RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: GRM-R03

Defending Zero Day

- Lessons from the Ebola Outbreak

Ebola Virus – History

- First detection in 1976 in Congo, Central Africa
  - Killed 288 people (88% fatality)
  - Disease was spread by close personal contact and by use of contaminated needles and syringes in hospitals/clinics.
  - Ebola is a river in Congo near the village where the first infection was found
- Second outbreak in 1995, again in Congo
  - Killed 250 people (81% fatality)
  - traced to patient-zero who worked in the forest adjoining the city.

Ebola Virus – History

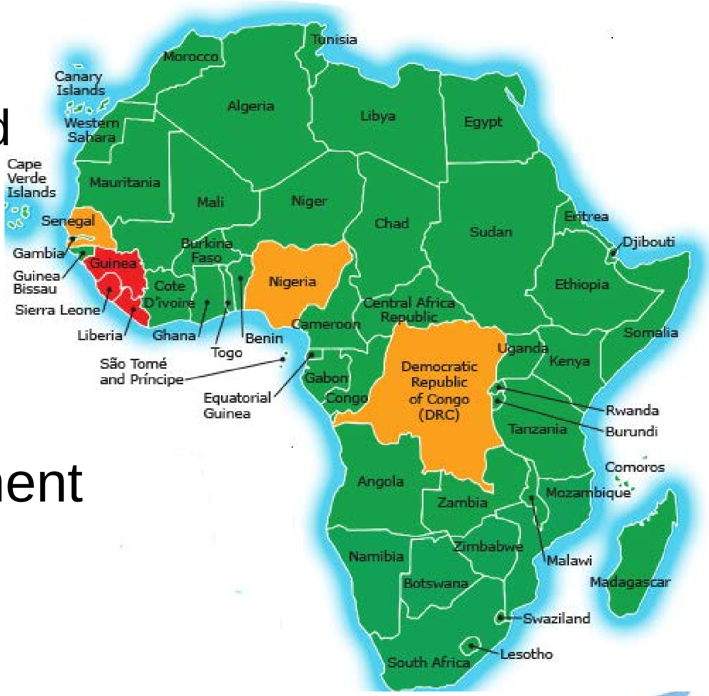
- Highly Contagious
  - Transmission from animals to humans and human to human
    - Through broken skin or mucous membrane
    - Close contact with infected patients and their body fluids.
    - Exposure to dead-bodies of infected patients

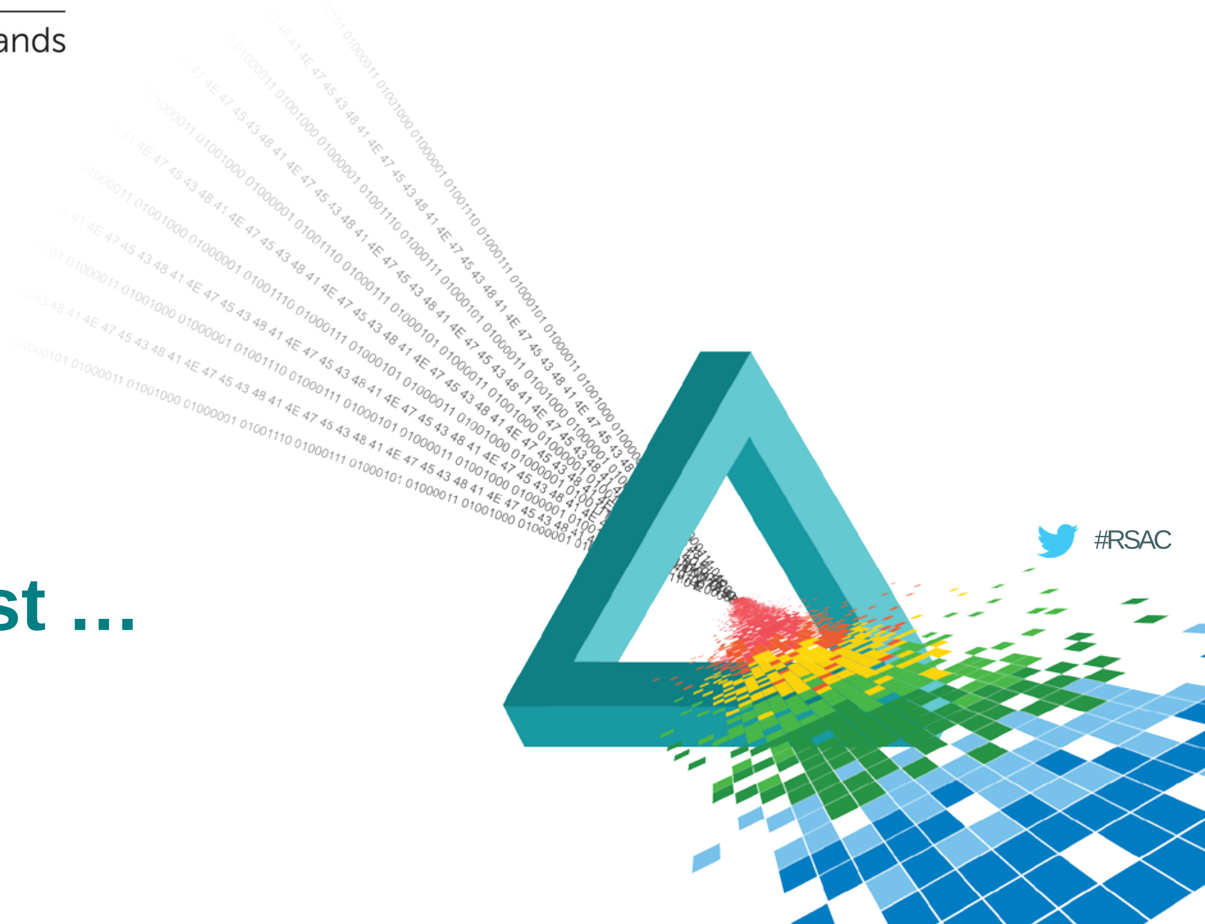
Ebola Cure

- No known cure or vaccines
  - In IT security parlance – a zero day exploit
- An equal opportunity killer
  - Ebola affects every human being – healthy or sick
  - Luckily in IT Security – very few universal exploit

Ebola Outbreak – 2014

- 4 Countries affected
  - Three failed to contain, 1 succeeded
- Liberia, Guinea, Sierre Leone
  - struggled to cope up
  - 14000 people died
- Nigeria , did a great job in containment
  - Only 8 people died





The Sad News first …

Guinea, Sierre Leone, Liberia

- Dec 2013 - Patient-zero in Guinea
  - 2 year old contacted the disease from Wild bats
- JAN-Feb 2014 - Spread out slowly
  - 5 deaths in immediate family
  - 8 deaths originating from a person who attended the funerals
- March 2014 - WHO declares outbreak
- March 2014 – June 2015
  - Spread to 2 neighbouring countries Liberia and Sierre Leone
  - Fatality rate ~ 50%
    - 30000 infections , 14000 deaths

Ebola Response

- Identify infected people
  - Quarantine/Treat the infected
- Contact Tracing
  - Who was in “contact” with the infected
  - Monitoring health status of these “contacts”
- Spread awareness
  - About precaution, detection and response

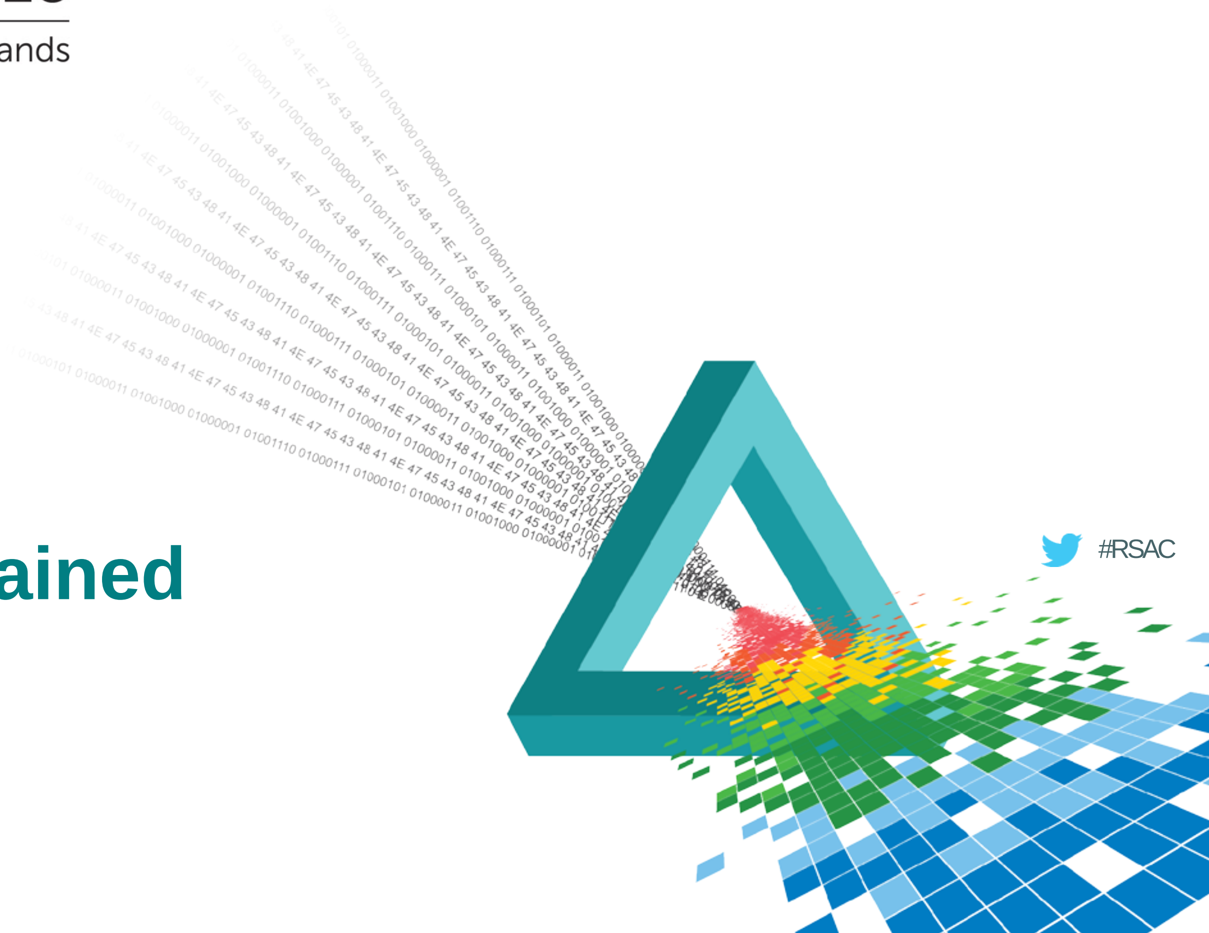
Safe Burial

Challenges

- Shortage of trained medical personnel
  - USA has 245 doctors/100000 people , Guinea has 10 doctors/100000 people
- Shortage of medical facilities
  - Shortage of Gloves , protective equipment , mattress for hospital beds
  - Death of medical staff due to lack of equipment
- Shortage of infrastructure
  - No technology or centralised facility for tracking status of “probable” cases
- Social Stigma for victims and care-givers
  - Lesser reporting by victims , increasing risk of transmission
  - Lesser number of voluntary care-givers, increasing fatality

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

How Nigeria contained Ebola

Ebola in Nigeria

- Nigeria
  - Most populous African country
  - Better medical facilities than first 3
- July 2014 : Patient-zero enters Nigeria (from Liberia)
  - Initially suspected as Malaria , Ebola was not detected until 3 days
    - Infects hospital staff
  - Patient zero dies on July 25
    - Other hospital staff died soon after
- Oct 2014 :WHO declared Nigeria Ebola Free
  - 20 infections, 8 deaths, no new infections till date

What Nigeria did right ?

- Securing Patient Zero
  - Patient identified and kept in quarantine
  - Not allowed to come into “contact” with others
- Efficient Contact tracing
  - 280 people identified as “contacts” of Patient zero. Total of 885 people tracked
  - Twice a day health check for these 885 people for 21 days
    - 18500 face-to-face visits by trained volunteers
- Better medical laboratories
  - For faster more accurate testing of samples

What Nigeria did right ?

- Learning for the past incidents
  - In 2012 , Nigeria has a similar incident against Polio Virus
  - Central Incident Response was used to track every child is getting vaccinated
  - This Center was converted into Ebola Emergencey Response centre for Contact tracing
- Good Governance
  - Declared a medical emergency on day of first detection
  - Presidential decree giving powers to track mobile devices and use law enforcement to track people at risk
  - Moving any corpse around the country required a letter , from the Ministry of Health, to certify that the death was not related to Ebola
  - Emergency Ebola phone hotline.

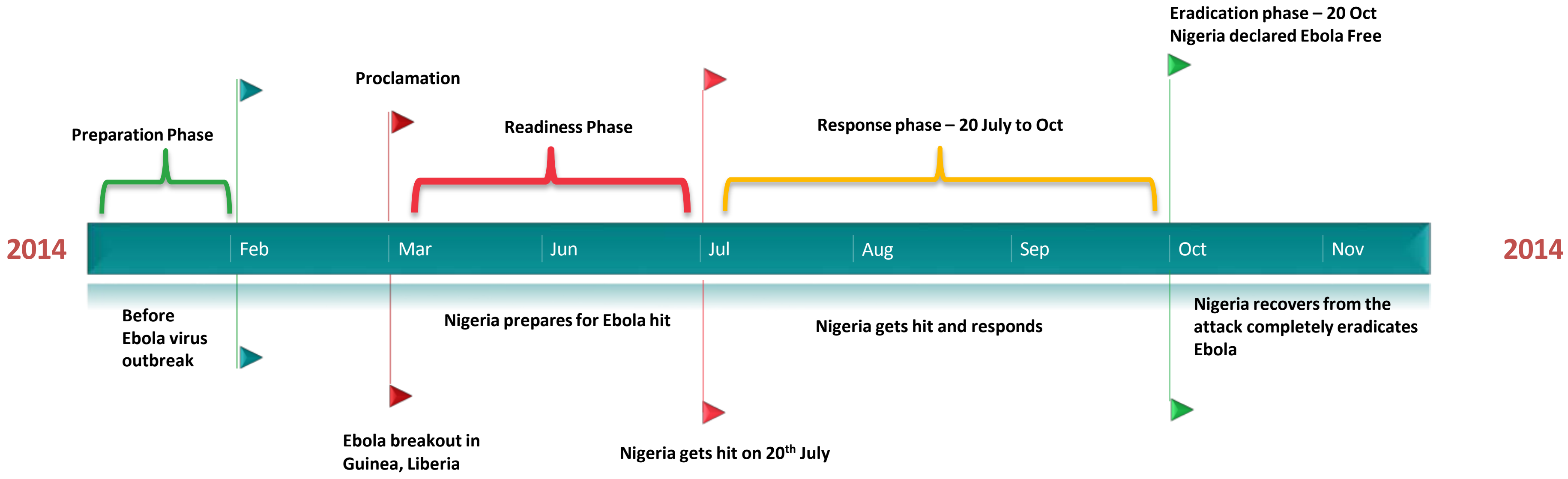
What Nigeria did right ?

- Awareness Campaign
  - Community approach to messaging
    - church leaders, military, doctors, government officials- all actively involved
  - Message of Hope
    - Earlier you report, higher the chances of saving your life
  - Make “Heroes” of patients and contacts
    - Save your Country by doing the right things of reporting
  - Android Mobile App for care givers
    - Set of questions to identify if person is infected
  - Work on the messaging
    - Keeping out Ebola, it is as easy as ABC (Avoid Body Contact)

What Nigeria did right ?

- Good Luck
  - Patient zero collapsed at airport and taken directly to hospital
    - If he was not quarantined at airport , he would have made untraceable “contacts”
  - Patrick Sawyer, a VIP , Liberian Civil servant, was not ready to accept his condition
    - Dr. Adadevoh was adamant in keeping him at hospital
      - Patient died on July 25
      - Dr. Adadevoh died of Ebola on Aug 21
- …..and some Bad Luck
  - Patient zero was on Liberian Health Ministry “watch list”
    - His sister had died of Ebola on July 8
  - Health Ministry did not update Immigration Ministry. So he could get out of country

In Summary – Ebola in Nigeria



Eradication phase – 20 Oct
Nigeria declared Ebola Free

Proclamation

Preparation Phase

Readiness Phase

Response phase – 20 July to Oct

Before
Ebola virus
outbreak

Nigeria prepares for Ebola hit

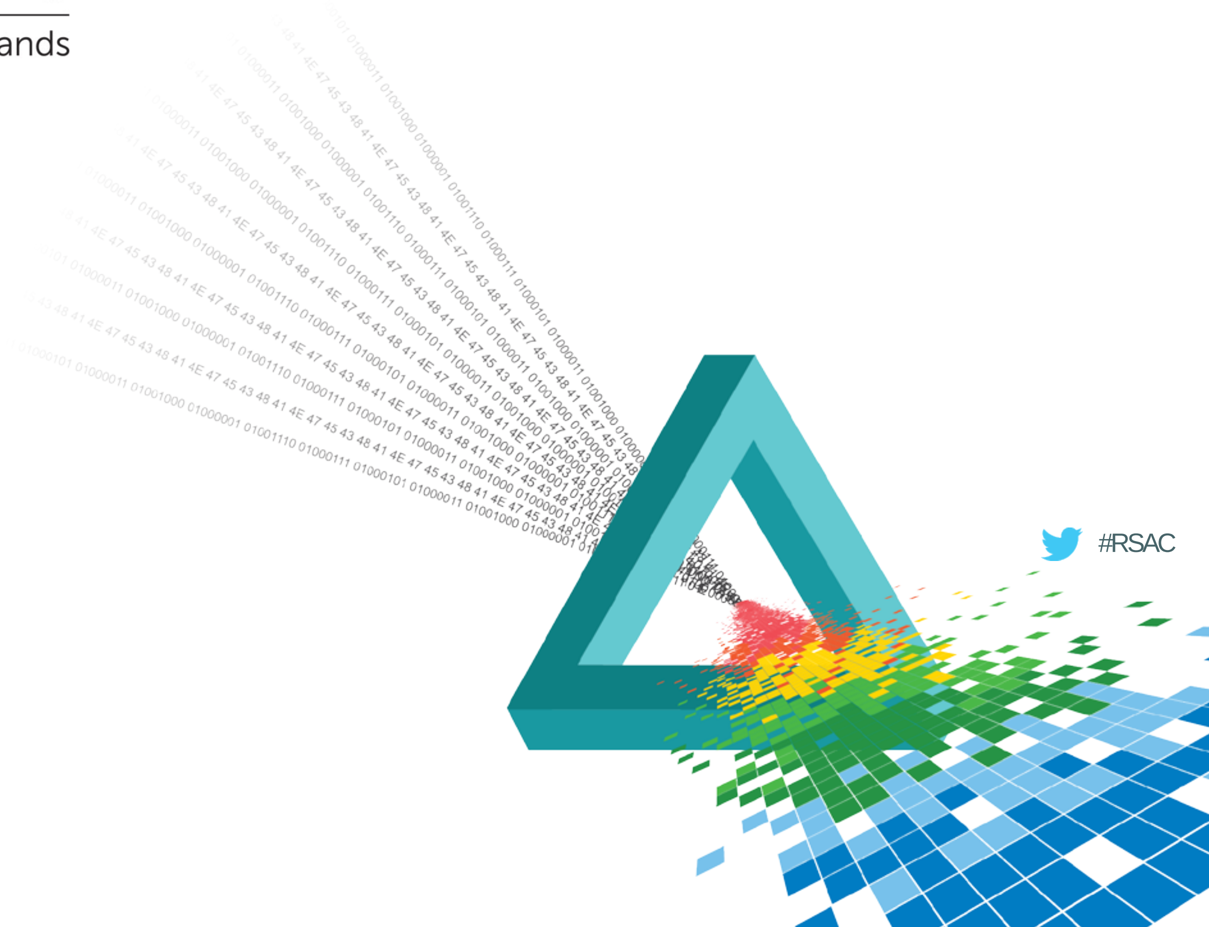
Nigeria gets hit and responds

Nigeria recovers from the attack completely eradicates Ebola

Ebola breakout in
Guinea, Liberia

Nigeria gets hit on 20th July

PALADION
BETTER SECURITY OUTCOMES



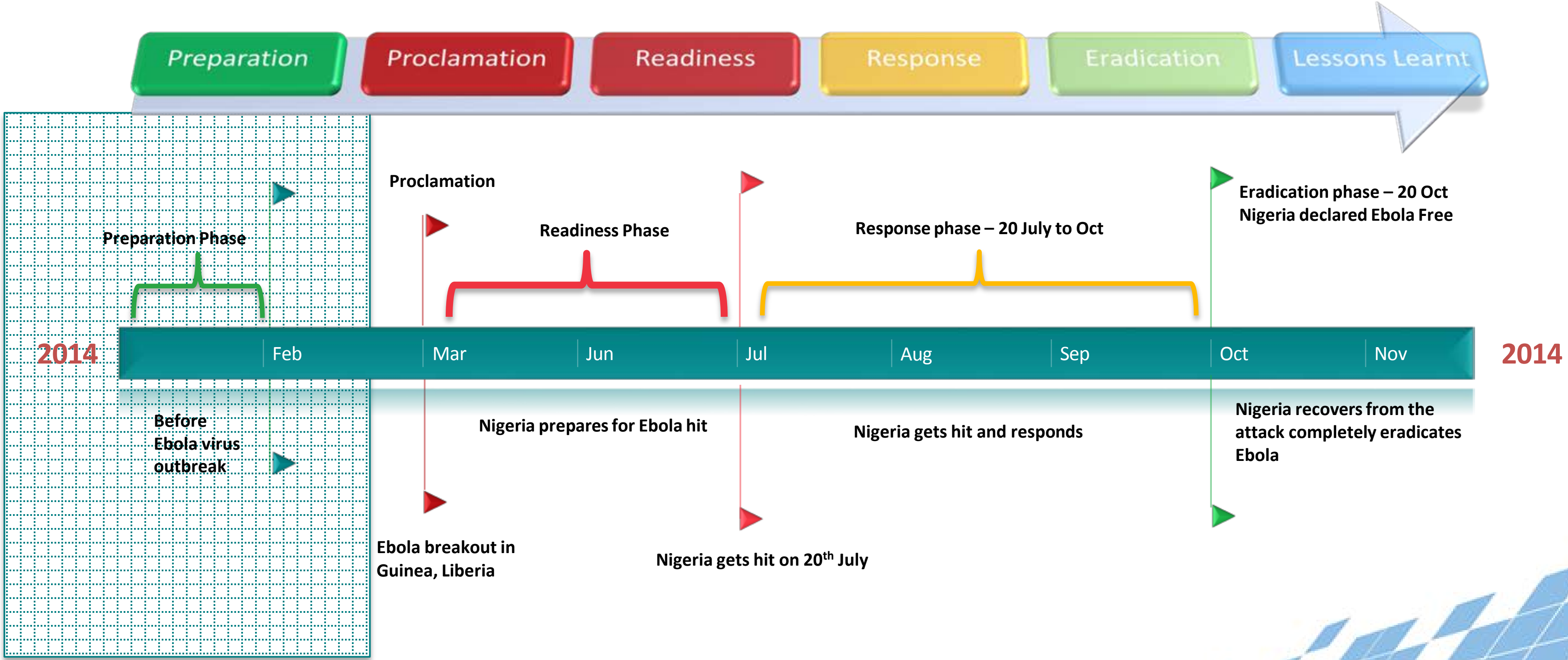
#RSAC

Zero Day

What is Zero Day ?

- Zero Day
  - refers to the number of days the community has to respond to a new threat or vulnerability
- Zero Day Vulnerability
  - A vulnerability for which no security fix is available
- Zero Day Exploit
  - An attack which exploits a zero day vulnerability

Different Stages



Preparation

Proclamation

Readiness

Response

Eradication

Lessons Learnt

2014

Feb

Mar

Jun

Jul

Aug

Sep

Oct

Nov

2014

Preparation Phase

Before Ebola virus outbreak

Proclamation

Ebola breakout in Guinea, Liberia

Readiness Phase

Nigeria prepares for Ebola hit

Nigeria gets hit on 20th July

Response phase – 20 July to Oct

Nigeria gets hit and responds

Eradication phase – 20 Oct Nigeria declared Ebola Free

Nigeria recovers from the attack completely eradicates Ebola

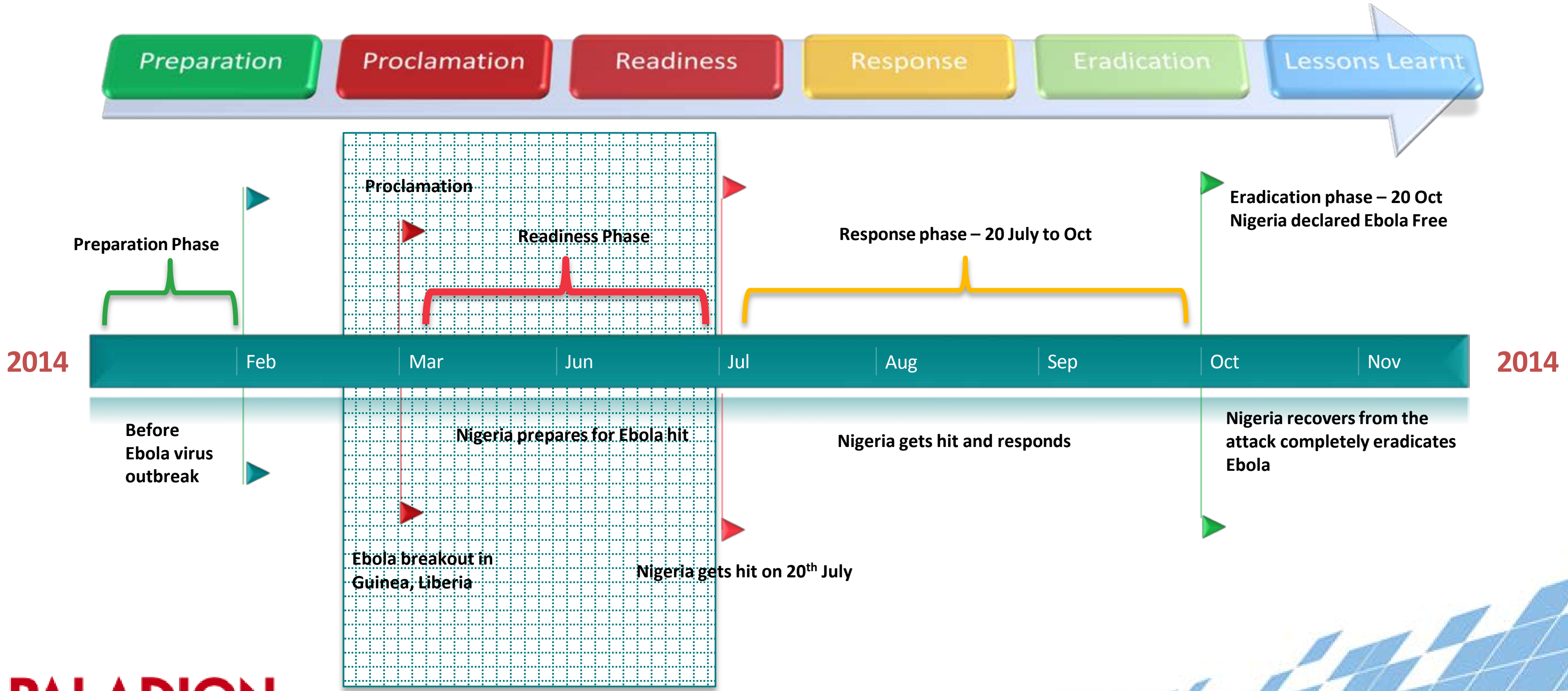
Preparation Stage

- Build the Team
  - Core CISO team , business support team , trainable volunteers
- Knowledge of own environment
  - Asset database , asset owners, asset security status
- Knowledge of your partners environment
  - SLA on incident response, security status
- Essential security tools
  - Tools for detection and response
- Effective governance structures
  - Faster decision making , enforcing decisions
  - No exceptions

Preparation Stage

- Testing facilities
  - Solutions need to be tested accurately and quickly in local environment
- Incident Drills
  - Ensure technologies , people and process readiness
  - Build relationships(outside CISO team), increase awareness
  - Test decision-enforcement capabilities
  - Test information exchange capabilities
- Awareness Campaign channels
  - Keep the channels active during good times
- Leverage Global & Local Security Intelligence Network
  - Subscribing to Global Threat and Vulnerability advisory forums
  - Sharing your threat intelligence

Zero Day Notification



Proclamation

Preparation Phase

Readiness Phase

Response phase – 20 July to Oct

Eradication phase – 20 Oct
Nigeria declared Ebola Free

Before
Ebola virus
outbreak

Nigeria prepares for Ebola hit

Nigeria gets hit and responds

Nigeria recovers from the attack completely eradicates Ebola

Ebola breakout in
Guinea, Liberia

Nigeria gets hit on 20th July

From “Plan” to “Do”

- Identification
  - How do I identify if I am being targeted
    - Signature based detection (exploit code, IDS/WAF signatures, TI feeds)
    - Non signature based detection - Network traffic patterns, End user behaviour patterns, End point behaviour
  - How do I identify vulnerable hosts
    - Asset database
    - Latest Vulnerability scan status database
    - On demand – vulnerability specific – scan

From “Plan” to “Do”

- How do I identify compromised hosts
  - File system changes
  - Network traffic patterns
  - System behaviour
  - General service outage
- Global Status tracking
  - Is the exploit evolving ?
  - Is the list of attackers available ?
  - Are there new ways to detect or prevent this

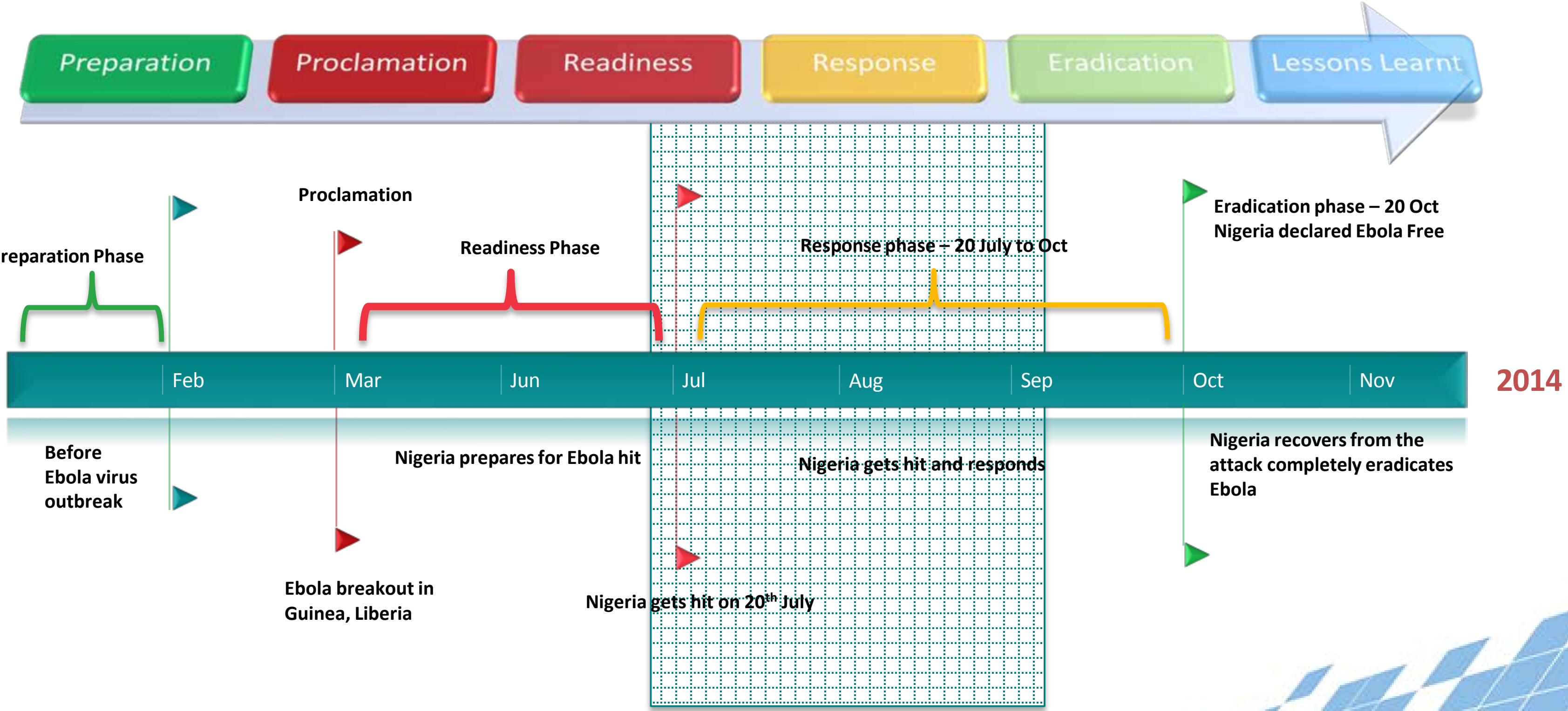
From “Plan” to “Do”

- Risk reduction
  - How can I reduce risk of infection
    - Shut down vulnerable service
      - Restrict access to vulnerable service
    - “BLOCK” on Border devices for attackers or attack patterns
- Train security volunteers
  - Educate the team on identification , response measures
- Increase Awareness
  - With users, customers. Partners
  - IT & Network operations team

From “Plan” to “Do”

- Do the Drill
  - For the specific exploit , do a table top walk through
  - Assign a Point of Contact
- Encourage Reporting

Infected !! – Contain and Eradicate



Preparation

Proclamation

Readiness

Response

Eradication

Lessons Learnt

Preparation Phase

Proclamation

Readiness Phase

Response phase – 20 July to Oct

Eradication phase – 20 Oct
Nigeria declared Ebola Free

Before
Ebola virus
outbreak

Nigeria prepares for Ebola hit

Nigeria gets hit and responds

Nigeria recovers from the
attack completely eradicates
Ebola

Ebola breakout in
Guinea, Liberia

Nigeria gets hit on 20th July

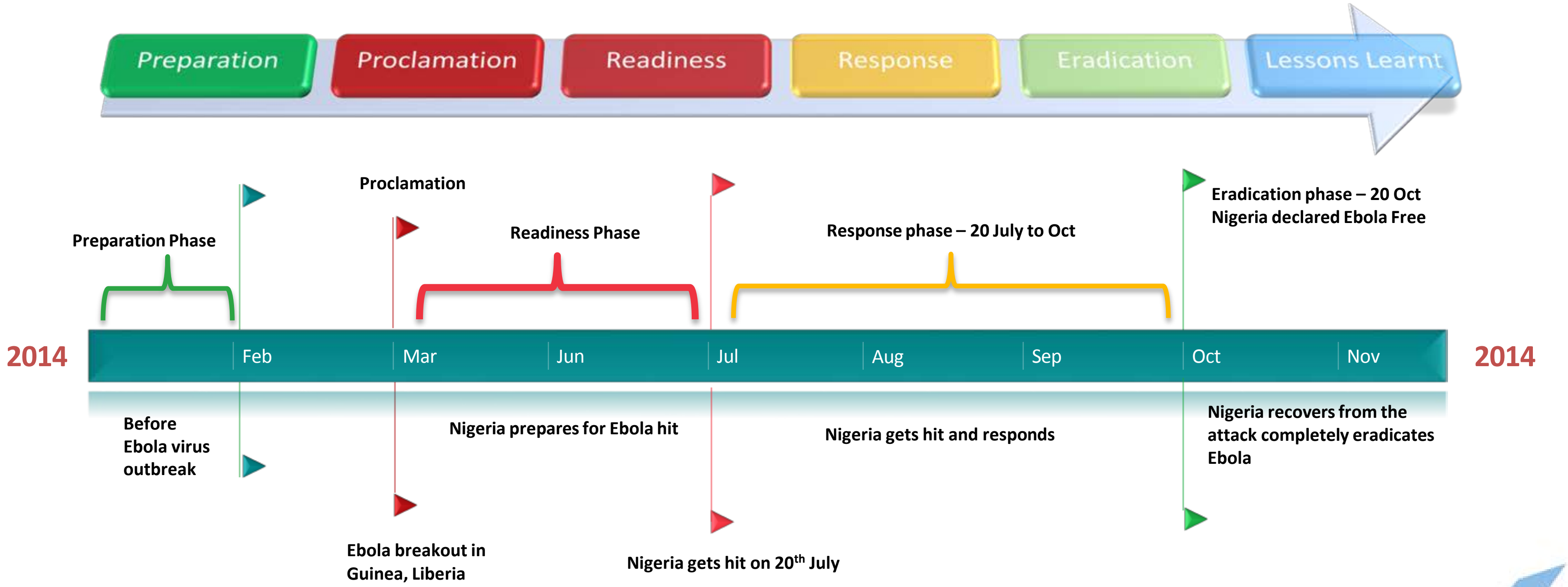
“We Got Hit” - Containment

- Quarantine infected systems
  - Isolate victim systems as much as feasible or disconnect
  - Segregate network with “potential” victims
- Increase gateway defence
  - Reduce chances of new infections & propagations
- Contact tracing
  - Identify internal and external contacts
  - Track health status of “potential” contacts

“We Got Hit” - Eradication

- Heighten Alert Level
  - Increase awareness on infection
- Clean up
  - Analyse the infection for mutants
  - Repair system or reconstruct
  - For endpoint infections, take a blackout window if needed
- Monitor
  - Monitor “cleaned” systems for re-infections
- Share Threat intelligence

Lessons Learnt



Preparation

Proclamation

Readiness

Response

Eradication

Lessons Learnt

Preparation Phase

Proclamation

Readiness Phase

Response phase – 20 July to Oct

Eradication phase – 20 Oct
Nigeria declared Ebola Free

Before
Ebola virus
outbreak

Nigeria prepares for Ebola hit

Nigeria gets hit and responds

Nigeria recovers from the attack completely eradicates Ebola

Ebola breakout in
Guinea, Liberia

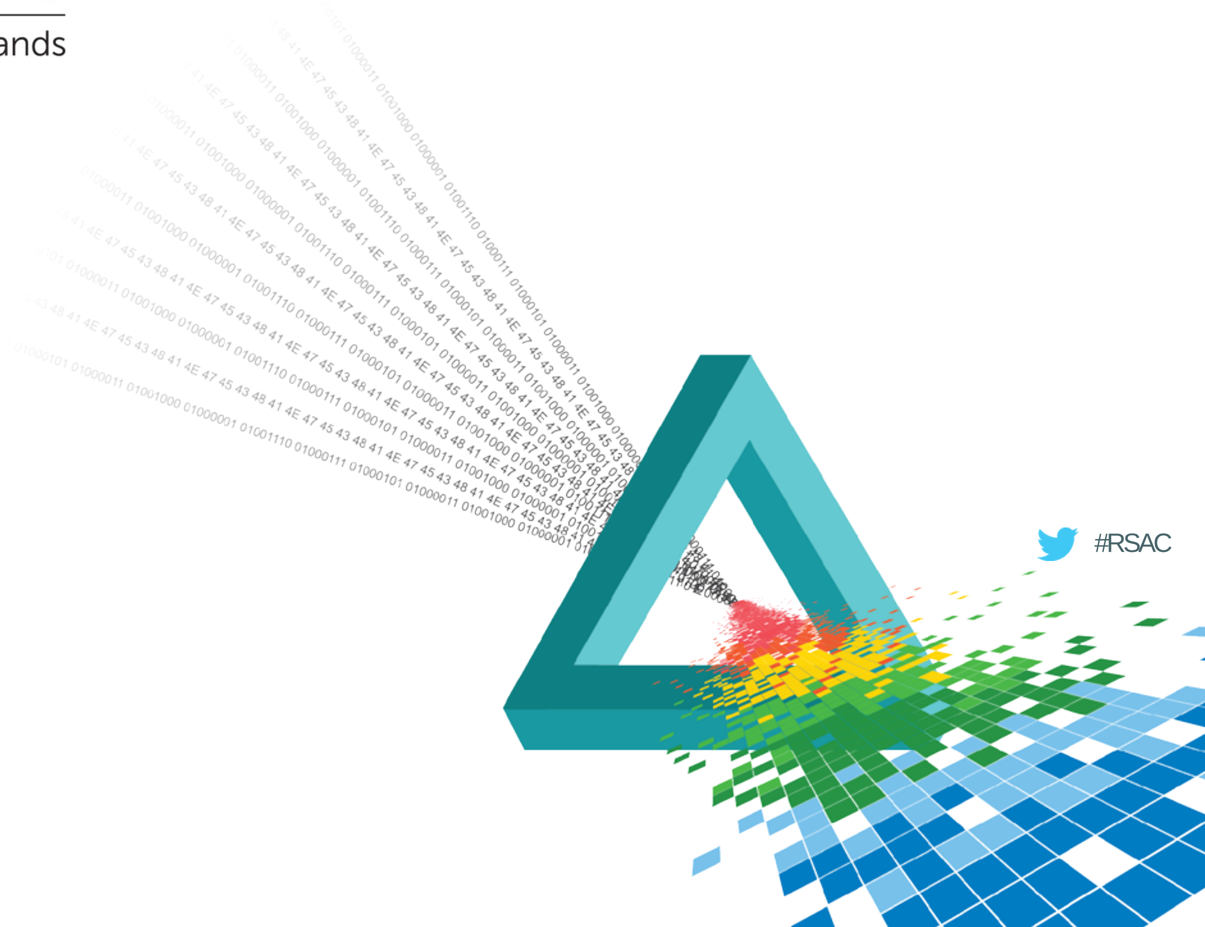
Nigeria gets hit on 20th July

Lessons Learnt

- Know your Assets , Know your vulnerabilities
- Maintain effective Security health surveillance systems
- Maintain team of Security Volunteers
- Practice Incident Drills
- Build and Maintain security awareness channels
- Have effective security governance structures
- Take (and share) threat intelligence

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Thank You