

# RSA®Conference2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: **SEC-R02**

## Understanding Threats Using Big Data and Contextual Analytics

**David M Dufour**

---

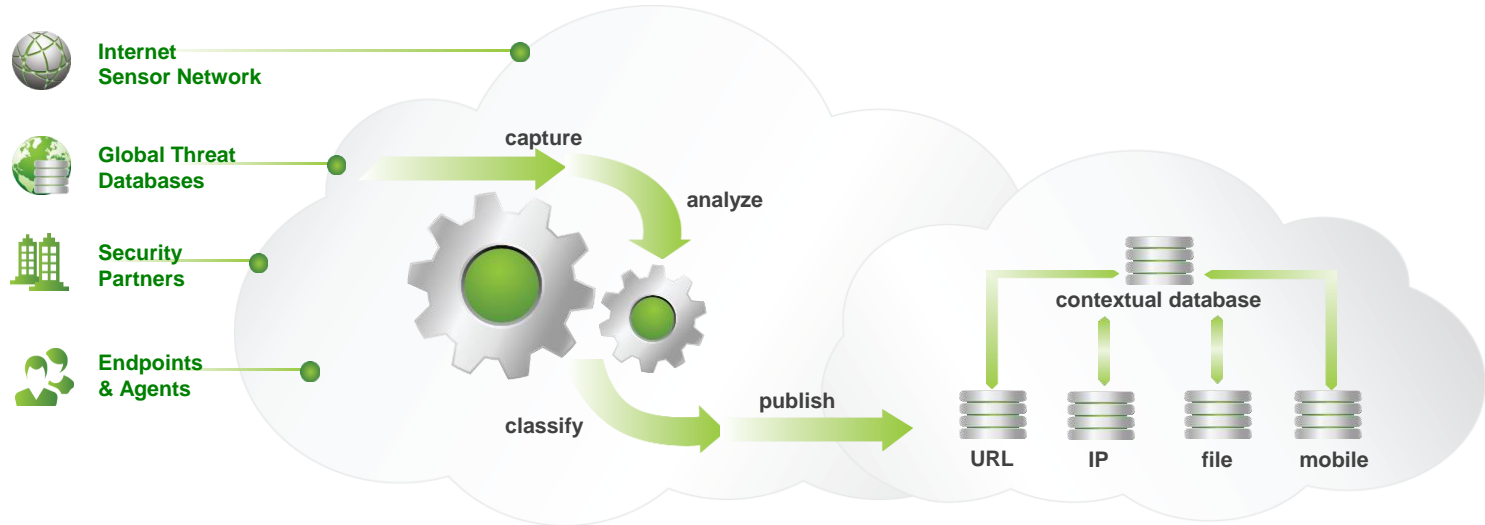
Senior Director of Security Architecture  
Webroot, Inc.  
@davidmdufour

# CHANGE

Challenge today's security thinking



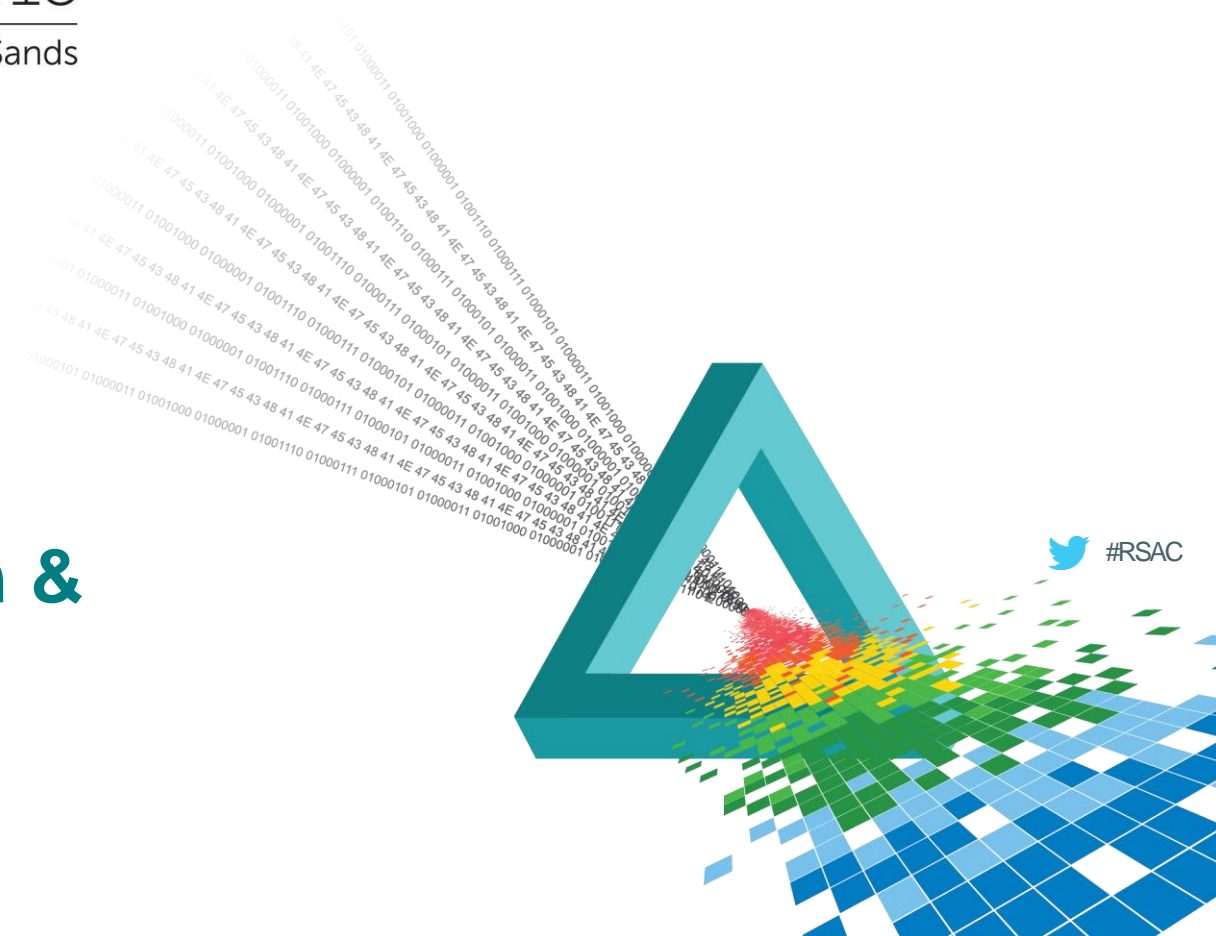
# Architecture Overview



# RSA<sup>®</sup>Conference2015

Singapore | 22-24 July | Marina Bay Sands

## Data Aggregation & Classification



# Collecting Data



## Active

Scanners  
Crawlers



## Passive

Endpoint Agents  
Naive User Simulators  
Victim Machines  
Exploit Honeypots  
Web App Honeypots  
Security Appliances



## 3<sup>rd</sup> Party

Security Partners  
Threat Databases  
Open Source Feeds

# Global Collection Network



# Human Versus Machine



Look for Patterns  
Mentally Create Rules  
Use Heuristics  
Find Silver Bullet  
Errors / Mistakes  
Fatigue

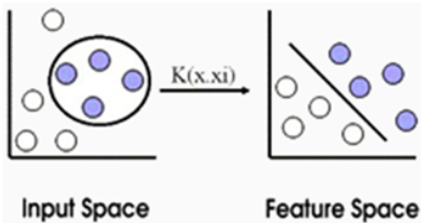


Must be Trained  
Complex  
No Bias  
Can Scale  
High Accuracy  
No Fatigue

# Machine Learning

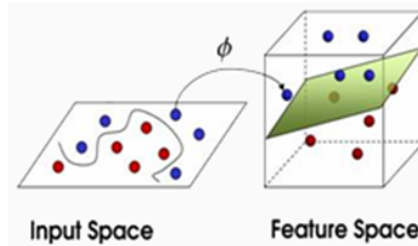
1<sup>st</sup> Generation

Bayesian Networks



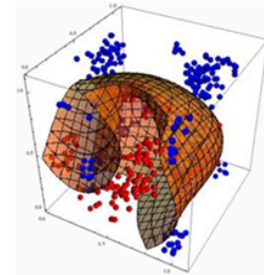
2<sup>nd</sup> Generation

Support Vector  
Machines (SVM)



3<sup>rd</sup> Generation

Maximum Entropy  
Discrimination (MED)



# Distributed Computing & Big Data



Microsoft Azure

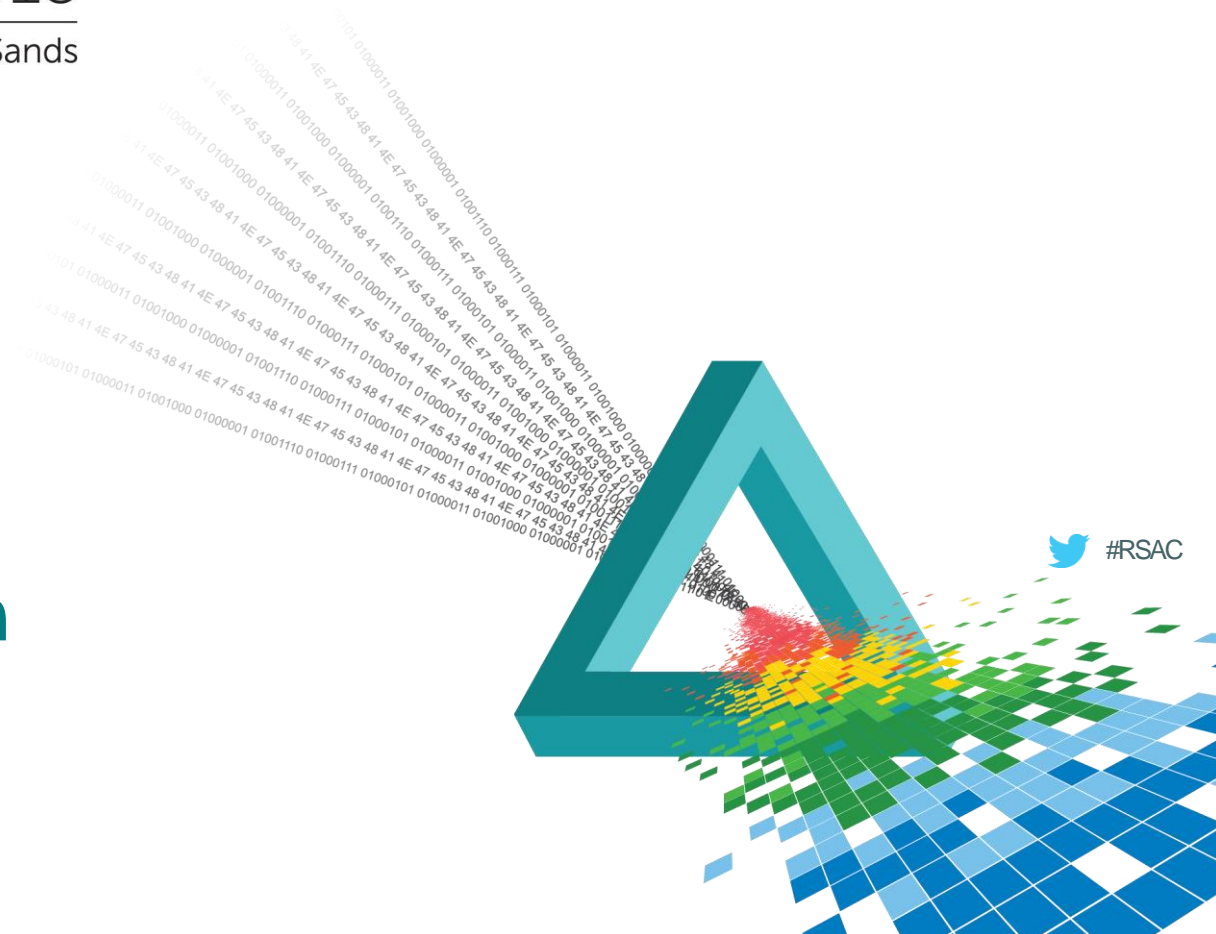




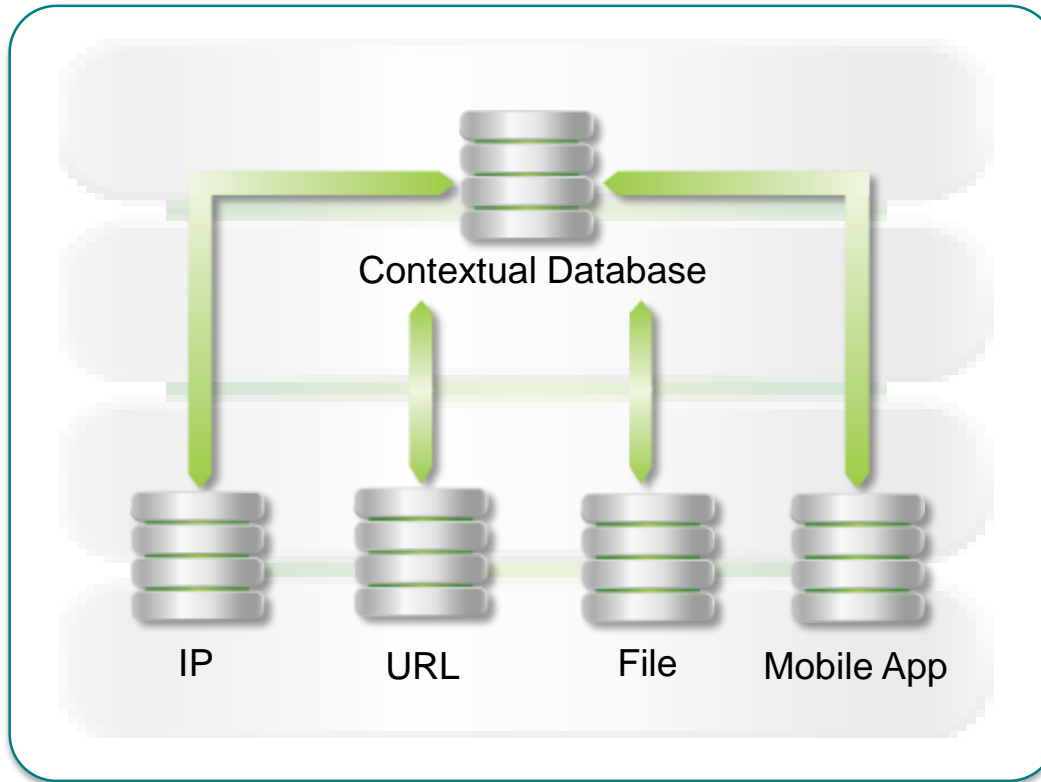
# RSA<sup>®</sup>Conference2015

Singapore | 22-24 July | Marina Bay Sands

## Contextualization

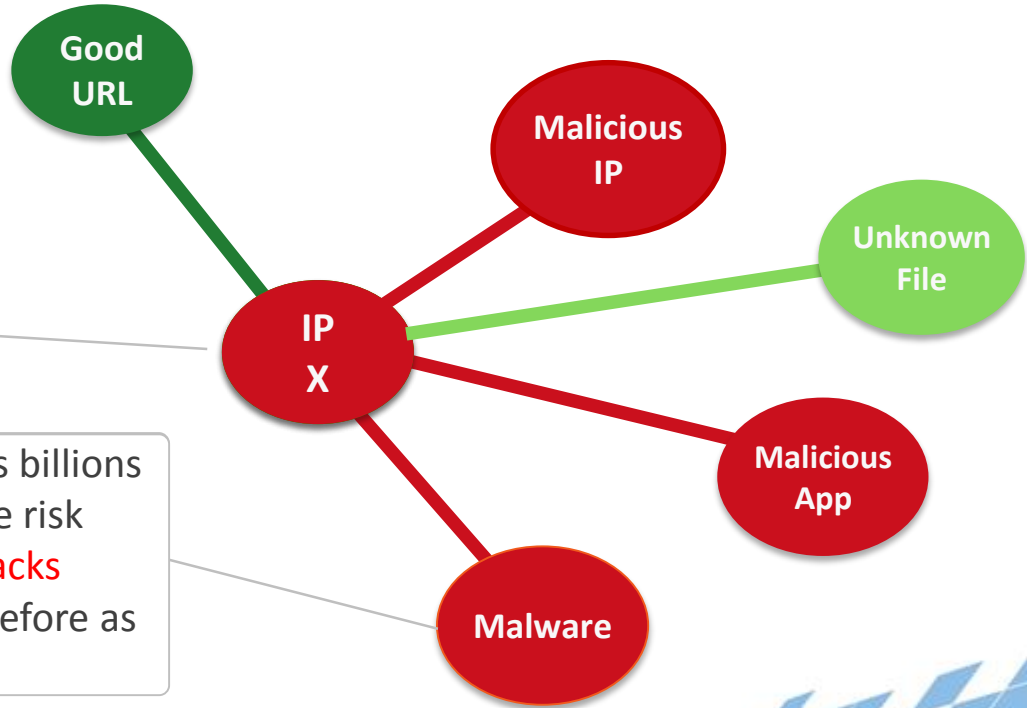


# Contextualization



# Contextual Threat Intelligence

Multiple Vector List		
IP	Score	
IP...	✓	95
IP...	✓	34
IP...	✓	78
IP X	✋	17
IP...	✓	93




This relational mapping is applied across billions of objects in real-time for more accurate risk assessment—helping **predict future attacks** even if an object has never been seen before as a threat.

# Contextual Lookup Example

tumblr.com

Geographic Information ⓘ



Country: United States  
High Risk: 1,274,813  
City: New York  
High Risk: 34,475

BrightCloud Information

BrightCloud Reputation Index
96

Domain Information:

URL	tumblr.com
Domain	tumblr.com
Scheme	http

Category Information:

Category Name	Social Network
Category Group	Productivity
Confidence	100

General Information:

Popularity	1
------------	---

Contextual Information

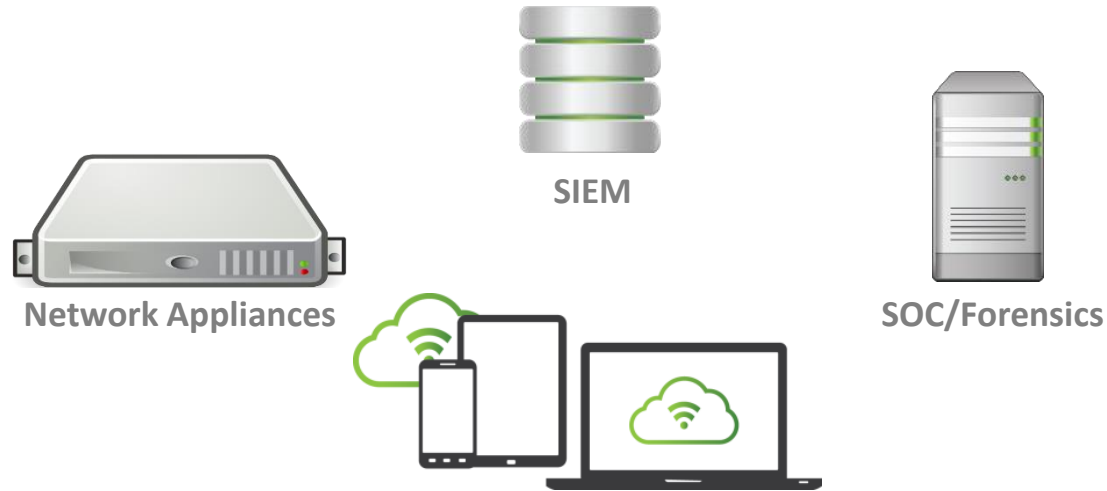
Virtually Hosted Domains Domains Mobile Apps

This is a threat-level distribution of domains that share the same IP as the URL you selected. Click on the View button to see the connections for that threat level.

Virtually Hosted Domains

Total:	97	
High Risk:	0	<a href="#">View</a>
Suspicious:	2	<a href="#">View</a>
Moderate Risk:	2	<a href="#">View</a>
Low Risk:	23	<a href="#">View</a>
Trustworthy:	70	<a href="#">View</a>

# Possible Uses of Contextual Data



# Now What? Apply

- ◆ Inventory data sources currently available
- ◆ Look for ways to apply this data more effectively
- ◆ Define gaps in both the data and application of the data
- ◆ Look for external tools and sources to help fill the gaps
- ◆ Ensure to review data, efficacy and processes quarterly

# RSA<sup>®</sup>Conference2015

Singapore | 22-24 July | Marina Bay Sands

Thank you.

