



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



..Welcome from RSA!!



RSA, more than an encryption algorithm

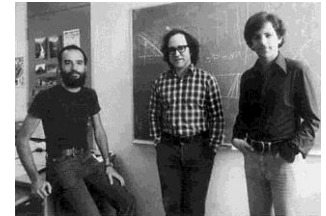
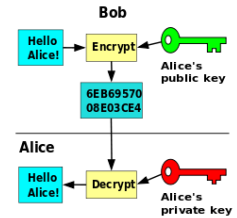
Ron Rivest, Adi Shamir and Leonard Adleman (who developed the RSA encryption algorithm in 1977) founded **RSA** in 1982

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?

The Telegraph

Home Video News World

USA Asia China Europe

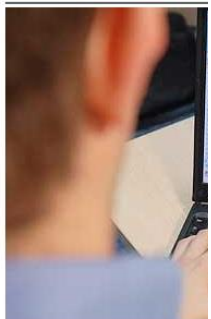
HOME » NEWS » WORLD NEWS »

China's global cyber

penetrates 103 co

A vast Chinese cyber-espionage network has been discovered by researchers.

f t p



The sophisticated computer attacks hit Estonia.

By Malcolm Moore in Shanghai
2:03PM BST 29 Mar 2009

DEUTERUS

Home Video News World

USA Asia China Europe

HOME » NEWS » WORLD NEWS »

US americas asia australia africa middle east

Russia accused of unleashing cyber war to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

📷 Bronze Soldier, the Soviet war memorial removed from Tallinn. Photograph: Timur Nisametdinov

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing concern across the western alliance, with Nato urgently examining the offensive implications.

While Russia and Estonia are embroiled in their worst dispute since the end of the Soviet Union, a row that erupted at the end of last month over Estonia's removal of the Bronze Soldier Soviet war memorial in Tallinn, the country has been subjected to a barrage of cyber warfare, disabling websites of government ministries, political parties, newspapers, banks and companies.

BloombergBusiness News Markets Insights Video

The Telegraph

Home Video News World Sport Finance Comment Culture Travel Life Women

USA Asia China Europe Middle East Australasia Africa South America Central Asia

France Francois Hollande Germany Angela Merkel Russia Vladimir Putin Greece Spain

HOME » NEWS » WORLD NEWS » EUROPE » GEORGIA

Georgia: Russia 'conducting cyber war'

Russia has been accused of attacking Georgian government websites in a cyber war to accompany their military bombardment.

f t p in



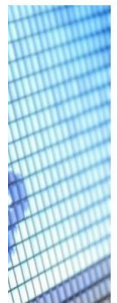
The official website of Mikheil Saakashvili, the Georgian President, was under external control since shortly before Russia's armed intervention.

By Jon Swaine
11:11AM BST 11 Aug 2008

Several Georgian state computer servers have been under external control since shortly before Russia's armed intervention into the state commenced on Friday, leaving its online presence in disarray.

Stolen Credit

ETS PHONES HARD



Print this article

Georgia
News » World News » Europe » Russia »

In Georgia



The James Bond house in Tbilisi



Victory Day parade



Begin' ting

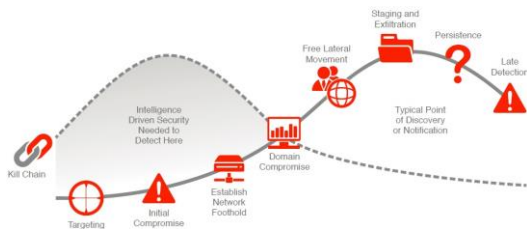
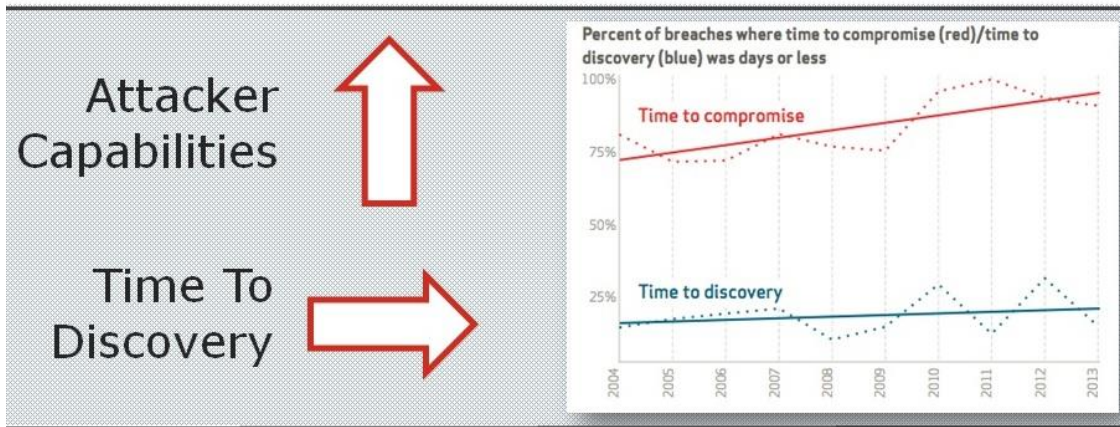
and it appear

5:29 AM

ce of malware.



Analysts feedback



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

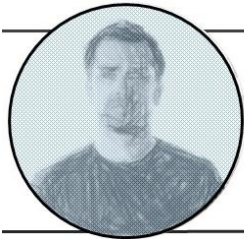
Percent of incidents that took **weeks or more to discover**

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



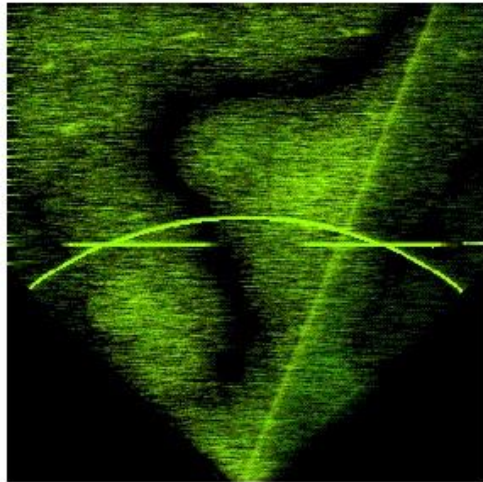
Tools & processes must
adapt to today's threats

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



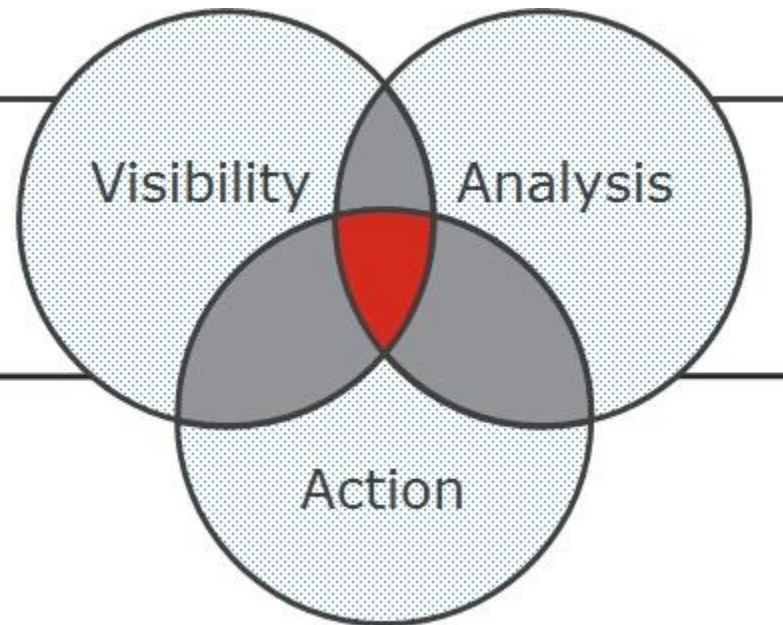
More Visibility
Context Aware
Automatic **Actions**
Reduce Human **Control**



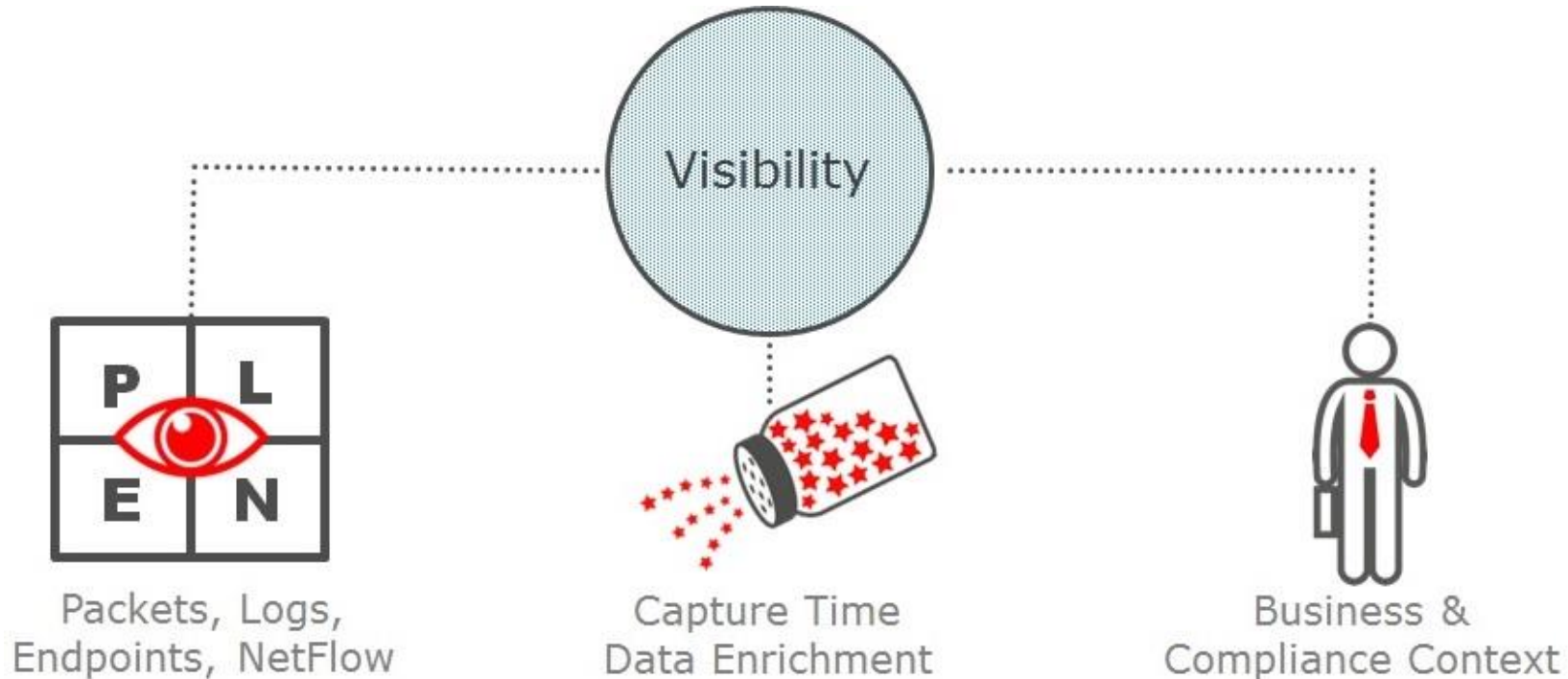
A strategy to help in cyber threat detection and response

TRANSFORM

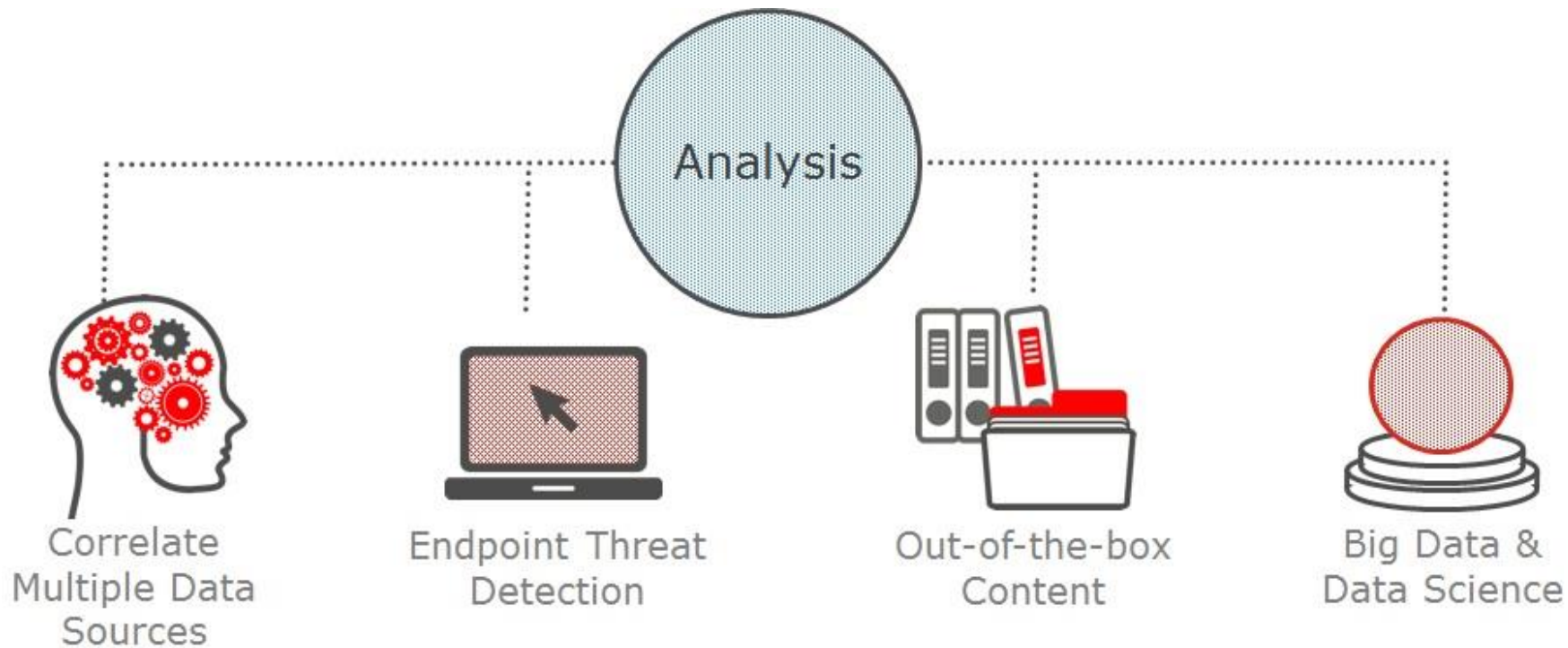
Intelligence-Driven Security



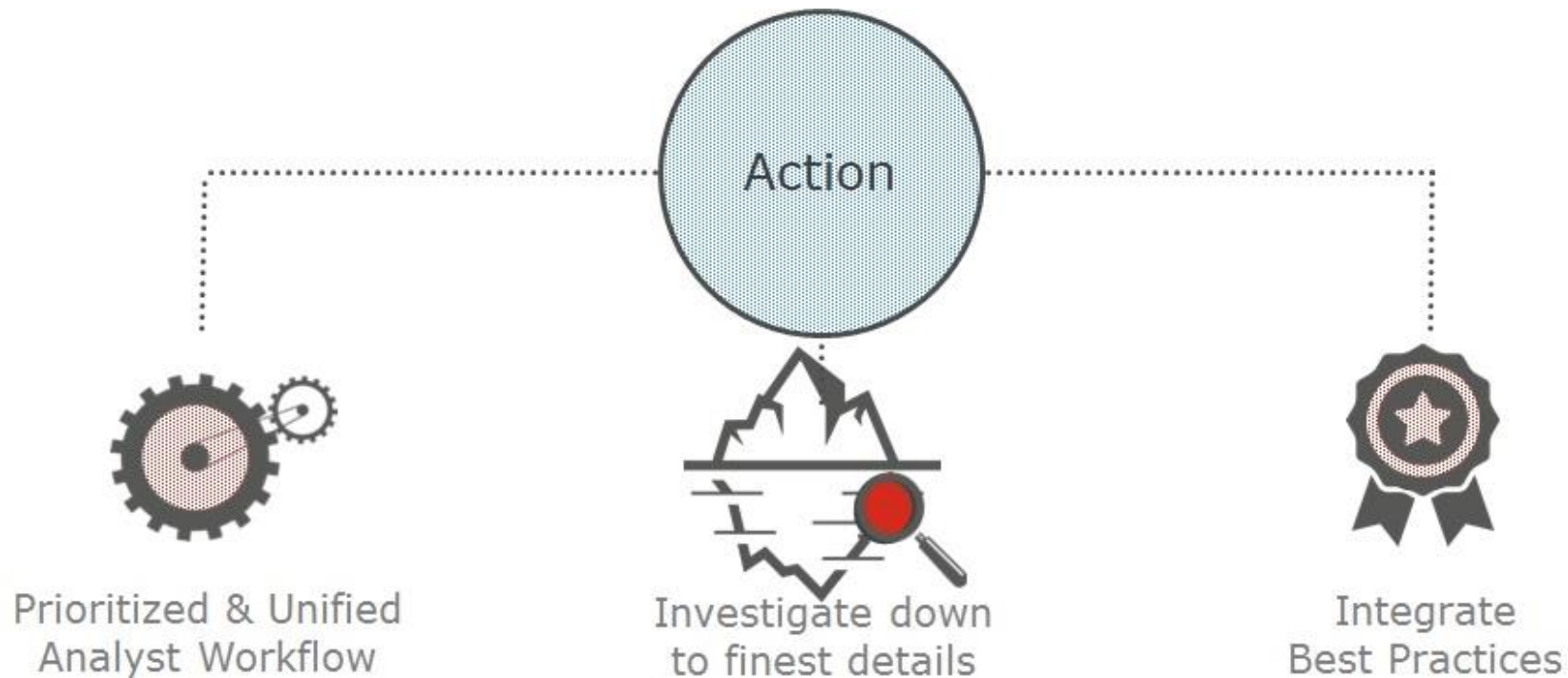
Visibility into digital activity within logs, the network and at end points



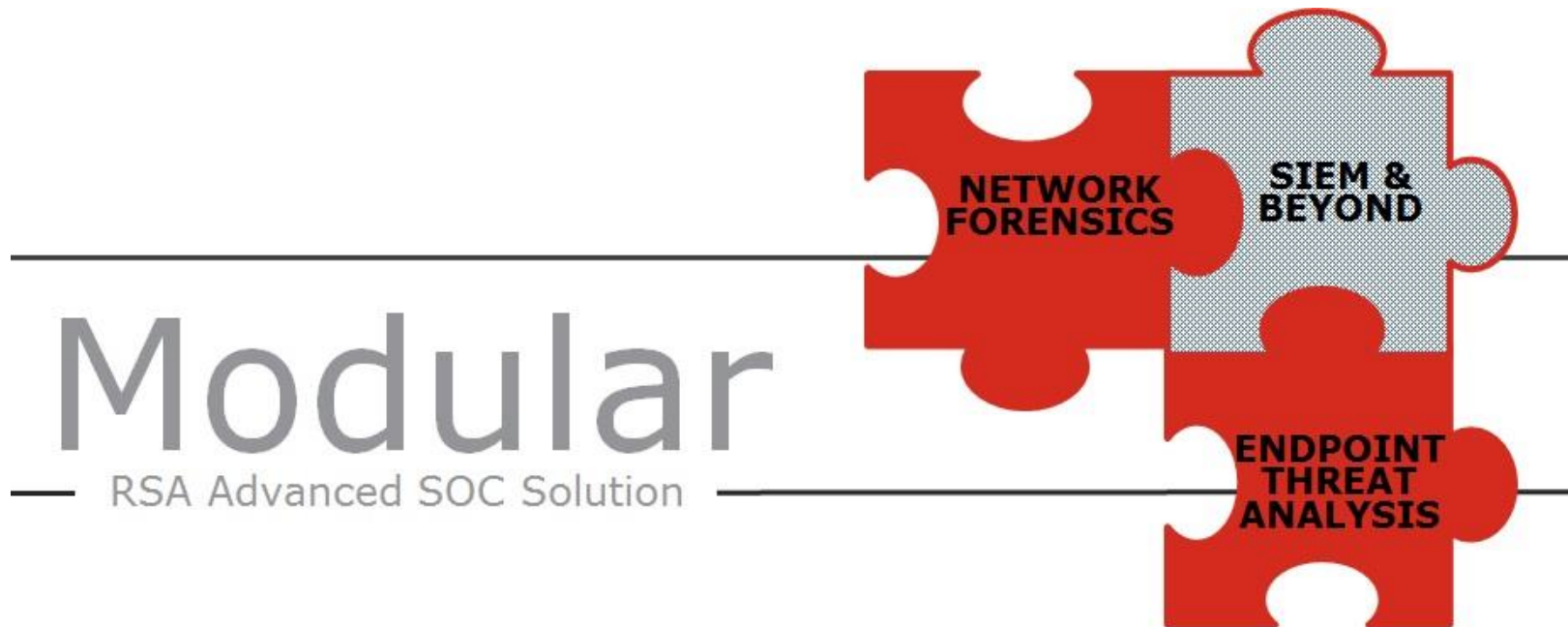
Analytics to uncover hidden threats and to guide decisions for an effective response



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



RSA Intelligence Driven Security solution

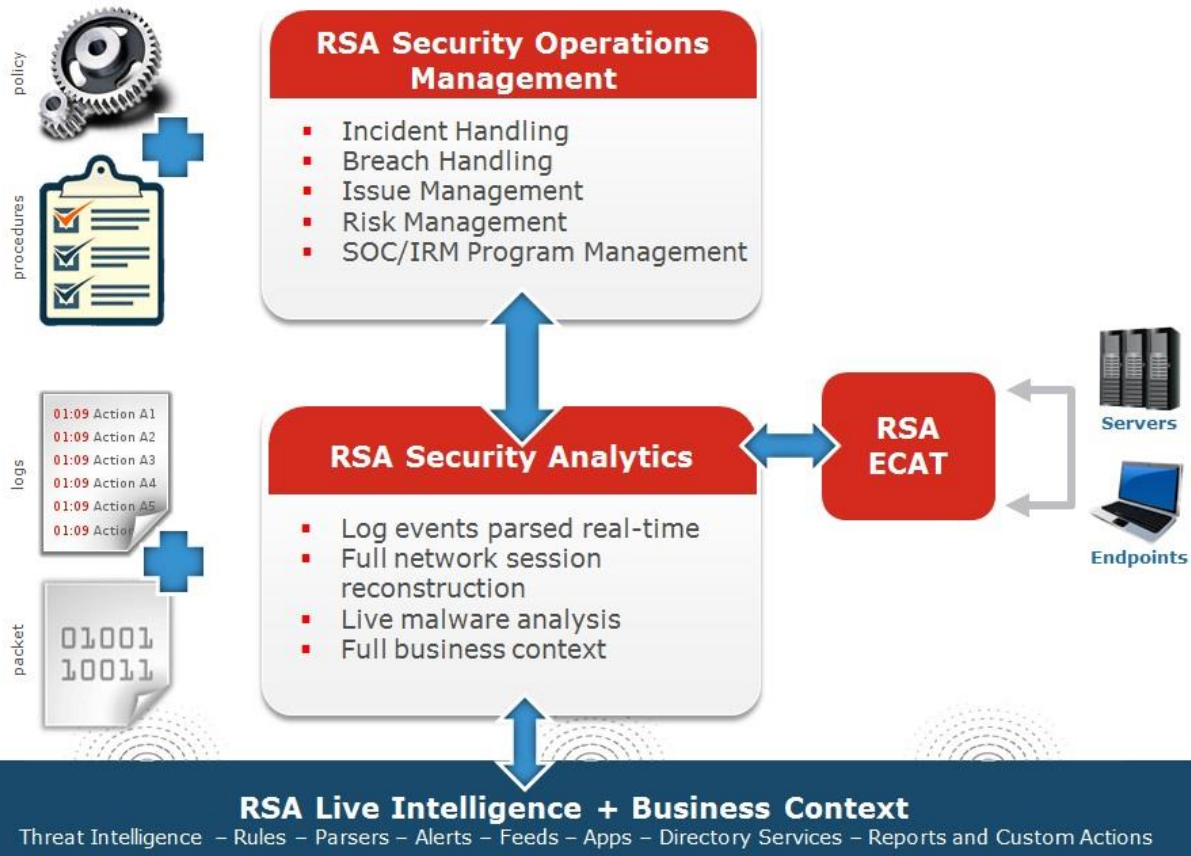


As You Grow, The Product Grows With You

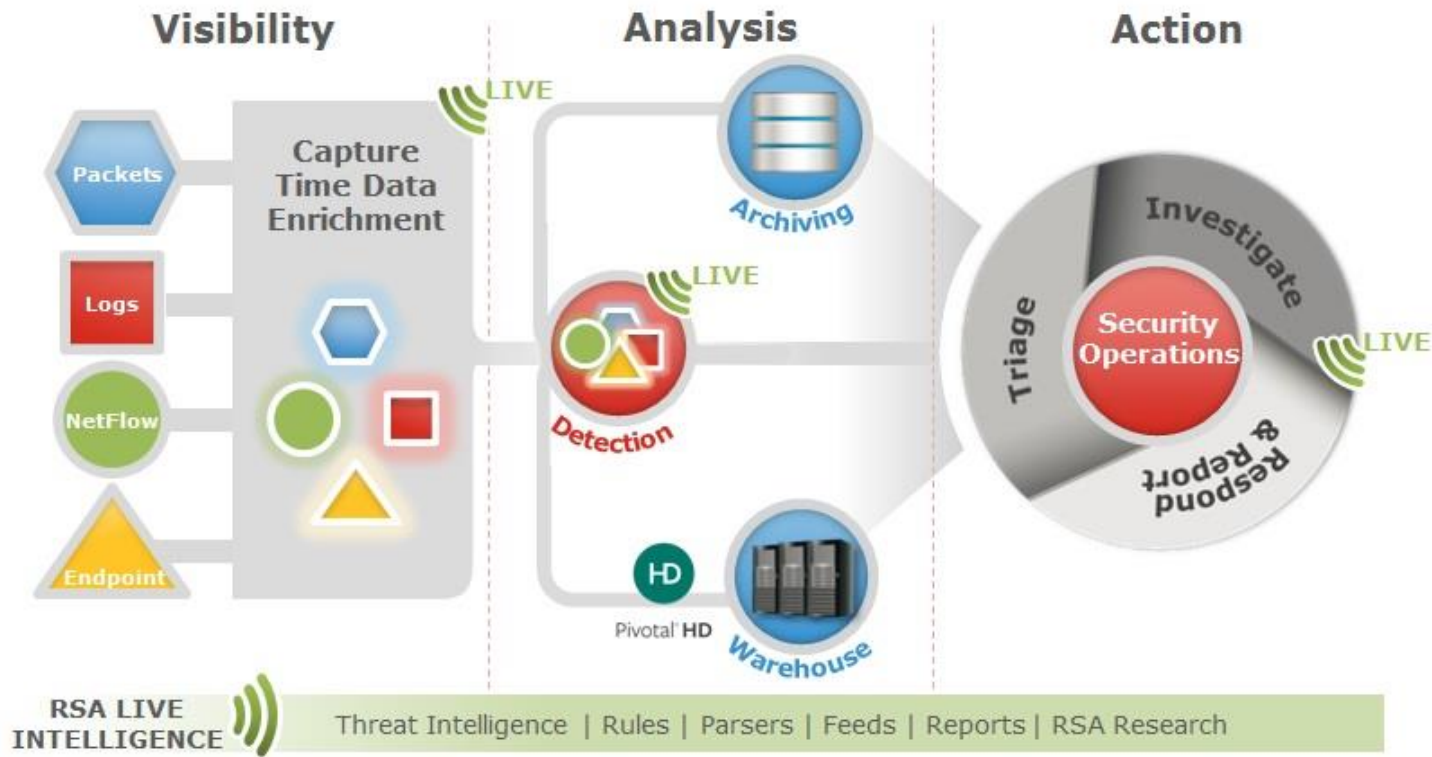


RSA Advanced SOC ecosystem

Full Visibility and Contextual Awareness

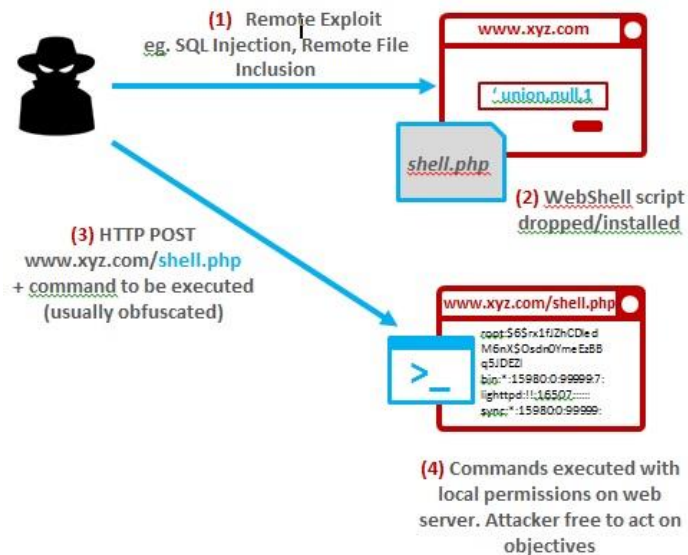


RSA Security Analytics (SIEM) module

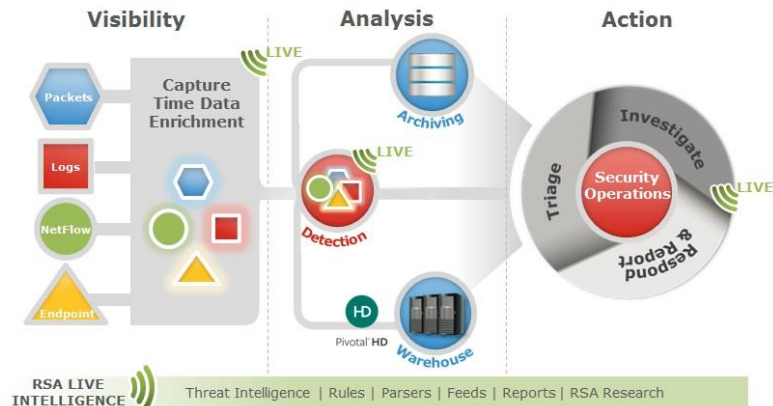


Live Demo: Use Case

WebShell Attack



Detection and Response

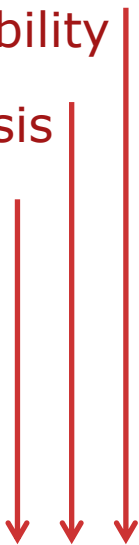


Live Demo: Results

Visibility

Analysis

Action



Alert on a possible Webshell Attack



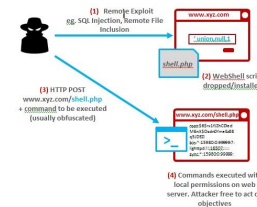
Confirmation of malicious activity from a **remote attacker**



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



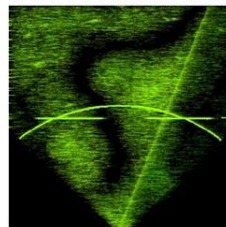
Reconstruction of WebShell attack



What we have learned today



1965 Aviation Radar



2015 Tactical Situation Display



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

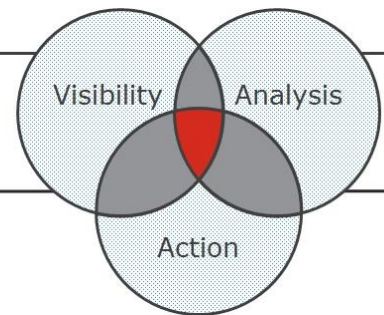
I NEED MORE THAN A SIEM TOOL. I NEED **BUILT FOR TODAY**

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

— SOC Manager —

TRANSFORM

Intelligence-Driven Security



Q&A time



..Thank you!!



EMC²

EMC, RSA, the EMC logo and the RSA logo are trademarks of EMC Corporation in the U.S. and other countries.