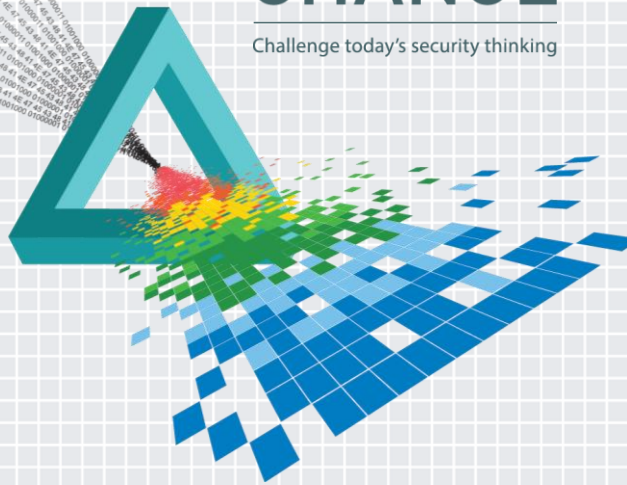
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



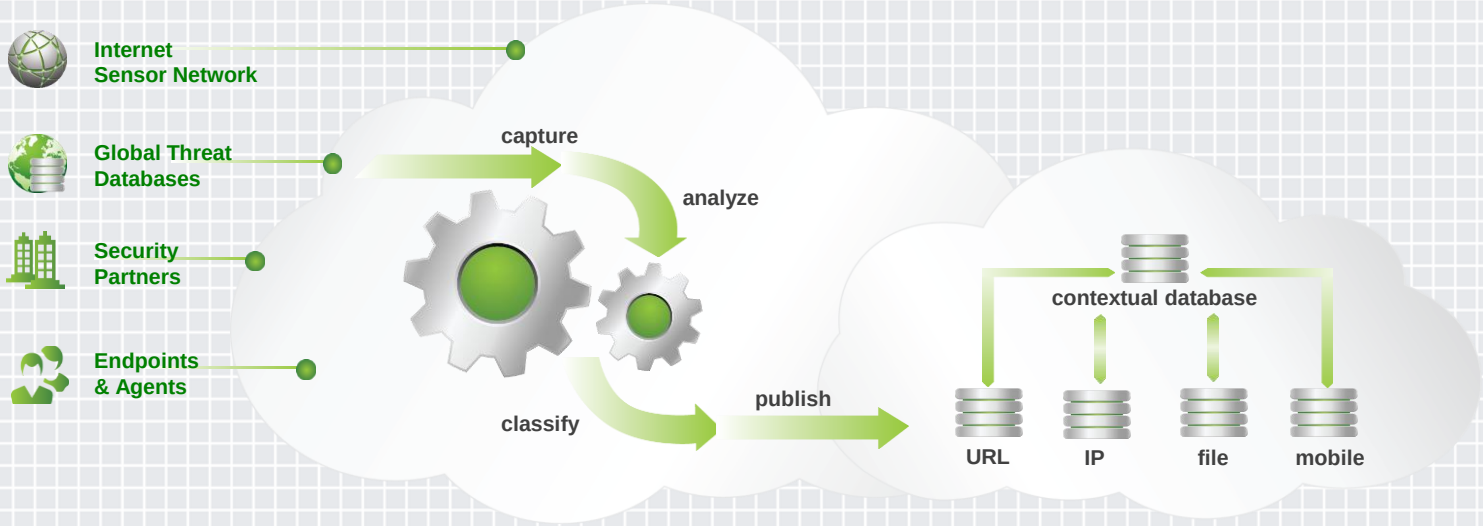
SESSION ID: DSP-F02

Understanding Threats Using Big Data and Contextual Analytics

David M. Dufour

Senior Director of Security Architecture
Webroot Inc.
@davidmdufour

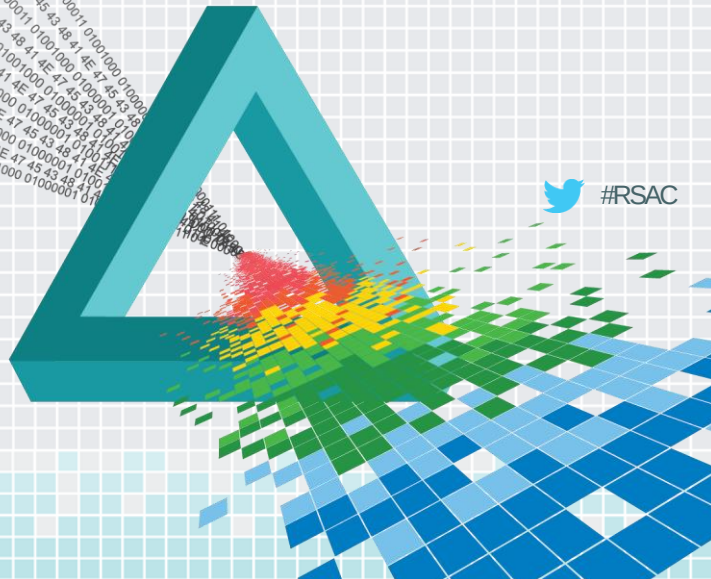
Architecture Overview



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Data Aggregation & Classification



Collecting Data

Active

Scanners

Crawlers

Passive

Endpoint Agents

Naive User Simulators

Victim Machines

Exploit Honeypots

Web App Honeypots

Security Appliances

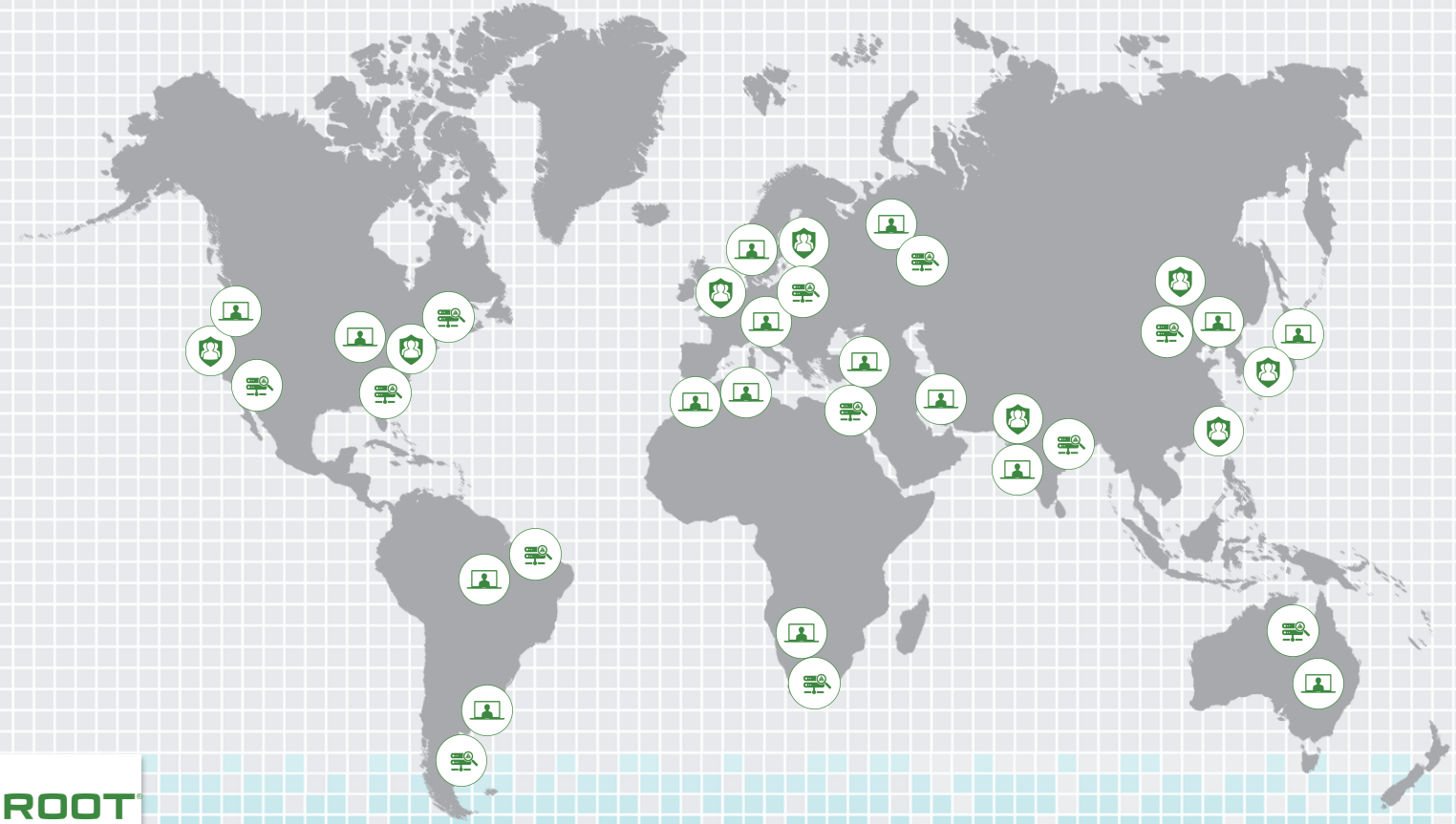
3rd Party

Security Partners

Threat Databases

Open Source Feeds

Global Collection Network



Human Versus Machine

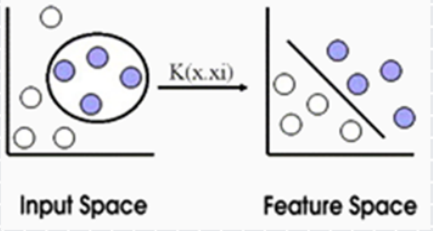
Look for Patterns
Mentally Create Rules
Use Heuristics
Find Silver Bullet
Errors / Mistakes
Fatigue

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

Machine Learning

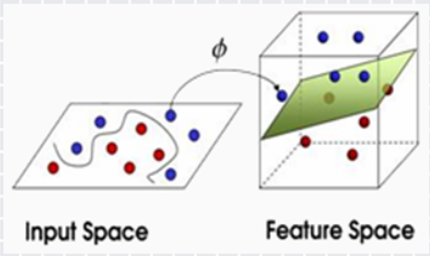
1st Generation

Bayesian Networks



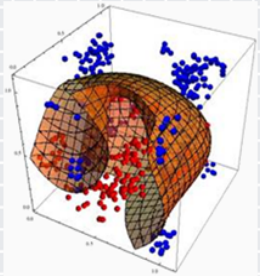
2nd Generation

Support Vector Machines (SVM)



3rd Generation

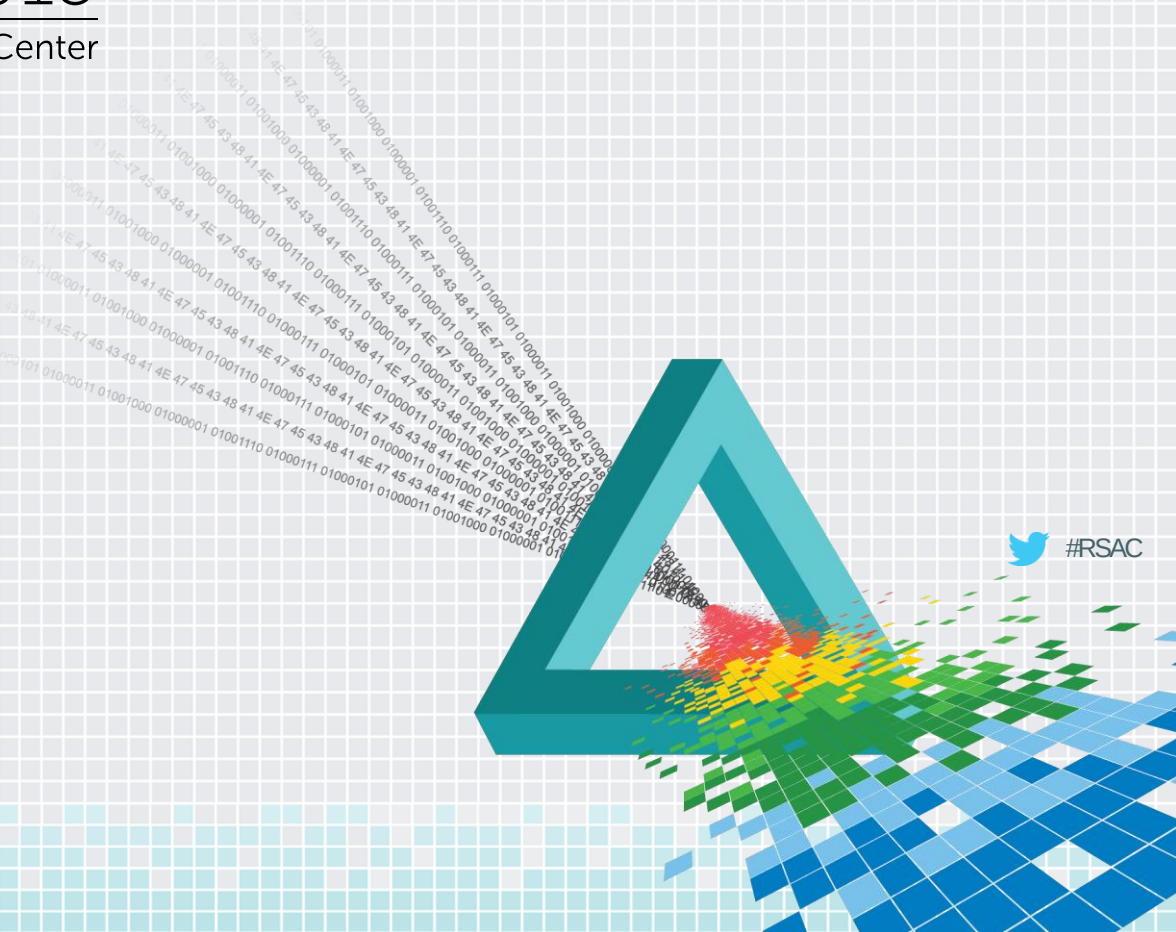
Maximum Entropy Discrimination (MED)



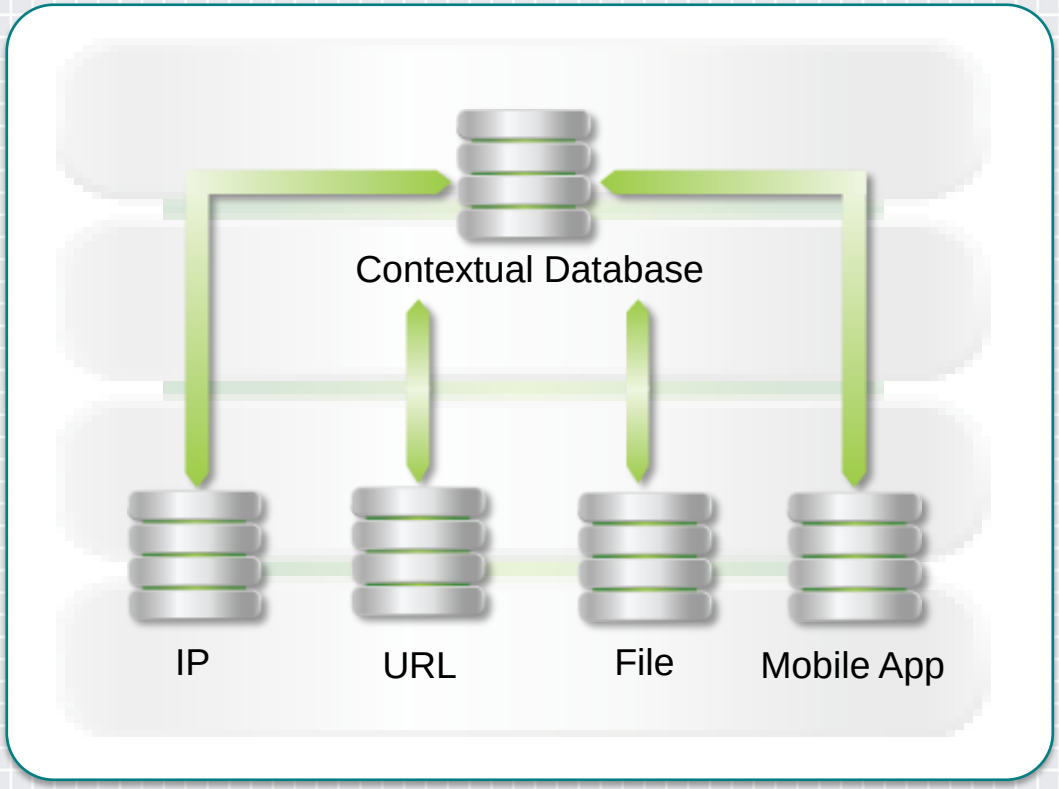
Distributed Computing & Big Data

Microsoft Azure

Contextualization

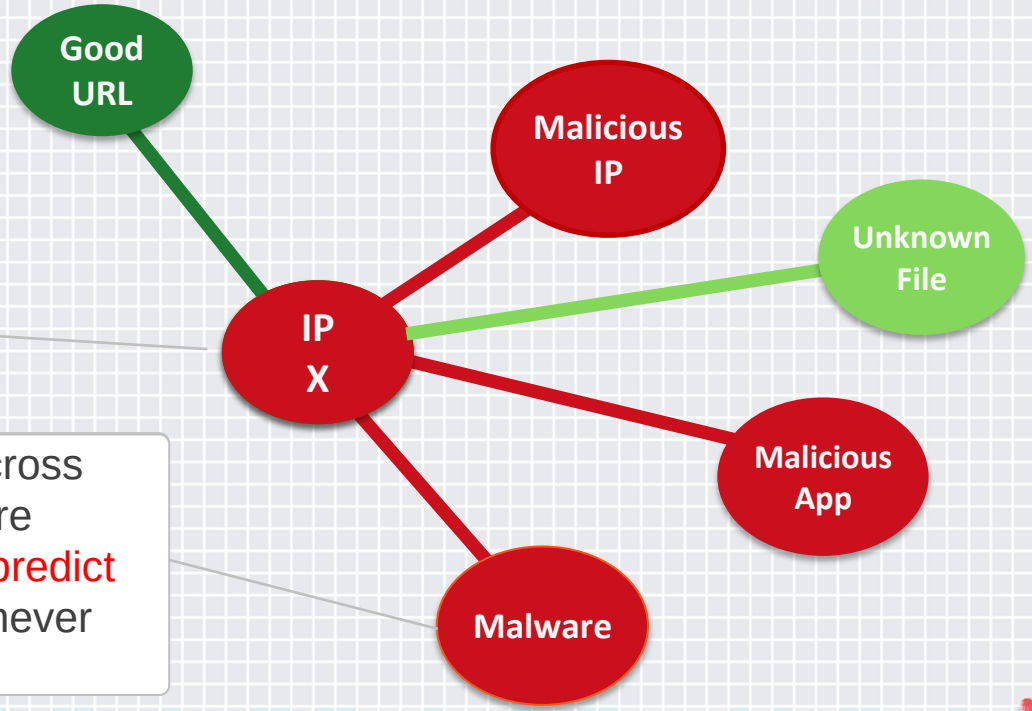


Contextualization



Contextual Threat Intelligence

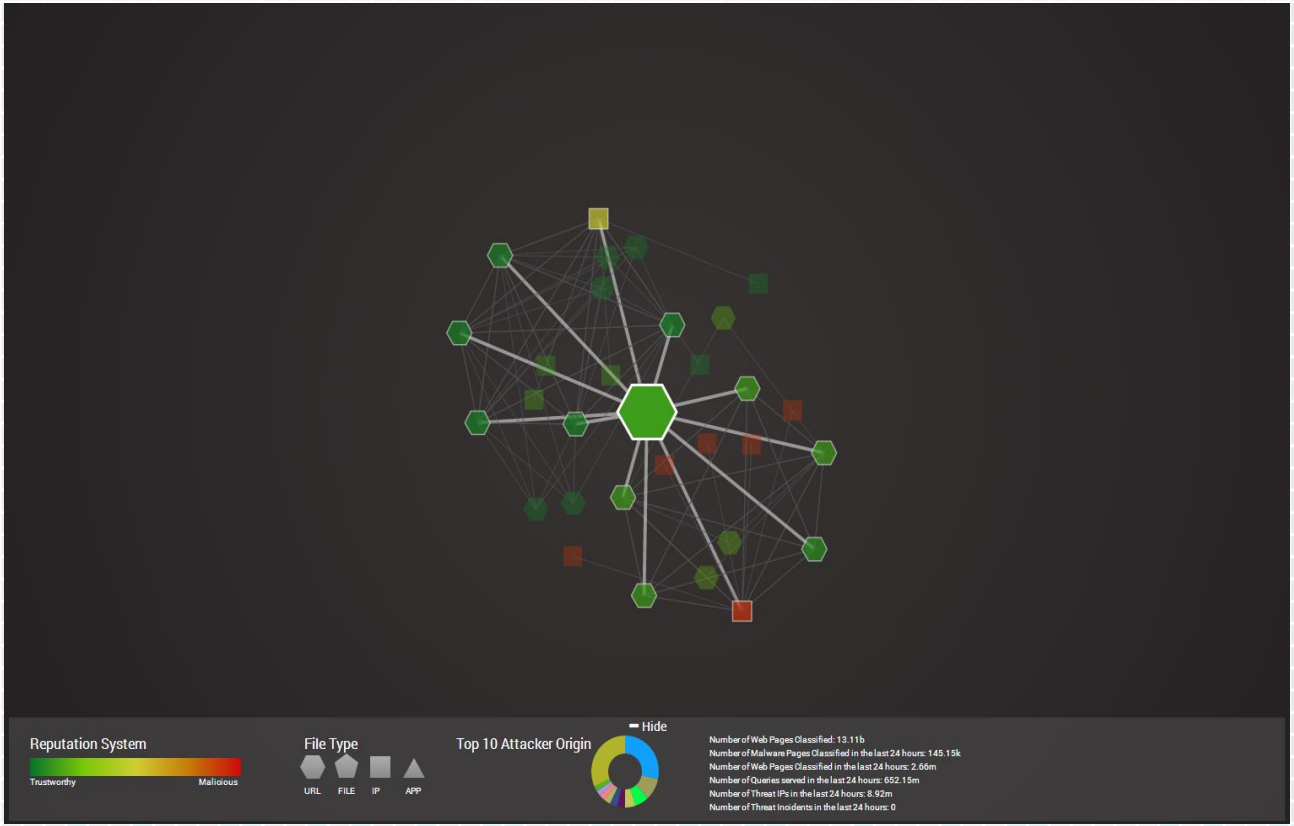
Multiple Vector List	
IP	Score
IP…	95
IP…	34
IP…	78
IP X	17
IP…	93



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.

WEBROOT

Contextual Lookup Example



Possible Uses of Contextual Data

Network Appliances

SIEM

SOC/Forensics

Now What? Application

- 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

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank you.