Compartiendo inteligencia de amenazas de forma sencilla con Minemeld.

Universidad Autonoma de Madrid & Universidad Carlos III de Madrid
www.uam.es & www.uc3m.es

UNIVERSIDAD AUTONOMA DE MADRID

uc3m

Minemeld (La Película)

Victor Barahona
Universidad Autónoma de Madrid

El escenario: red de la UAM

- Direccionamiento público (Clase B)
- 40K usuarios CPSC
  - la mayoría administran su PC
- 20K equipos siempre-conectados a una red de alta velocidad
- Una red abierta
  - lo que no está prohibido, está permitido :-(
- La jungla
  - redes del campus
- El orden
  - Infraestructura TIC

Casting: actores principales

- 2 x PaloAlto 5050
  - Core de red & seguridad
  - 2012 - ahora
- SIEM (Security Information & Event Manager)
  - Qradar OEM
  - 2008 - ahora
- CERT UAM (2 personas)
- Comunidad RedIRIS
- Minemeld
  - 2016

Primer Acto: La búsqueda

- Tātari
  - proyecto interno - basado en ACLs en el router ¡Mal!
- PanOS 5.0: DBL/EBL
  - https://panwdbl.appspot.com/
  - Pero cuando vas a añadir la lista numero 11...
- Buscando algo más óptimo
- Y llega: Minemeld
  - Marzo 2016
  - Jornadas PaloAlto - UC3M
  - Luigi Mori

Segundo Acto: Minemeld la solución

- Gestiona múltiples block-list
- Conecta las block-list con el dispositivo de seguridad
- Minemeld:
  - Flexible
  - Vendor neutral
  - Extensible
  - OpenSource
- Minemeld :
  - Miners: recolectan
  - Processor: agregan
  - Output: filtran

Segundo Acto: minemeld la solución

Fuentes Gratuitas

- Alienvault Reputation
- Bambenek
- BadIPs
- Binary Defense
- Blocklist.de
- Bruteforcelocker
- DShield
- Emerging Threats Open
- Feodotracker
- HailaTaxii
- Malwaredomain
- OpenBL
- Openphish
- Ransomwaretracker
- Spamhaus
- SSLBL
- Virt
- Virustotal

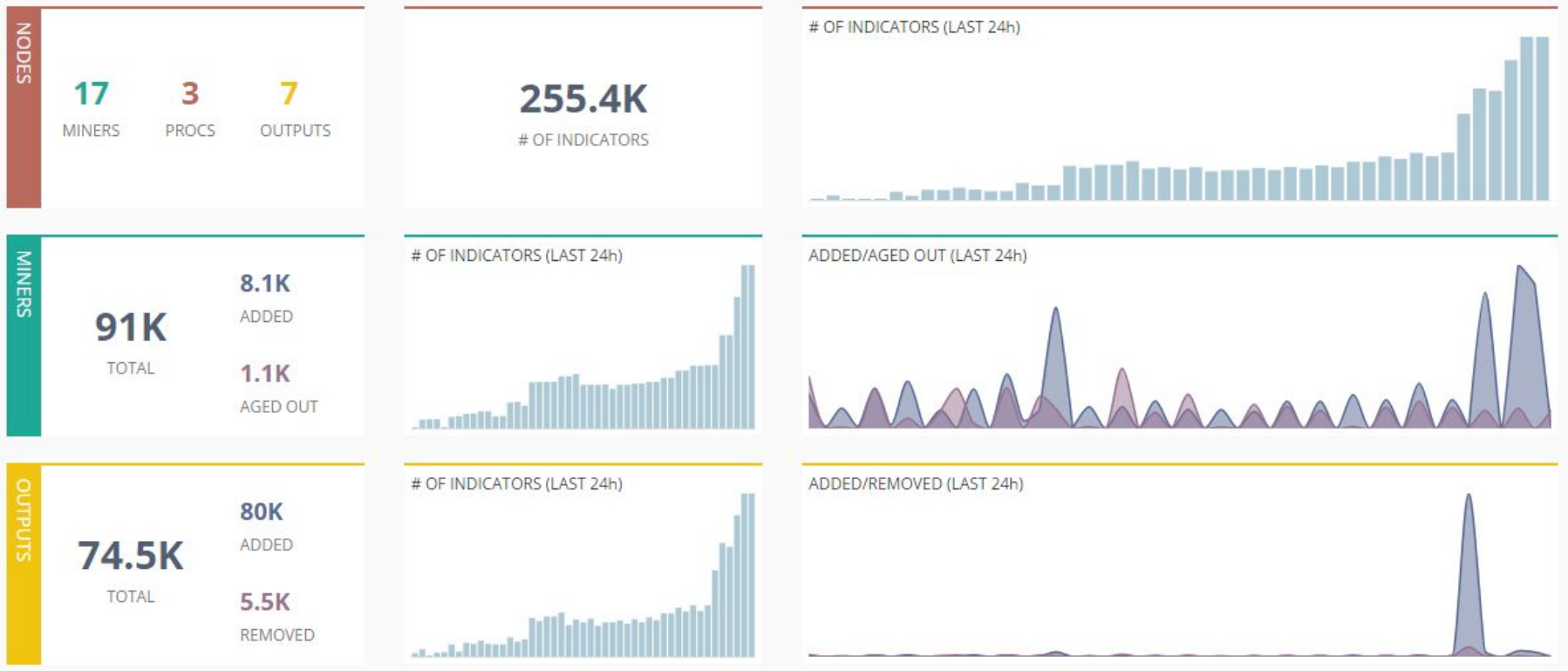
Listas de Infraestructuras

- AWS (Amazon, CloudFront, Route3, EC2)
- Azure CloudIP
- Google GCE
- Office365
- Torexit

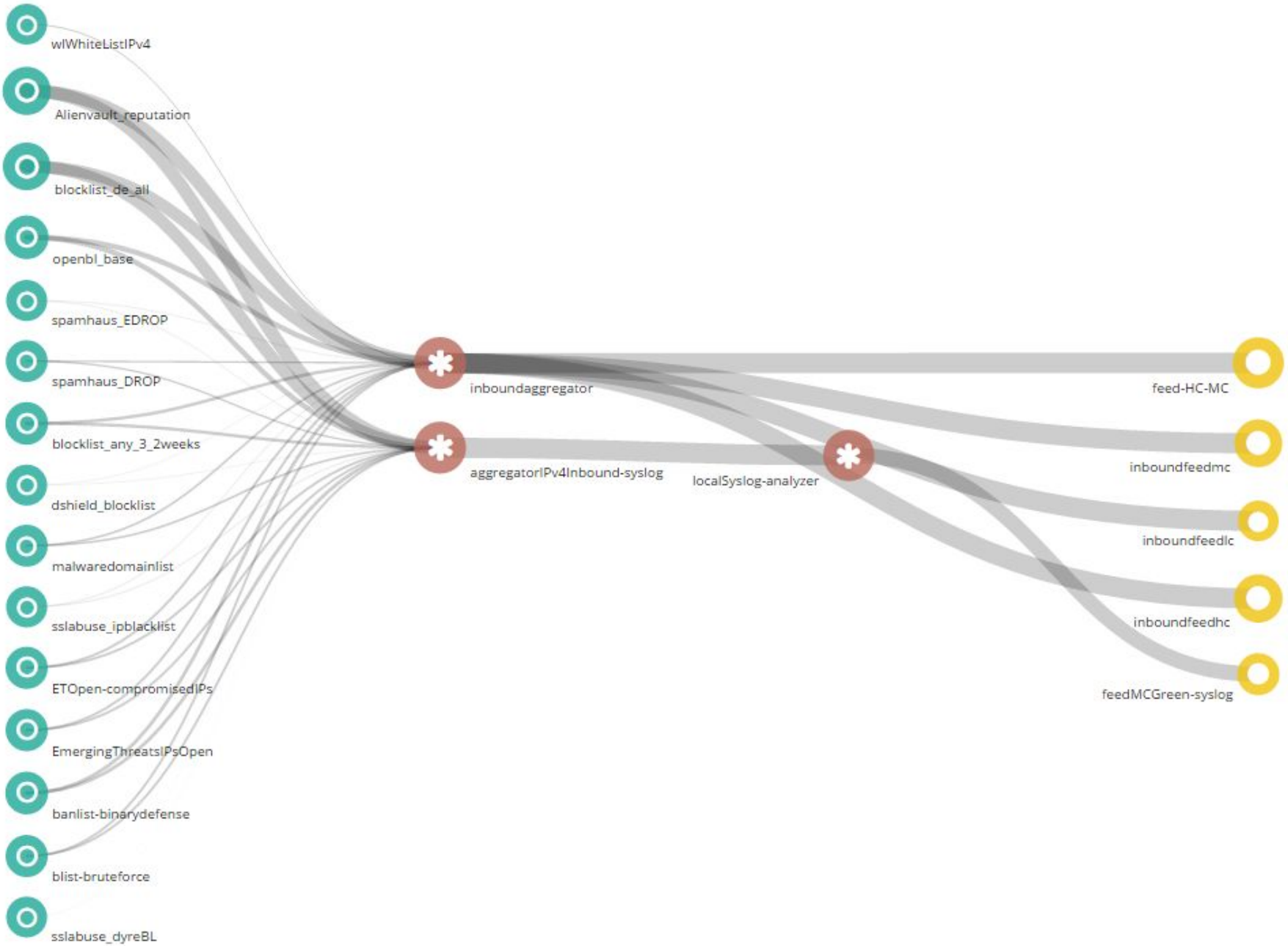
Fuentes comerciales

- Anomali
- AusCERT
- Autofocus
- RecordedFuture
- Phishme
- Proofpoint
- Themediatrust
- Threatq

Segundo Acto: minemeld la solución



CONNECTION GRAPH



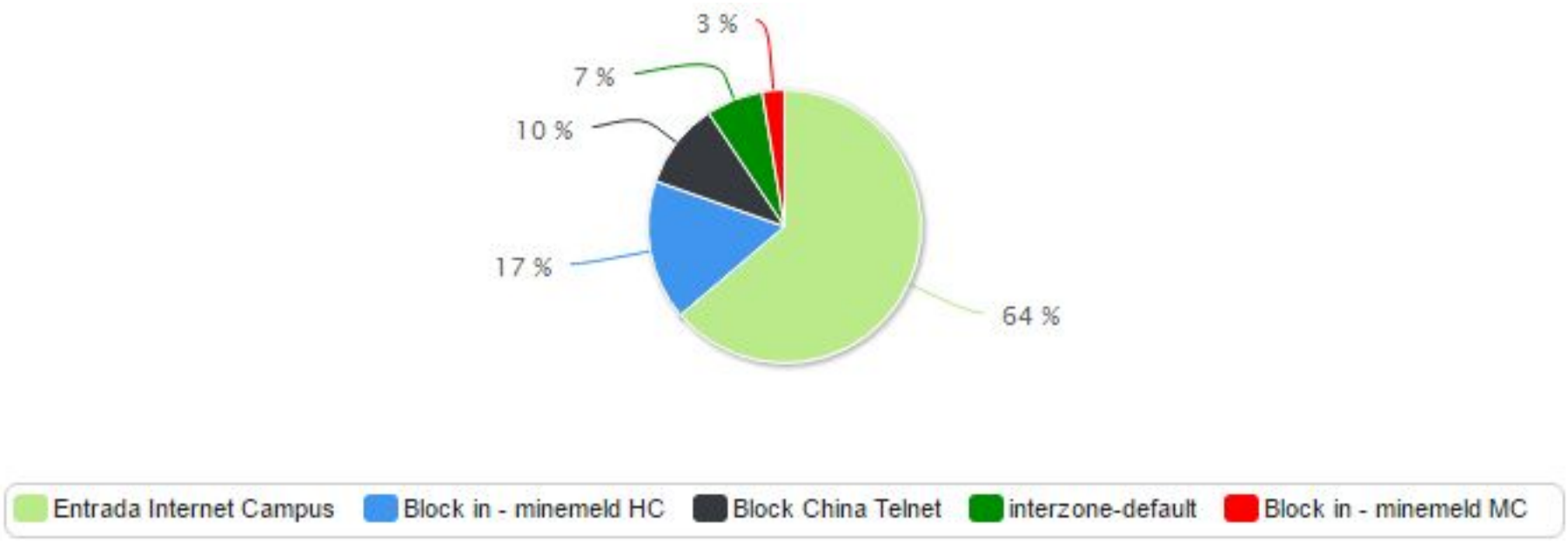
localSyslog-analyzer NODE

LOGS

SOURCES

METRIC	SINCE ENGINE START	HISTORY (LAST 1H)
ALIENVAULT.REPUTATION	1754717	
BADIPS.ANY_3	652609	
BINARYDEFENSE.BANLIST	110996	
BLOCKLIST_DE.ALL	240183	
BRUTEFORCEBLOCKER.BLIST	1622	
DSHIELD.BLOCK	95005	
ET.COMPROMISED_IPS	1654	
ET.OPEN	1654	
OPENBL.BASE	11400	
SPAMHAUS.DROP	0	
SPAMHAUS.EDROP	5	

Segundo Acto: minemeld la solución



Tercer Acto: los resultados

- Beneficios:
  - entre el 15-20% del tráfico de internet es (felizmente) descartado.
  - >300-800 drop/sec.
  - Filtrado de la red Tor de entrada.
- Hemos contribuido a la comunidad con un miner (`ETOpen.compromisedIPs`) :-)
- Problemas:
  - Límite de 50K IP en DBL/EBL
  - Estamos a la espera de actualizar a PANOS 7.1 para subir el limite a 150K
  - 150K se nos quedará pequeño pronto :-(
- Próximos pasos:
  - Syslog-miner: integrar los logs de PA como fuente.
  - Crear reglas trampa para actuar como “sinkhole”
  - Compartir listas con la comunidad
  - Uso de listas basadas en URL (PANOS 7.1) para limitar el phishing

Continuará...

Minemeld encuentra a ELK

Una relación con mutuos beneficios

Rafael Calzada
Universidad Carlos III de Madrid

Contexto: Quienes somos y de dónde venimos

- Universidad media con cuatro campus separados
  - 50 kms de distancia entre ellos.
- Más jóvenes que la mayoría
  - 27 años
- Compramos nuestro primer firewall hace tres años
  - SI, un PA-5050, SOC quería Alta Disponibilidad y tolerancia a fallos… pero no hubo suerte (se colaron otras prioridades)
    - Pero no nos dimos por vencidos y el segundo está de camino.
- Proyecto de Gestión de Logs
  - Debido a la necesidad de un SIEM, decidimos explorar una aproximación OpenSource
  - Tras un año evaluando data-sheets, elegimos ELK
  - ¿Adivinais cuál es nuestra más grande fuente de información? ¿y la segunda?

Role & feeling about Computer Security

- “Lo mejor que te puede pasar es que no sepan que existimos”
  - Si lo sabes es que que TIENES problemas
- Lo mismo para el Firewall
  - El mejor firewall, es transparente para el tráfico legítimo y te previene el de los chicos malos.
- ¿Cómo le enseñas todo esto a la Dirección?
  - Informes sobre conexiones y ataques bloqueados.
    - Correlaciona con la reducción de carga en el equipamiento del core de la red.
  - ¿Conoces Panorama? Yo también.
    - Es una buena herramienta para gestionar dispositivos PA y hacer informes, pero nos gustaría recoger información de otras fuentes (servidores web, encaminadores, radius, conmutadores, etc).

Vida del proyecto

- 2014:
  - Reutilizamos un servidor DL580 (5 años) y un MSA (5 años y 14 TB de HDD)
    - Le dopamos con 76 GB of RAM (1.300€)
  - Empezamos con logs de PA
    - Alrededor de 90M eventos/día
  - Después, leer, leer y aprender un montón
- 2015:
  - El bebe se hizo grande y lo presentamos en sociedad
    - RedIRIS JJTT 2015 Tenerife
- 2016:
  - 1 nuevo nodo “reacondicionado” con 74 GB de RAM.
  - 22 TB HDD para el MSA
  - Gestionando sobre 200M de eventos/día (más de 150M del PA)
  - Próximamente:
    - Otro nodo reacondicionado con 76 GB de RAM
    - 1 servidor nuevo con 128 GB de RAM y 4TB de SSD
  - Más de 25k € para un proyecto que empezó como un sueño.

¿Y que tiene esto que ver entre PaloAlto y Minemeld?

- Cuales son los beneficios de usar Minemeld
  - Aprox 10% de sesiones bloqueadas debido a reglas de Minemeld
    - Telnet bloqueado en otra regla y es el 40% de las sesiones
    - ¿Que pasa si bloqueamos una IP interna?
      - Será muy probablemente un equipo comprometido
  - ¿Donde viven los chicos malos?
- ¿Cómo pensamos alimentar MineMeld?
  - Simplemente guardaremos la información en ELK y a buscar
    - Hay diferentes niveles de confianza dependiendo de los parámetros de búsqueda.
  - Alimentar Minemeld de sink-holes
    - Cuidado con “Source Address Spoofing”

Me callo para mostraros unas imágenes y un video...


16-10-2016 02: 00

¿Alguna pregunta?

Próximamente:
Tpot, la chica nueva

El ménage à trois, con el que siempre soñamos

Gracias por su atención