RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SPO1-RO4

SENDING A HUMAN TO DO A MACHINE'S JOB: ADDRESSING THREATS WITH ANALYTICS

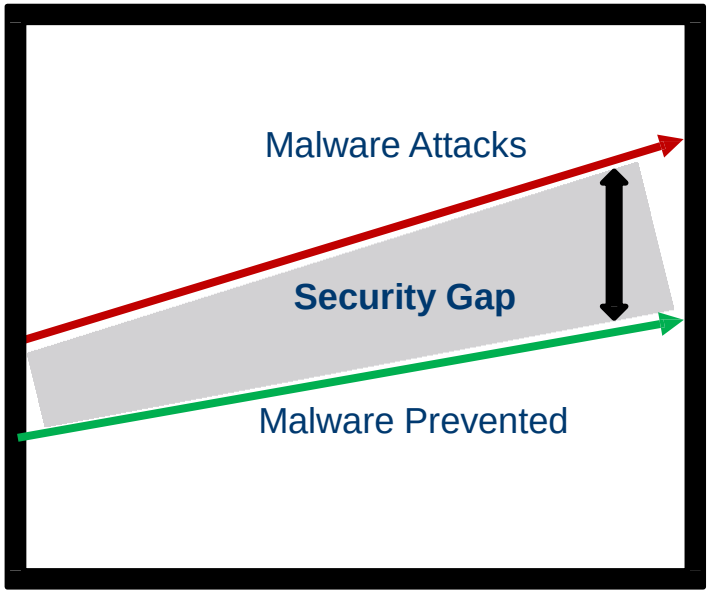
Nick Bilogorskiy

Cybersecurity Strategist
Juniper Networks
@belogor

Agenda

- Where are we now?
- Where did we go wrong?
- Behavioral analytics architecture
- Simplify incident response
- Automate incident response
- Q&A

The Security Gap is Growing



- The threat landscape is becoming increasingly complex and continues to grow
- The “always on,” 24/7 nature of cybercrime is straining security personnel

Number of Alerts Generated Each Week

12,172 Alerts

Source: Ponemon Institute and Juniper Networks, October 2017

Number of Alerts Investigated Each Week

518 Investigated

Source: Ponemon Institute and Juniper Networks, October 2017

Time Wasted Chasing False Positives Each Week

352.3 Hours

Source: Ponemon Institute and Juniper Networks, October 2017

Annual Cost of Chasing False Positives

$1,145,000

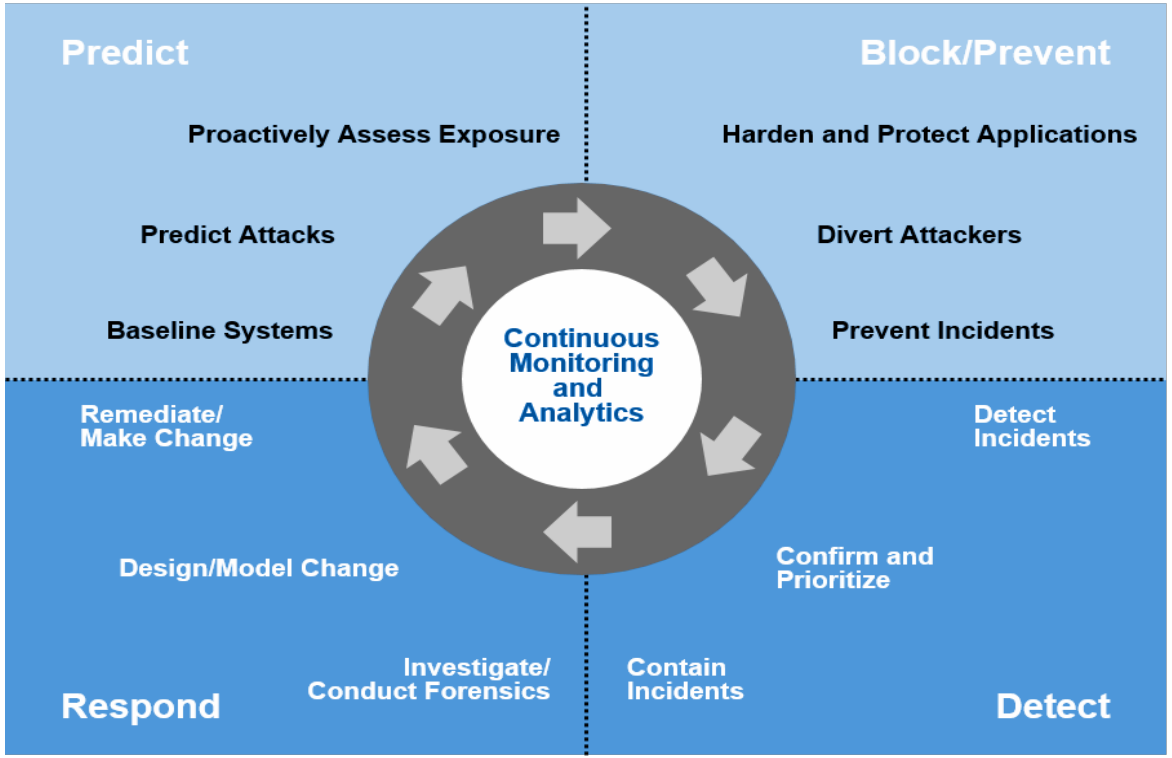
Source: Ponemon Institute and Juniper Networks, October 2017

Average Annual Company Cost of Breaches

$7,000,000

Source: Ponemon Institute, 2016

Where Did We Go Wrong?



Traditional approach:

Prevent

Where Did We Go Wrong?

Traditional approach: Prevent

- Threats bypass the Prevent layer
- Breach goes undetected – for a while
- IR teams work hard to resolve
- Business experiences are disrupted
- Lost data, lost money, lost reputation

Why Can't the Prevent Layer Stop Everything?

Performance limits the effectiveness of prevention

Fast – What can be done in milliseconds?

- Pattern / rule matching – Static analysis; have we seen this before?
- Reputation matching – IP address, domain name, URL on blacklist?

Slow – What happens if the process takes too long?

- Sites load slower (SWG)
- Applications open slower (Endpoint AV)
- All network traffic goes slower (Firewalls)

Why Can’t the Prevent Layer Stop Everything?

Advanced malware

- Constantly changes its “look”; Prevent layer can’t match pattern
- Kills processes in endpoint security software; can’t send alerts
- Complex; multi-channel C&C callback process; no unusual traffic

Lesson

Security leaders must move from trying to prevent every threat and acknowledge that perfect protection is not achievable Enterprise must assume that it is already compromised.

Gartner, 2016

Security leaders must look to simplify operations and automate remediation steps for when breaches do occur.

Where Did We Go Wrong?

Relying on a human to do a machine's job

- By 2019, there will be 6 million job openings for security professionals – but only 4.5 million available to fill those roles.
- 92 percent of ISACA's survey respondents say it will be difficult to find skilled cybersecurity candidates.
- Cybersecurity specialists will see an average pay rise of 7% in 2018

CSO

ISACA
Trust in, and value from, information systems

How Behavioral Analytics Can Help

Analytics promise to provide better visibility, improved detection and enhanced workflows. Analytics solutions are increasing detection accuracy and providing security pros with better data with which to make decisions.

FORRESTER®

How Behavioral Analytics Can Help

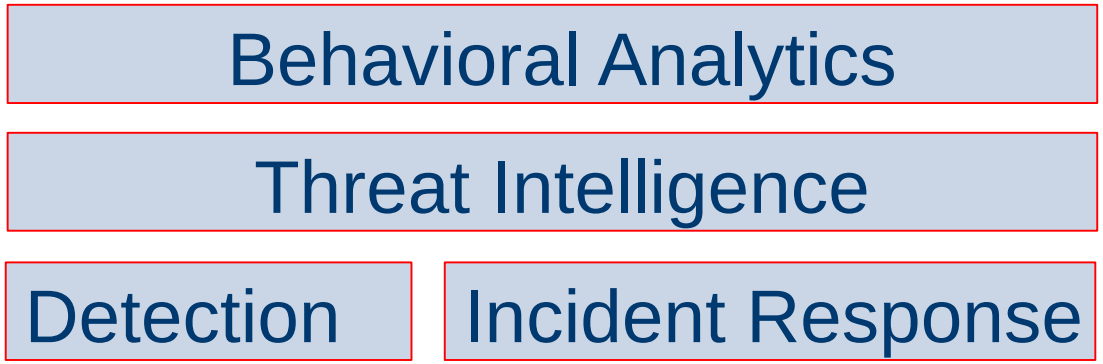
- Analytics collects, correlates and understands data from multiple sources to identify advanced threats.
- It continuously learns threat behaviors and automatically works with security tools to contain threats.

New Security Paradigm

- Addressing the new threats through context, correlation, **machine learning** and actionable intelligence.
- Security devices and applications must be sharing actionable threat intelligence across IT infrastructure, locations and organization boundaries.
- Intelligence must be actionable – prioritized correctly, filtered from false positives and ready to use

Behavioral Analytics vs. Threat Intelligence

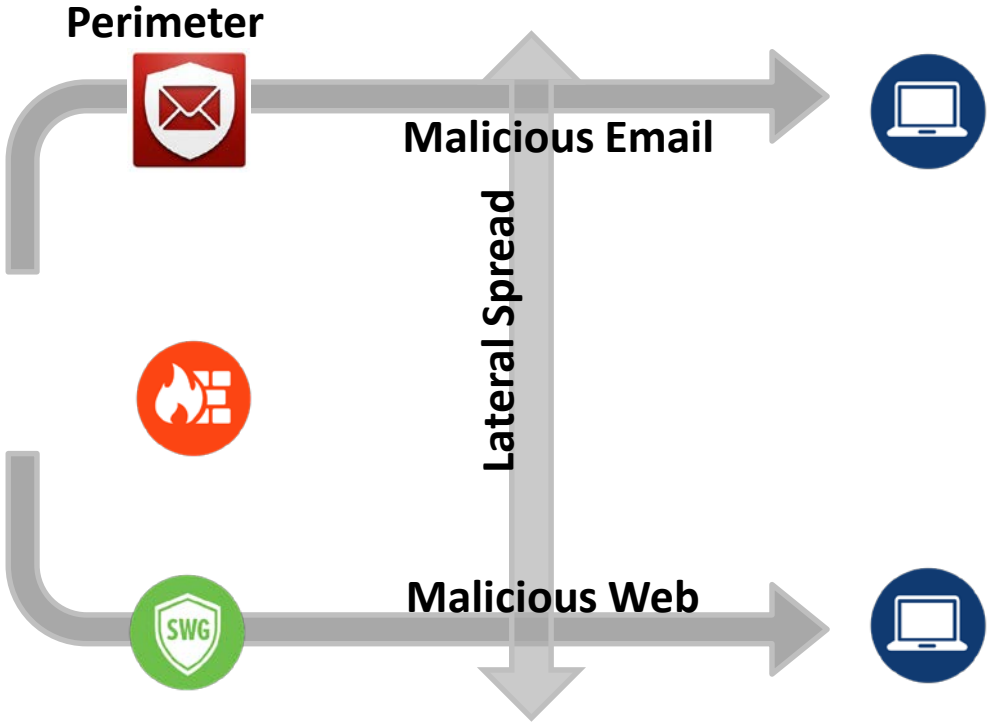
- Behavioral analytics generates new threat intelligence
- Threat intelligence is applied to power incident response and detection



Behavioral Analytics Use Cases

Team	Use case	Question
Threat Intel hunters	Moving from big data to the endpoint to find infections	“Who got infected?”
Digital Forensics Incident Response (DFIR) hunters	Moving from infected endpoint backwards to big data to find root cause	“How they got hit?”

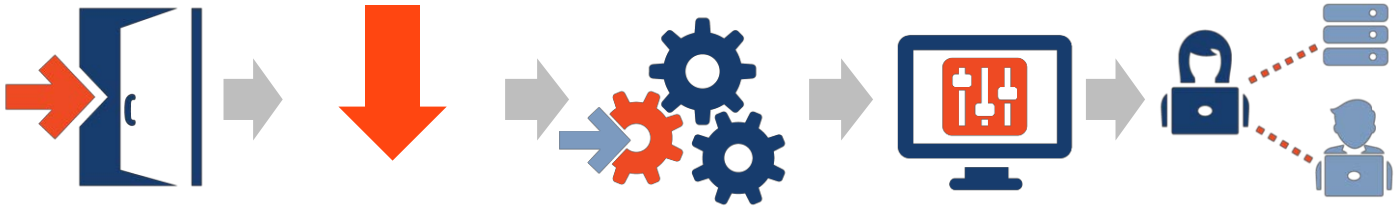
Requirement: Primary Attack Vectors



Behavioral analytics should detect and correlate events from all primary attack vectors: Web, Email and Lateral spread

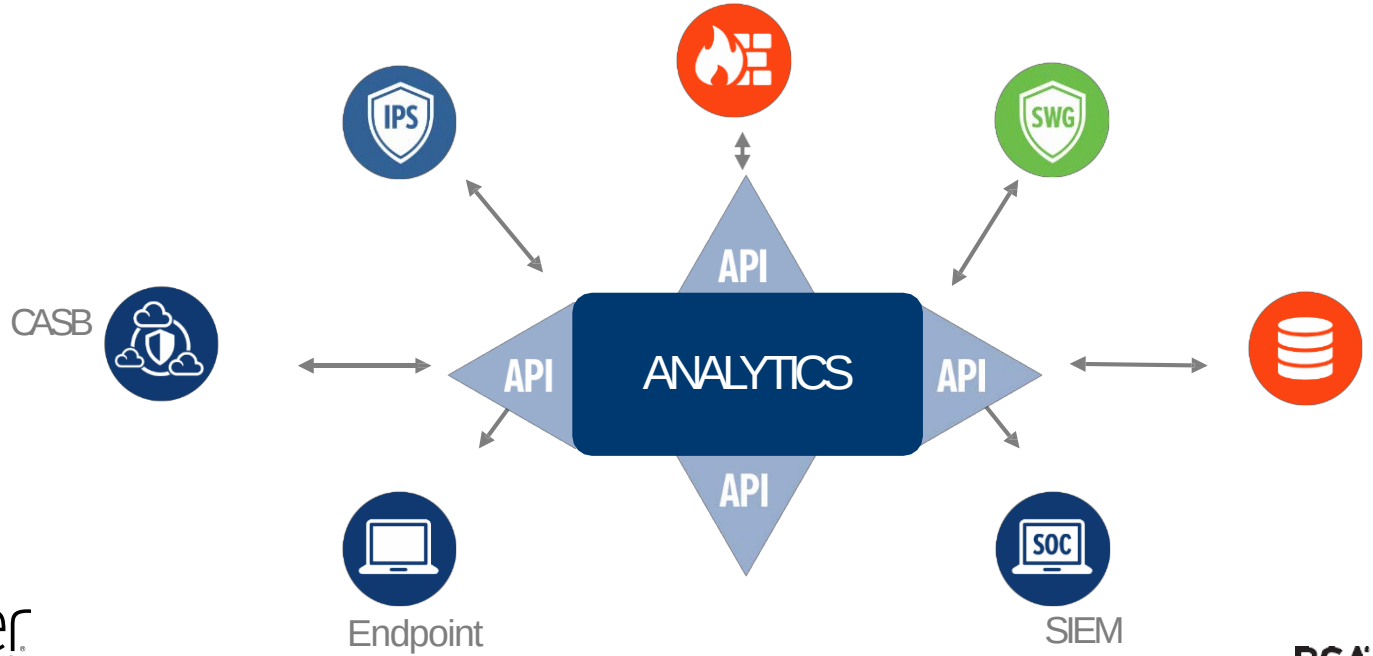
Requirement: Killchain

Behavioral analytics should detect and correlate events in all parts of the killchain

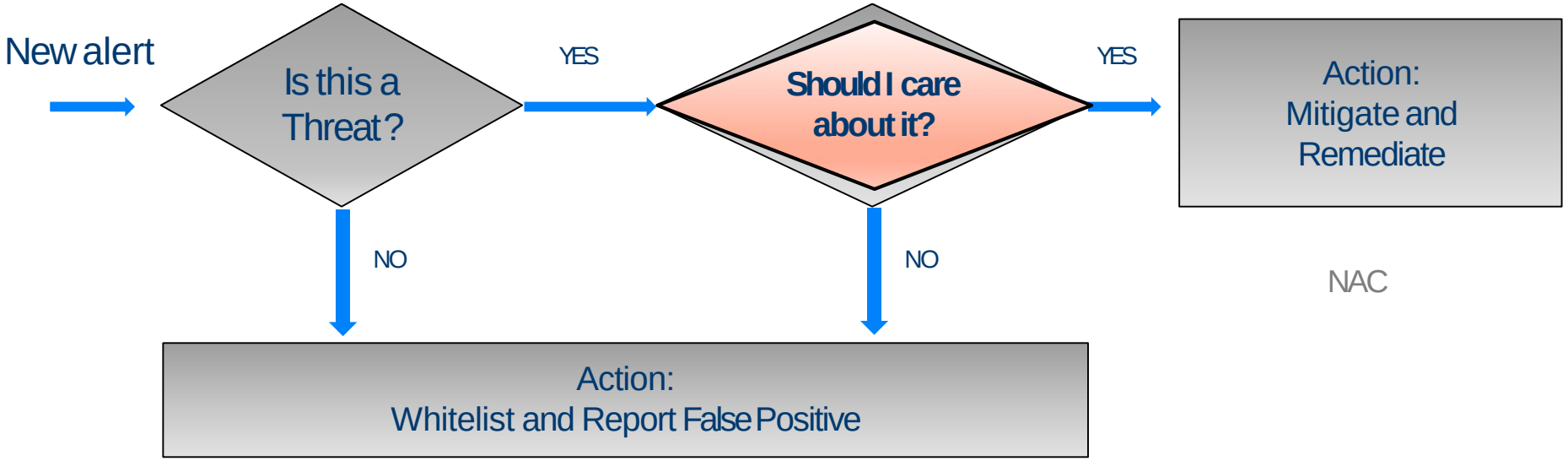


Requirement: Open APIs

Behavioral analytics solutions should rely on Open APIs to enable information exchange with other vendors



Typical Incident Response Process



You Should Care if Incident Risk is **High**

Goal: Better prioritization of effort

Intersect incident targets with asset values

- E.g. Guest network activity vs. data center network anomaly

Factor in scope and progression context

- How close to “Action on Objectives”

Has attack been disabled by other controls?

Behavioral Analytics Simplifies Response Process

- Source, target, payload, etc.
- Threat vector – web, email, document, lateral spread
- Behavior – Trojan, reconnaissance, C&C, exfiltration
- Prioritized consolidated threat profiles for IR team
- Extract end-user information from active directory
- Allows incidents to be identified by username rather than IP address or DNS machine name

Attack Evidence, Scope and Progression

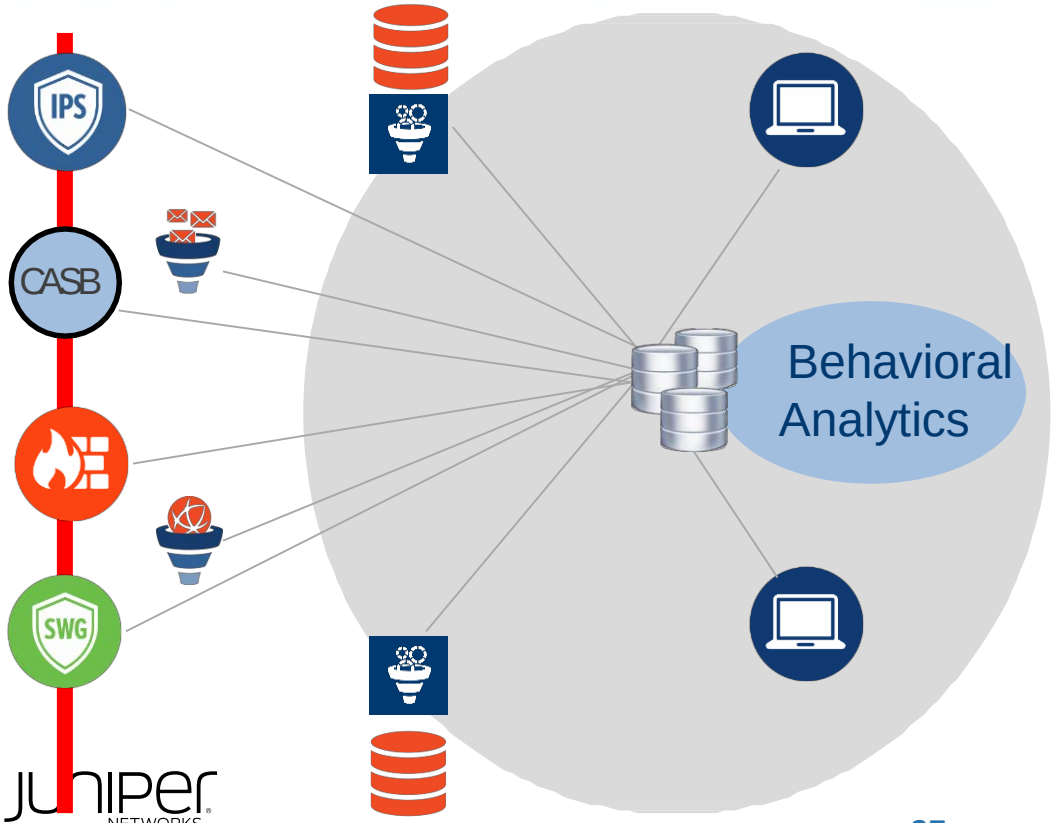
Collect malicious objects: files, PCAPS, network telemetry

- Needed to verify incident
- Needed to determine effective and appropriate mitigation

Attack Scope

- Which devices/users are affected?
- How long has attack been active?
  - Requires time series data normalized by resource extending back weeks, months, (years?)

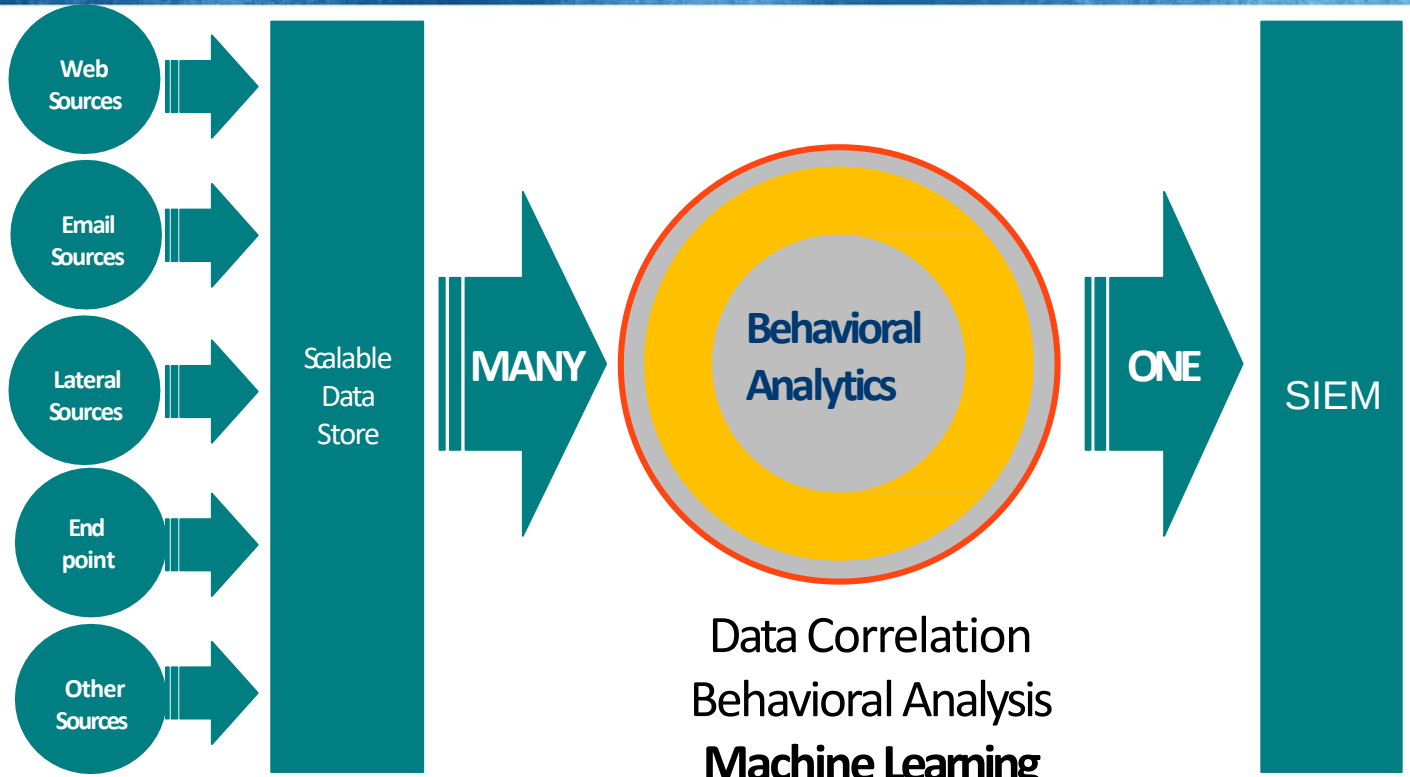
Behavioral Analytics – Simplifies Incident Response



- Collect data from web, email, etc.
- Analyze/detect advanced threat
- Identify infected host/user
- Ingest meta data from all sources
- Correlate all related host events
- Consolidate events on timeline
- Present as one security incident

- Reduces noise from SIEM alerts
- Eliminates manual correlation
- Provides insight into threat
- Simplifies incident response

Behavioral Analytics – Simplifies Incident Response



Data Correlation
Behavioral Analysis
Machine Learning

Less
Raw data feeds
Manual labor
False positives
Wasted time

More
Correlated events
Accurate incidents
SOC/IR efficiency

Behavioral Analytics for Interactive Investigations

Ingest → Store → Analyze → Visualize

Write Optimized,
Infinite Scale
With Commodity HW

Native Detection Engines (exploits, files, network)

Analytics Engines (context, correlation)

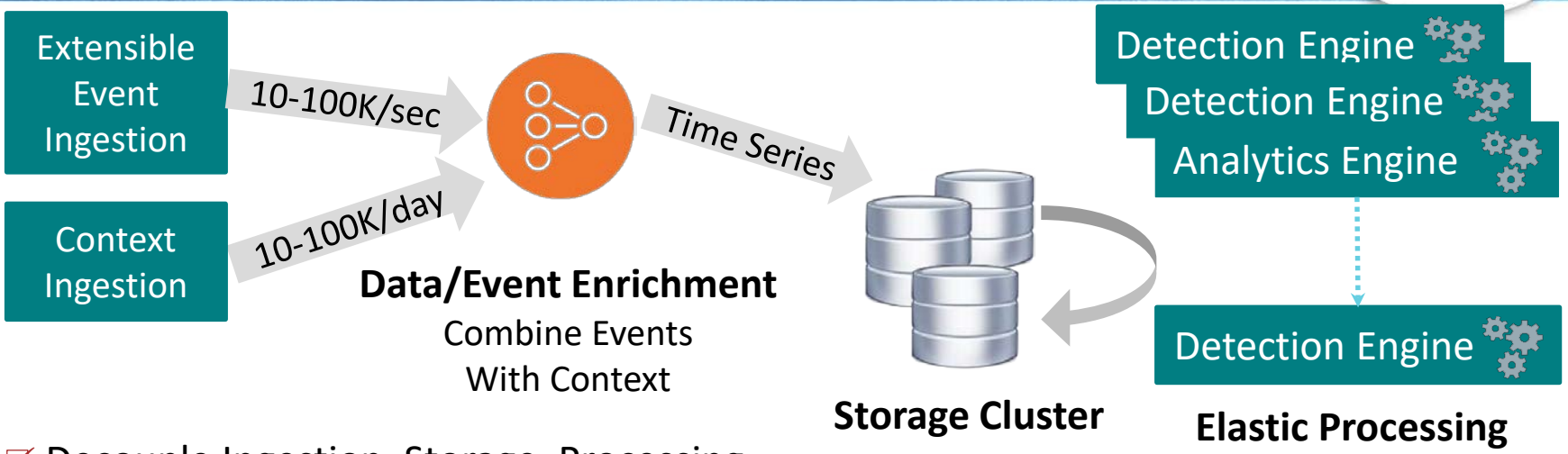
Prioritization, Risk Analysis

- Host/User Timeline
- Threat Migration
- Incident View
- Threat Hunting

Input Raw data and Log data ingested and analyzed from multiple network, detection, and identity sources

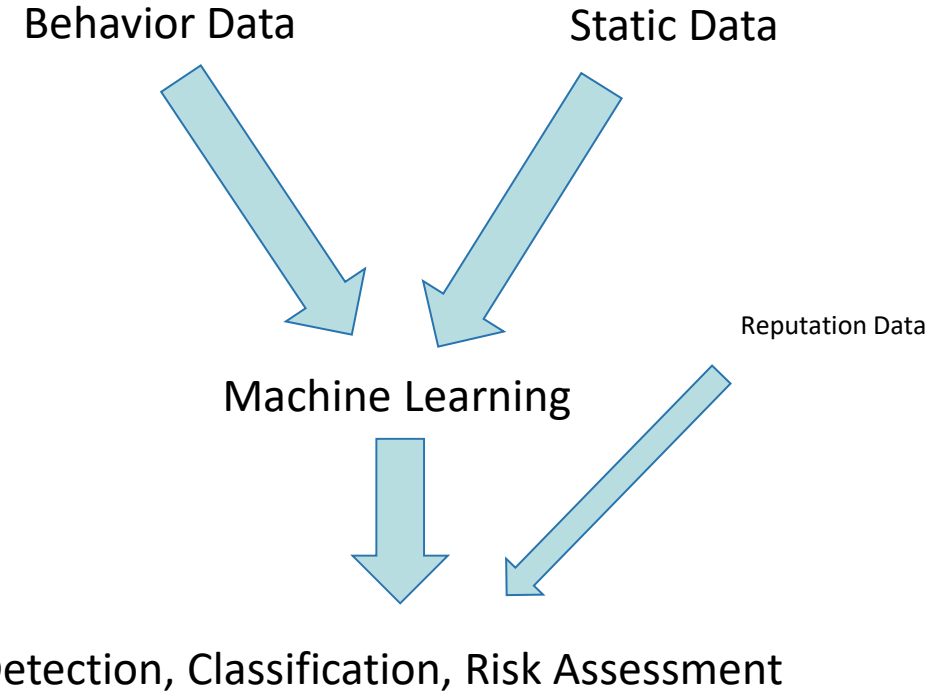
Output Example: Consolidated, correlated timeline view of all incidents for a compromised host or named user

Behavioral Analytics Architecture



- ☑ Decouple Ingestion, Storage, Processing
- ☑ Collect raw data for detection, not just logs
- ☑ Add Endpoint Identity to all data
- ☑ Extend to arbitrary time horizon
- ☑ Elastic Detection processing

Automation with Machine Learning



Automation of Common IR Tasks

Malware Investigation Tasks	Manual Effort Time
Identify Host and User	10 min
Collect AV and EDTR data for given host	25 min
Collect network data (NGFW, SWG)	25 min
Analyze & Correlate	35 min
Determine progression and scope	15 min
Contain the threat	10 min
TOTAL TIME	**2 hours**

Source: https://www.cyphort.com/resources/#calc

Automation in Action

Investigation Task	Using Automation	Manual Process
Chasing False Positives	38 hours	**390 hours**
Post-breach Mitigation	37 hours	**195 hours**
Investigating Breach Indicators	55 hours	**177 hours**
Total time taken	130 hours	**722 hours**

Automation gives **~80% Time Savings** over Manual Processes

Reducing Cybersecurity Costs & Risks Through Automation Technologies, November 2017

Remember

Behavioral analytics simplifies and automates incident response for security teams through:

- Correlation of signals across various vendors
- Prioritizing incidents on threat risk
- Adding identity context and timeline visualization
- Integrating with existing controls for threat mitigation

QUESTIONS?

Email: mikolab@juniper.net

Twitter: @belogor