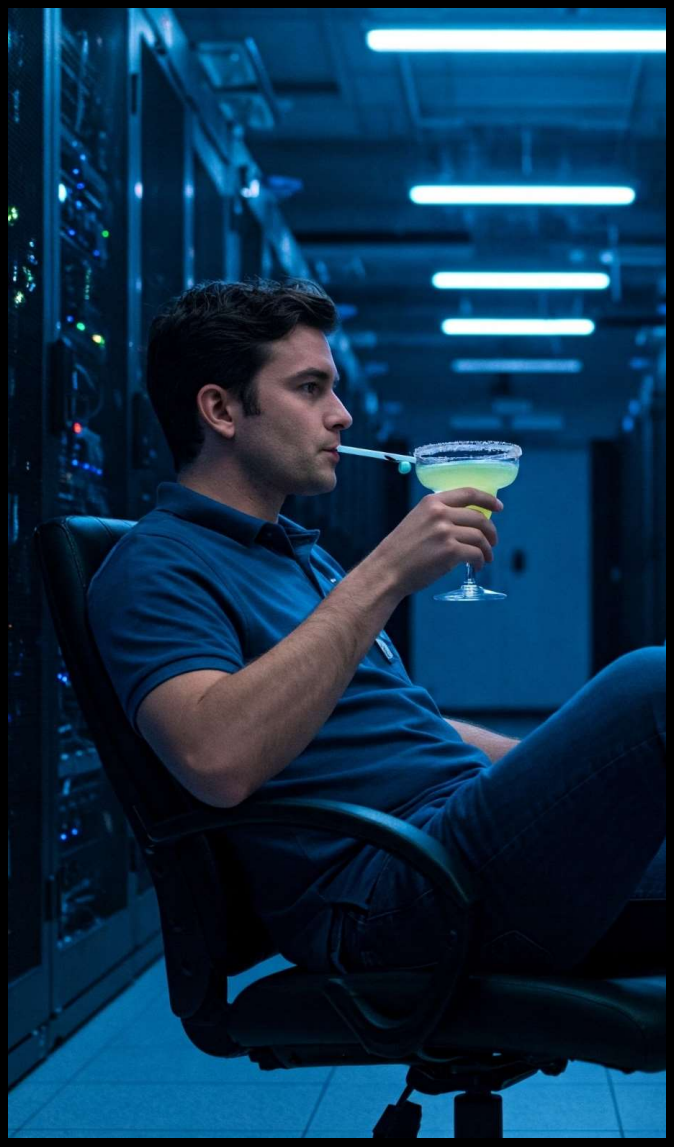
Estrategias de mitigacion en Infraestructuras IXP

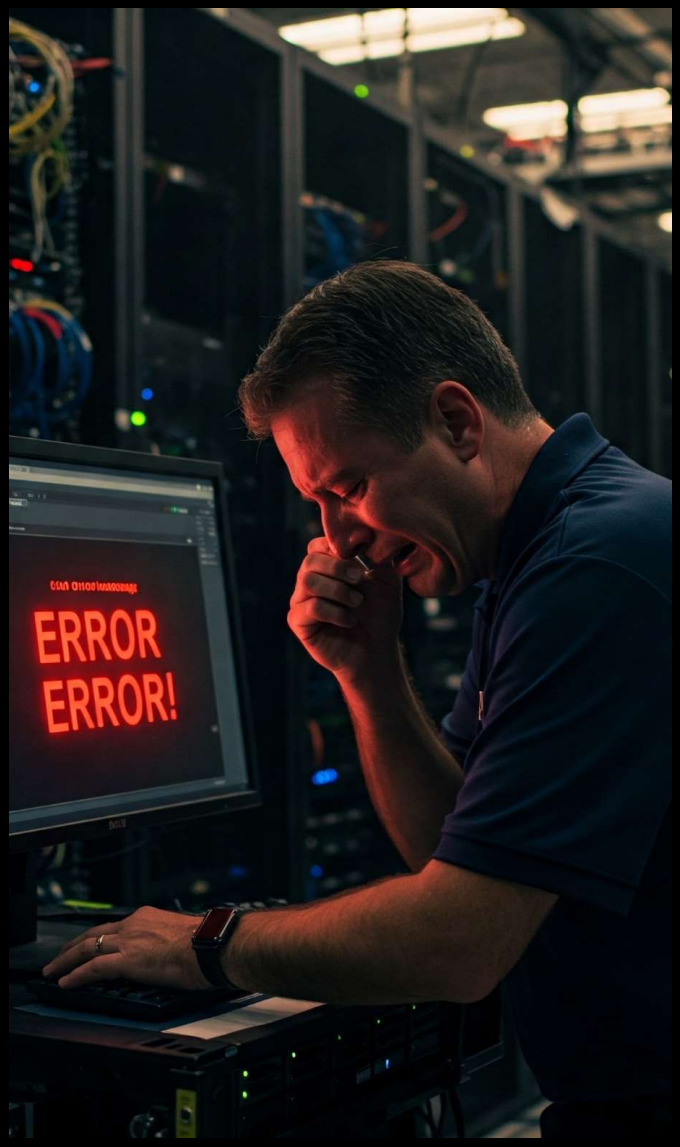
Ing. Martin Fuentes
Sales Engineering SOLA

radware

CUAL ES LA REACCION DEL EQUIPO TECNICO DE TU EMPRESA ANTE UN ATAQUE DDOS?

radware




ERROR
ERROR!

¿Qué es un ataque DDoS?

Es un tipo de ataque, que busca saturar los recursos de la victima, de forma que queden **inaccesibles para los usuarios**

1. **Ataques Aplicacion**
   Ataques enmascarados en solicitudes legitimas, que buscan saturar los recursos del WebServer
2. **Ataques Protocolo**
   Ataques orientados a la capa de comunicacion, que buscan saturar las capacidades de los dispositivos.
3. **Ataques Volumetricos**
   Ataques de gran volumen de trafico, que buscan saturar el bandwidth disponible

+127%

Crecimiento promedio del volume de ataques, 2024 vs. 2023

+265%

Crecimiento en los ataques WEBDDoS Mitigados H1’24 vs. H2’23

61%

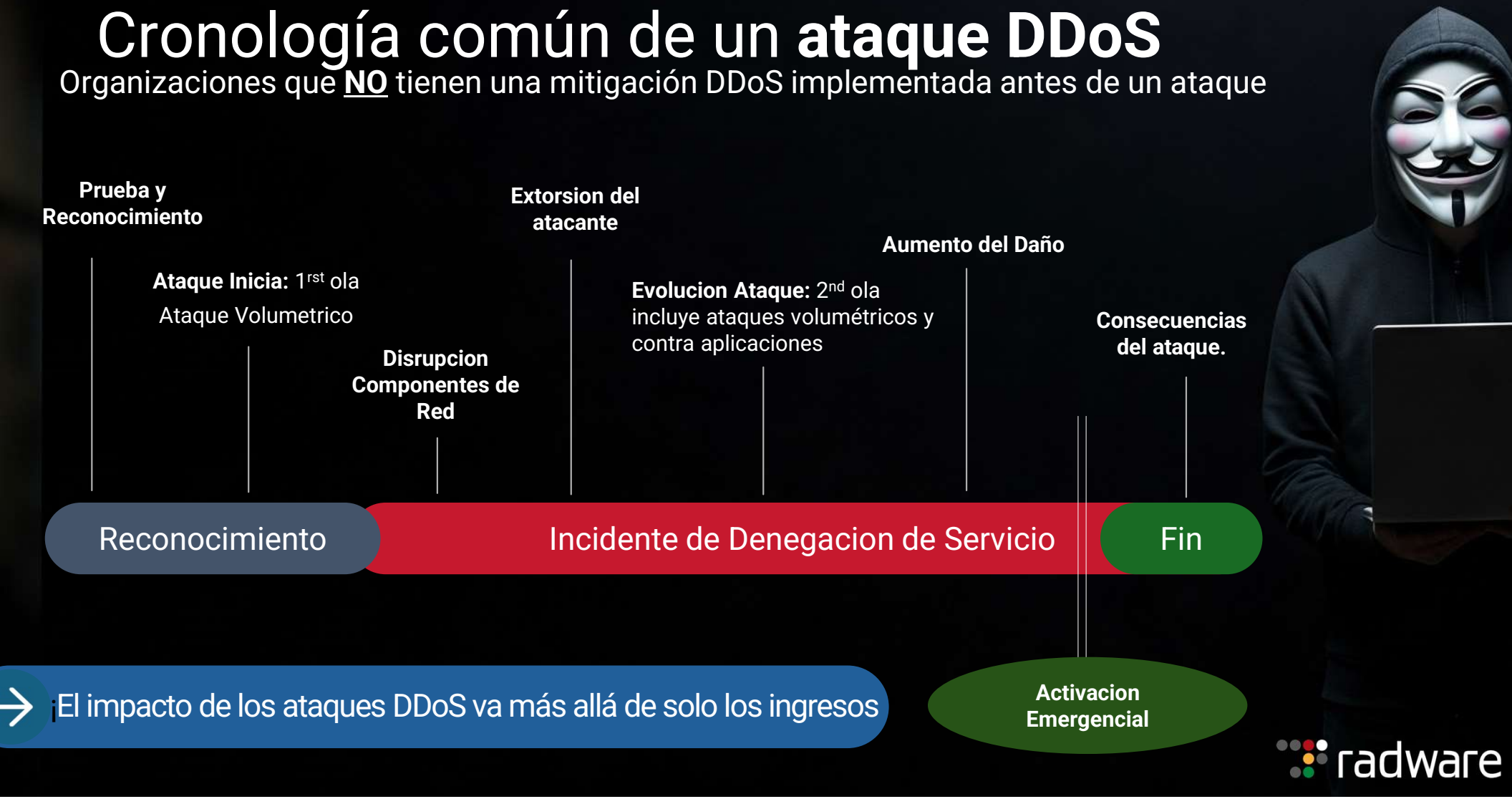
Crecimiento en las transacciones de BAD BOTS, H1’24 vs. H2’23

Los ataques de Denegacion de Servicio, aumentan en frecuencia, tamaño y complejidad, en todos los vectores.

radware

Cronología común de un **ataque DDoS**

Organizaciones que **NO** tienen una mitigación DDoS implementada antes de un ataque



radware

Herramientas Modernas de Ataque **Todo-en-Uno** en Github

Los atacantes no distinguen entre vectores de ataque como WAF, DDoS y bots.

Necesitamos una plataforma integrada para superar las herramientas de ataque todo-en-uno

Features And Methods

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk_captcha
  - STRESS | Send HTTP Packet With High Byte
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP "if (isset($_COOKIE))"
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Expliot
  - XMLRPC | WP XMLRPC expliot (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BYPASS | Bypass Normal AntiDDoS
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website

DDoS attack vectors

Bot attack vectors

Web application exploits

Built-in bypass again common defenses

radware

FASES DEL DIAGNOSTICO

REPETIR

DETECCION
Estoy Bajo Ataque?

CARACTERIZACION
Quien me esta atacando?

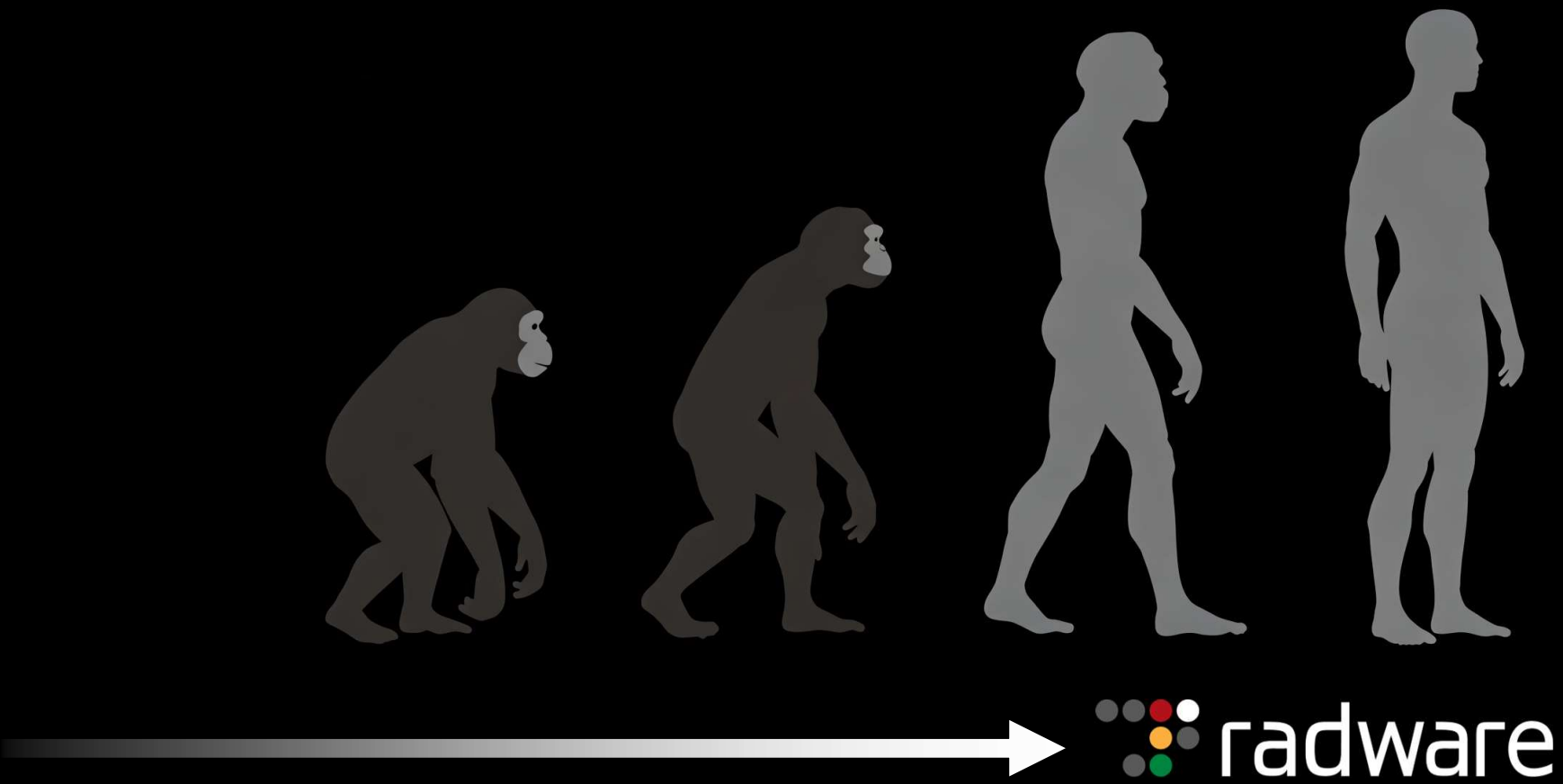
MITIGACION
Que Accion Tomo?

TERMINACION
Finalizo El evento??

- No es trivial: un ataque en sus primeros estadios puede confundirse con otros tipos de incidente
- Quien y Como me ataca? Donde buscar la informacion? Como correlacionarla?
- A mas burda la medida, mayor el impacto. Mientras mas quirurgica, mas transparente para el usuario
- Realmente finalizo o es un ataque de rafaga (BURST)? Continua pero cambio la morfologia del ataque?

radware

EVOLUCIÓN EN LAS ESTRATEGIAS DE MITIGACIÓN



radware

FASE 1: FUERZA BRUTA

DETECCION
Estoy Bajo Ataque?

CARACTERIZACION
Quien me esta atacando?

MITIGACION
Que Accion Tomo?

TERMINACION
Finalizo El evento??

- **Impacto Significativo en Operaciones:** Deben descartar todos los elementos de la red ya que no se tiene Certeza del ataque.
- Analisis de Logs, Flows y Debugs de Consola.
  Complejo ante ataques avanzados (DDoS)
- Accion limitada: ACL/Flowspec (Basico), Ratelimit (Ataque simple), Blackhole (Indisponibilidad)
- Control manual.
  Riesgo ante ataques multivector o BURST

TTM: HORAS

radware

FASE 2: AUTOMATIZACIÓN

DETECCION
Estoy Bajo Ataque?

- Consolidacion de informacion estadistica mediante analisis de flujos y otros origenes de datos.
- Uso de ML/IA
- Unica Consola

CARACTERIZACION
Quien me esta atacando?

- Analisis estadistico para busqueda de patrones (multiples variables)
- Limitado por muestreo 1:XXXX

MITIGACION
Que Accion Tomo?

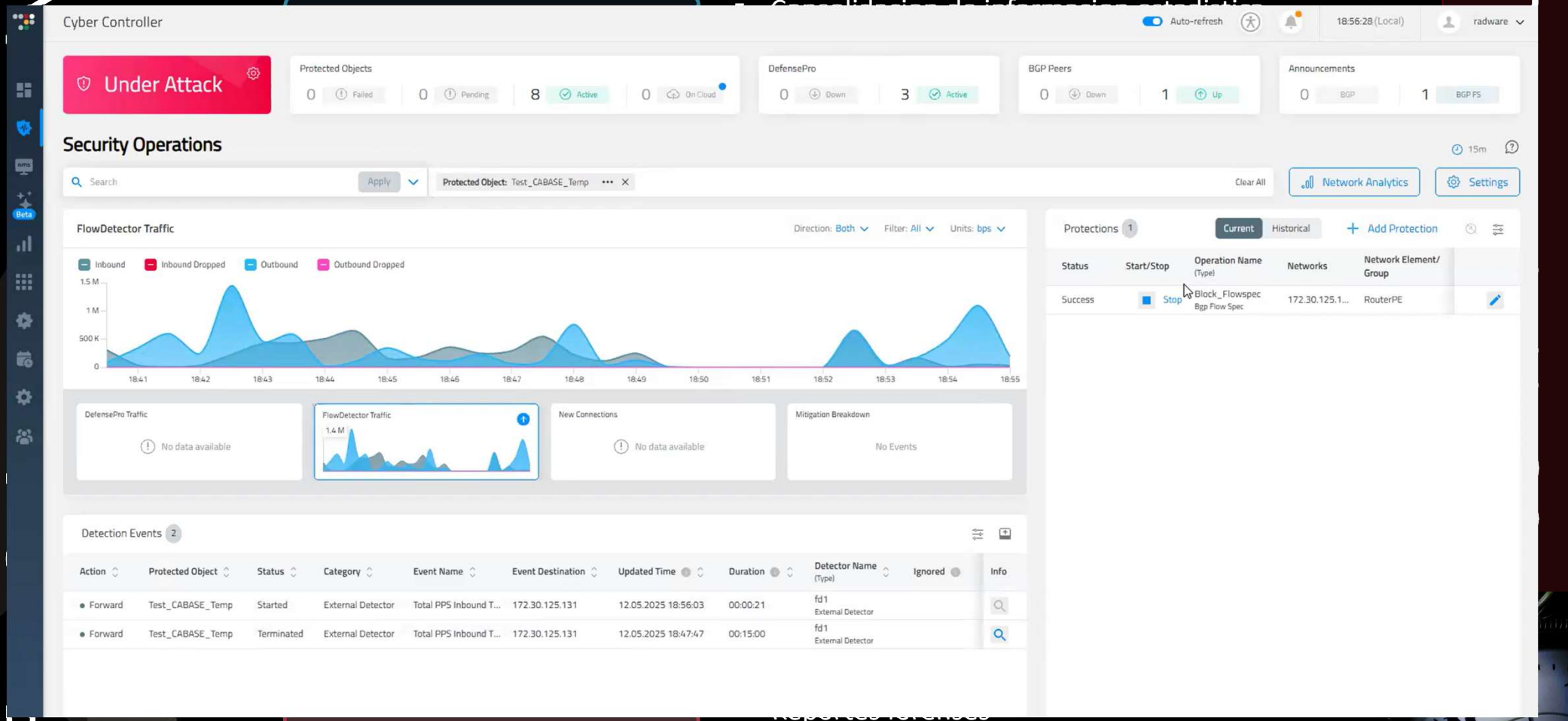
- Acciones puntuales sobre routers: BH, ACL, Ratelimit, BGP Flowspec (no quirurgico)

TERMINACION
Finalizo El evento??

- Deteccion Automatica de fin del evento.
- Restauracion de las configuraciones.
- Reportes forenses

TTM: MINUTOS

radware


Cyber Controller
Auto-refresh
18:56:28 (Local)
radware
Under Attack
Protected Objects
0 Failed
0 Pending
8 Active
0 On Cloud
DefensePro
0 Down
3 Active
BGP Peers
0 Down
1 Up
Announcements
0 BGP
1 BGP FS
Security Operations
15m
Search
Apply
Protected Object: Test_CABASE_Temp
Clear All
Network Analytics
Settings
FlowDetector Traffic
Direction: Both
Filter: All
Units: bps
Inbound
Inbound Dropped
Outbound
Outbound Dropped
1.5 M
1 M
500 K
0
18:41
18:42
18:43
18:44
18:45
18:46
18:47
18:48
18:49
18:50
18:51
18:52
18:53
18:54
18:55
DefensePro Traffic
No data available
FlowDetector Traffic
1.4 M
New Connections
No data available
Mitigation Breakdown
No Events
Protections 1
Current
Historical
Add Protection
Status
Start/Stop
Operation Name (Type)
Networks
Network Element/ Group
Success
Stop
Block_Flowspec
Bgp Flow Spec
172.30.125.1...
RouterPE
Detection Events 2
Action
Protected Object
Status
Category
Event Name
Event Destination
Updated Time
Duration
Detector Name (Type)
Ignored
Info
Forward
Test_CABASE_Temp
Started
External Detector
Total PPS Inbound T...
172.30.125.131
12.05.2025 18:56:03
00:00:21
fd1
External Detector
Forward
Test_CABASE_Temp
Terminated
External Detector
Total PPS Inbound T...
172.30.125.131
12.05.2025 18:47:47
00:15:00
fd1
External Detector

radware

FASE 3: CLEANPIPE

DETECCION
Estoy Bajo Ataque?

iBGP

CARACTERIZACION
Quien me esta atacando?

MITIGACION
Que Accion Tomo?

TERMINACION
Finalizo El evento??

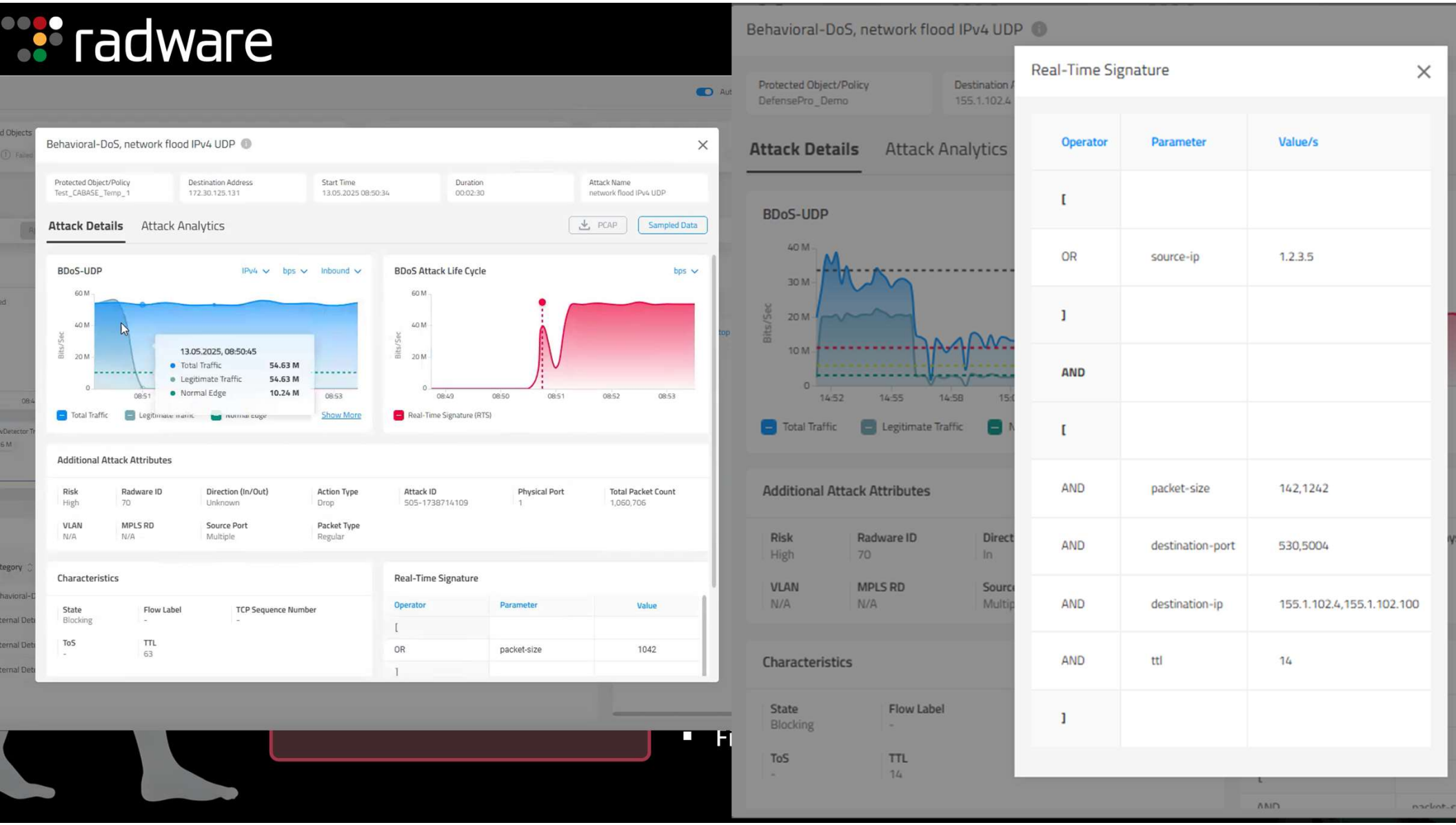
- Consolidacion de informacion estadistica mediante analisis de flujos y otros origenes de datos.
- Uso de ML/IA
- Unica Consola

- Analisis estadistico para busqueda de patrones (multiples variables)
- Solucion de Proposito Especifico: Todo el trafico recibido -> Insumo para politica en tiempo real

- Control Absoluto del trafico. Mitigacion Quirurgica no basada en Ratelimits (18s)
- Acciones complementarias sobre la red.
- Recalculo de firmas en tiempo real

- Capacidad de mitigacion de ataques BURST y Multivector.
- Finalizacion automatica

TTM: SEGUNDOS


radware
Behavioral-DoS, network flood IPv4 UDP
Protected Object/Policy
Test_CABASE_Temp_1
Destination Address
172.30.125.131
Start Time
13.05.2025 08:50:34
Duration
00:02:30
Attack Name
network flood IPv4 UDP
Attack Details
Attack Analytics
PCAP
Sampled Data
BDoS-UDP
IPv4
bps
Inbound
60 M
40 M
20 M
0
Bits/Sec
13.05.2025, 08:50:45
Total Traffic 54.63 M
Legitimate Traffic 54.63 M
Normal Edge 10.24 M
08:51
08:53
Total Traffic
Show More
BDoS Attack Life Cycle
bps
08:49
08:50
08:51
08:52
08:53
Real-Time Signature (RTS)
Additional Attack Attributes
Risk
High
Radware ID
70
Direction (In/Out)
Unknown
Action Type
Drop
Attack ID
505-1738714109
Physical Port
1
Total Packet Count
1,060,706
VLAN
N/A
MPLS RD
N/A
Source Port
Multiple
Packet Type
Regular
Characteristics
State
Blocking
Flow Label
-
TCP Sequence Number
-
ToS
-
TTL
63
Real-Time Signature
Operator
Parameter
Value
[
OR
packet-size
1042
]
Behavioral-DoS, network flood IPv4 UDP
Protected Object/Policy
DefensePro_Demo
Attack Details
Attack Analytics
BDoS-UDP
40 M
30 M
20 M
10 M
0
Bits/Sec
14:52
14:55
14:58
Total Traffic
Legitimate Traffic
Additional Attack Attributes
Risk
High
Radware ID
70
VLAN
N/A
MPLS RD
N/A
Characteristics
State
Blocking
Flow Label
-
ToS
-
TTL
14
Real-Time Signature
Operator
Parameter
Value/s
[
OR
source-ip
1.2.3.5
]
AND
[
AND
packet-size
142,1242
AND
destination-port
530,5004
AND
destination-ip
155.1.102.4,155.1.102.100
AND
ttl
14
]

FASE 4: SCRUBBING

DESBORDE

MITIGACION
Que Accion Tomo?

- Evolucion del CLEANPIPE
- Desborde a la nube, con capacidad de mitigacion de mas de 15 Tbps.
- Uso de BGP (redes /24)

TERMINACION
Finalizo El evento??

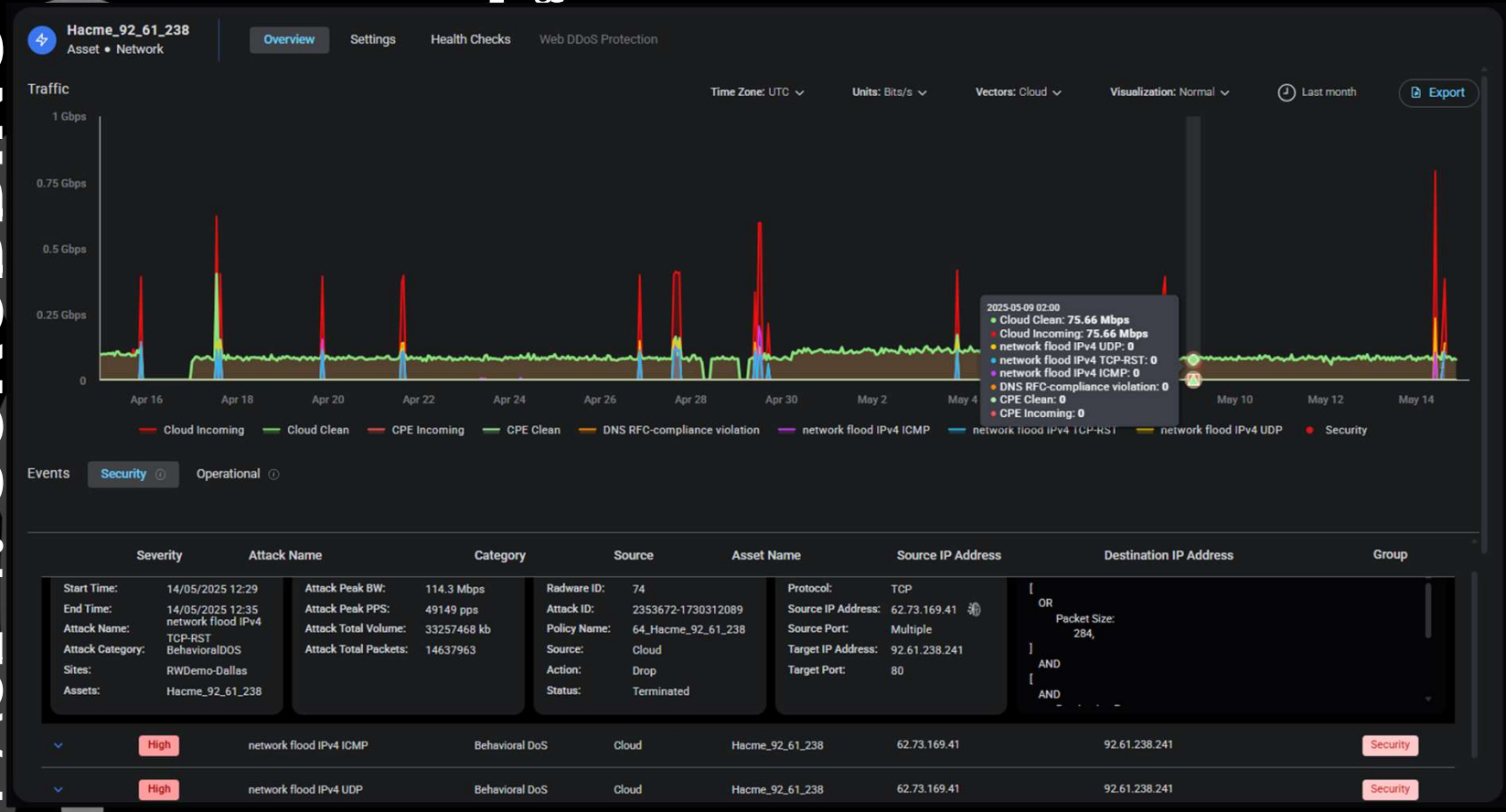
- Derivacion de retorno manual o automatica.
- Notificacion automatica

TTM: SEGUNDOS

FASE 4: SCRUBBING

DESB

TT



COMO ALCANZAR EL "ESTADIO MARGARITA"?

(SIN LA PLAYA ESO SI)

- **CLARIDAD EN LA ESTRATEGIA:** Solo Proteger nuestra infraestructura o garantizar el Servicio al cliente?
- **TIPO DE MITIGACION:** Basica (Ratelimits) o Avanzada (Firmas en tiempo real)
- **DETECCION INTELIGENTE:** Throughput o Analisis estadistico?
- **INVERSION, NO GASTO:** Proteger el Revenue del negocio
- **TCO:** Que carga operative genera? Que novedades incorpora?

MUCHAS GRACIAS!!

Ing. Martin Fuentes
Sales Engineering SOLA