Machine Learning in Cybersecurity

An Introduction

Hari Shankar
Cyber Security Architect
@harryskrishna

Disclaimer

- I am a Cybersecurity architect first, and then an ML enthusiast, who is currently exploring the use of ML in detecting cyber attacks.
- This talk will focus more on the application of ML in Cybersecurity
- Follow-up talk will delve deeper into the algorithms and their tuning
- If you see any jargons you don't understand, pls stop me and ask

We will cover…

- Cybersecurity - a primer
- Need for ML in cybersecurity
- Current state with examples

Cost of cyber crime is rising

- Cybercrime costs average enterprise **$17m per year***
- Cost **grew at 15% CAGR** over last three years
- Any given cybercrime can cost significantly more
- **Target's** 2014 hack cost company approximately **$162m. Yahoo's** 2016 hack might cost upwards of **$100m**
- Costs not just financial, also reputational

Source: 2016 Cost of Cyber Crime Study & the Risk of Business Innovation, Ponemon Institute

Hackers growing more sophisticated

- Amateur hackers giving way to **professionals**
- Developing **new, more sophisticated, methods**
- Professional hackers make their **services available for a fee**
- **Costs to commit** cybercrime dropping
- Average subscription fee for a one hour/ month **DDoS package is roughly $38***

Source: Q2 2015 Global DDoS Threat Landscape, Incapsula

Perimeter Defense Inadequate

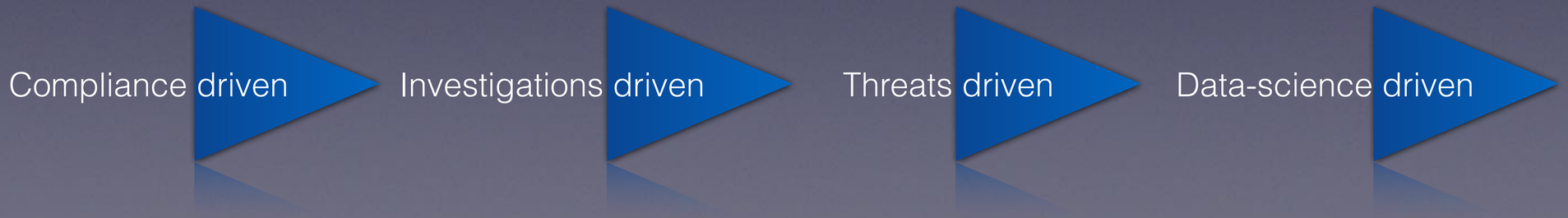
- Defending the perimeter **no longer enough**
- No **100%, fool-proof way to keep bad actors out**
- Some **threats come from within**
- The idea of a **perimeter becoming obsolete** with mobile, cloud, IoT
- Need better methods for **threat detection inside the network**

Need for ML In Cybersecurity

Data Science for Cybersecurity

Security must move beyond signature-based matching

- Necessary defense direction: Find the Unknown
- Need an advanced platform: Security is a Big Data problem
- Multiple decentralized sources of traditional or unconventional data
- Need a platform for better BI, reporting, and cross-source correlation
- Develop intelligence: Security is an Advanced Analytics problem

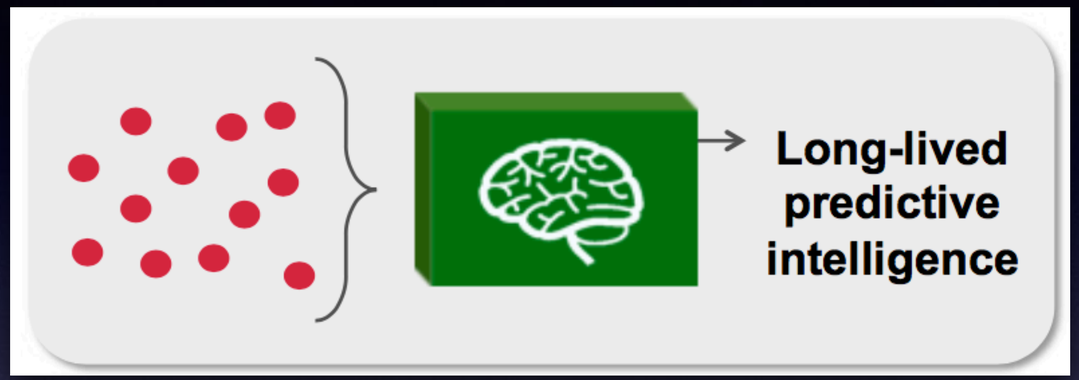


Data Science for cybersecurity

Signatures

- How the threat looks
- Find threats that you've seen before
- Snapshot in time
- No local context

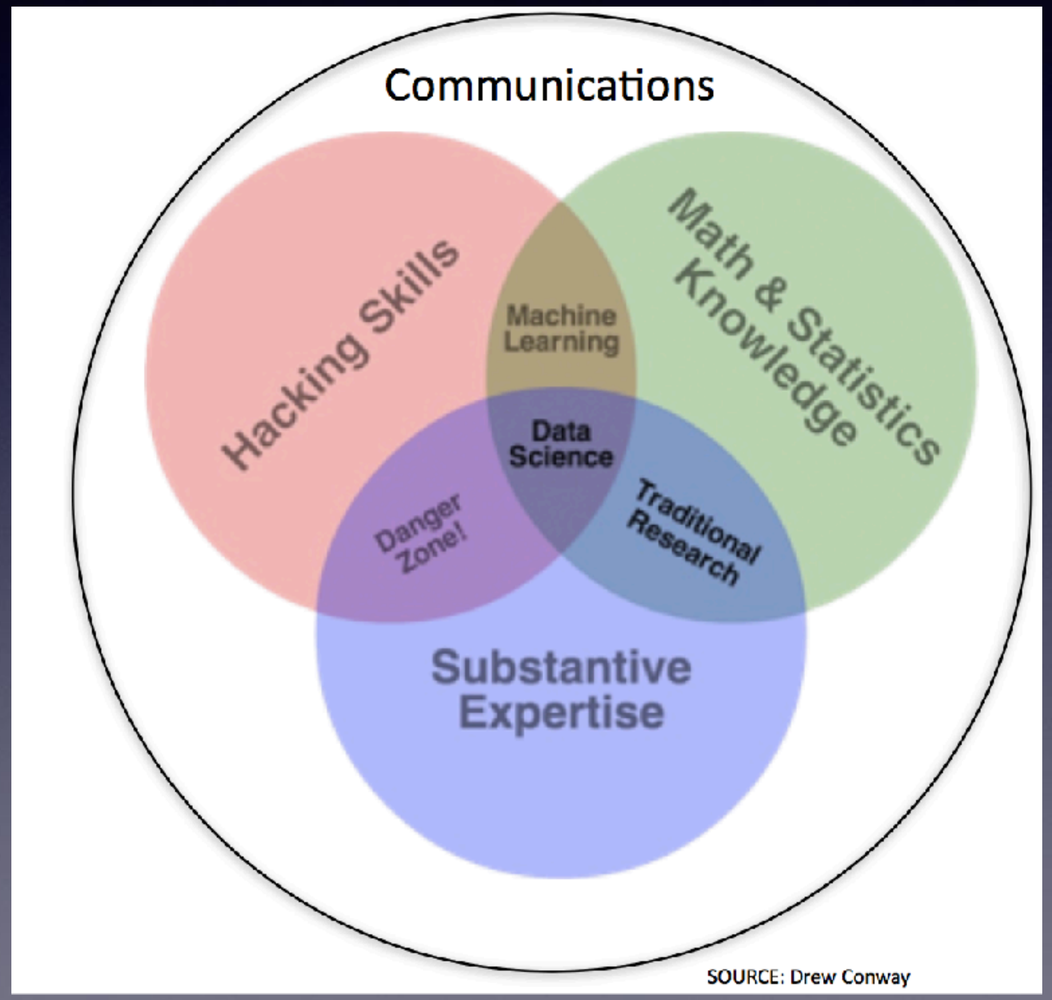
Data Science



- What the threat does
- Find what all threats have in common
- Learning over time
- Local learning and context

(Security) Data Scientist

"Data Scientist (n.): Person who is better at statistics than any software engineer and better at software engineering than any statistician"
- Josh Willis, Cloudera



Basic Process

- Determine the security use case
- Acquire & "clean" data
- Analyse data
- Examine outcomes
- Visualize & communicate results
- Lather, rinse and repeat

ML In Cybersecurity

Some Examples…

Supervised ML in cybersecurity

Supervised ML naturally suited to classification (yes/no) problems; transactions can be viewed under a good / bad lens:

- **Spam:** Is a given email message spam?
- **Online fraud:** Is a given financial transaction fraudulent?
- **Malware:** Is a given file malware?
- **Malicious URLs / domains / IPs:** Is a network connection to a given URL (resp. domain, IP address) associated with malicious activity?

Note these applications are not new; they have been studied in academia and/or have been implemented in commercial use for many years.

Unsupervised ML in cybersecurity

Unsupervised ML can be used to cluster data – which can help identify outliers; e.g., by baselining normal behavior and find instances outside the norm:

- Is there an abnormal amount of network traffic from a particular host?
- Is there a significant increase in failed log-in attempts?
- Is a user accessing resources he or she does not normally access (or that would not be normally accessed by his or her peer group)?
- Are there access patterns that are too “regular” to be associated with a human?
- Is a user working during hours outside his or her normal behavior?
- Is a user connecting from or to unusual geographic locations (or a set of geographic locations that does not make sense)?

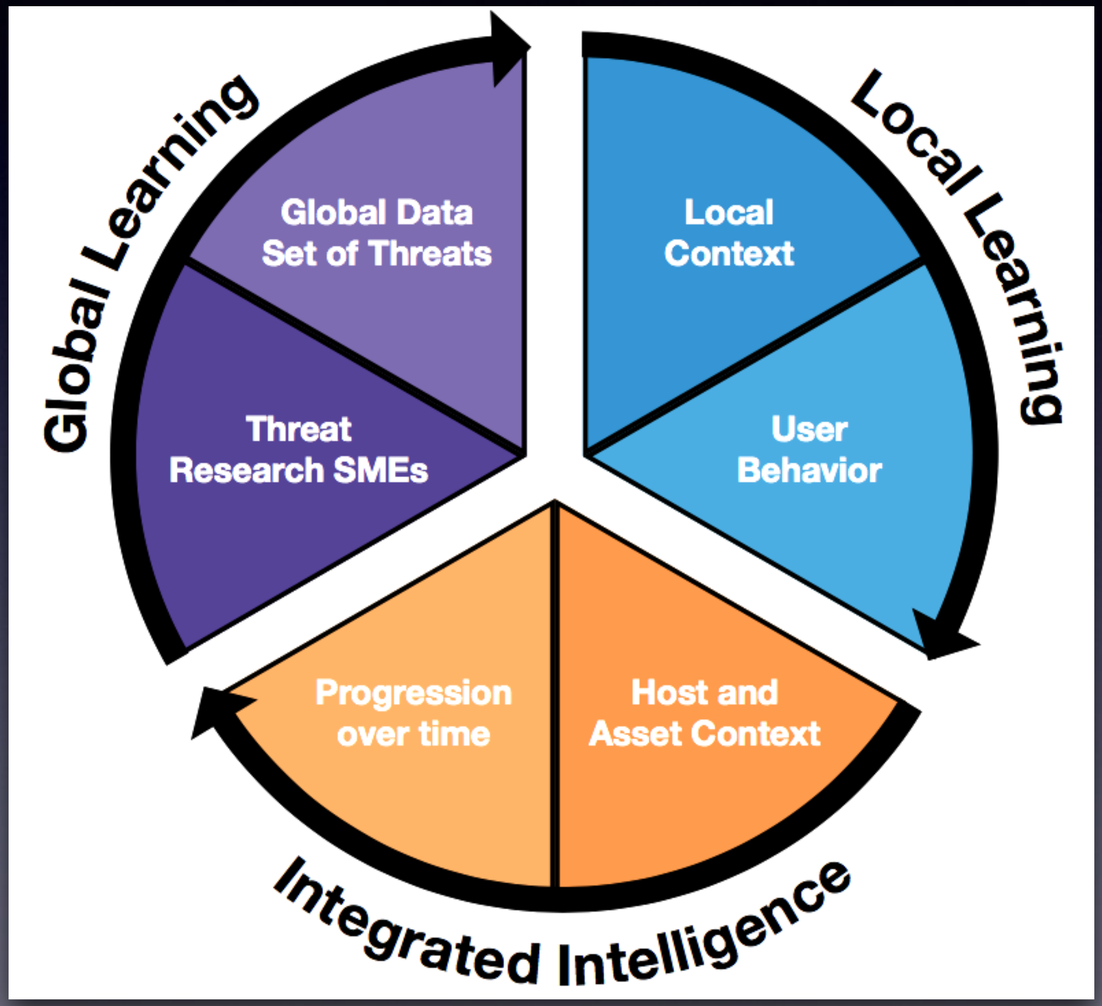
ML in action - Incident Detection

ML in action - Incident Detection

Global Learning
Identifying the fundamental traits that threats share in common
Techniques:
• Supervised machine learning, heuristics
Example:
• Random forest

Local Learning
Identify what is normal and abnormal in the local network
Techniques:
• Unsupervised machine learning, anomaly detection
Example:
• K-means clustering

Integrated Intelligence
Connect events to reveal the larger attack narrative
Techniques:
• Event correlation and host scoring
Example:
• Bayesian networks

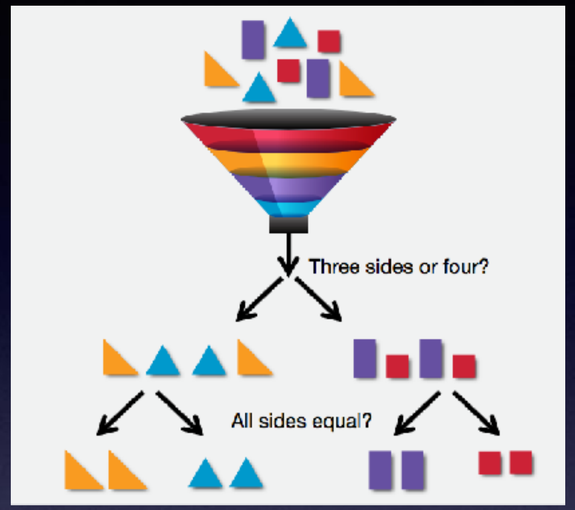


Detecting C&C using Random Forest

1. Detection model not based on a specific sample; instead RF is used to put an unknown sample through a battery of tests before classifying

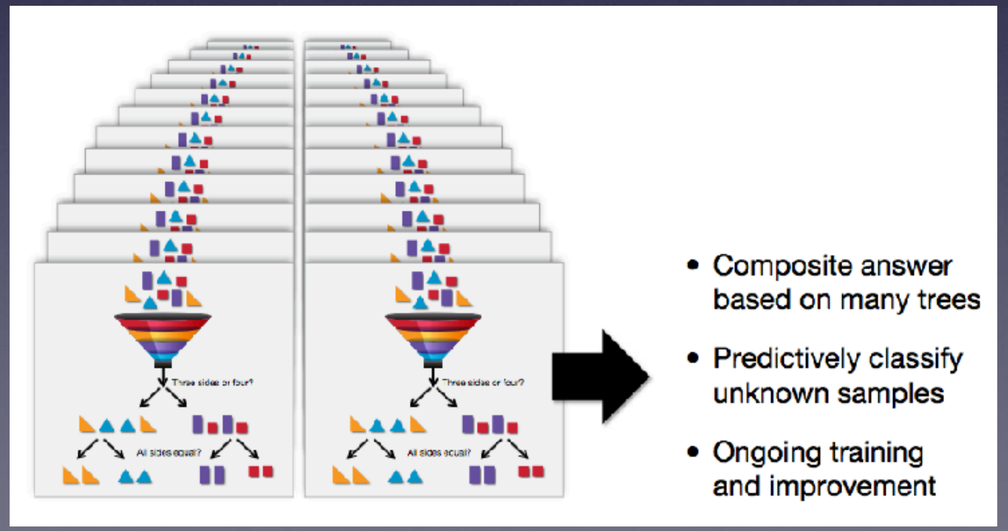
2. Then, Security Data Scientists augment it by correcting the classification

3. As behaviour changes, training set changes & model adapts



Detecting C&C

- RF used to analyse traits in HTTP headers, to identify unique patters of C&C behaviour
- Data Scientists analyse wide range of C&C traffic, and focus on traits that are largely common across malware
- Reduced dependancy on new variants, and signatures
- Works in real-time - identify botnets, banking malware, mobile malware
- Global learning



Real-time detection of C&C

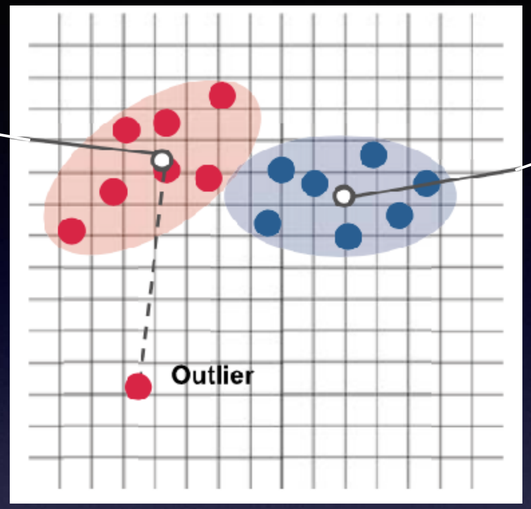
Detection Summary

- Internal Host: mfinn-mbp
- External C&C Servers: 108.161.189.6, 54.230.46.243, 176.34.177.58, 94.31.29.128, 54.217.214.141, 54.230.47.78
- Observed Behaviors:
  - Bad User-Agent: 8
  - Higher Risk Geo: United Kingdom, Ireland
- Data Sent: 6.7 KB
- Data Received: 15.1 KB

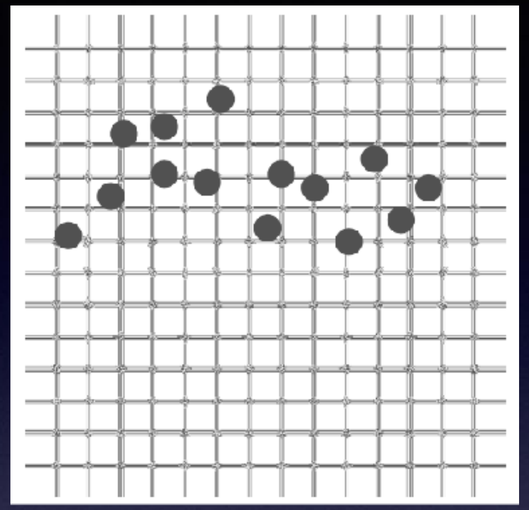
Recent Activity

Tags	C&C Server	Observed Behavior	Bytes Sent
+	54.230.47.78 mirror10.installsmart.com	Suspicious HTTP Header Construction	135 bytes
+	54.230.47.78 mirror10.installsmart.com	Bad User-Agent Suspicious User Agent: Browser name in comment field	135 bytes

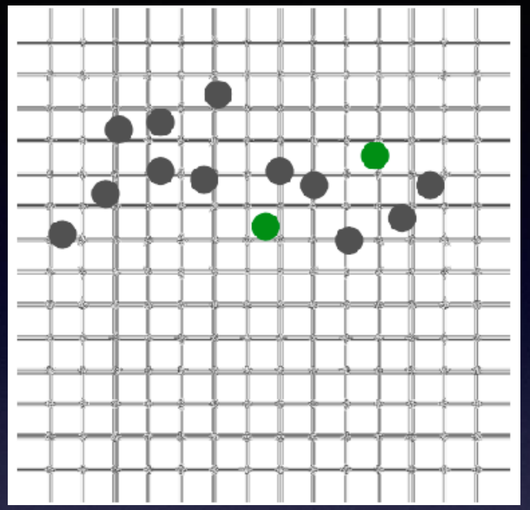
Unsupervised ML - K-means clustering for anomaly detection



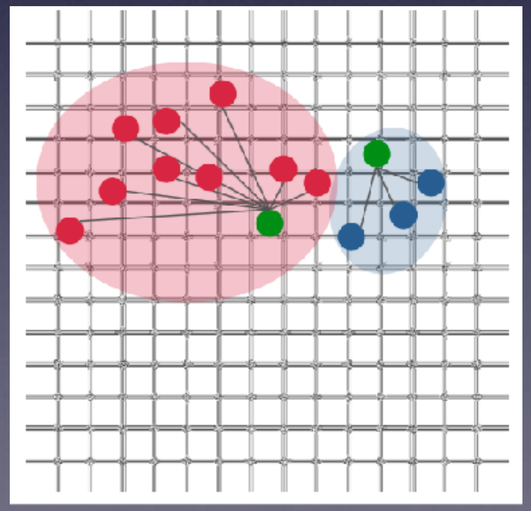
Two groups or clusters, with 1 centroid each



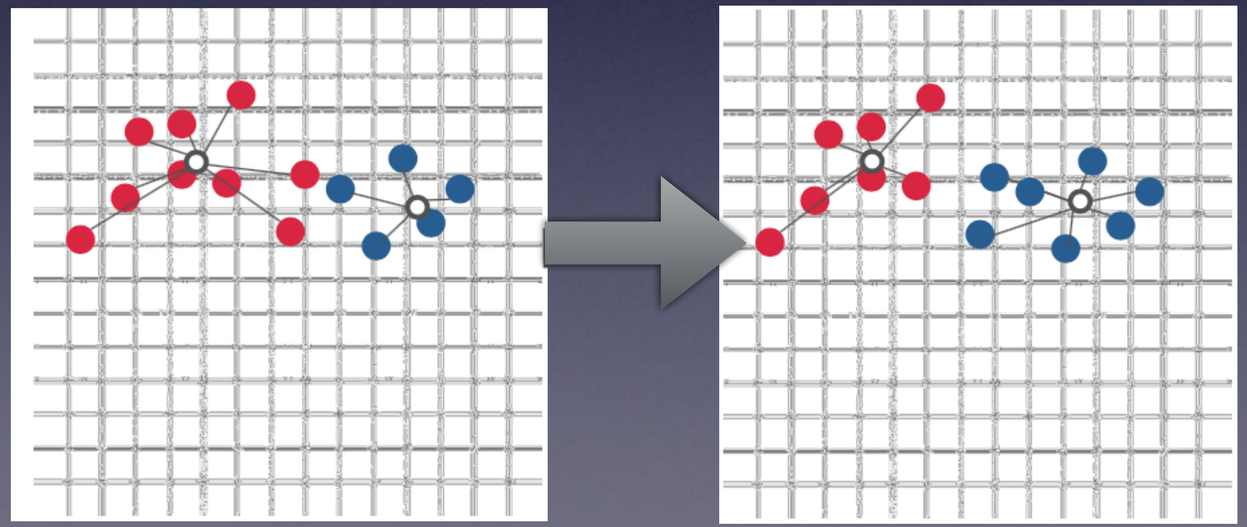
Remove distinctions



New centroids randomly selected



Data points re-classifed

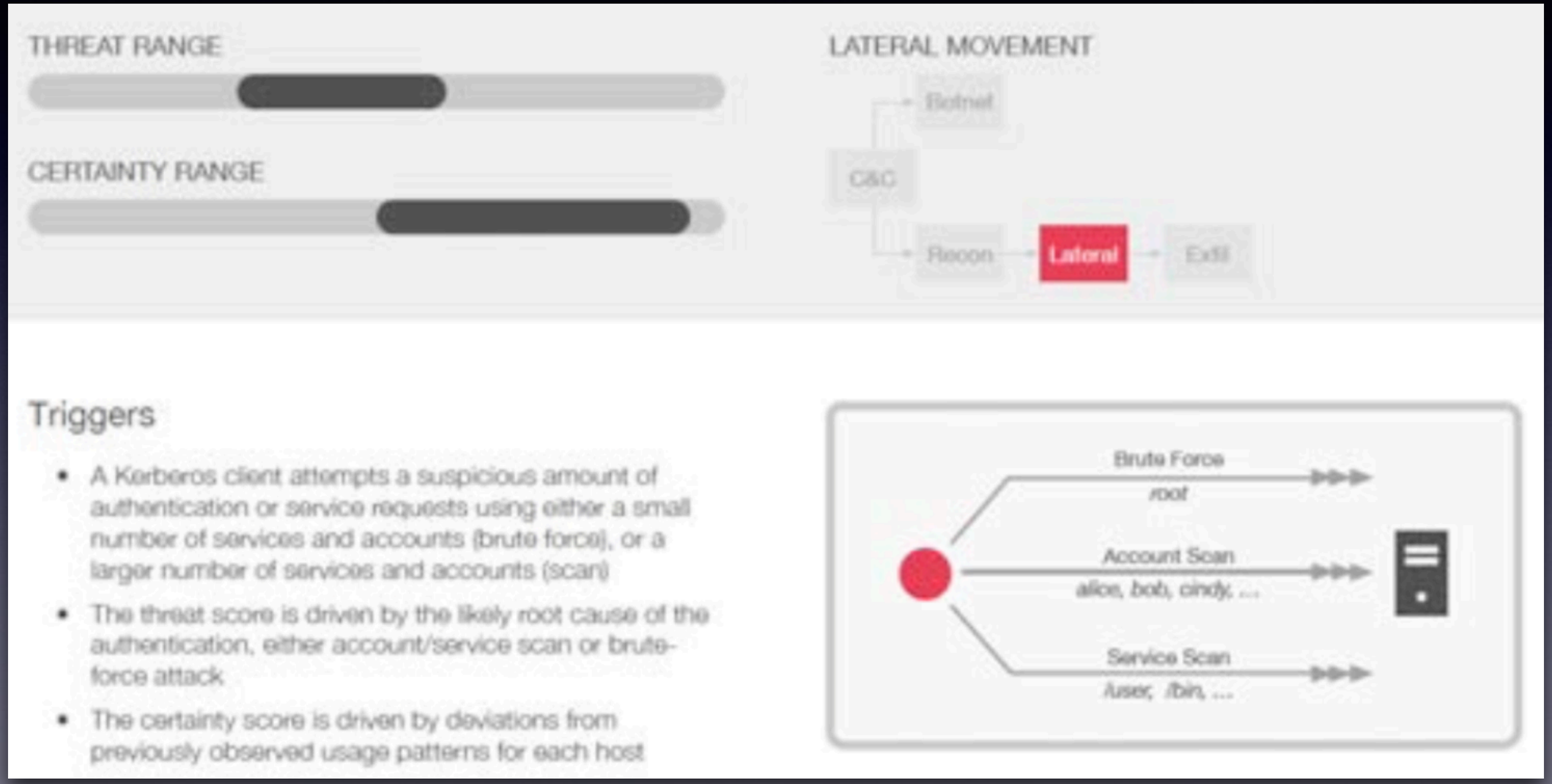


After few iterations, the model stabilises

K-means clustering to detect unauthorised Kerberos client

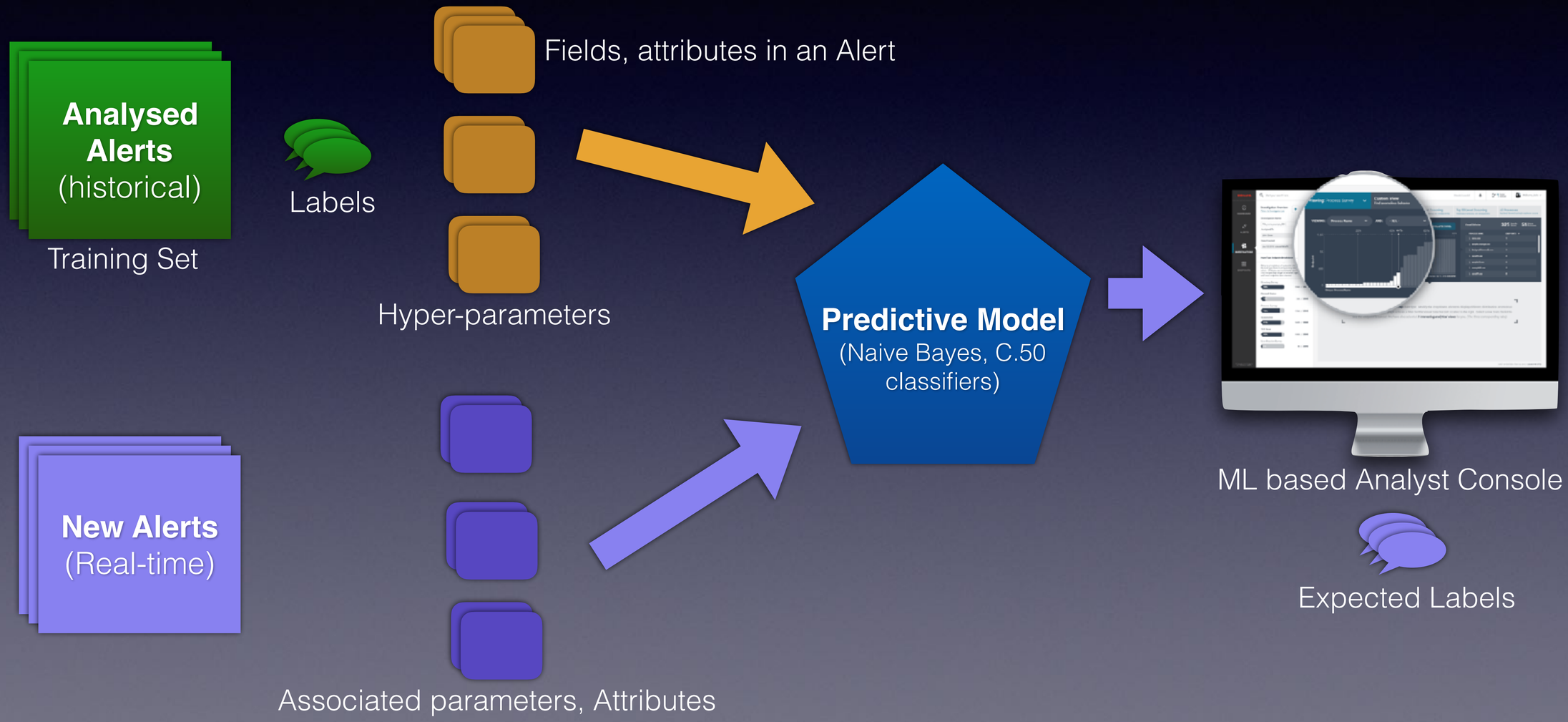
- Kerberos tokens used to establish “trust” between network nodes
- Attackers use “pass the hash” to steal tokens from trusted hosts, to create fake ones
- A baseline of Kerberos traffic from every host in a network - user accounts, services run, etc..
- When a user account is compromised, it can be seen used on new hosts. Or a user account accessing new network services
- Indication of an attacker trying to enumerate a user account or services, or gain access to privileged/secure network zones

Real-time detection of Kerberos token compromise



ML in action - Incident Triage

ML for better Incident Triage



ML in action - Incident Response

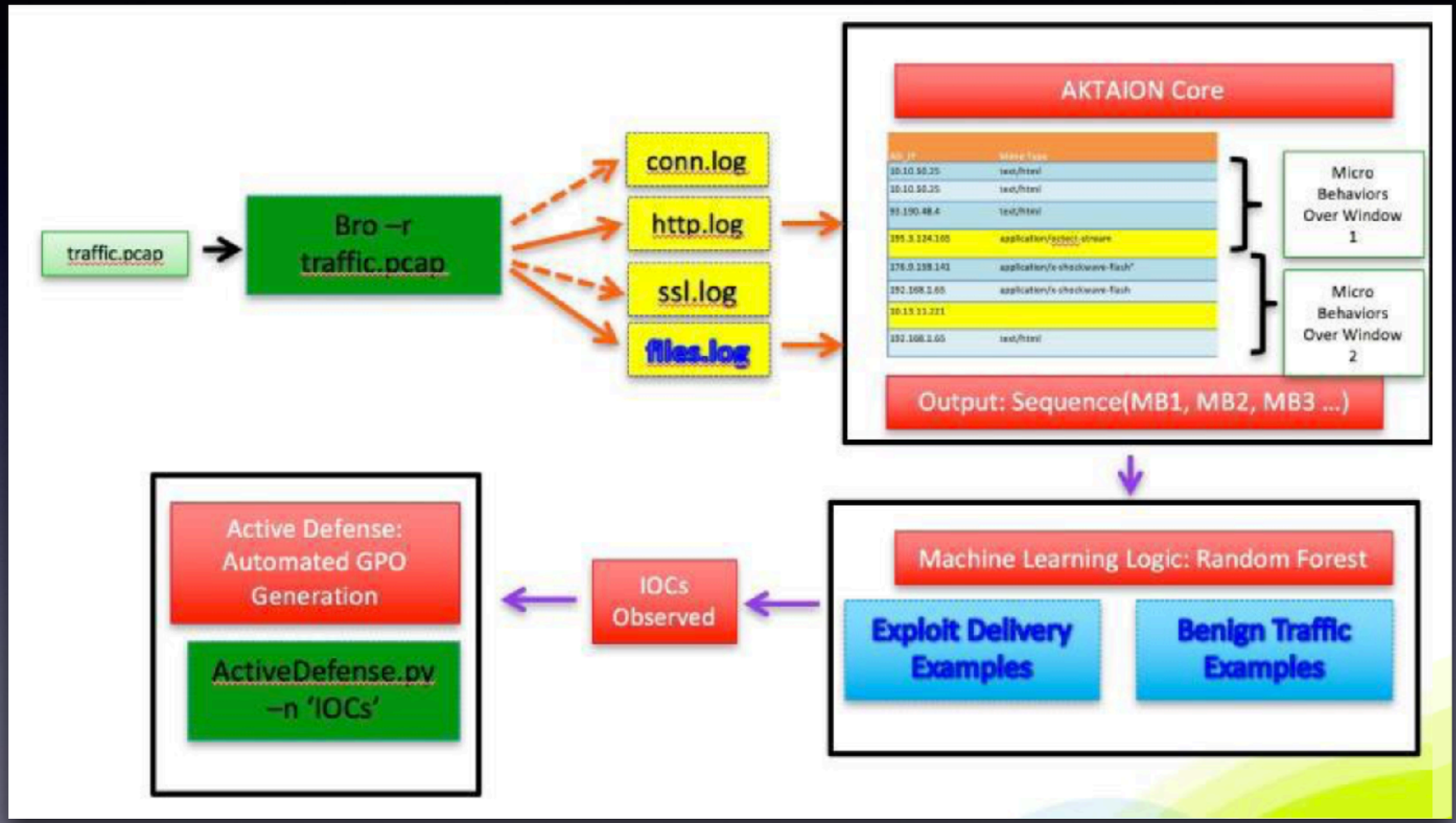
ML in action - Incident Response

- Automating the Incident response (bot driven - block, isolate, contain, remediate…)
- Holy grail of ML in Cybersecurity - early stages, research in progress, PoC

Blocking Ransomware using ML

- Ransomware network traffic analyzed using ML open source tool: (Aktaion - https://github.com/jzadeh/Aktaion)
- This tool analyzes Micro Behaviors present in Ransomware
- Output of tool is input to python script which builds main indicators for GPO generation
  (Executable name, Domain, IP Address)
- Python scripts executes SSH into an AD host that can push GPO into Windows Domain via powershell.

Blocking Ransomware using ML



Thank you…

Hari Shankar
Cyber Security Architect
@harryskrishna

LinkedIn Profile