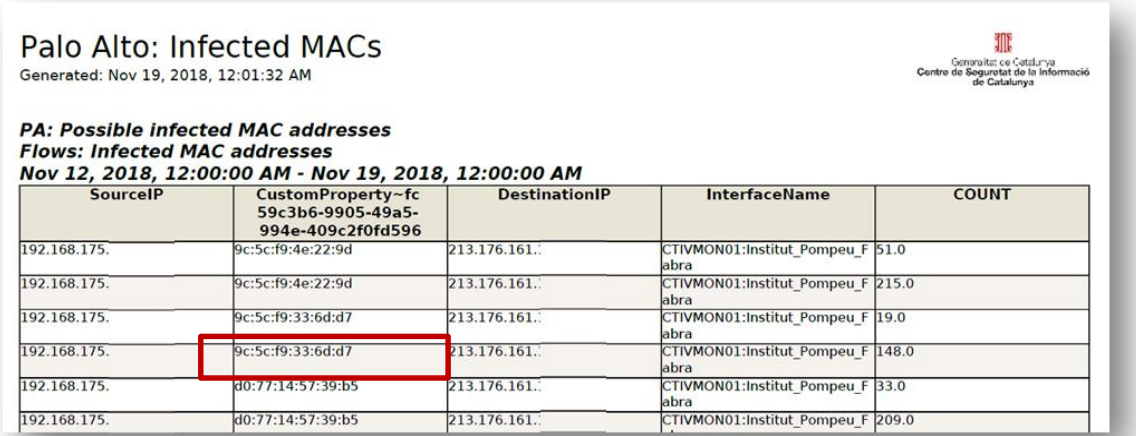
Ratio identificación: **32%**

- Solo es válido para tráfico web
- Pérdida de visibilidad en HTTPS

Posibles soluciones

2ª Aproximación – **Correlación de eventos**

- Filtrado de contenidos
- DHCP
- Netflows
- Proxies



Palo Alto: Infected MACs

Generated: Nov 19, 2018, 12:01:32 AM

Generalitat de Catalunya
Centre de Seguretat de la Informació de Catalunya

PA: Possible infected MAC addresses
Flows: Infected MAC addresses
Nov 12, 2018, 12:00:00 AM - Nov 19, 2018, 12:00:00 AM

SourceIP	CustomProperty~fc 59c3b6-9905-49a5-994e-409c2f0fd596	DestinationIP	InterfaceName	COUNT
192.168.175.	9c:5c:f9:4e:22:9d	213.176.161.	CTIVMON01:Institut_Pompeu_Fabra	51.0
192.168.175.	9c:5c:f9:4e:22:9d	213.176.161.	CTIVMON01:Institut_Pompeu_Fabra	215.0
192.168.175.	9c:5c:f9:33:6d:d7	213.176.161.	CTIVMON01:Institut_Pompeu_Fabra	19.0
192.168.175.	9c:5c:f9:33:6d:d7	213.176.161.	CTIVMON01:Institut_Pompeu_Fabra	148.0
192.168.175.	d0:77:14:57:39:b5	213.176.161.	CTIVMON01:Institut_Pompeu_Fabra	33.0
192.168.175.	d0:77:14:57:39:b5	213.176.161.	CTIVMON01:Institut_Pompeu_F	209.0

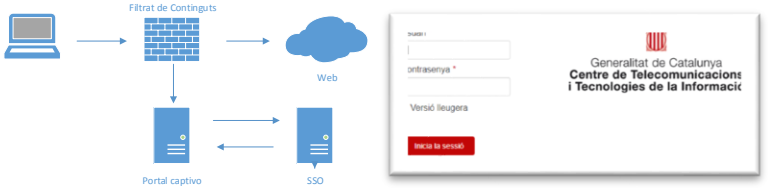
Ratio identificación: **84%**

- Tiempos y esfuerzo muy elevados en la integración de fuentes: 1 año -> 10 redes
- Requiere inventarios actualizados

Posibles soluciones

3ª Aproximación – **Autenticación en el Single Sign-On (SSO)**

- Se redirige al navegador a un **portal captivo** para forzar que este autentique vía SSO
- Si ya esta autenticado, **obtendremos automáticamente la identificación** del mismo vía SSO.
- En cas negativo, en el mejor de los casos el usuario puede que se autentique manualmente.



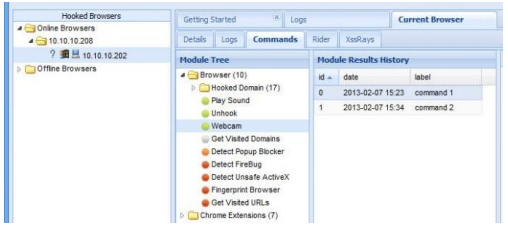
Ratio identificación: **42%**

- Solo válido para tráfico web.
- Requiere que el usuario ya este autenticado o que este se autentique.

Posibles soluciones

4ª Aproximación – **Inyección Framework Javascript (BEEF)**

- Se redirige al navegador a un **portal captivo** para forzar que este autentique vía SSO
- Se inyecta al usuario un framework javascript (BEEF) que permita interactuar con el navegador y ejecutar funciones que permitan identificar la maquina.



BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Ratio identificación: **12%**

- Solo válido para tráfico web.
- La evolución de los navegadores hace que muchas módulos ya no sean validos.

Posibles soluciones

5ª Aproximación – **SuperCookie**

- Se redirige al navegador a un **portal captivo** y se inyecta una super cookie para todo los dominios internos.

  Set-Cookie: CESICAT_10.X.X.X=192.18.1.X; domain=gencat.cat; Path=/

- Posteriormente se cruza el trafico de navegación hacia el resto de dominios para verificar si es viable su identificación mediante las URLS de navegación.

```
GET /path/login?user=GPTCPN002X
Domain: subdomain.gencat.cat
Cookie: CESICAT_10.X.X.X=192.18.1.X
```

Ratio identificación: **26%**

- Solo válido para tráfico web.
- Requiere que el endpoint infectado curse tráfico a dominios internos.

Posibles soluciones

6ª Aproximación – **TestWare**

- Se redirige al navegador a un **portal captivo,** donde se descarga un fichero que contiene el TEST de EICAR y tiene el siguiente nombre.

  CESICAT-10_X_X_X-192_18_1_X.txt

- El antivirus instalado en el endpoint genera un alerta que será posteriormente enviada a la consola central de gestión donde se podrá gestionar la información concreta del dispositivo.

Ratio identificación: **49%**

- Solo válido para tráfico web.
- Requiere que el endpoint infectado disponga del antivirus funcionando

Posibles soluciones

7ª Aproximación – **Emulación C&C**

- Se redirige al navegador a un **portal captivo,** y en función del código malicioso detectado se emula el C&C (H-Worm, Mirai, Nuclear Bot, …)
  - Ejecución
  - Desinstalación

```
select case cmd(0)
  case"excecute"
      param=cmd(1)
      execute param
  case"update"
      param=cmd(1)
      oneonce.close
      set oneonce=filesystemobj.opentextfile(installdir&installname,2,false)
      oneonce.write param
      oneonce.close
      shellobj.run"wscript.exe //b "&chr(34)&installdir&installname&chr(34)
      wscript.quit
  case"uninstall"
      uninstall
  case"send"
      download cmd(1),cmd(2)
```

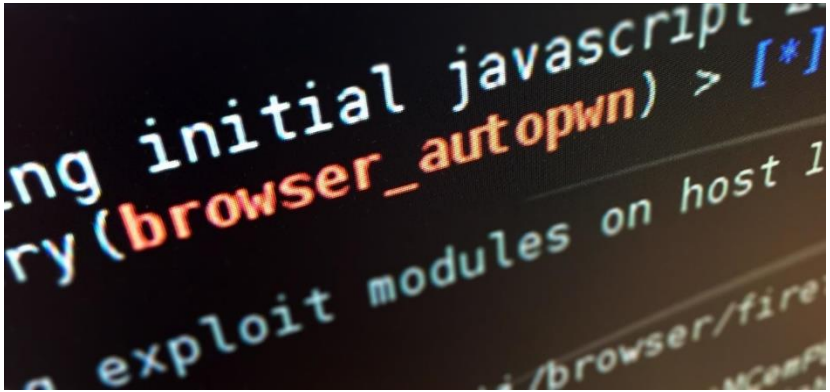
Ratio identificación: **32%**

- Solo válido para C&C conocidos.

Posibles soluciones

8ª Aproximación – **ExploitKit**

- Se redirige al navegador a un **portal captivo,** y en función del navegador se intenta explotar posibles vulnerabilidades para controlar posteriormente la maquina



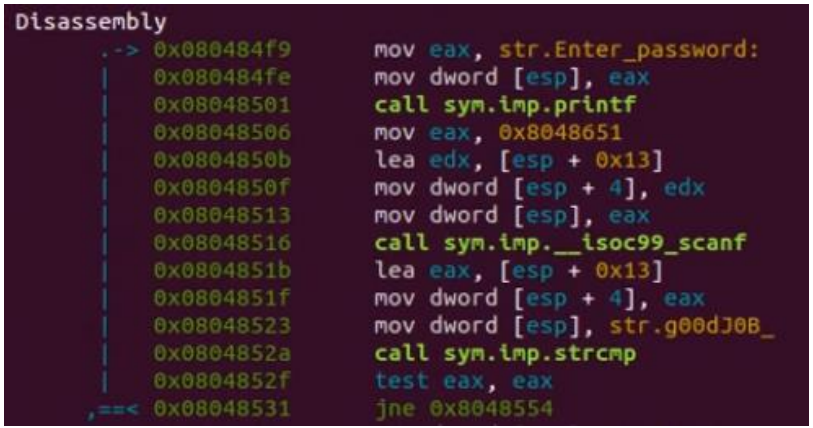
Ratio identificación: **27%**

- Solo válido para sistemas infectados mediante navegación

Posibles soluciones

8ª Aproximación – **GoodWare**

- **Ejecución de código malicioso modificado** (GoodWare) con el objetivo de infectar el mismo equipo y ejecutar acciones de identificación (envío de información del equipo al portal captivo).



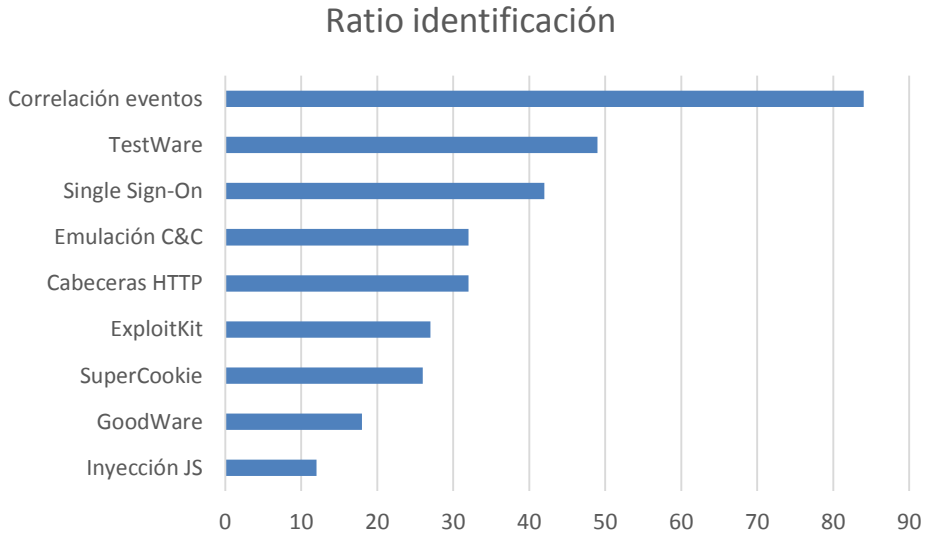
Ratio identificación: **18%**

- Requiere de conocimiento en desarrollo/reversing de código malicioso.
- Esfuerzo elevado por el nivel de muestra de código malicioso.

Posibles soluciones

Resumen

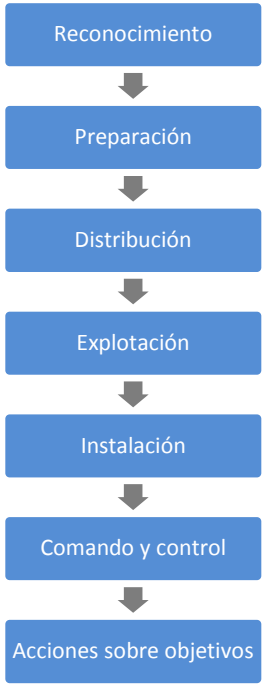
- Después de analizar las diferentes aproximaciones, su ratio de contribución y su dificultad de **implementación** se determino que la mejor aproximación es la **conjunción de todas aquellas cuyo ratio de identificación es superior al 25%**.



Implementación

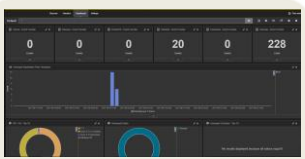
Sinkhole avanzado - Objetivos

- **Análisis del malware**.
  - Visualización y clasificación de todas las conexiones de la máquina infectada
  - Identificación de mutaciones, nuevos dominios, etc.
  - Clasificación.
- Correlación de la información de la navegación, resolución DNS, antivirus y eventos de autenticación del usuario.
- **Reconocimiento de la fase de la infección** basado en el Cyber Kill-Chain
- **Interacción con el malware.**



Implementación

Sinkhole avanzado - Arquitectura



Reporting

elasticsearch

Funcionamento

22, 2222, 23, 2223

21, 42, 8081, 80, 135, 443, 445, 1433, 1723, 1883, 1900, 3306, 5060,5061, 69

9200

https/ 64297

80

NFQ

Cowrie

Dionaea

Elastic Pot

ELK

Glastopf

Honey trap

Suricata

Metasploit

Dockerfile

Fuentes

Σ

DNS

Filtrado de contenidos

IPS

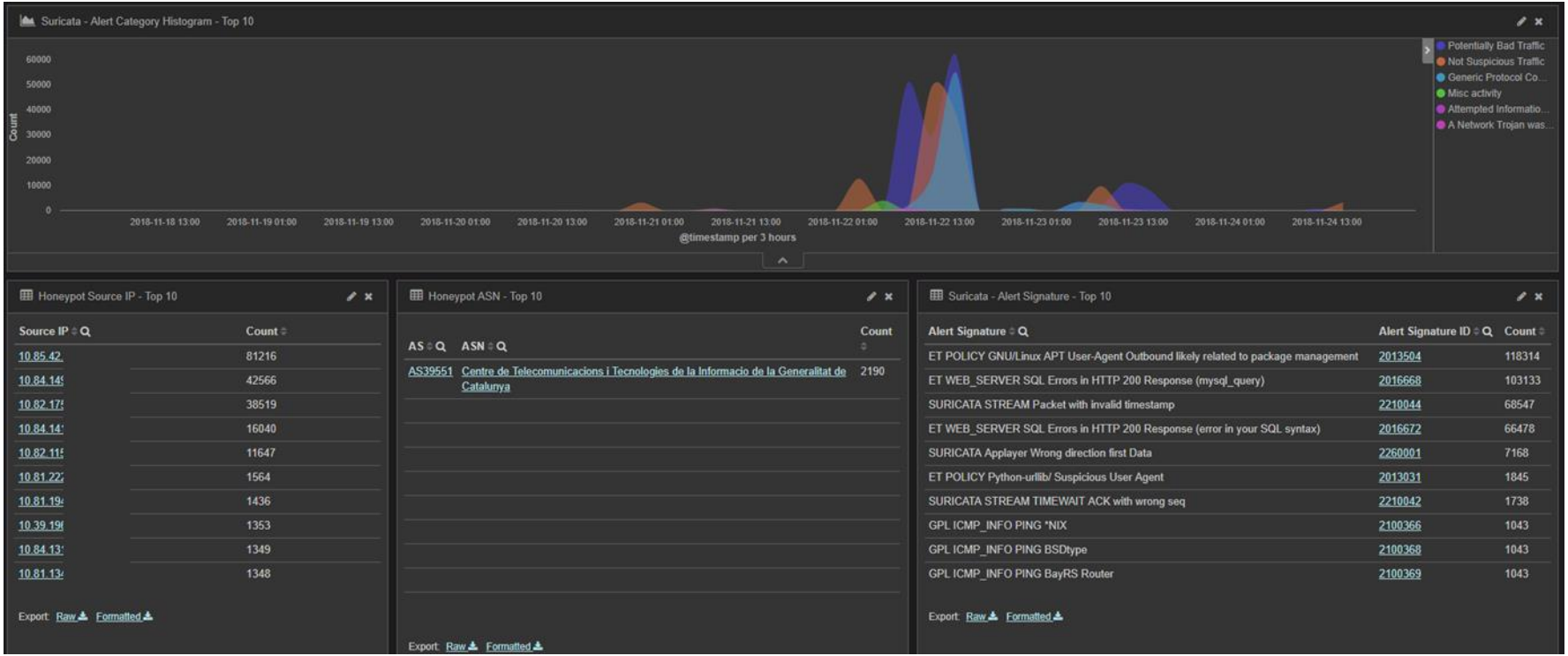
FW

Single Sign On

AV

Implementación

Sinkhole avanzado - Análisis



Consideraciones

- Marco legal general
- Generación de políticas y normativa interna
- Tipologías de usuarios
- Instrucciones operativas con proveedores

Ruegos y preguntas

xpanadero@cesicat.cat

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

CCN-CERT centro criptológico nacional