RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: SPO1-T08

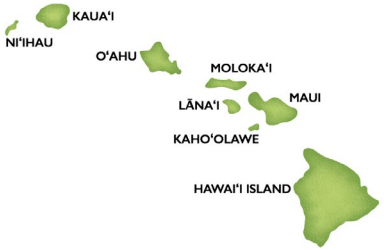
Machine Learning: The What and Why of AI

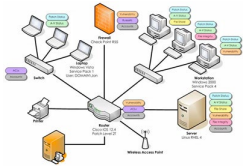
TK Keanini

Distinguished Engineer
Cisco
@tkeanini

Hello My Name is TK Keanini

(Pronounced Kay-Ah-Nee-Nee)





Broderbund

Cisco Systems

Morgan Stanley

nCircle
Proactive Network Security

Lancope

CISCO

Security Analytics Versus Other Analytics

Outcomes

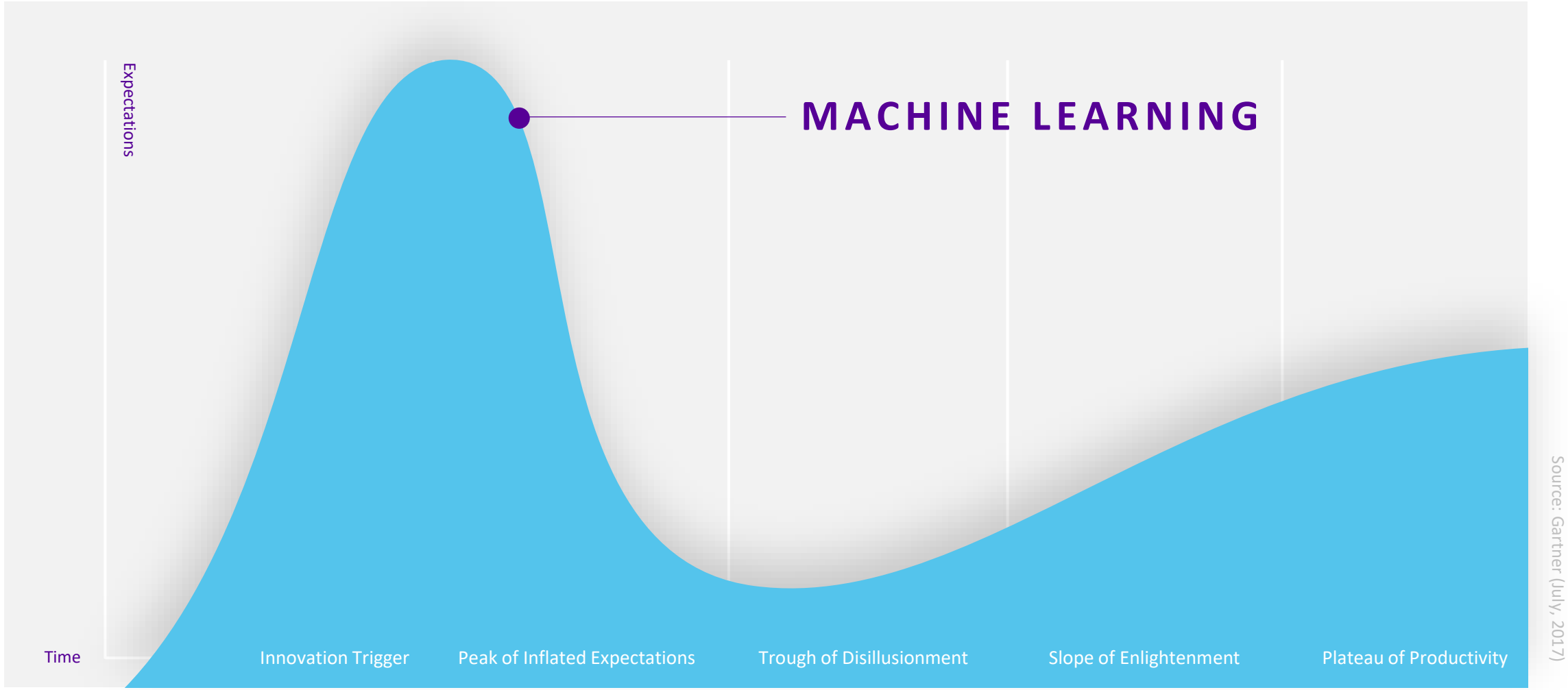
Synthesis/Analytics

Telemetry

Security Analytics focus on augmenting or automating these functions

- Incident Responder
- Security Analyst
- Security Operations
- Threat Hunter
- Compliance and Policy
- Business Continuity
- Cybercrime fighting

Gartner Hype Cycle for Emerging Technologies | 2017



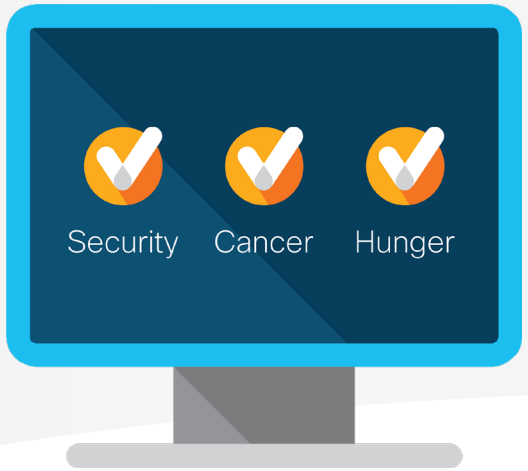
Vendors Got Us Here

"Advanced Threats are no match for A.I."

"Our machines detect threats others cannot"

"100% predictive"

How We Disservice Machine Learning



Silver Bullet Marketing

No Explanation or Discussion

Limited Guidance

RSAConference2019

Machine Learning:
What It Is

"Field of study that gives computers the ability to learn without being explicitly programmed."

Arthur Samuel's definition of machine learning in 1959

Clustering

Instance Based

Regularization

Ensemble

Bayesian

Rule System

Ground Truth

Machine Learning Algorithms

Classifier

Regression

Decision Tree

Neural Network

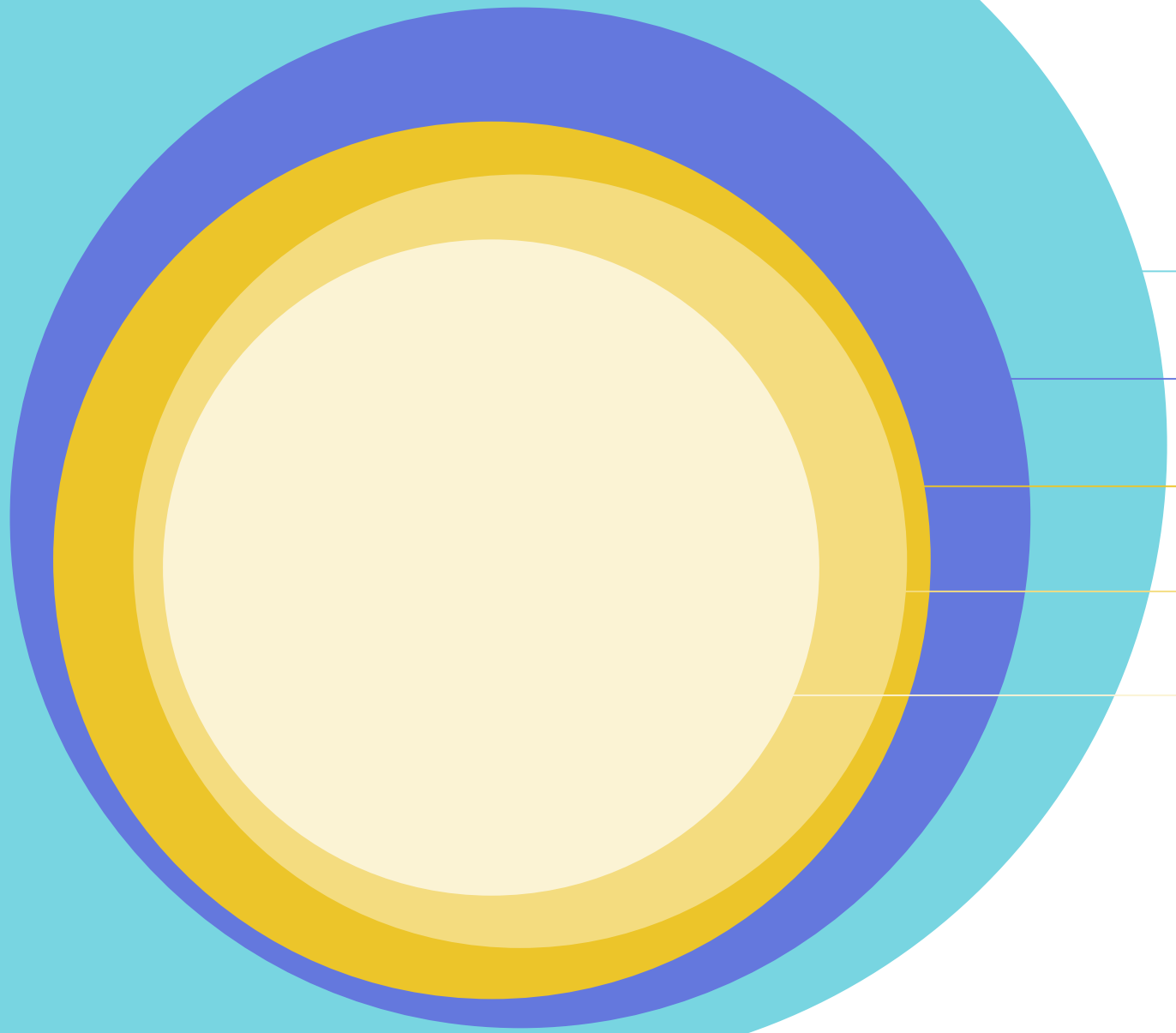
Deep Learning

Dimensionality Reduction

NERD ALERT

Let’s define the helpful data science terms

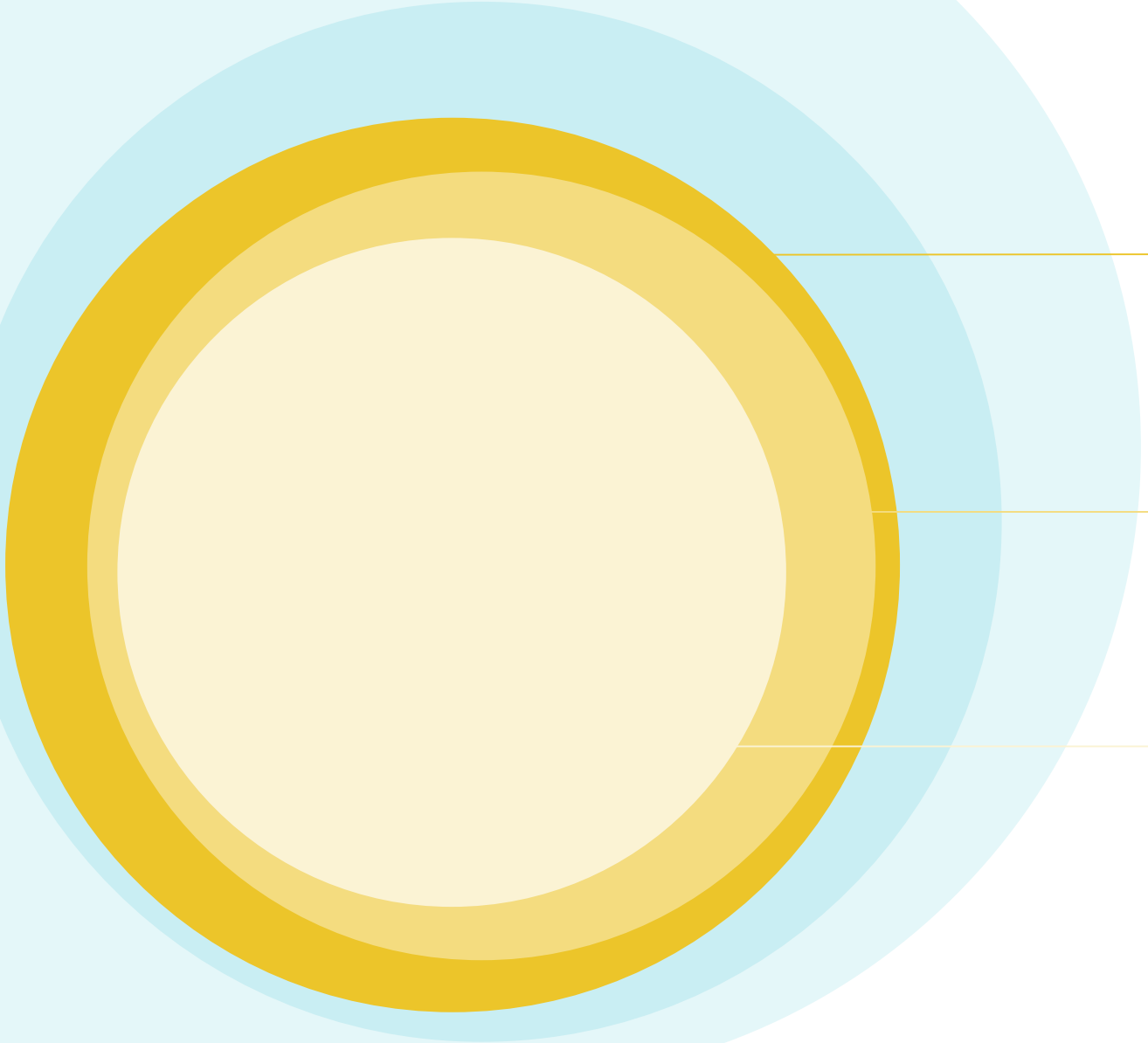
Machine Learning



The Big Picture

- Artificial Intelligence
- Machine Learning
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

Machine Learning



Common Techniques

Supervised Learning

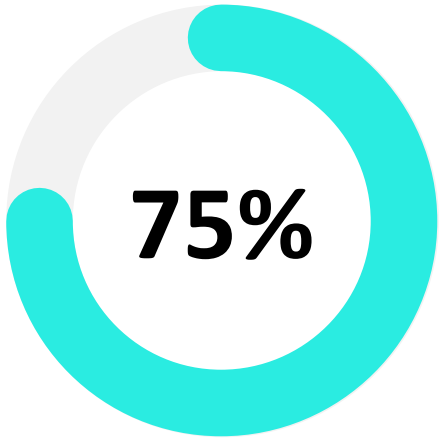
You know the question you are trying to ask and have examples of it being asked and answered correctly

Unsupervised Learning

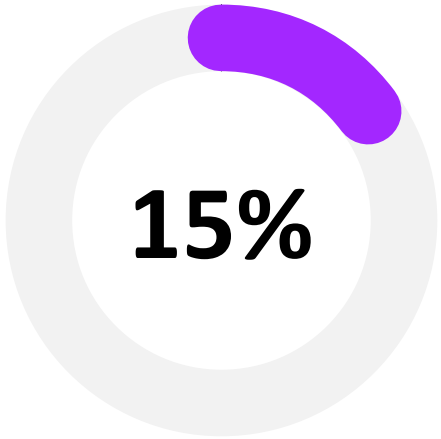
You don't have answers and may not fully know the questions

Reinforcement Learning

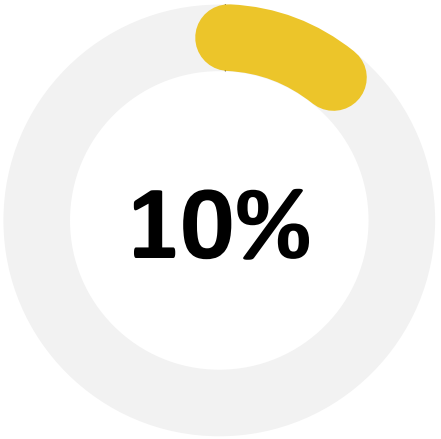
“The other” category
Trial and error behavior
effective in game scenarios



Supervised Learning



Unsupervised Learning



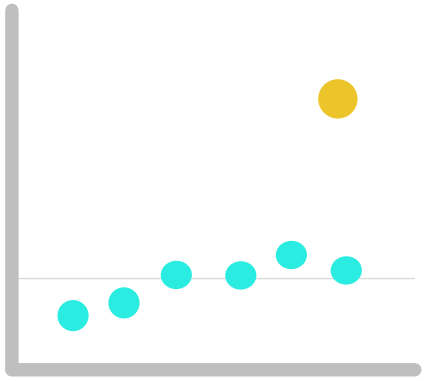
Other

(Reinforcement Learning, etc.)

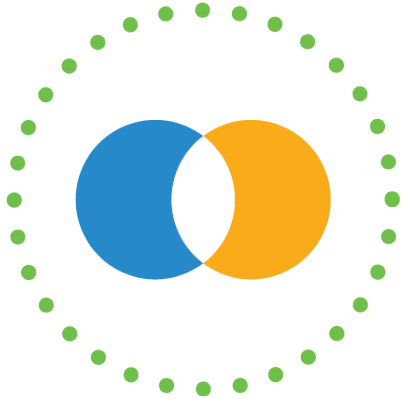
What Did We Do Before Machine Learning?

Use in Combination with Machine Learning

Simple Pattern Matching



Statistical Methods



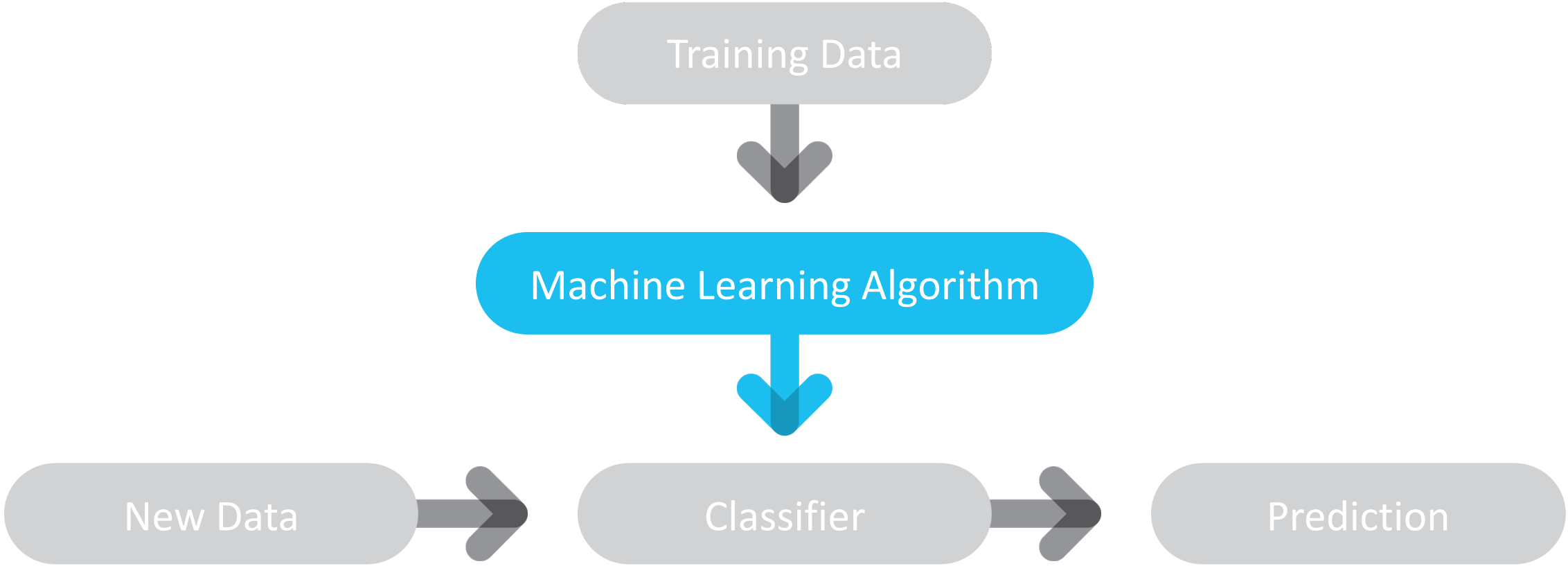
Rules and First Order Logic (FoL)

RSAConference2019

Machine Learning:
Techniques

“Field of study that gives computers the ability to learn without being explicitly programmed.”

Training Classifiers (Supervised Learning)



Ground Truth Used in Supervised Learning

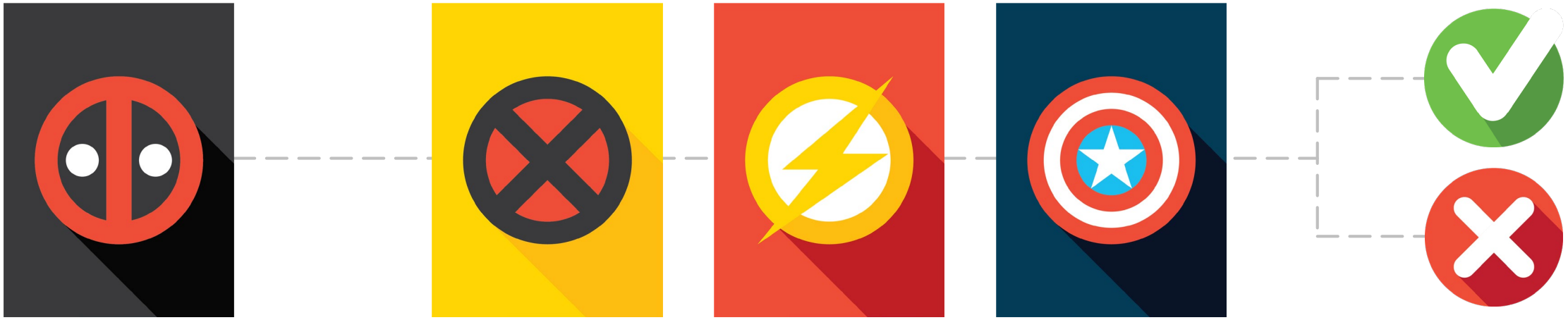
- The **'Ground Truth'** is the pairing of example questions and answers.
- If you can phrase a problem as *'we know this is right, learn a way to answer more questions of this type'*.
- Success depends greatly on the dataset expressing the Question -> Answer mapping.

RSAConference2019

Machine Learning:
Pitfalls

What Is At Stake Matters

Because you watched Deadpool, you might like…



Deadpool

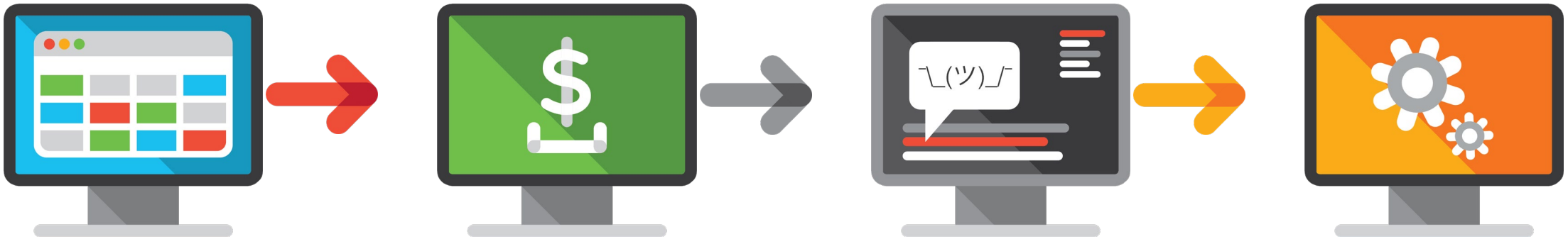
X-Men: First Class

The Flash

Captain America:
The First Avenger

How Did You Come to That Conclusion?

"The Explainability Problem"



Normal Workflow

CFO daily calendar

Irregular Activity

ML detects "suspicious" activity and suggests remediation

Quarantined

However, ML cannot articulate *why* it wants to remediate

Loss of Time and Resources

RSAConference2019

Machine Learning:

For Security

Why Is Machine Learning So Useful in Security?

Static

With limited variability or is well-understood

Evolving Security

The security domain is always evolving, has a large amount of variability, and is not well-understood

Insider Threats and Behavioral Security Analytics

Attackers

They’re not breaking in, they are logging in

Detecting

Through novelty and outliers

Events

Turn weak signals into a strong ones

Example: Cisco Encrypted Traffic Analytics

Industry's first network with the ability to find threats in encrypted traffic **without decryption**

Avoid, stop, or mitigate threats faster then ever before | Real-time flow analysis for better visibility

Public Disclosure of Research in 2016

Cisco Research

Known
Malware Traffic

Known
Benign Traffic

Extract Observable
Features in the Data

Employ Machine
Learning techniques
to build detectors

Known Malware
sessions detected
in encrypted traffic
with high accuracy

"Identifying Encrypted Malware Traffic with Contextual Flow Data"

AISec '16 | Blake Anderson, David McGrew (Cisco Fellow)

Example: Encrypted Traffic Analytics

Outcomes

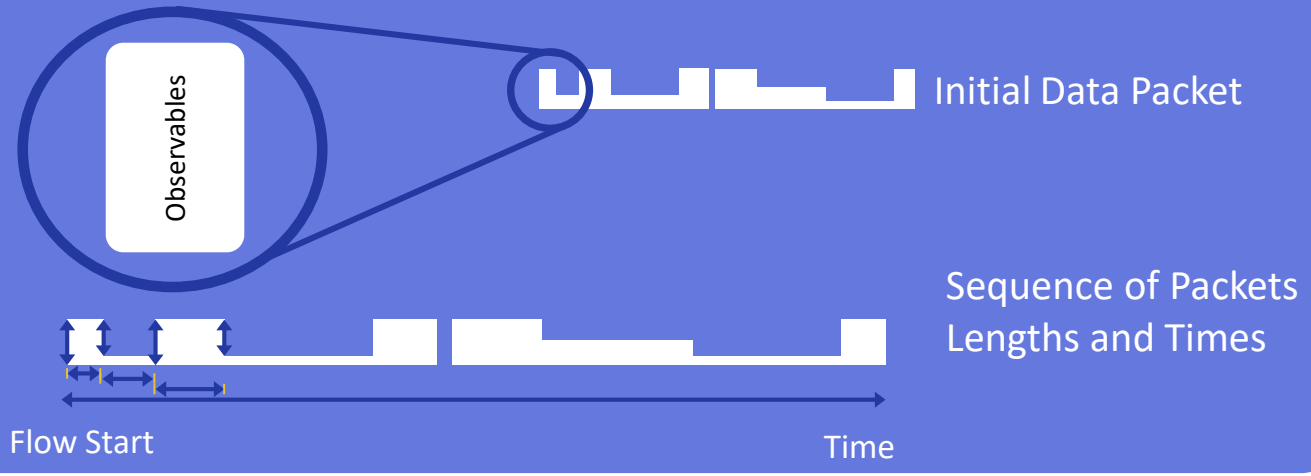
Detection of Malware without Decryption

Cryptographic Compliance

Synthesis/Analytics

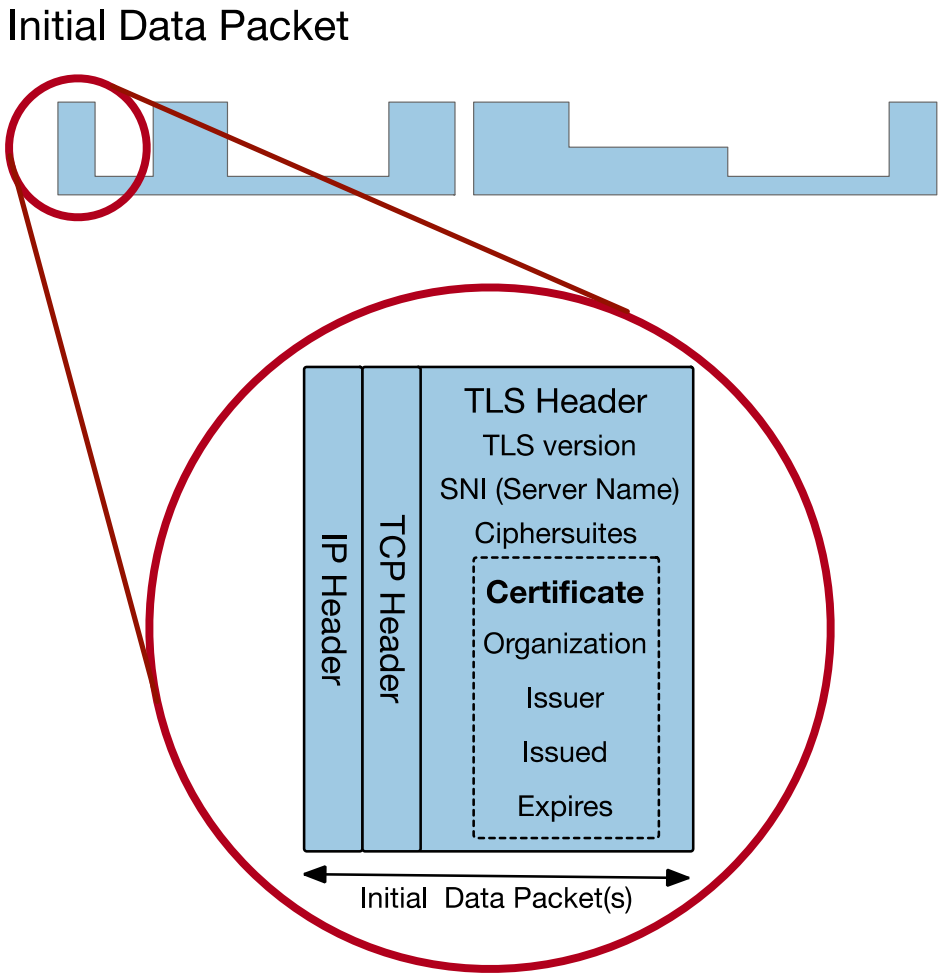
Analytics Pipeline of Diverse Methods

Telemetry

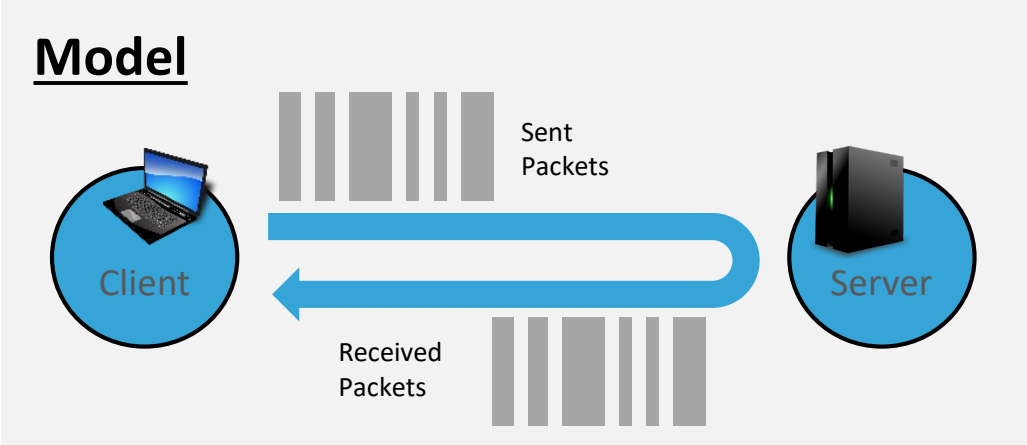


Initial Data Packet

- HTTPS header contains several information-rich fields
- Server name provides domain information
- Crypto information educates us on client and server behavior and application identity
- Certificate information is similar to whois information for a domain
- And much more can be understood when we combine the information with global data

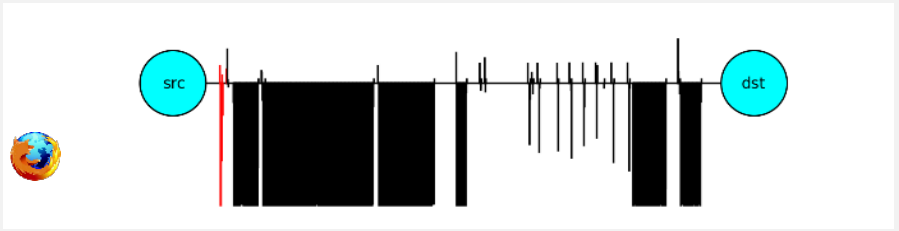


SPLT Shows TLS Metadata Differences



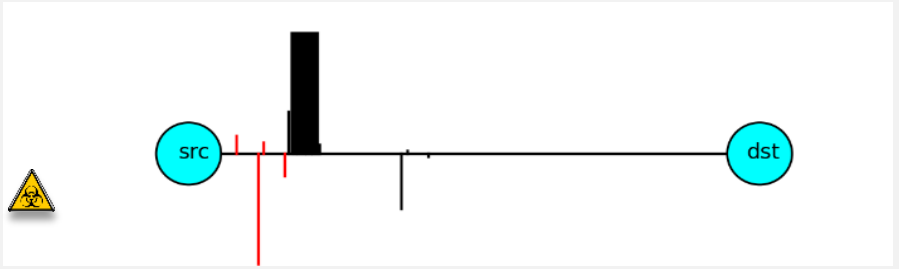
Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic.

Google Search Page Download



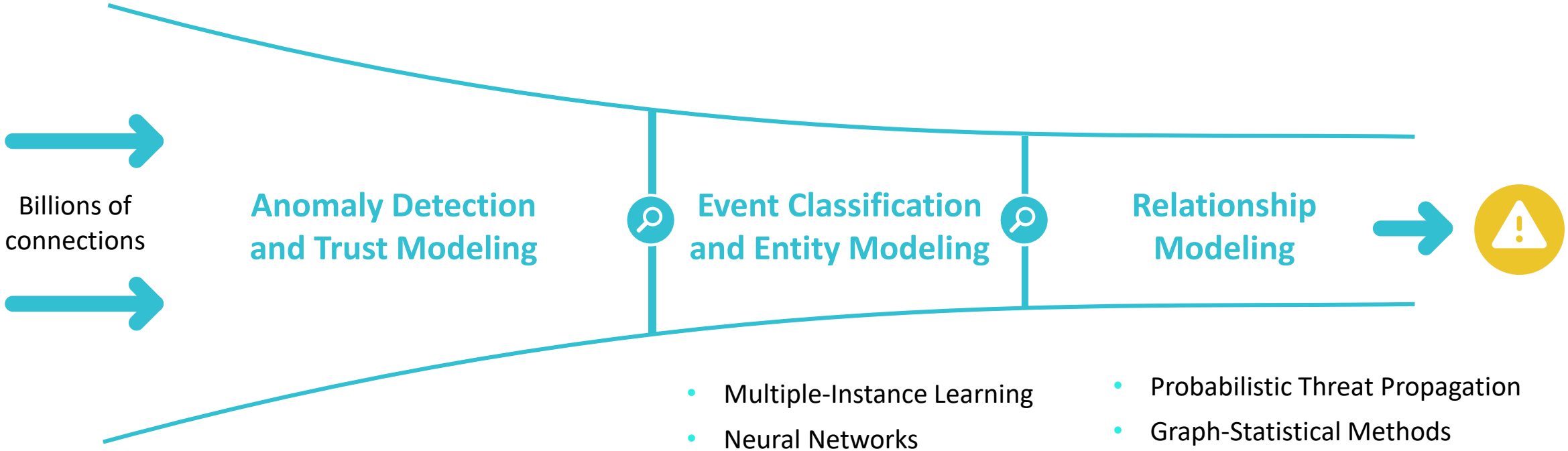
Initiate Command & Control

Exfiltration & Keylogging



Multi-layer Analytical Pipeline

Cascade of specialized layers of Machine Learning algorithms

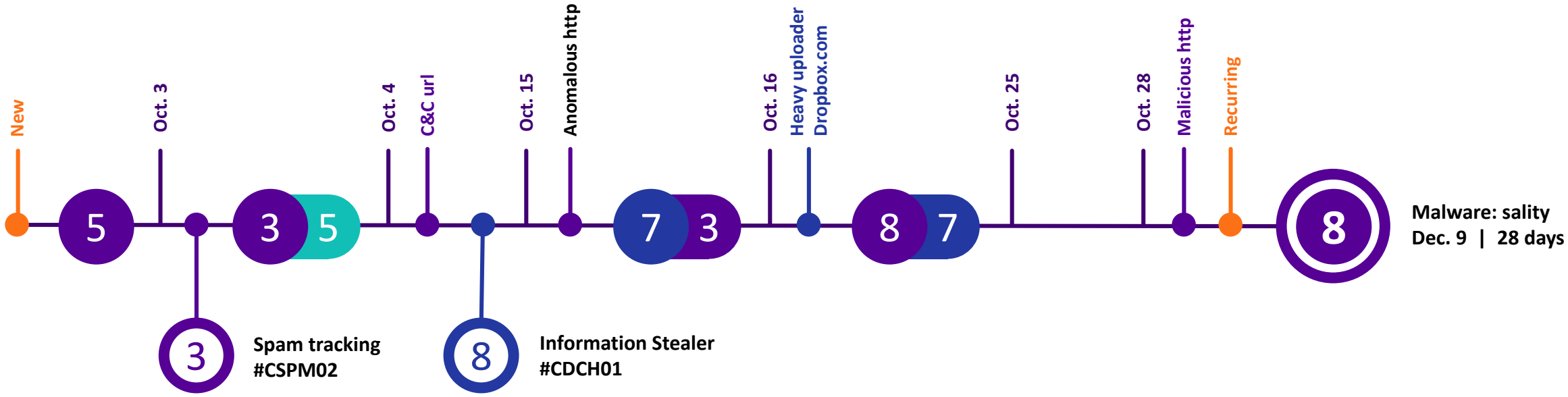


- Statistical Methods
- Information-Theoretical Methods
- 70+ Unsupervised Anomaly Detectors
- Dynamic Adaptive Ensemble Creation

- Multiple-Instance Learning
- Neural Networks
- Rule Mining
- Random Forests
- Boosting
- ML: Supervised Learning

- Probabilistic Threat Propagation
- Graph-Statistical Methods
- Random Graphs
- Graph Methods
- Supervised Classifier Training

Security That Shows Its Work



Measure the Right Things

Efficacy of the Assertions

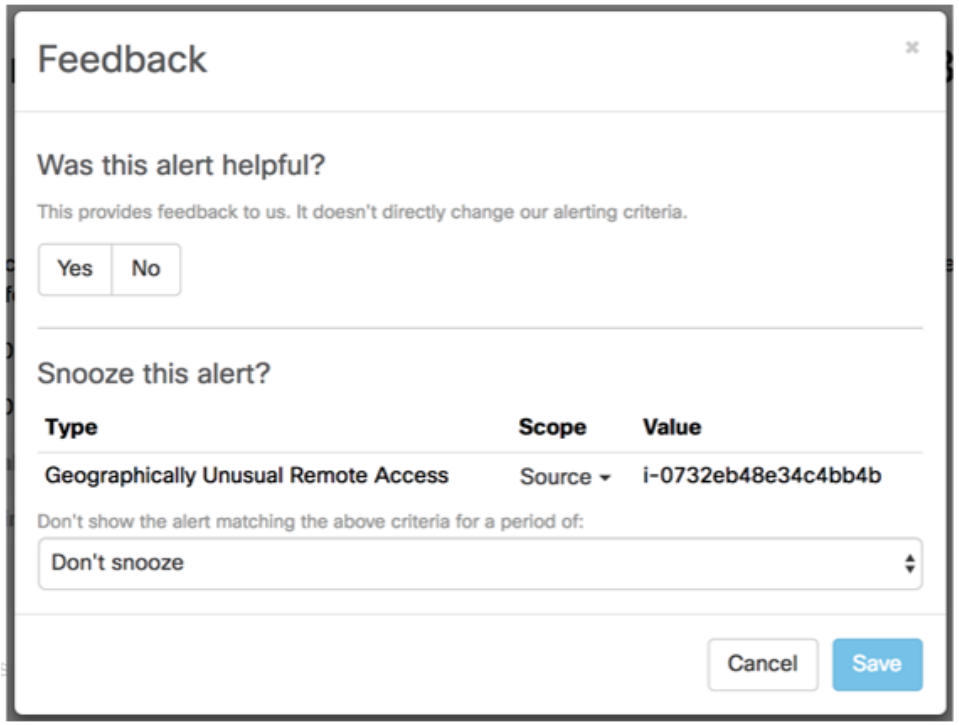
True/False Positive

True/False Negative

Overfitting/Underfitting

Root Mean Squared Error

How Helpful Was This Alert?

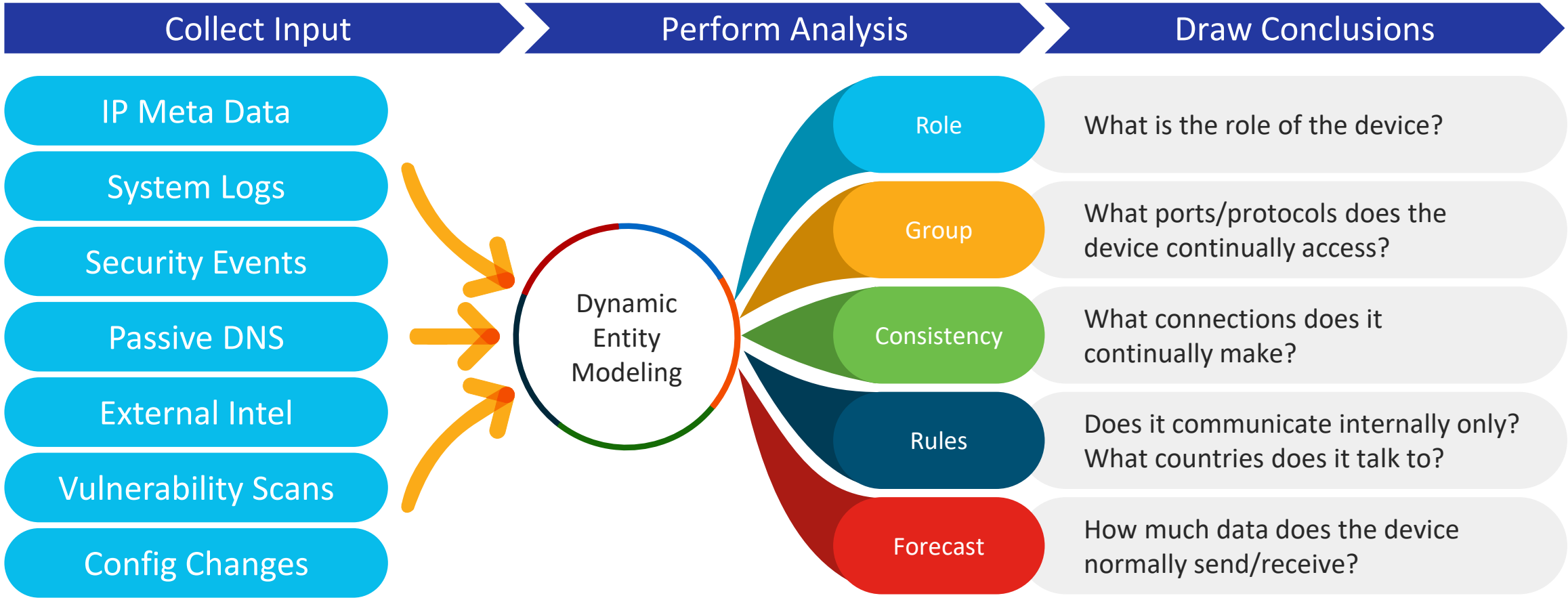


In the end, it is not the math that matters, it is you **the customer that matters!**

2018	Stealthwatch Cloud Alerts Marked Helpful by Customers (%)
Jan	95.91%
Feb	94.52%
Mar	94.75%
Q1 (Jan-Mar)	**94.45%**
Apr	97.23%
May	94.97%
Jun	91.70
Q2 (Apr-Jun)	**94.63%**

Late-binding Modeling to Detect Security Events

Dynamic Entity Modeling



Serverless Security

How Can You Secure a Server When There is No Server?

Serverless Computing is a cloud computing execution model in which the cloud provider dynamically manages the allocation of machine resources (ie the servers)

Serverless Anomaly Detection

Amazon Lambda function that normally connects to two internal resources connecting to an unexpected third

Historical Outlier Observation

One of the source's metrics deviated significantly from its historical baseline.

Time	Source	Time Window	Type	Metric	Expected Value	Outlier	Probability	Sample Size	
3/13/17 12:00 AM	lambda:RDSQueryLogger	1d	device	Bytes Out	12,097,460.313	142,117,719	0.37%	42	✖
3/13/17 12:00 AM	lambda:RDSQueryLogger	1d	device	Internal Bytes Out	12,097,460.313	142,117,719	0.37%	42	✖

Static Connection Set Deviation Observation

Device normally talks to a static set of (internal/external) devices, but has recently started/stopped talking to new/normal devices.

			Normal Connections		New Connections		Lost Connections			
Time	Source	Type	Set	Count	Set	Count	Set	Count	History Length (Days)	
3/13/17 12:00 AM	lambda:RDSQueryLogger	internal	10.0.10.193 , 10.0.12.134	2	10.0.255.29	1	-	0	35	✖

Serverless Detection of an Unusual API Call

AWS CloudTrail Event Observation

AWS CloudTrail event reported for the device.

Time	Source	Account ID	User	Source IP	Event
3/28/17 8:23 AM	Network	757972810156	awslambda_963_20170328112232282	54.91.191.63	DeleteNetworkInterface
3/26/17 12:44 PM	Network	757972810156	awslambda_346_20170326162935979	54.91.191.63	DeleteNetworkInterface

Serverless Behavioral Analytics

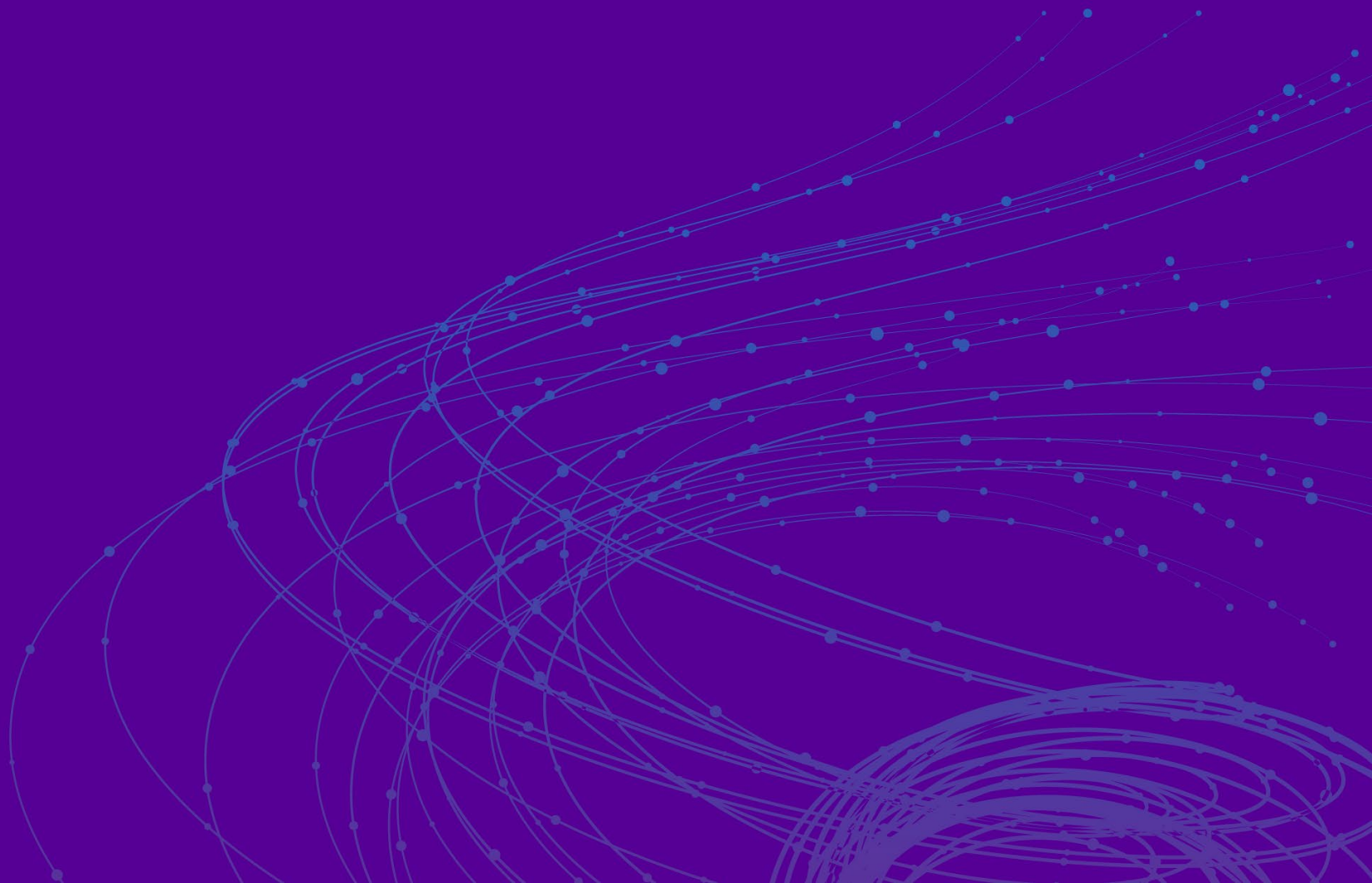
AWS Lambda Metric Outlier Observation

An AWS Lambda function had unusual activity on one of its metrics.

Time	Source	Account ID	Function name	Metric	Old value	New value
3/30/17 9:00 PM	192.168.43.147	23456789012	lambda:rds-poller	Invocations	21	182

RSAConference2019

Conclusion



What to Ask Your Vendor

How are you applying Machine Learning in your product and why?

How do you measure its effectiveness?

Regarding supervised learning, what are you using for 'ground truth'?

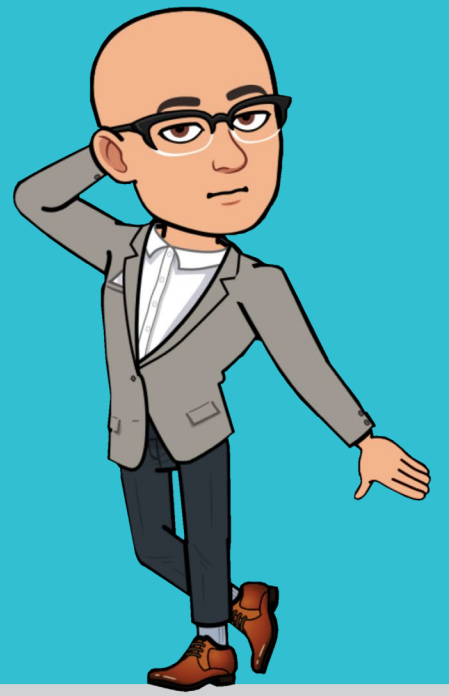
What non-machine learning are you using and why?

What papers or open-source have you published regarding your analytics?

For the ML based assertions, what entailments are provided?

A Good Machine Learning Approach

- Be Pragmatic
- Entailments
- Analytical pipeline, over single technique
- Measure helpfulness, not mathematical accuracy
- Be Transparent with your science, publish papers and open source



NERD ALERT

Thank you!

References

Learn More….

Cisco Stealthwatch Enterprise
Cisco Stealthwatch Cloud
Encrypted Traffic Analytics

Basic References

- Blog: Detecting Encrypted Malware Traffic (Without Decryption)
- Blog: Learning Detectors of Malicious Network Traffic
- Blog: Transparency in Advanced Threat Research
- Blog: Turn Your Proxy into Security Device
- Blog: Securing Encrypted Traffic on a Global Scale
- Blog: Closing One Learning Loop: Using Decision Forests to Detect Advanced Threats

Make Your Head Hurt Reading Material

- Identifying Encrypted Malware Traffic with Contextual Flow Data, Blake Anderson and David McGrew, AISEC ‘16
- Grill, M., Pevny, T., & Rehak, M. (2017). Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. Journal of Computer and System Sciences, 83(1), 43-57.
- Komarek, T., & Somol, P. (2017). End-node Fingerprinting for Malware Detection on HTTPS Data. In Proceedings of the 12th International Conference on Availability, Reliability and Security (p. 77). ACM.
- Jusko, J., Rehak, M., Stiborek, J., Kohout, J., & Pevny, T. (2016). Using Behavioral Similarity for Botnet Command-and-Control Discovery. IEEE Intelligent Systems, 31(5), 16-22.
- Bartos, K., & Rehak, M. (2015). IFS: Intelligent flow sampling for network security–an adaptive approach. International Journal of Network Management, 25(5), 263-282.
- Letal, V., Pevny, T., Smidl, V. & Somol, P. (2015). Finding New Malicious Domains Using Variational Bayes on Large-Scale Computer Network Data. In NIPS 2015 Workshop: Advances in Approximate Bayesian Inference (pp. 1-10).
- Rehak, M., Pechoucek, M., Grill, M., Stiborek, J., Bartoš, K., & Celeda, P. (2009). Adaptive multiagent system for network traffic monitoring. IEEE Intelligent Systems, 24(3).