

RSA®Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CIN-R04

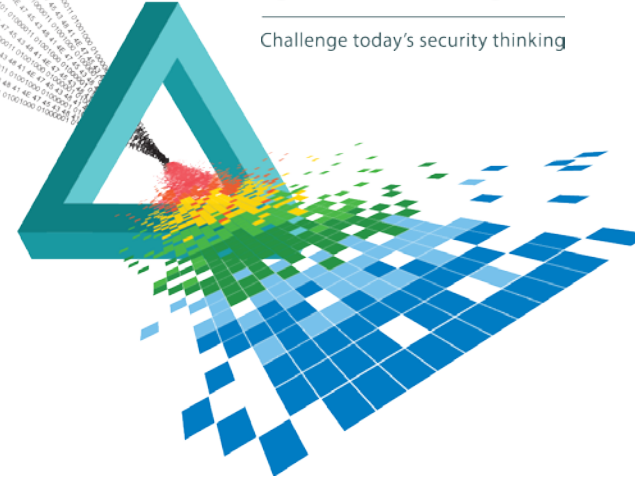
Security intelligence: the truth is out there

Tamer El Refaey

Senior Director, Security Monitoring and Operations
du

CHANGE

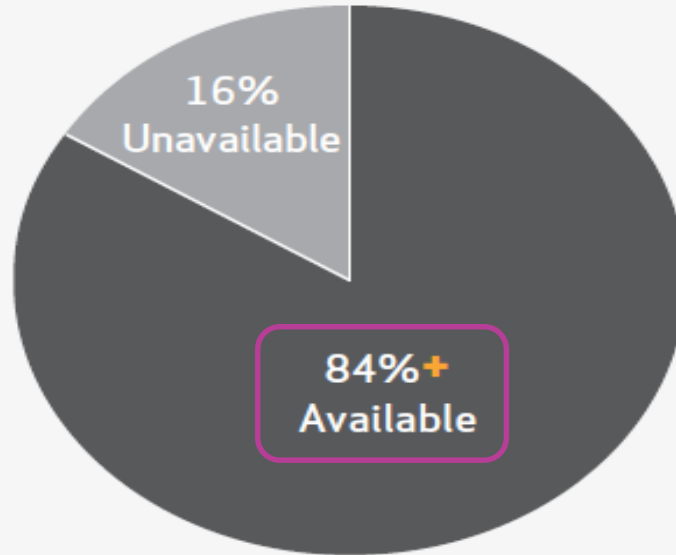
Challenge today's security thinking



2015



Figure 46. Availability of log evidence for forensics by percent of breaches*

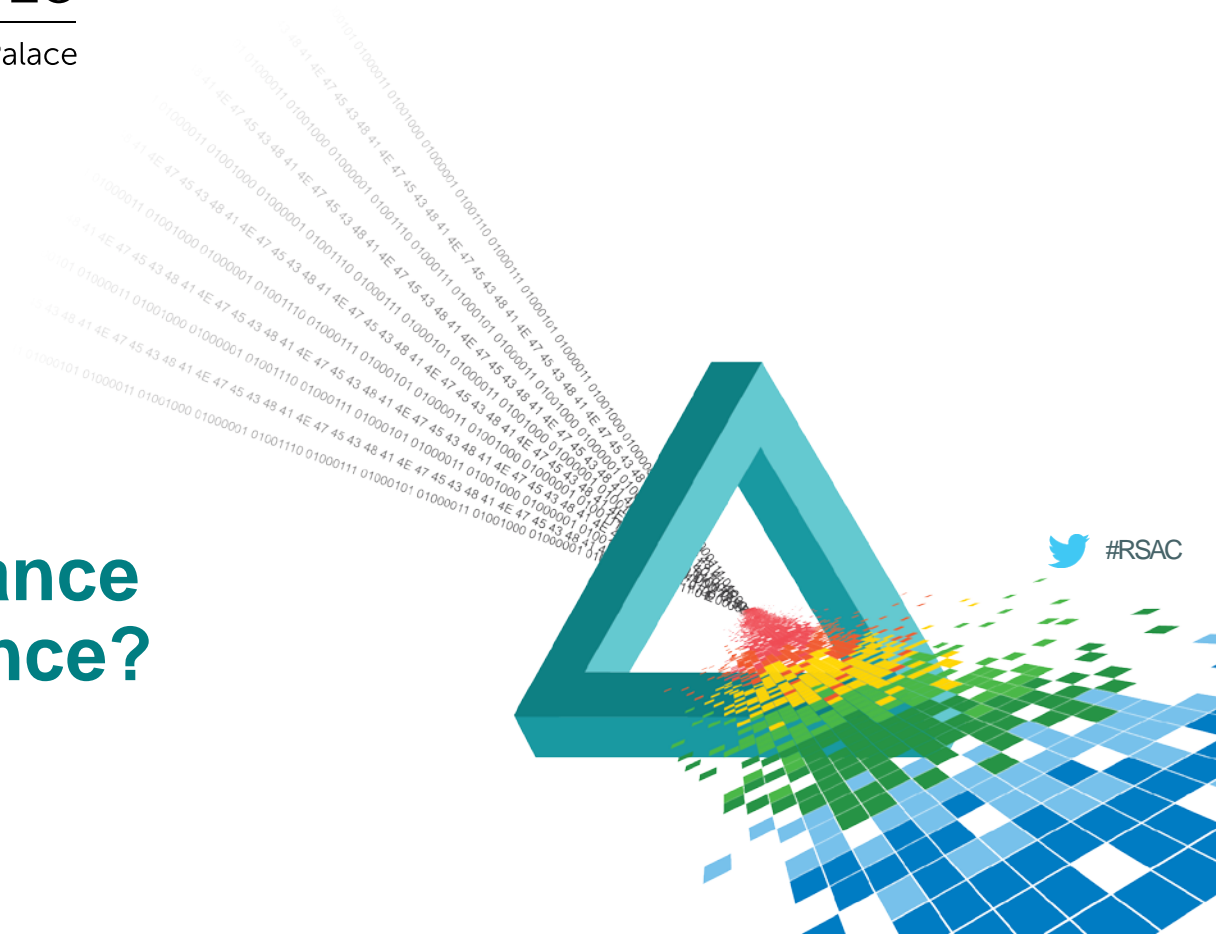


*Verizon caseload only

RSA[®]Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

How can we enhance security intelligence?



“Knowledge is having the right answer.
Intelligence is asking the
right question”

Unknown

What to
protect?



What are your organization's crown jewels?



Compromised Assets by Percent of Breaches involving IP theft

Type	Category	
Database server	Servers	48%
File server	Servers	32%
Finance/Accounting staff	People	29%
Human resources staff	People	29%
Documents	Offline Data	28%
Regular employee/end-user	People	28%
Web/application server	Servers	25%
Mail server	Servers	12%
Directory server (LDAP, AD)	Servers	6%
Executive/Upper Management	People	6%
Desktop/Workstation	User Devices	5%



Critical systems



Classified data



High value targets



What to
protect?

Why are we
a target?

Major motivation behind cyber attacks



40%
Criminal



50%
Hacktivism



3%
State
sponsored



7%
Corporate
espionage

Why you may become a target?



Hundreds of Dutch web sites hacked by Islamic hackers

In what appears to be a mass defacement, where several hundred domains take advantage of a shared hosting provider, starting as of this Friday, an...



By Dancho Danchev for Zero Day | August 25, 2008 -- 13:46 GMT (14:46 BST) | Topic: Security

'ANONYMOUS' DECLARES WAR ON AUSTRALIA OVER INTERNET FILTERING

KIM ZETTER SECURITY 09.09.09 6:13 PM

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014

GULF NEWS SAUDI ARABIA

October 9, 2015 | Last updated 6 minutes ago

UAE NEWS BUSINESS SPORT OPINION LEISURE LIFE&STV
UAE 10 GULF 11 MENA 12 EUROPE 13 AFRICA 14 ASIA 15 AMERICAS 16

Theft of Saudi documents suggests Iranian hack

Iran is escalating use of social media and cyberattacks to promote its regional policies

CBSNEWS

Video US World Politics Entertainment Health

France hit by unprecedented wave of cyber attacks

PARIS -- Hackers have targeted about 19,000 French websites since a rampage by Islamic extremists **left 20 dead last week**, a top French cyberdefense official said Thursday as the president tried to calm the nation's inflamed religious tensions.




CLOUDFLARE

Blog home

The DDoS That Almost Broke the Internet

27 Mar 2013 by Matthew Prince



What to
protect?

Why are we
a target?

How my
environment
looks like?

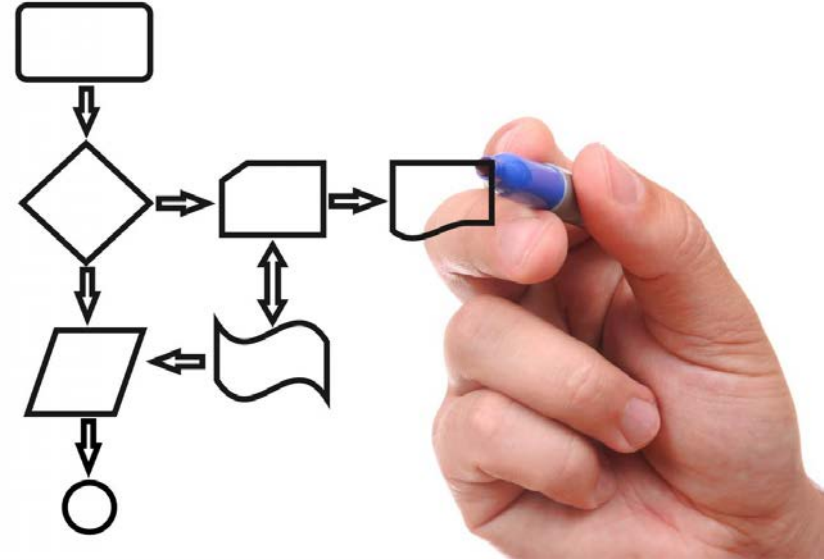


**“Know *yourself* and you will
win all the battles”**

Sun Tzu

Existing business processes

- ◆ Update exchange rates (banking)
- ◆ Service provisioning (telecom)
- ◆ Items price change (retail)
- ◆ Patients data access (medical)



Identity and privilege access data

- ◆ Link people to account IDs
- ◆ Who has access to what?
- ◆ Access business rules
- ◆ System/DB Administrators
- ◆ Access logical confinement



User and endpoint baselines


- ◆ Known applications
- ◆ Internet uploads
- ◆ Empty space
- ◆ Printing patterns
- ◆ Rare binaries



Network and system baselines

- ◆ Traffic patterns
- ◆ Dangerous commands
- ◆ Sudden reboots
- ◆ Abnormal configuration changes





What to
protect?

Why are we
a target?

What indicates
a compromise?

How my
environment
looks like?



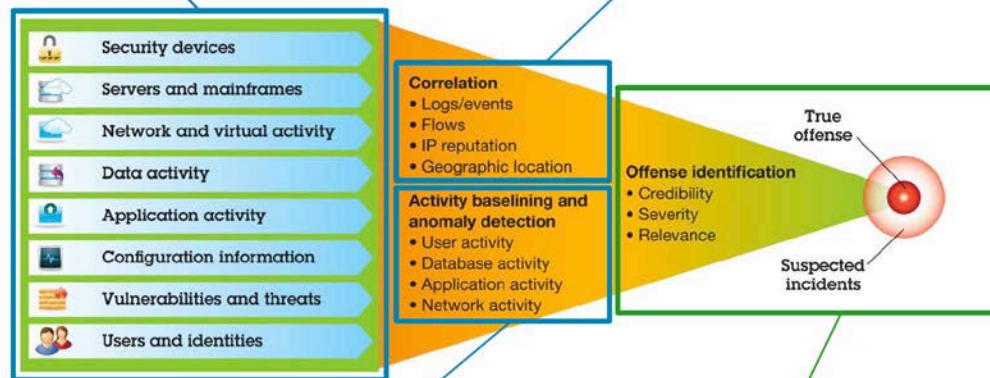
SIEM

Monitor everything

Logs, network traffic, user activity

Correlate intelligently

Connect the dots of disparate activity



Detect anomalies

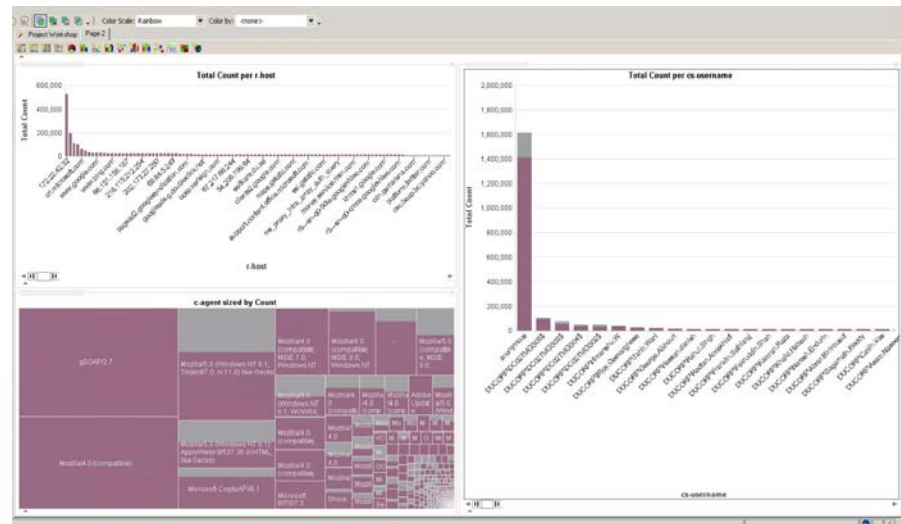
Unusual yet hidden behavior

Prioritize for action

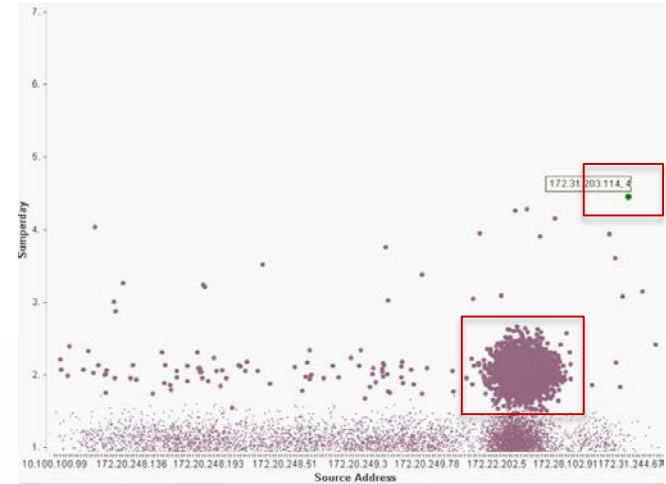
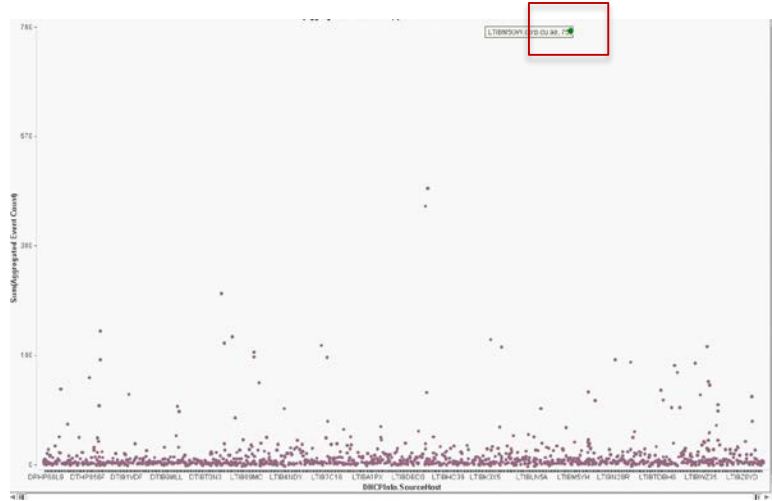
Attack high-priority incidents


RSA®
Conference
2015

Abu Dhabi



Security analytics





How good are
my intel
sources?

What indicates
a compromise?

How my
environment
looks like?

Why are we
a target?

What to
protect?



Malware analysis and
sandboxing



Advanced database
activity monitoring

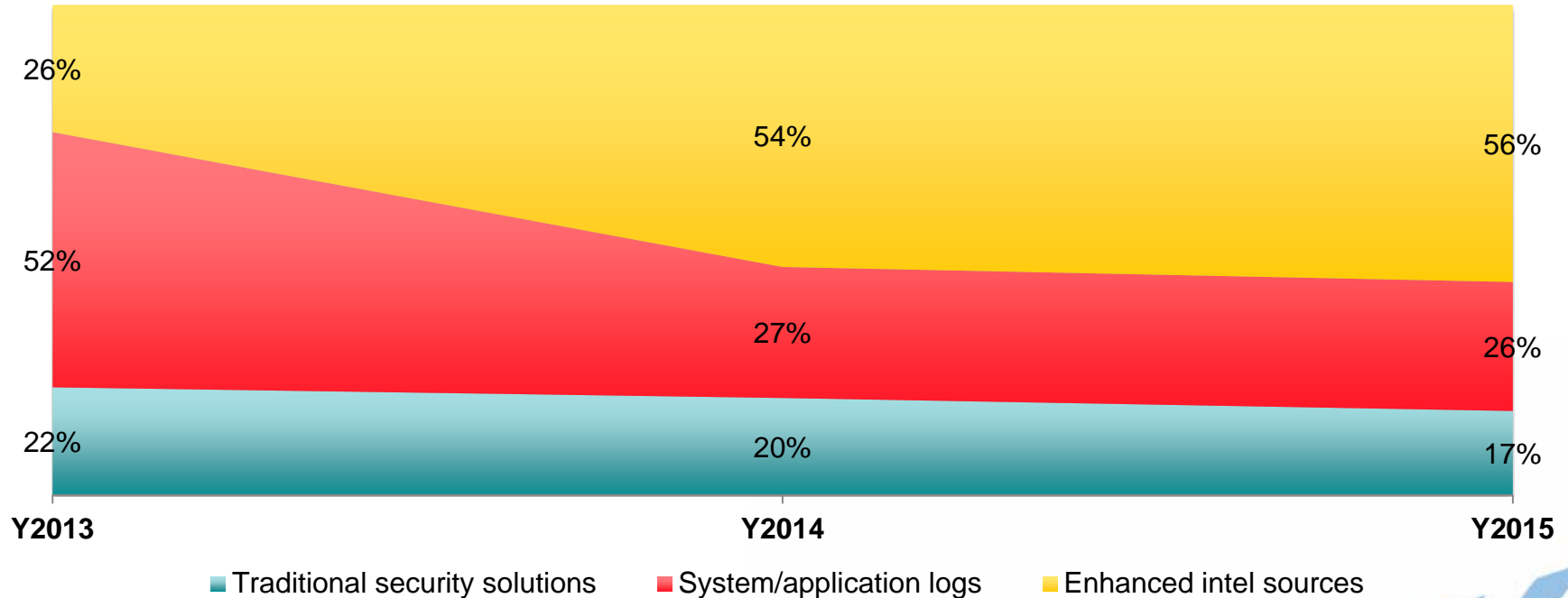


Endpoint advanced
visibility



Open source
intelligence

Incident detection by intelligence source





How to measure
performance?

How good are
my intel
sources?

What indicates
a compromise?

How my
environment
looks like?

Why are we
a target?

What to
protect?



Are “response time” and “number of false positives” your main concerns?

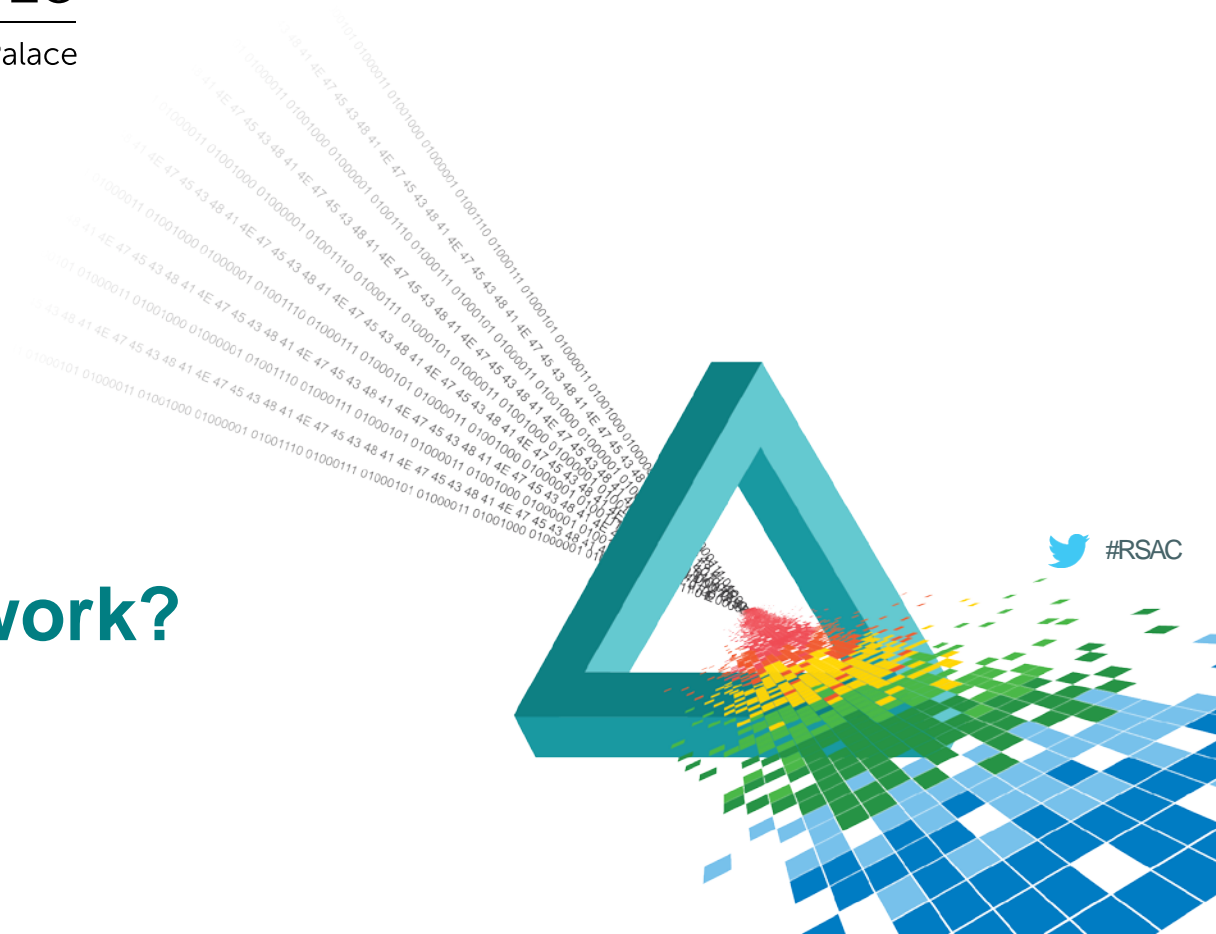
Recommended security intelligence KPIs

- ◆ How much security noise you are handling?
- ◆ In which phase you can detect a security incident?
- ◆ How quick can you detect a security incident?
- ◆ How quick you respond to a security incident?
- ◆ Who detects the security incident?
- ◆ How many breaches Vs incidents?

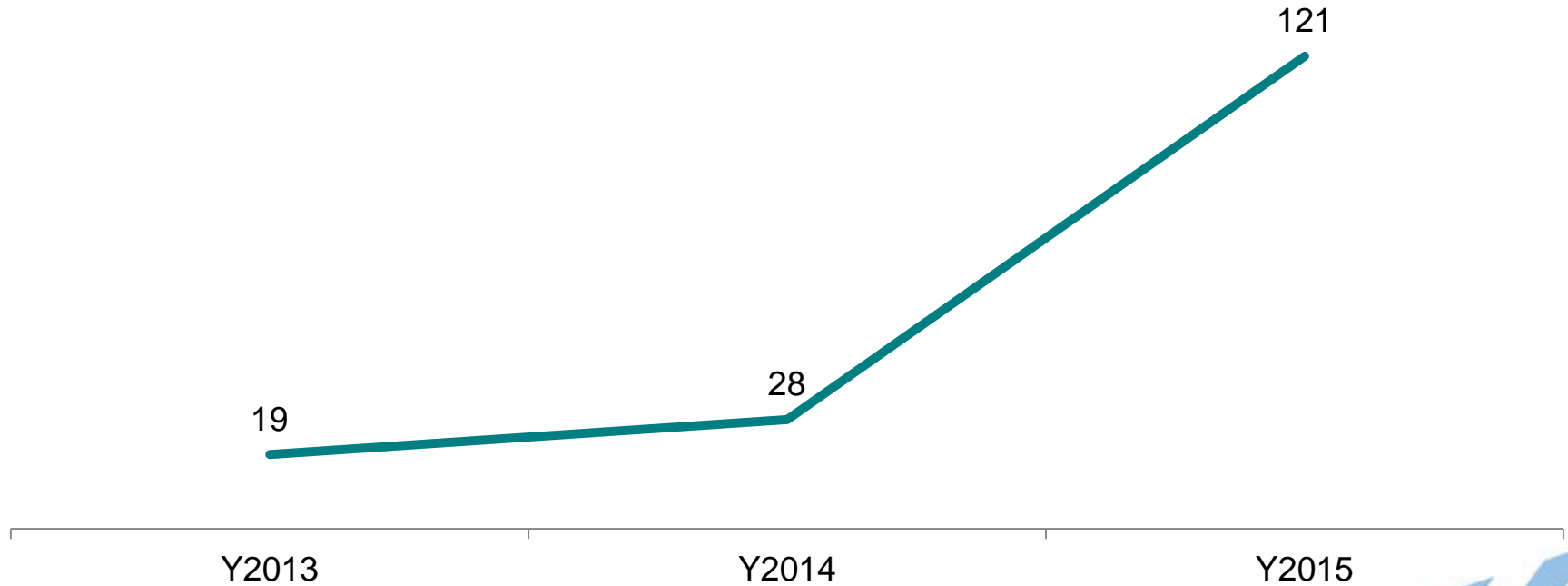
RSA[®]Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

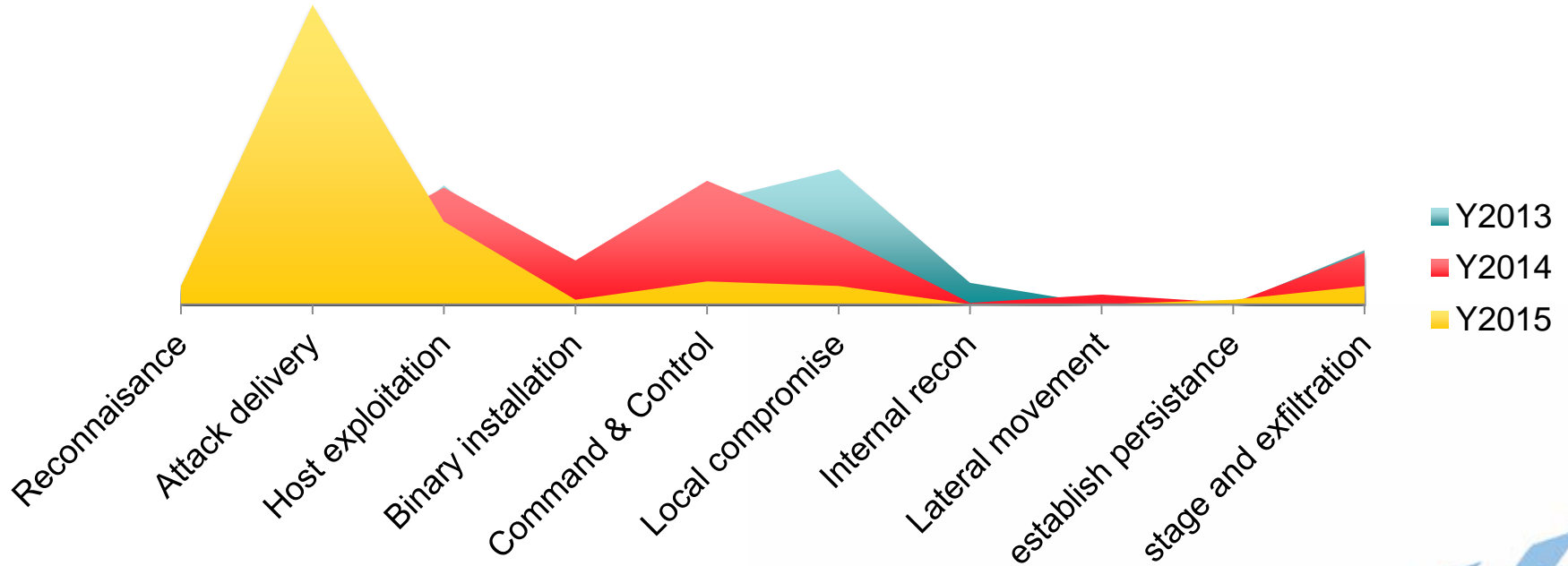
Does this really work?



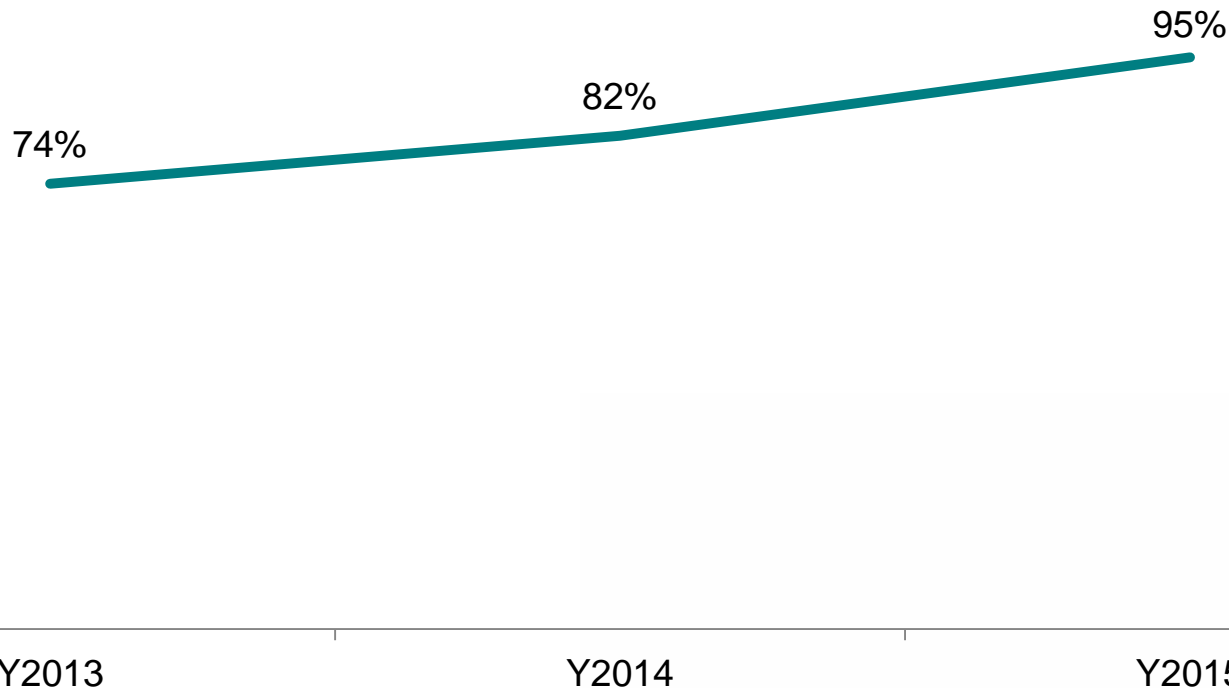
Number of true incidents for every 1,000 alerts



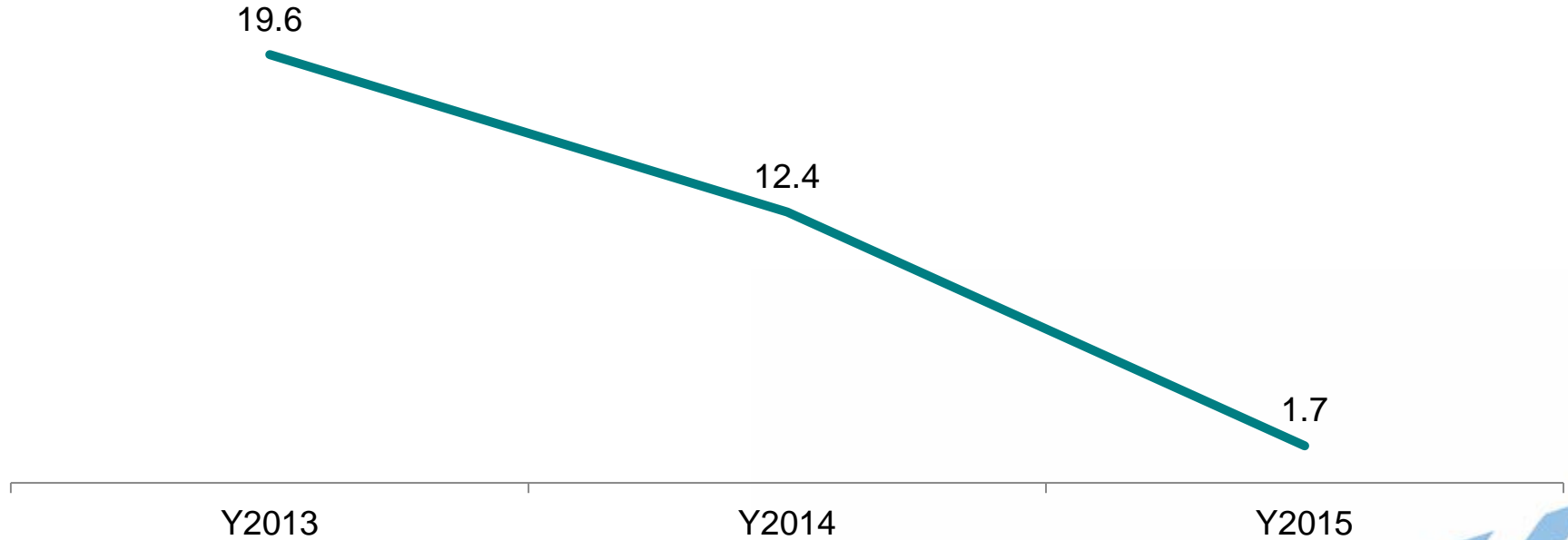
Incident detection by attack phase



% of compromise attempts detected within 24 hours



Average number of days between initial compromise attempt and detection



Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Decide the appropriate security KPIs for your organization and what their targets should be
- ◆ In the first three months following this presentation you should:
 - ◆ Identify critical assets, processes, and high value targets within your organization
 - ◆ Understand who the threat actors and their motivations are
 - ◆ Know your environment and what its good state is
- ◆ Within six months you should:
 - ◆ Build different use cases that would look for IOCs in your environment
 - ◆ Select the security intelligence solutions that you would consider to implement

RSA[®]Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

Questions?

