RSA
The Security Division of EMC

UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

EMC²
where information lives

Welcome and Information Day

Intelligence Driven Security
A strategy to help in cyber threat detection and response

Università degli Studi di Roma - Tor Vergata
Dip. di Ingegneria Elettronica
Rome, 15 October 2015

RSA

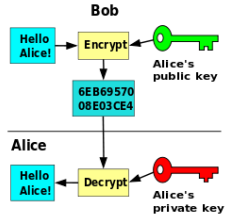
..Welcome from RSA!!

RSA
The Security Division of EMC

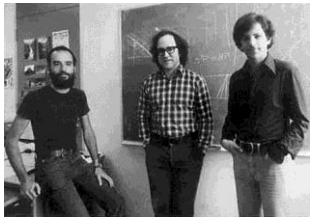
UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

RSA

RSA, more than an encryption algorithm



Ron Rivest, Adi **S**hamir and Leonard **A**dleman (who developed the RSA encryption algorithm in 1977) founded **RSA** in 1982



SecurID authentication token was one of the first security solution provided from RSA

In 2006 with the acquisition of the company by **EMC Corporation**, RSA became part of a big family (VMWare, Pivotal, ..)

Today RSA is one of the major worldwide computer and network security company, its solutions help organizations to deal against **advanced security threats**

What about this session (..and whoami) ?

Francesco Gelo
RSA Pre-Sales Technology Consultant

Giovanni Napoli
RSA Pre-Sales Manager Europe South

.. in other words We work with our Sales team to find **solutions** (with RSA products) to **customer pains**

We were one of **You** ☺.. and after University We started to work in various IT and Security companies

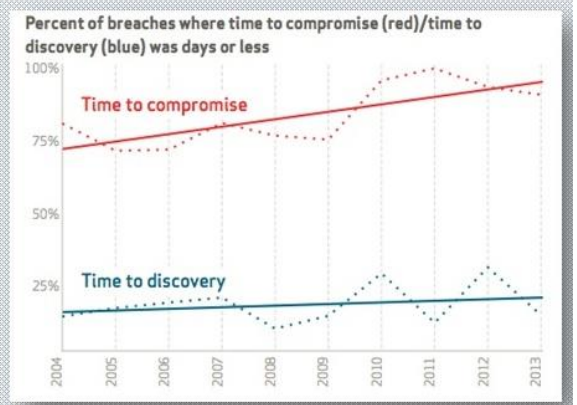
In **today session** We'll share with you what we see about current Security issues, and how we move around them to help organizations to deal with **new advanced security threats**

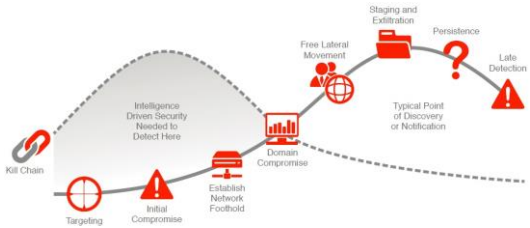
Did you hear of them?

Analysts feedback

Attacker Capabilities

Time To Discovery



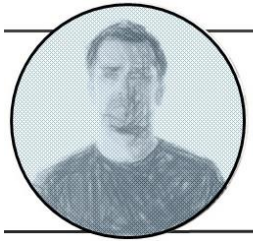


85% Percent of cases where victims learned about their breach **from an external party**

Percent of incidents that took **weeks or more to discover** **83%**

(VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT)

Our customers feedback

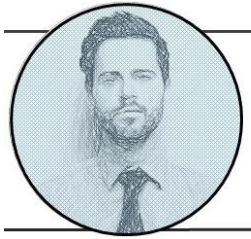


WE'RE **MISSING ATTACKS**. I KNOW THEY'RE HAPPENING, I JUST CAN'T SEE THEM

SOC Analyst

I NEED MORE THAN MY CURRENT SIEM TOOL. I NEED SOMETHING **BUILT FOR TODAY'S THREATS.**

SOC Analyst



I HAVE A GREAT GROUP BUT I NEED A **MORE EXPERIENCED AND MORE EFFICIENT TEAM**. RIGHT NOW ATTACKERS HAVE THE UPPER HAND.

SOC Manager

Security Team (SOC, CIRC, CERT, ..)

..and RSA perspective

The attack surface is expanding

Security teams are missing attacks

Attackers are becoming more sophisticated

Teams need to increase experience & efficiency

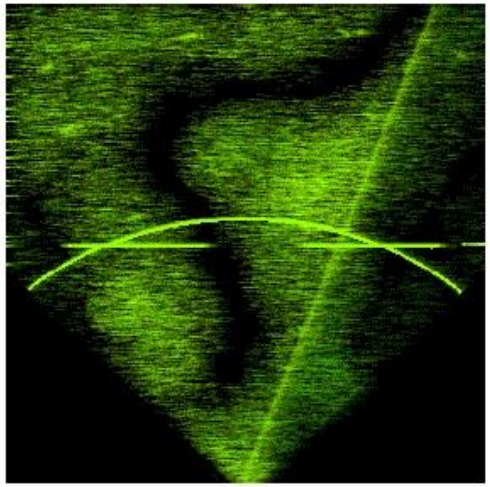
Existing strategies & controls are failing

Tools & processes must adapt to today's threats

Which is the solution for current new threats?

Radar evolution example

1965 Aviation Radar



Visibility
Manual Tuning
Highly Skilled Task
Require Human Control

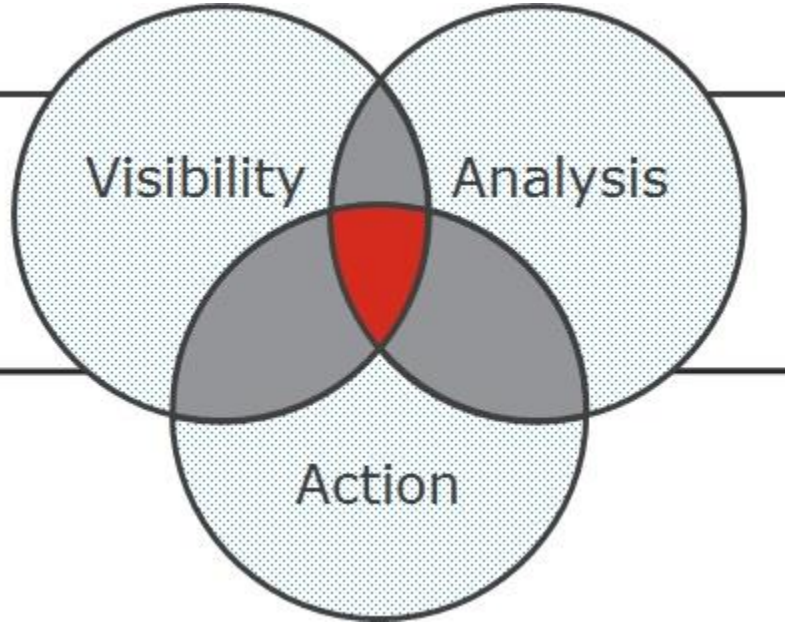
2015 Tactical Situation Display

More Visibility
Context Aware
Automatic **Actions**
Reduce Human **Control**

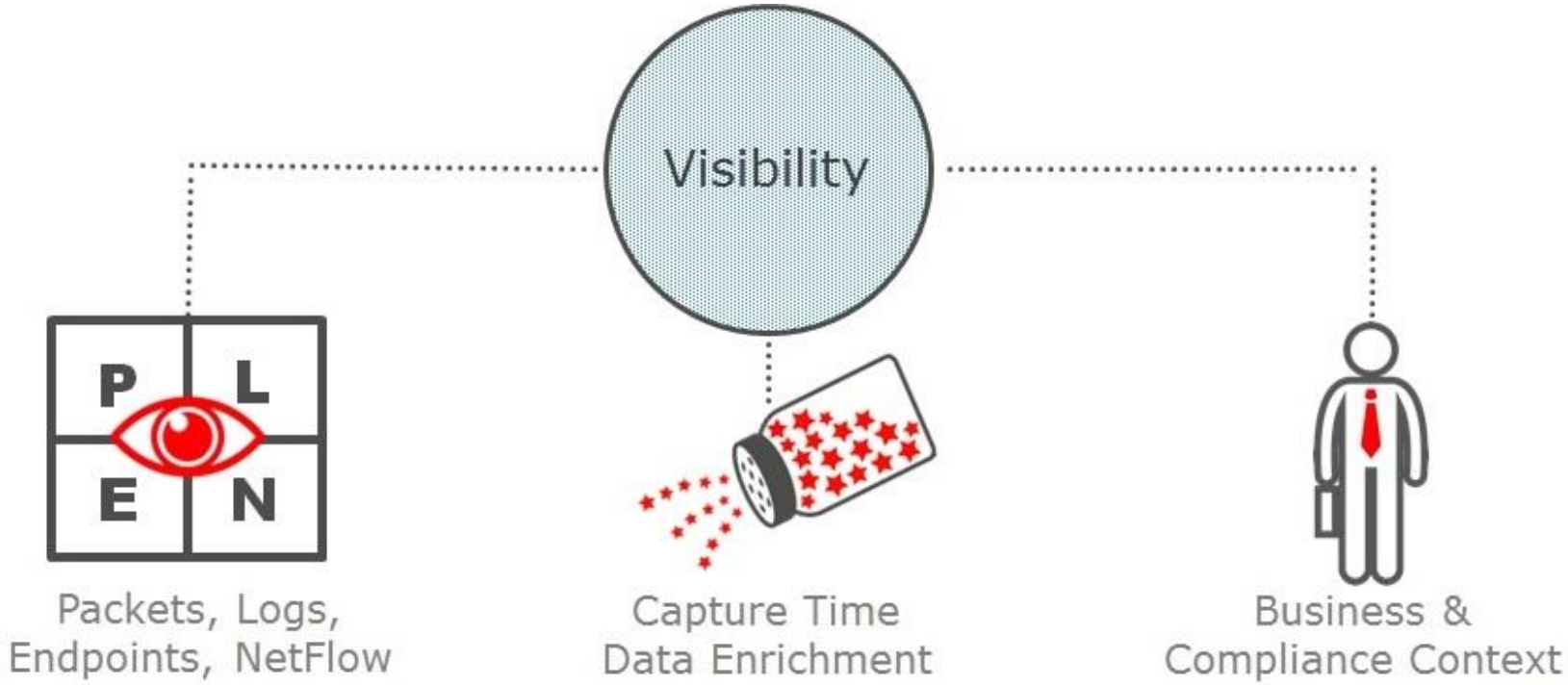
A strategy to help in cyber threat detection and response

TRANSFORM

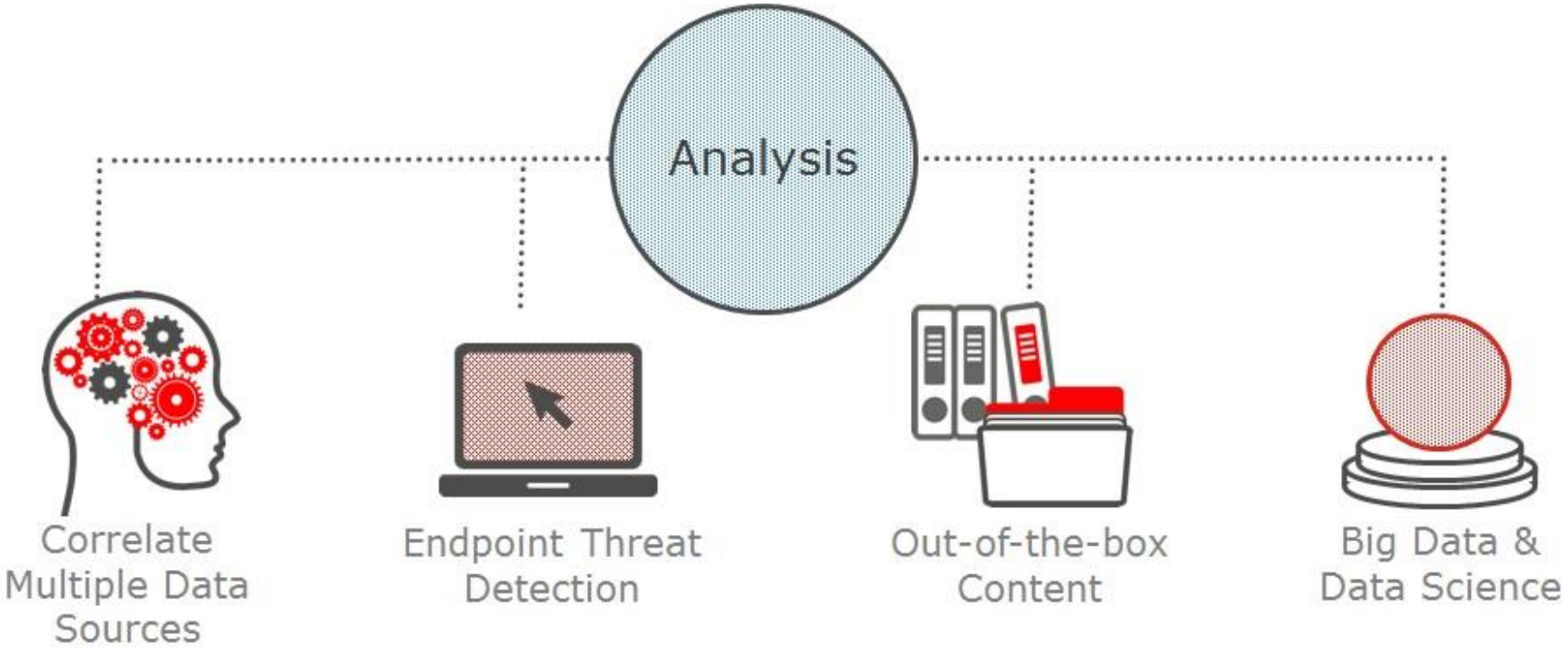
Intelligence-Driven Security



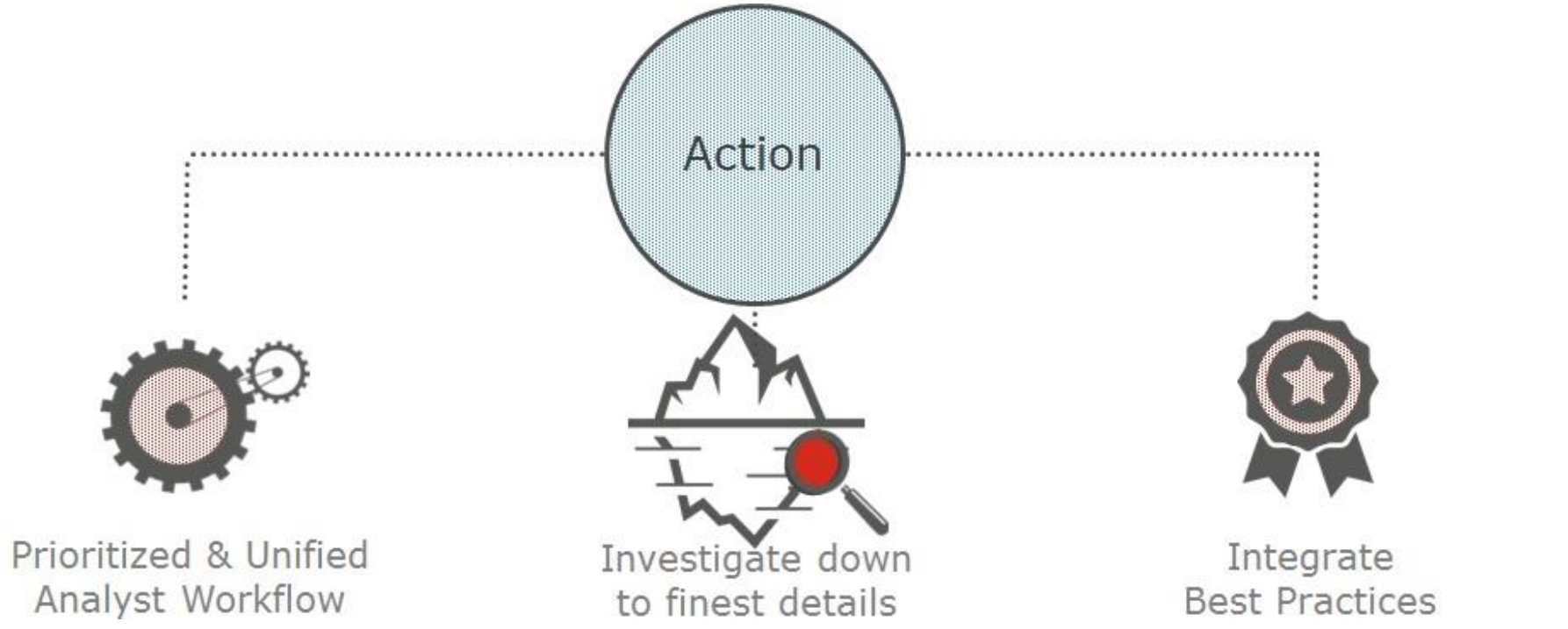
Visibility into digital activity within logs, the network and at end points



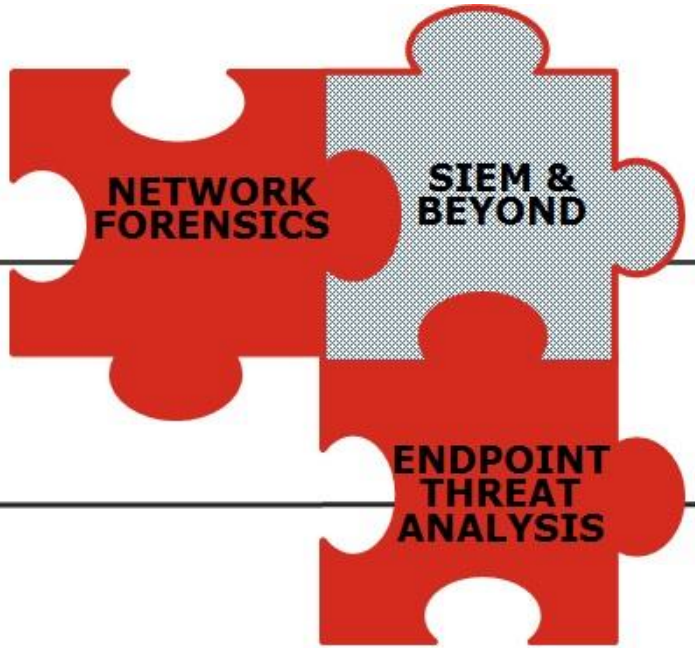
Analytics to uncover hidden threats and to guide decisions for an effective response



Activation of incident response processes to make security teams to be more efficient



RSA Intelligence Driven Security solution



Modular

RSA Advanced SOC Solution

As You Grow, The Product Grows With You

RSA Advanced SOC ecosystem

Full Visibility and Contextual Awareness

RSA Security Operations Management

- Incident Handling
- Breach Handling
- Issue Management
- Risk Management
- SOC/IRM Program Management

RSA Security Analytics

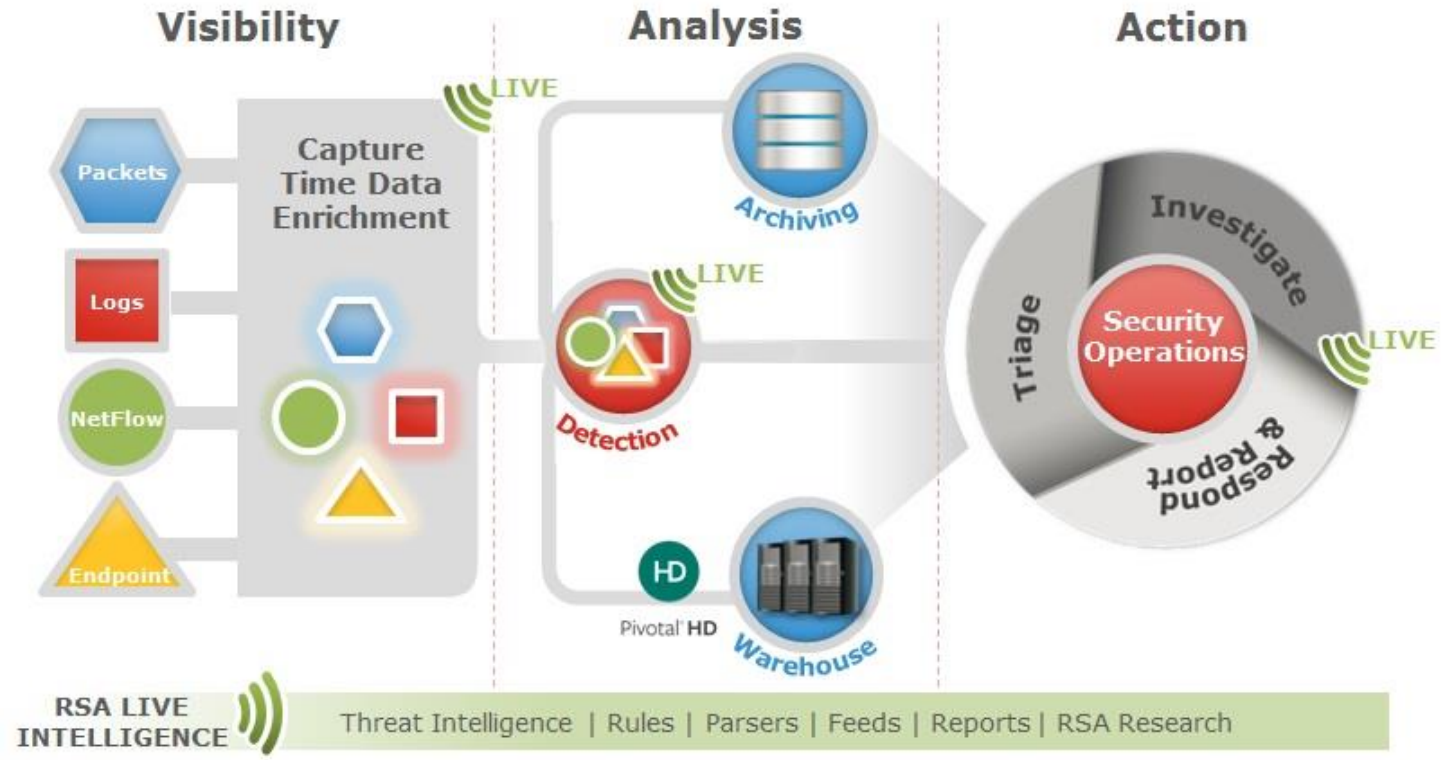
- Log events parsed real-time
- Full network session reconstruction
- Live malware analysis
- Full business context

RSA ECAT

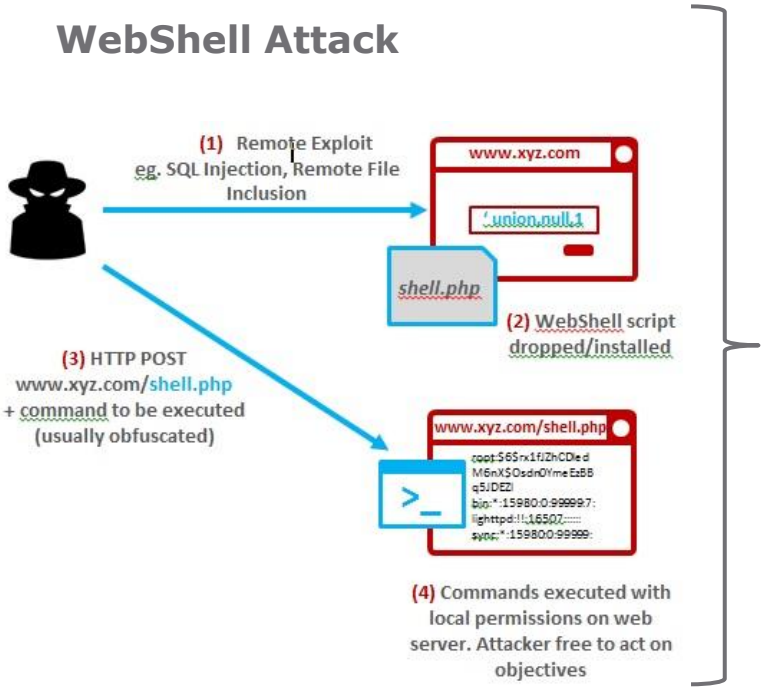
RSA Live Intelligence + Business Context

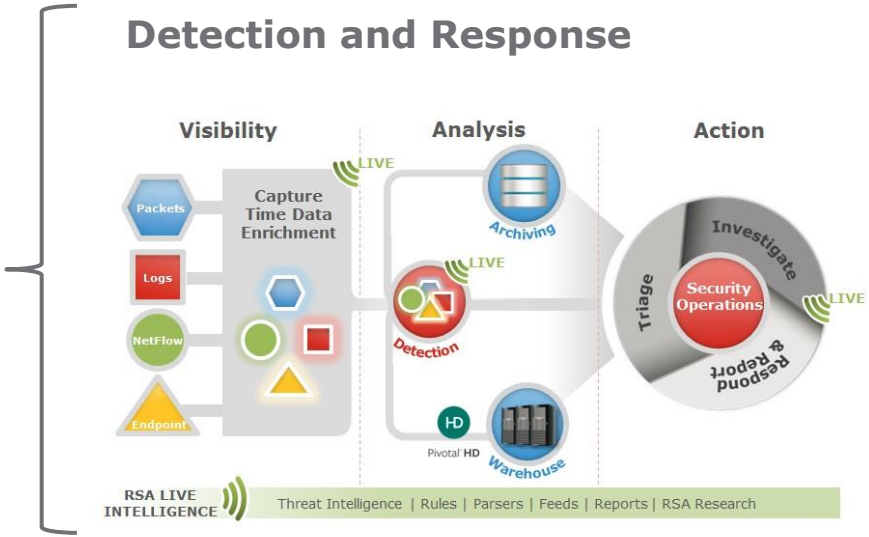
Threat Intelligence – Rules – Parsers – Alerts – Feeds – Apps – Directory Services – Reports and Custom Actions

RSA Security Analytics (SIEM) module



Live Demo: Use Case





Live Demo: Results

Visibility

Analysis

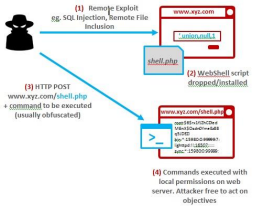
Action

Alert on a possible Webshell Attack

Confirmation of malicious activity from a **remote attacker**

FTP file upload to a remote **drop zone**

Reconstruction of WebShell attack



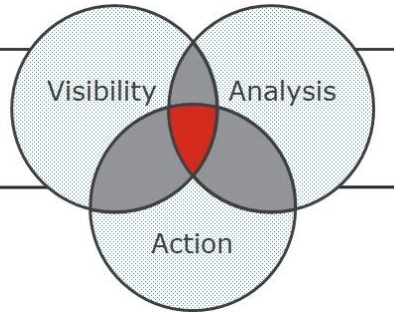
What we have learned today

1965 Aviation Radar

2015 Tactical Situation Display

TRANSFORM

Intelligence-Driven Security



Q&A time

..Thank YOU!!

EMC²