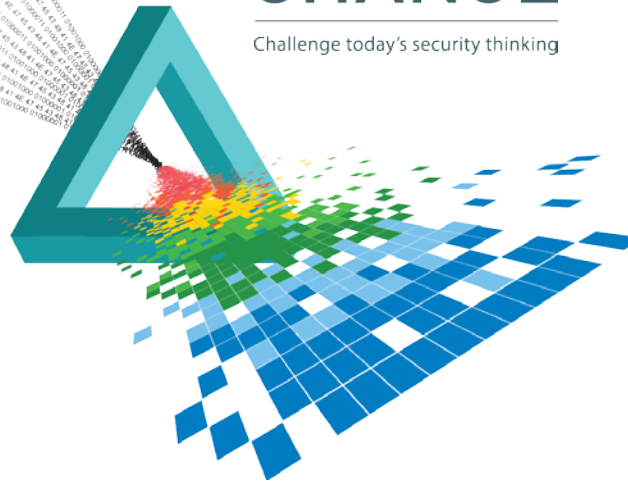
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking



SESSION ID: SPO-R04

The Time Is Now—A New Era for Cybersecurity

Ashok Sankar

Senior Director Cyber Strategy
Raytheon|Websense

Neil Thacker

Information Security & Strategy Officer, EMEA
Raytheon|Websense

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SPO-R04

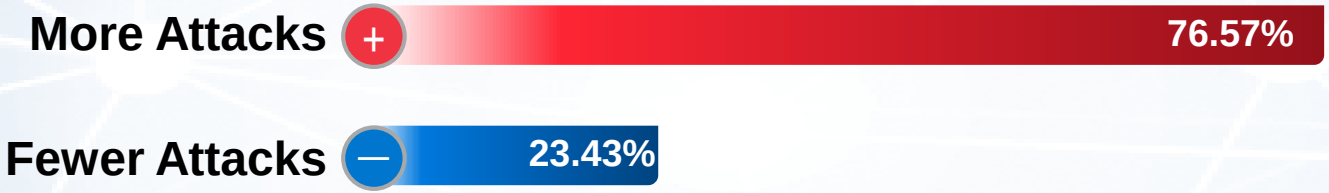
The Time Is Now—A New Era for Cybersecurity

Ashok Sankar

Senior Director – Cyber Strategy
Raytheon | Websense
@ashoksankar

Increasing Attacks

In 2014 has your enterprise experienced an increase or decrease in security attacks as compared to 2013?

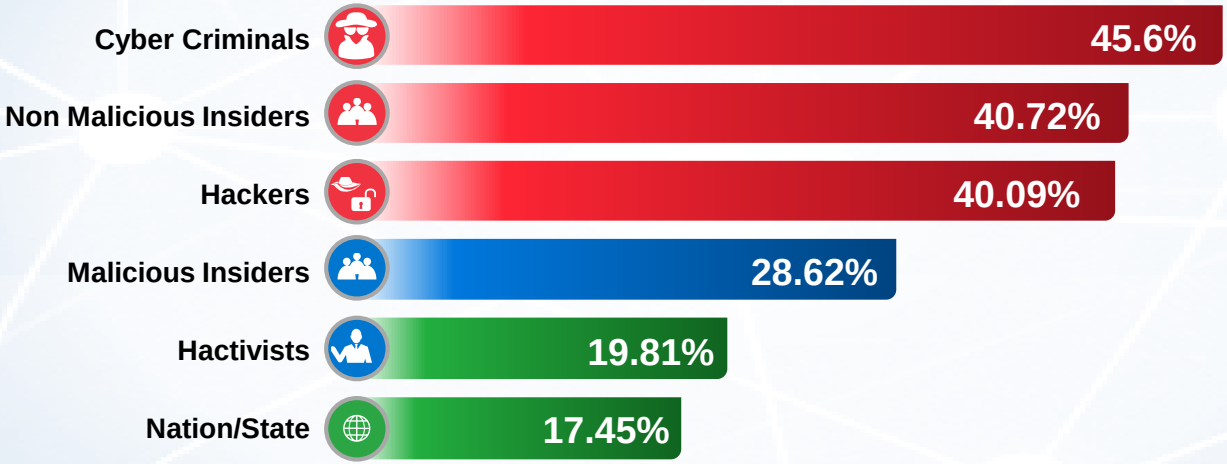


82.5% Enterprises expect to be breached in 2015

Source: State of Cybersecurity: Implications for 2015, An ISACA and RSA Conference Survey

The New Adversaries

Which of the following threat actors exploited your enterprise in 2014?



Source: State of Cybersecurity: Implications for 2015, An ISACA and RSA Conference Survey

The New Enterprise Landscape

EVOLVING BUSINESS ENVIRONMENT

- Dissolving Security Perimeter
- Embracing Mobility and Cloud Computing
- Extending Value Chain of Partners / Supply Chain / Contractors

MORE DANGEROUS THREAT LANDSCAPE

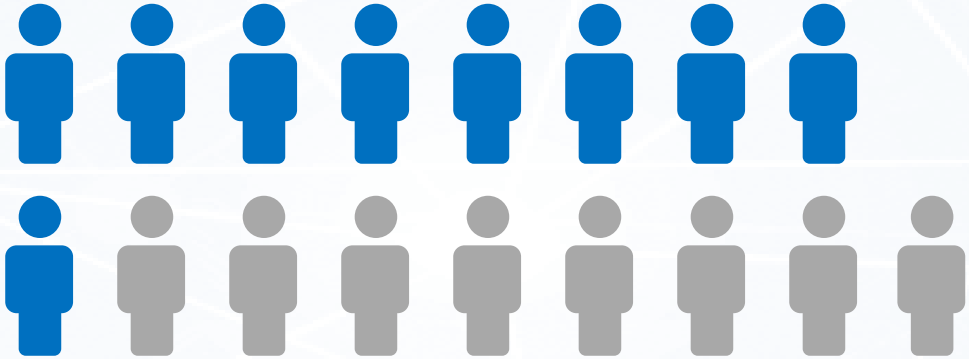
- More Than Just Malware
- Threats Vectors Span Multiple Channels
- Insider Threat Widening

COMPLEXITY & FRAGMENTATION

- Too many tools
- Too many alerts
- Not enough skills and manpower to deal with this complexity

Cybersecurity Skills Gap Grows

2013
2.25 million



2017
4.25 million

The shortage of skills compounds the rise in security incidents

Source: 2013 (ISC)2 Global Information Workforce Study

= 250,000

Chasing Alerts is a Failing Strategy

Malware Containment Survey Results:
Hours Spent on Alerts

198.8 Approximate # of hours per week spent investigating infections

229.9 Approximate # of hours per week spent cleaning or fixing infected devices

395 Approximate # of hours per week wasted chasing erroneous alerts

Malware Containment Survey Results:
Malware Alerts Per Week

16,937 Average # of malware alerts per week

4%	19%	40%
Alerts that get investigated	Reliable alerts	Infections that go undetected

Source: Ponemon Institute, 2015

How Do We….

- Continue to fuel business velocity?
- Absorb innovations as needed for the business?
- Stop the adversary from dictating our priorities?
- Confidently navigate the risks in today's changing IT environment?
- Become resilient?

Need a Strategic Response

EVOLVING BUSINESS ENVIRONMENT

MORE DANGEROUS THREAT LANDSCAPE

COMPLEXITY & FRAGMENTATION

1 ADVANCED THREAT PROTECTION

THREAT DEFENSES THAT MODEL THE BEHAVIOR OF COMPLEX MULTI-STAGE ATTACKS.

2 END-TO-END VISIBILITY

CONTINUOUSLY MONITOR ACTIVITIES INCLUDING USER BEHAVIORS ACROSS YOUR ENTERPRISE.

3 ADVANCED ANALYTICS

INTUITIVELY TURN DATA INTO INSIGHTS AND ANSWERS THAT DRIVE ACTION.

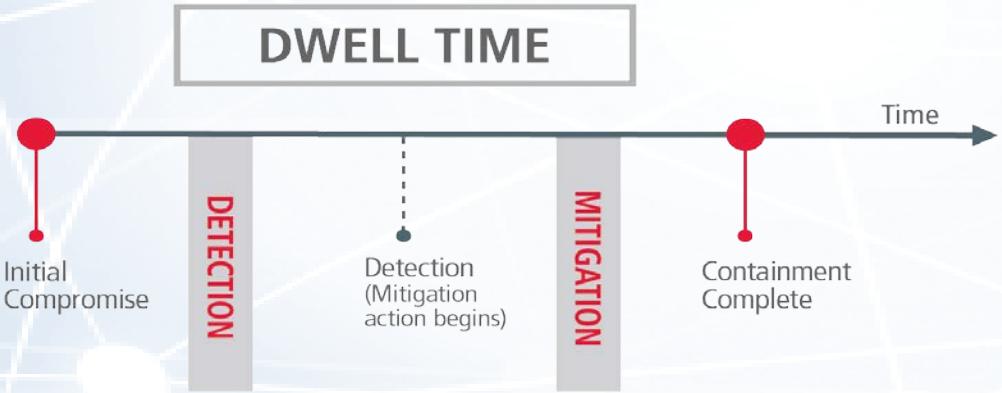
4 ADAPTIVE SECURITY

APPLY CONTEXT RICH INTELLIGENCE TO STOP AND CONTAIN EMERGING THREATS.

Focus: Dwell Time Reduction

206 Days Mean time to identify a breach[1]

69 Days Mean time to contain a breach[1]



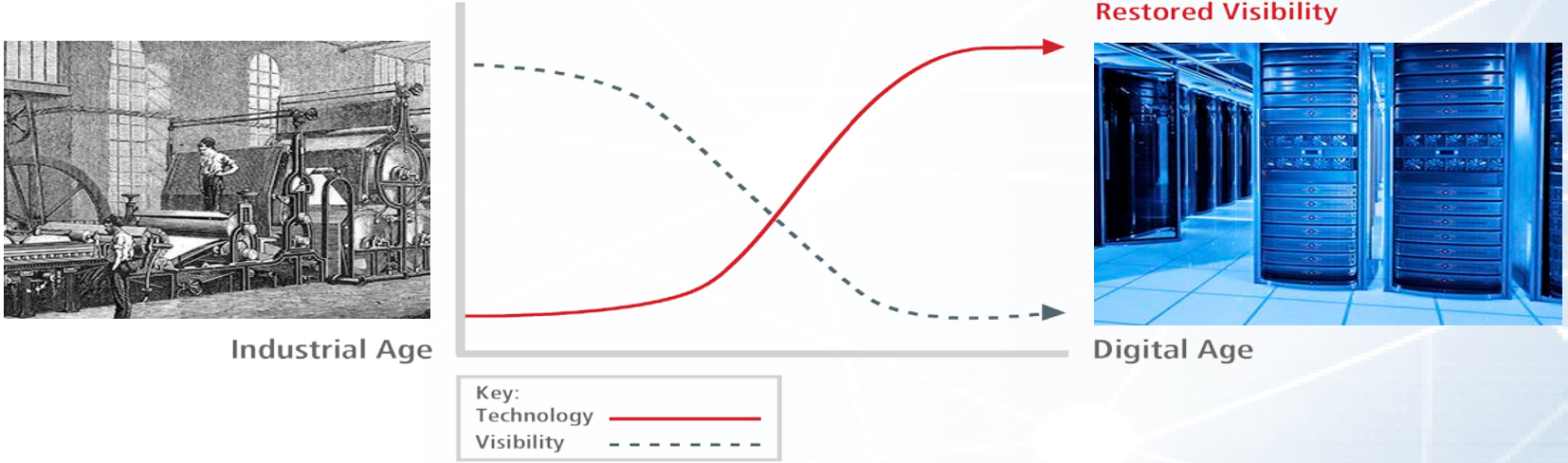
"It is better to have 100 attackers on your network for 10 minutes than a single attacker for 6 months. ***If dwell time trends down then cyber security is improving****"*

Jeff Brown, Raytheon CISO

[1]*Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2015*

End-to-end Visibility

- The digital revolution has obfuscated visibility
- Organizations cannot manage threats they cannot see



But is visibility really just more content?

Context ~~Content~~ is KING!

"Context is critical to turning huge amounts of security data into actionable insight and identifying those things that represent the most risk in an organization." - *Neil MacDonald, Gartner*

Analytics Takes Center Stage

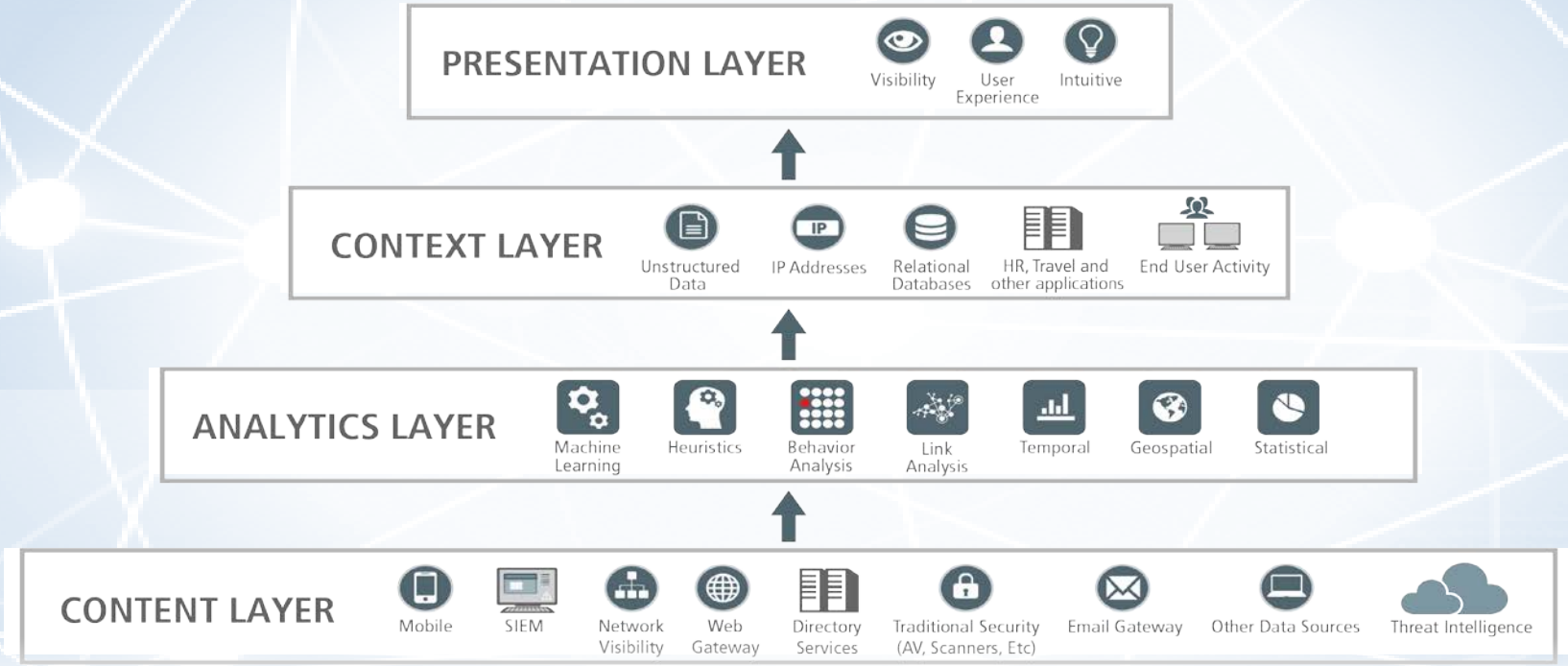
Understand and Prioritize

- Automation can help plow through mountains of information
- Discover more about an entity that you know about (reactive/prevent)
- Investigate to understand patterns, find anomalies (proactive/detect)

Adaptive Security boosts Resiliency

Feedback for prediction and preventative action

Cyber Risk Management Approach



Take Aways

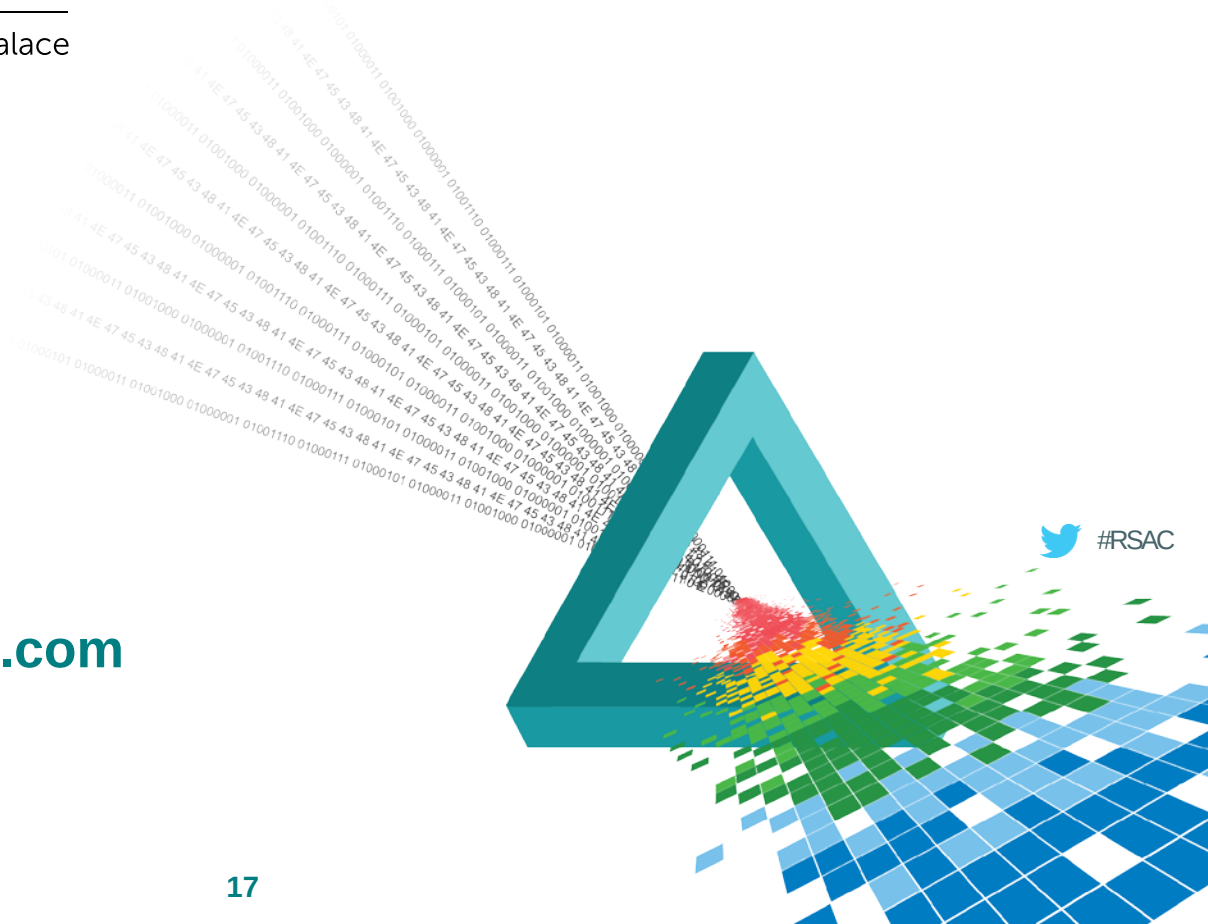
- A determined adversary will break in – not a matter of ‘If’ but ‘When’
- Prevention is ideal but need containment strategies
- Rethink cyber strategies to adapt to the landscape
- Resiliency is key to operation in the new normal

Ashok Sankar

Raytheon | Websense

ashok.sankar@raytheon.com

@ashoksankar

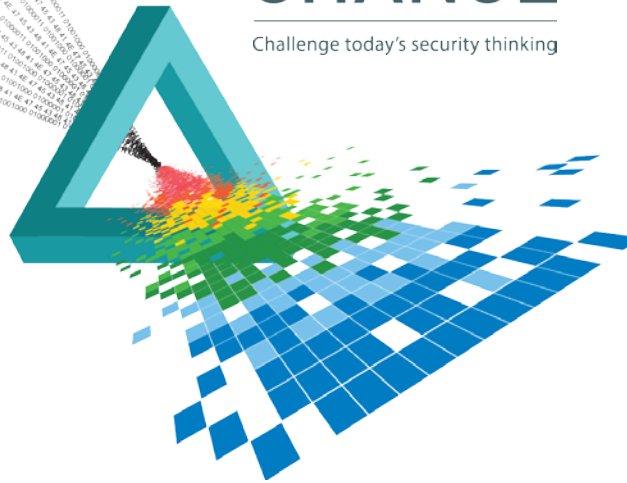


RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking



SESSION ID: SPO-R04

The Time Is Now—A New Era for Cybersecurity

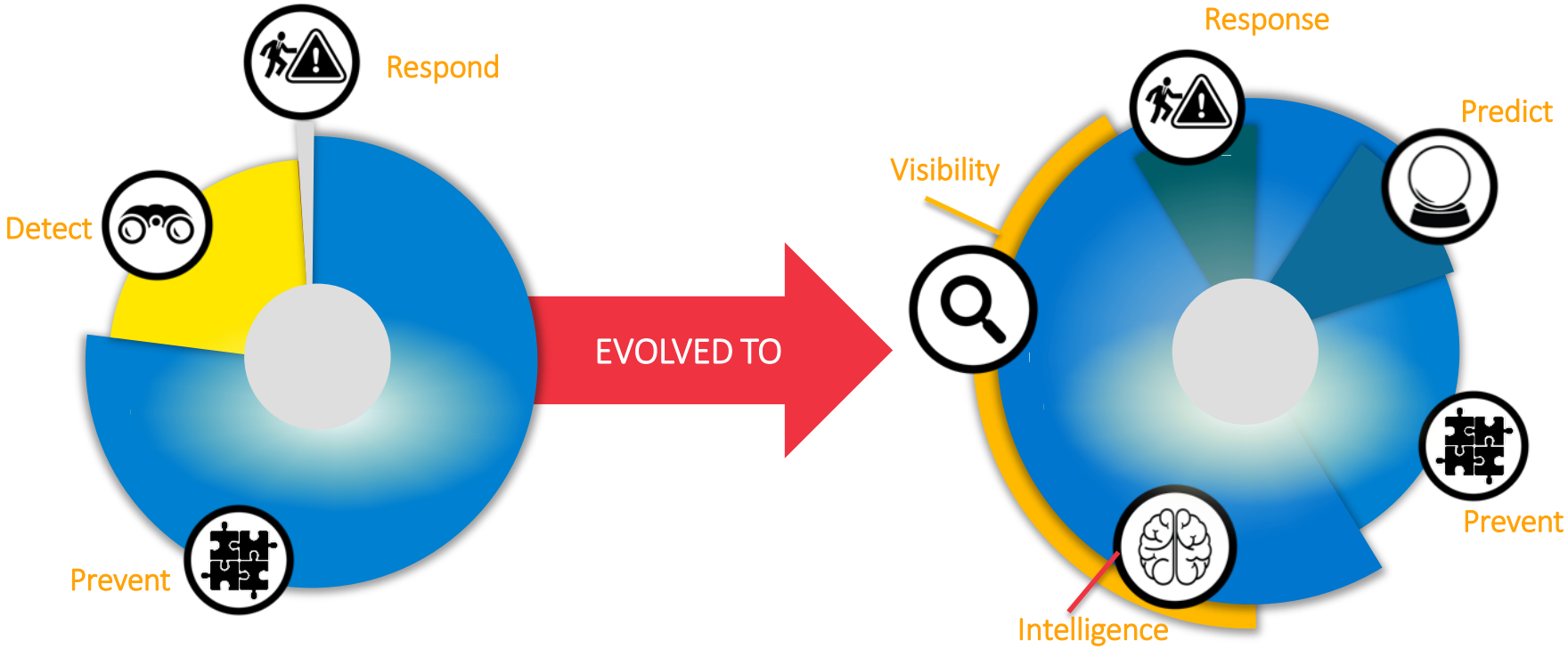
Neil Thacker

Information Security & Strategy Officer EMEA

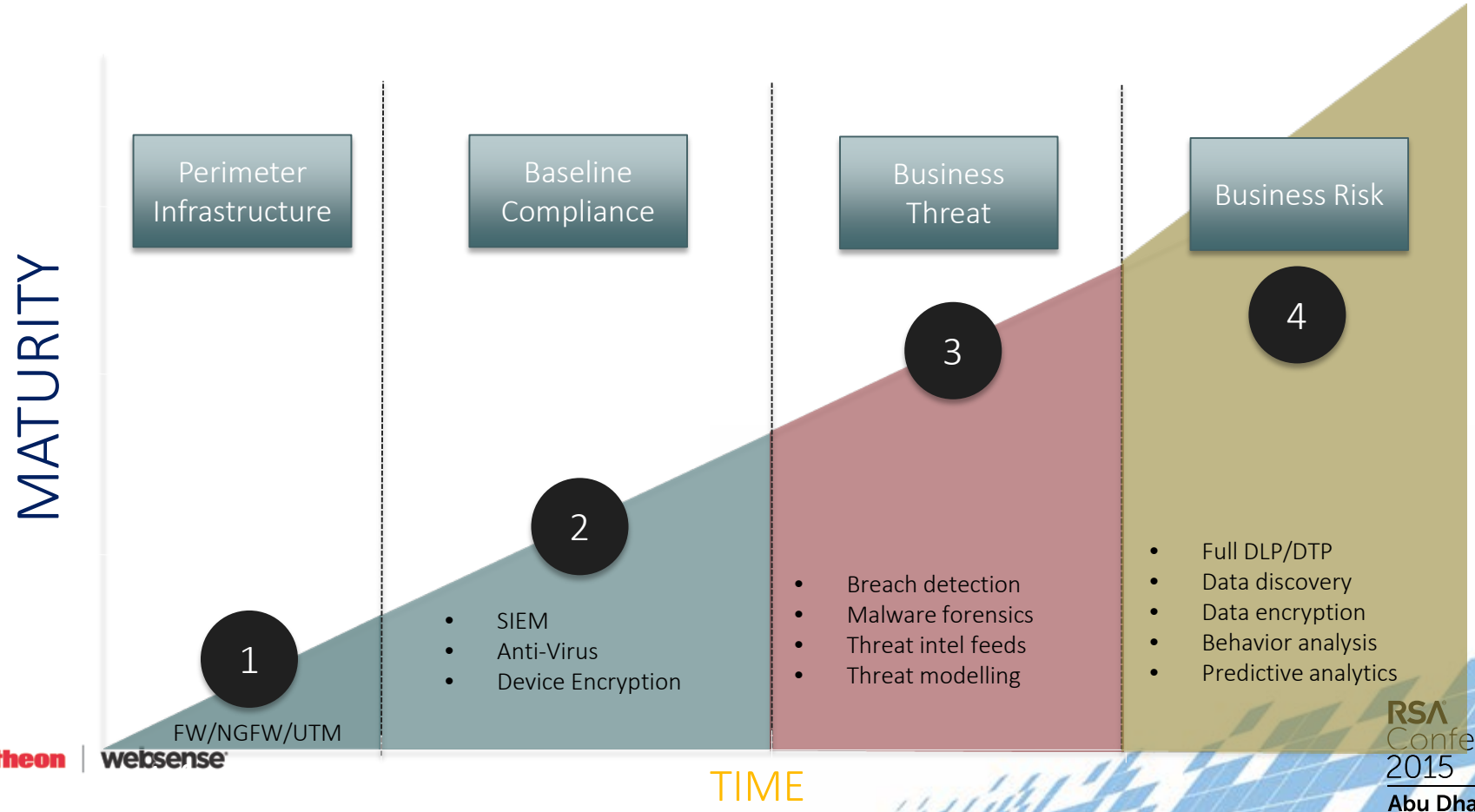
Raytheon | Websense

@nt_hacker

Intelligence, Visibility & Prediction (2000-2015)



From infrastructure security to risk management

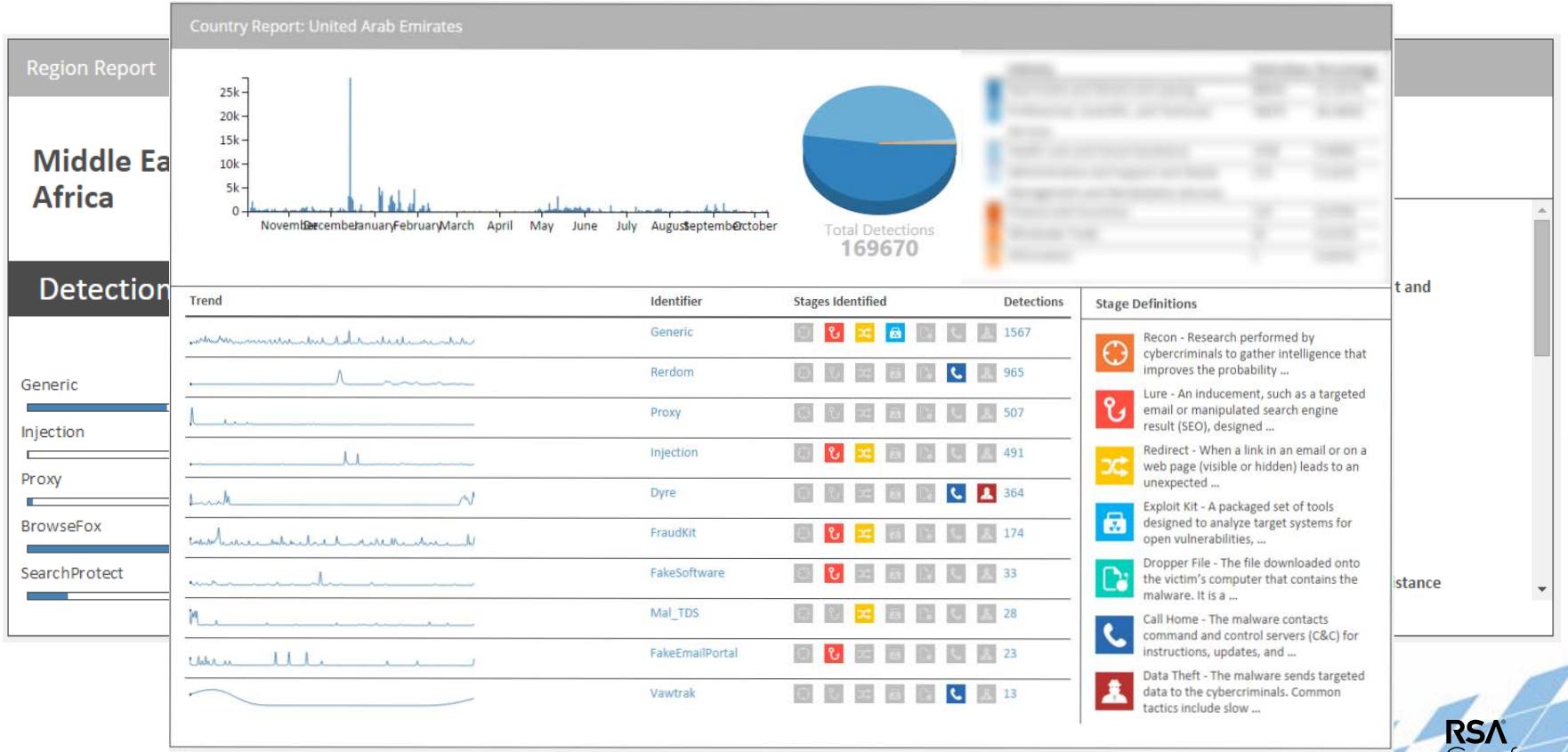


Threat landscape

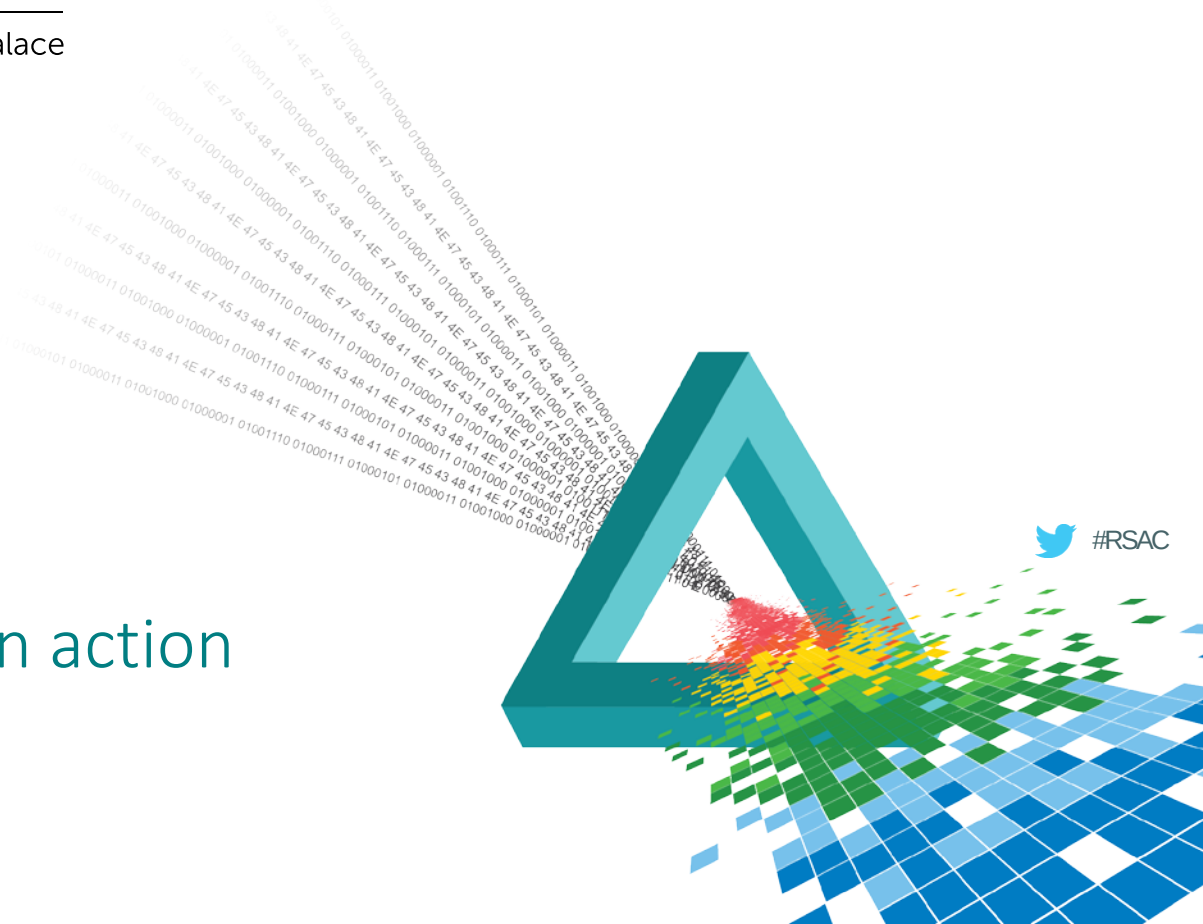
Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑

Source: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

Threat landscape



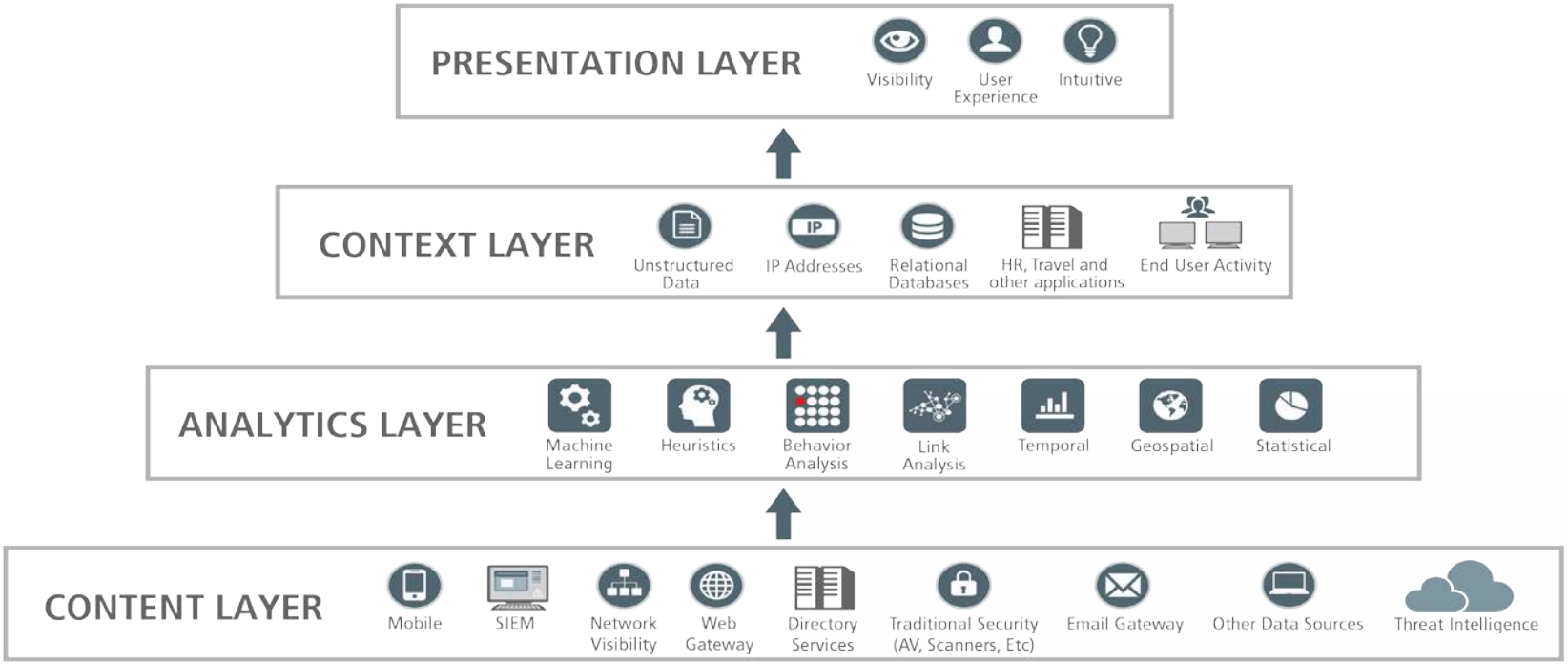
Threat actors



Demo
Analytics & Context in action

Demo

A Layered Approach for the New Normal



Neil Thacker

Raytheon | websense

nthacker@websense.com

@nt_hacker