

A hand is shown holding a glowing orange arc that is part of a futuristic, circular interface. The interface consists of concentric white circles and lines, with a central orange sphere. The text 'SECURITY SOLUTIONS' is overlaid on the interface, with 'SECUR' and 'SOLUTIONS' in white and 'ITY' in orange. The background is dark with a grid pattern.

SECURITY SOLUTIONS

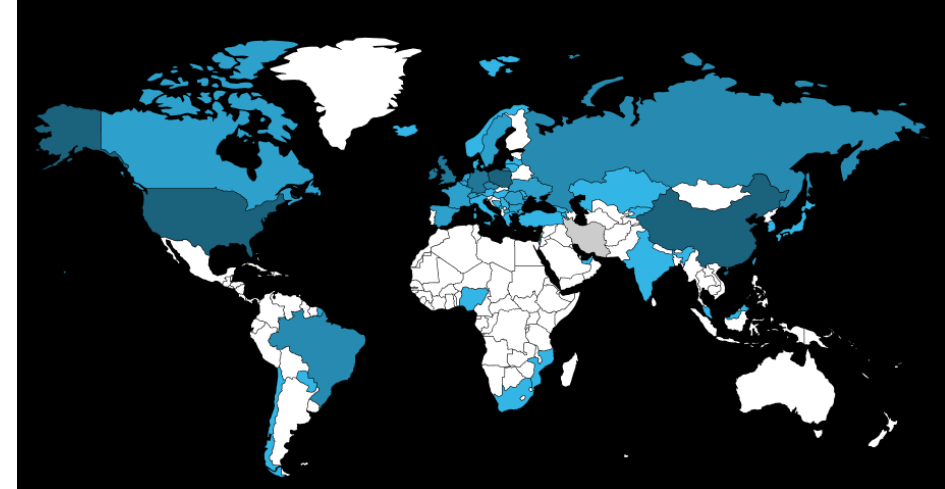
immediate



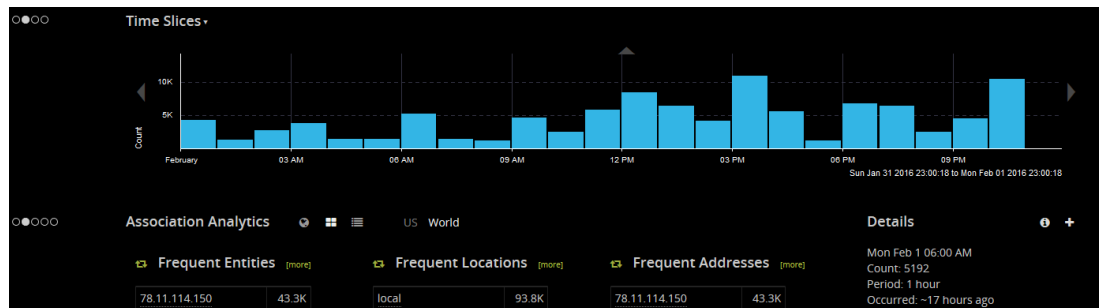
**insight**

# Zagadnienia

- Podejście do tematu analizy
- Cechy Immediate Insight
- Przykłady użycia
- Podsumowanie



immediate  insight

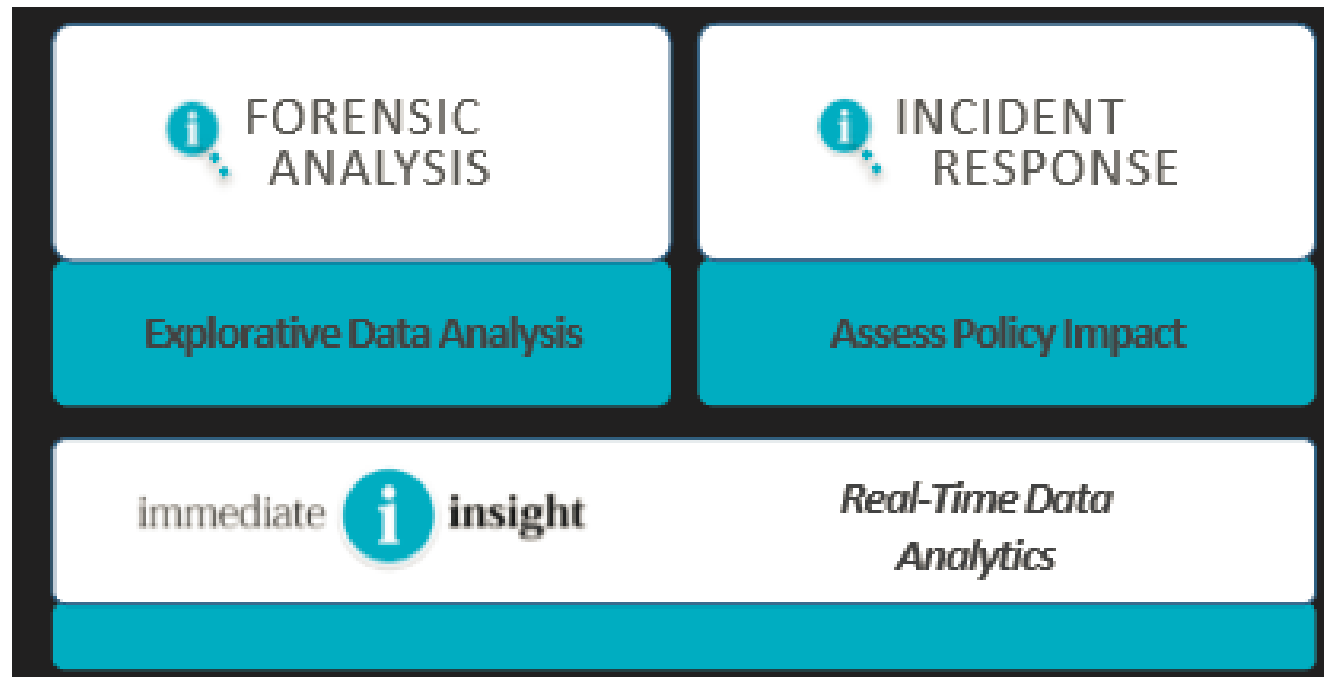


A screenshot of a dashboard titled "Tools". It features four main categories: "Explore" (Events, Entities, Details), "Analytics" (Trending, Most Common, Most Unusual), "Perspective" (Timeline, Location, Live Feed), and "Shared" (Tags, Notes, Alerts). Each category is represented by a colored box with icons and text.

# Codziennosc

- Mamy problem w sieci z wydajnością – ale systemy monitorujące o niczym nie alertują
- Mamy incydent bezpieczeństwa, nastąpił wyciek danych, nie zadziałały mechanizmy ochronne
- Został wygenerowany alert w systemie monitoringu lub systemie SIEM, ale nie wiemy co leżało u podstaw
- Zaczynając dochodzenie nie znamy wszystkich pytań, pojawia się ich coraz więcej w miarę analizy konkretnego zdarzenia
- Prowadząc dochodzenie, czy analizę potrzebujemy platformy do koordynacji działań i wymiany informacji

# Immediate Insight – uzupełnienie SIEM-a





# Platforma analityczna – odkryć nieznanne

## The IT Data Analysis Landscape

	Structured Data Aggregation	Visualize the Known	Discover the Unknown
Owner	Vendors	Data Scientists	SMEs
Delivery	Predefined Reports	Custom Dashboards	Data Discovery Workflow
Use Cases	Compliance	Security Operations	Integrated Operations

# Inne podejście

Platformy  
do wizualizacji ,  
Dashboards

**Trends**

*Przekształcenie danych w liczby,  
wykresy, alarmy po przekroczeniu  
zdefiniowanych wartości,  
wizualizacja trendów.*

SIEM-y

**Knowns**

*Otrzymywanie predefiniowanych  
rzeczy – wynik działania w oparciu o  
sygnatury, reguły, zdefiniowane  
raporty – wizualizacja tego co wiem,  
że może się zdarzyć.*

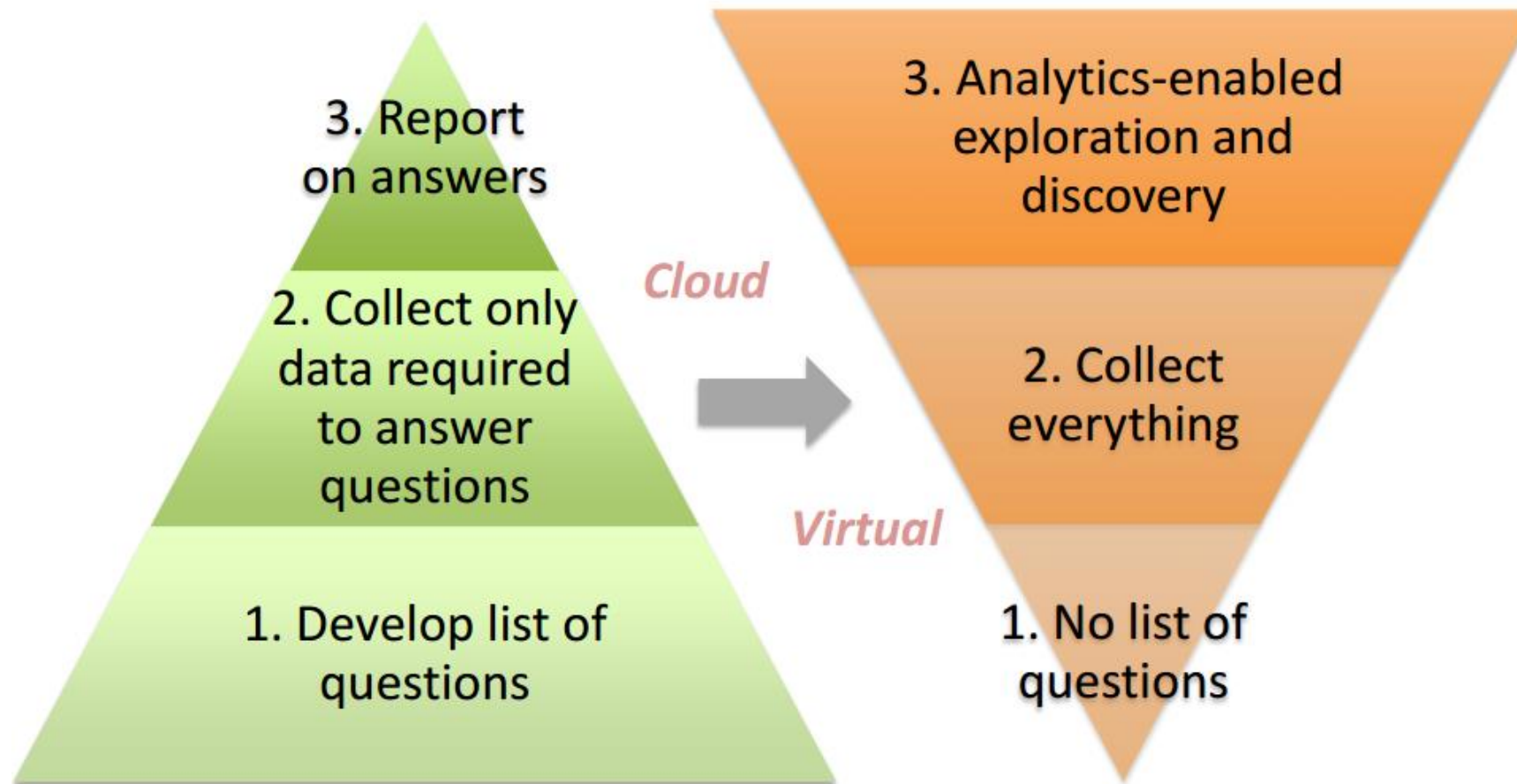
Immediate  
Insight

**UnkNOWns**

*Gdzie zacząć jeśli mam problem, a nie  
mam na panelach „czerwonego  
światła” i alertów ?*

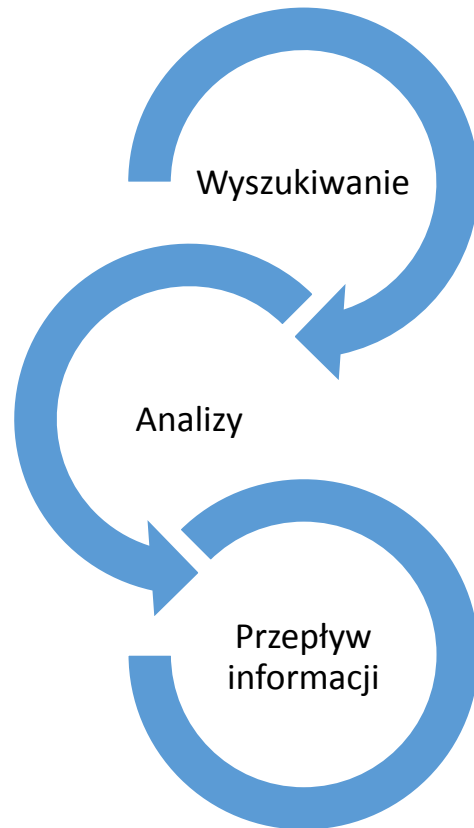
*Kiedy mam „czerwone światło” lub  
zostało wygenerowane ostrzeżenie jak  
znaleźć „dlaczego” ?*

# Znane vs Nieznane





# Filozofia Immediate Insight



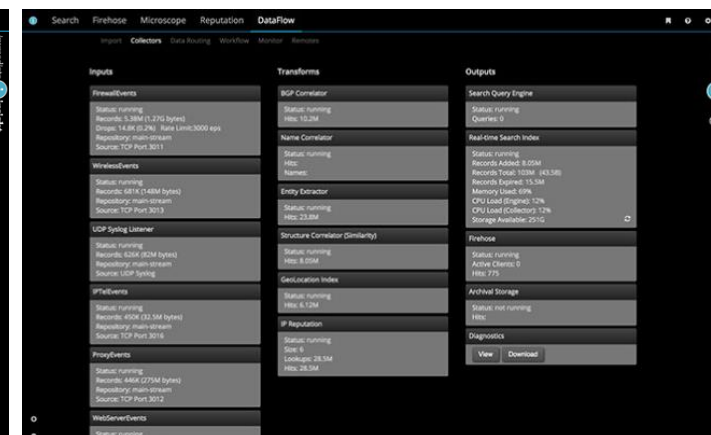
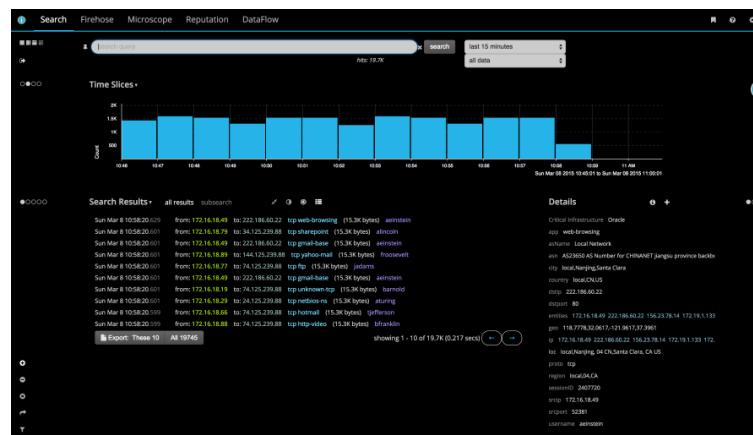
Inne podejście do pracy z danymi:

- **Odkrycie rzeczy związanych z danymi**
- **Praca w czasie rzeczywistym i z danymi historycznymi**
- **Łatwość użycia – naturalny język**
- **Pozwala znaleźć odpowiedź**
- **Możliwe zapytania ad-hoc**
- **Nie wymaga parsowania**

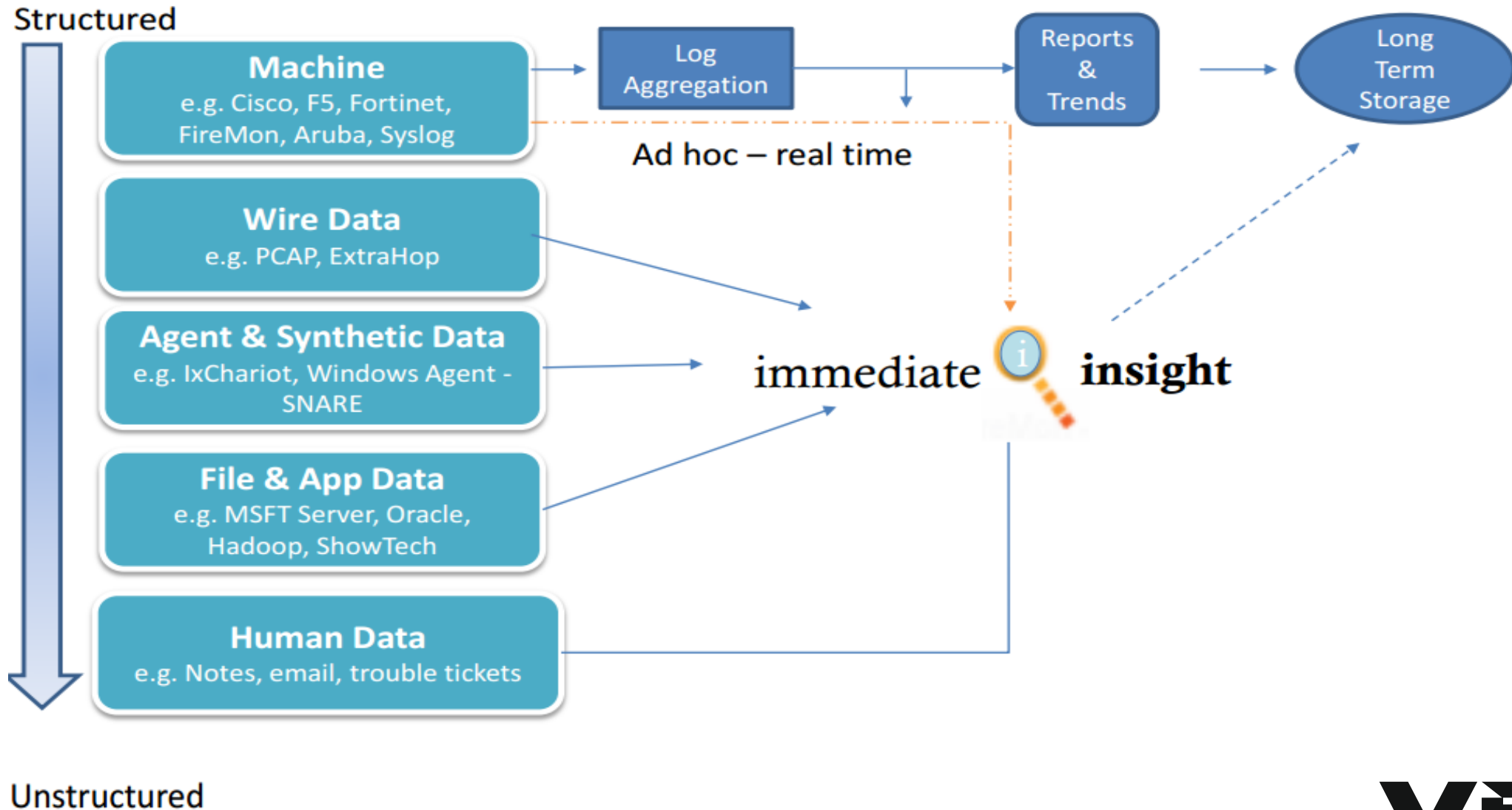


# Platforma dla „myśliwych” i „tropicieli”

- Rozszerzenie funkcjonalności SIEM
- Analiza Big Data
- Platforma do analityki śledczej i wsparcia reagowania na incydenty bezpieczeństwa



# Źródła danych



search query [x] search [last hour] [all data]

Tools

- Explore**
  - Events
  - Entities
  - Details
- Analytics**
  - Trending
  - Most Common
  - Most Unusual
- Perspective**
  - Timeline
  - Location
  - Live Feed
- Shared**
  - Tags
  - Notes
  - Alerts

Search Results all results subsearch

Mon Jun 29 11:22:19.160	<14>(Lumin-Lab-SJ) cp_stack_mgr: INFO lte_sierra.c(4556) usb1: lte_sierra_modem_nmea_listen_cb() got nmea GGA sentence, len: 76
Mon Jun 29 11:22:18.488	Failed password for root from 43.255.189.80 port 51845 ssh2
Mon Jun 29 11:22:18.483	<38>Jun 29 02:22:18 i-insight sshd[25435]: Failed password for root from 43.255.189.80 port 51845 ssh2
Mon Jun 29 11:22:18.156	<14>(Lumin-Lab-SJ) cp_stack_mgr: INFO lte_sierra.c(4556) usb1: lte_sierra_modem_nmea_listen_cb() got nmea GGA sentence, len: 76
Mon Jun 29 11:22:17.166	<14>(Lumin-Lab-SJ) cp_stack_mgr: INFO lte_sierra.c(4556) usb1: lte_sierra_modem_nmea_listen_cb() got nmea GGA sentence, len: 76
Mon Jun 29 11:22:16.283	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost= 43.255.189.80 user=root

Details

logFacility 1  
logSeverity 6  
tags cradlepoint



Tools

Explore

- Events
- Entities
- Details

Analytics

- Trending
- Most Common
- Most Unusual

Perspective

- Timeline
- Location
- Live Feed

Shared

- Tags
- Notes
- Alerts

Association Analytics

US World

Frequent Entities [more]

192.168.2.40	71.2K
192.168.2.88	25.6K

Frequent Locations [more]

local	73.6K
Ashburn, VA US	22.7K

Frequent Addresses [more]

192.168.2.40	71.2K
192.168.2.88	25.6K

Frequent Users

jwalker	71K
alincoln	8.67K
aeinstein	3.34K
jjones	1.99K

Frequent Apps

ssl	1.17K
web-browsing	702
yahoo-mail	585
bittorrent	585

Frequent Networks [more]

AS15169 Google Inc.	38.5K
AS14618 Amazon.com, Inc.	15.6K
AS4788 TM Net, Internet Service Provider	14.3K

Frequent Sources

FirewallEvents	101K
Traffic Generator:/home/insight/logdata/firewalltraffic.txt	101K

Frequent Names

www.facebook.com	4.75K
bits.wikimedia.org	2.71K
en.wikipedia.org	2.55K
www.google.com	2.24K
upload.wikimedia.org	2.23K
profile.ak.fbcdn.net	2.21K



## Get Insight

Counts ▼ Change ▼

### Priority FireEye Threats

Period: Last 24 Hours  
Current: Tue Apr 15 2014 16:39:18  
Versus: Same Time Yesterday

11	+450% ↑	Malware on Critical Infrastructure - Oracle
8	+300% ↑	Malware Infection for IT Admin <i>Command &amp; Control traffic detected from an IT user with administrative privileges</i>
6	-14% ↓	Malware for Executive Management
1	-50% ↓	Malware - Twitter Compromised

### Palo Alto Networks Events

7.62K	+43.0% ↑	Connections Denied
9	no change	Allowed Connections to Untrusted Domain

### Workflow Monitor

1	+ ↑	Malware Detected, Clean Up Required
0	-100% ↓	Malware Detected, Twitter Administrator
0	-100% ↓	Malware Detected, Executive
2	+ ↑	Malware Detected

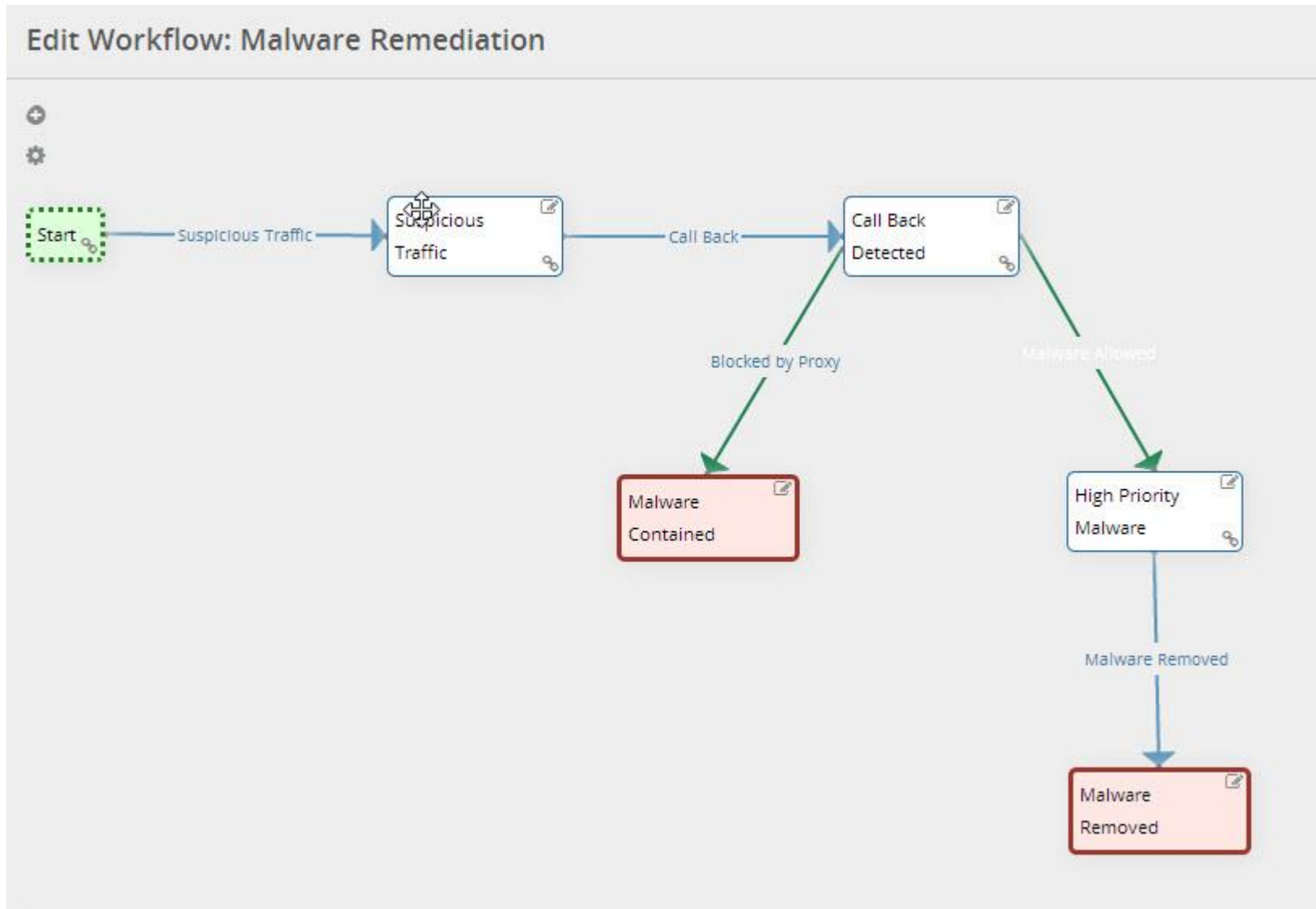


### Mobile Device Compliance

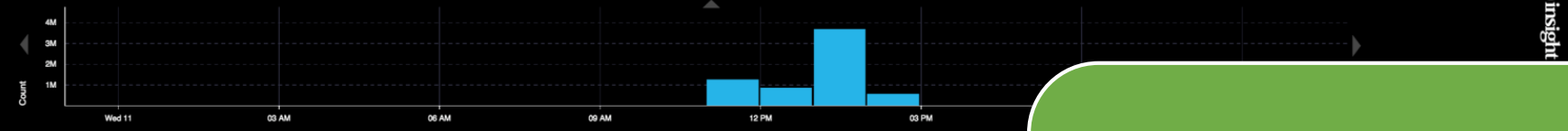


## Workflow Tracking Summary

	Active	Completed
High Risk Epic Access: 4	Unmanaged Wireless Device:2 Encryption Disabled:1 High Risk Epic Access:1 Medium Risk Epic Access:0	Encryption Enabled:0 Posture Analyzed:0
Malware Remediation: 0	Command and Control:0 Malware Contained:0	Urgent Cleanup Required:0 Malware Removed:0
Performance Checker: 3	Slow Performance:2 Critical Performance:1	Performance Normal:4
Suspicious Activity: 1	Outbound Spam Email:0 Bitcoin Detected:0	P2P Detected:1 Host Scanned:0



Time Slices



Association Analytics

Frequent Entities

192.168.2.40	2.72M
172.16.255.255	1.38M
172.16.0.0	1.38M
0.0.0.0	1.22M
208.85.40.20	1.13M
192.168.2.88	992K
192.168.2.1	992K
8.8.4.4	680K
23.21.222.178	397K
172.16.18.41	346K

Frequent Locations

local	3.11M
Oakland, CA US	1.13M
US	784K
Mountain View, CA US	748K
Ashburn, VA US	713K
Cambridge, MA US	306K
Pantal, 05 MY	281K
San Francisco, CA US	241K
New York, NY US	180K
Santa Clara, CA US	161K

Frequent Addresses

192.168.2.40	2.72M
172.16.255.255	1.38M
172.16.0.0	1.38M
0.0.0.0	1.22M
208.85.40.20	1.13M
192.168.2.88	992K
192.168.2.1	992K
8.8.4.4	680K
23.21.222.178	397K
172.16.18.41	346K

Frequent Users

jjones	1.65M
barnold	288K
jwalker	284K
lholt	284K
aeinstein	25.6K
jsmith	17.8K
wsmith	8.94K
ahoff	8.94K
gwashtington	8.94K
bhamilton	4.47K

Frequent Apps

ssl	
web-browsing	
bittorrent	
yahoo-mail	
gmail-base	
vnc-http	
http-video	
ms-exchange	
hotmail	
twitter-base	

Frequent Networks

AS15169 Google Inc.	1.43M
AS40428 Pandora Media, Inc	1.13M

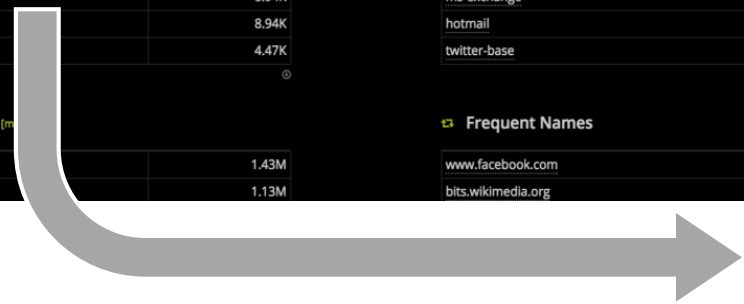
Frequent Names

www.facebook.com	
bits.wikimedia.org	

Frequent Users

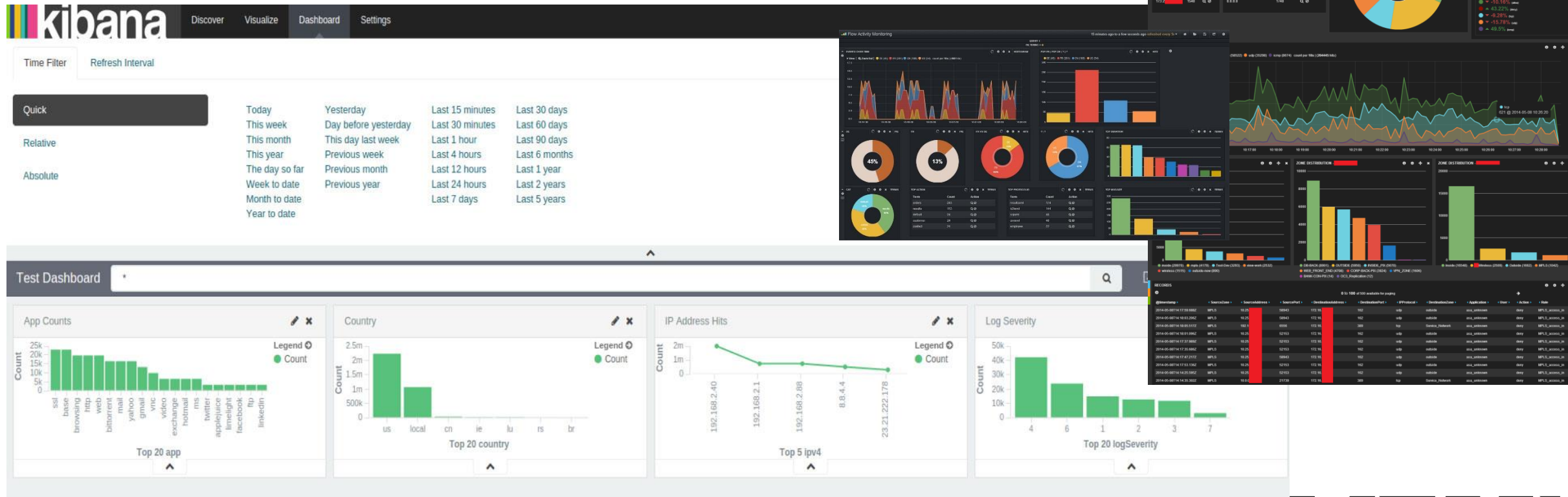
jjones	1.02M
barnold	255K
jwalker	254K
lholt	253K
jsmith	6.16K
wsmith	3.07K
gwashtington	3.07K
ahoff	3.07K
tjefferson	1.53K
jadams	1.53K

Wzbogacenie danych nie związanych z Palo Alto informacjami pochodzącymi z danych uzyskanych z Palo Alto



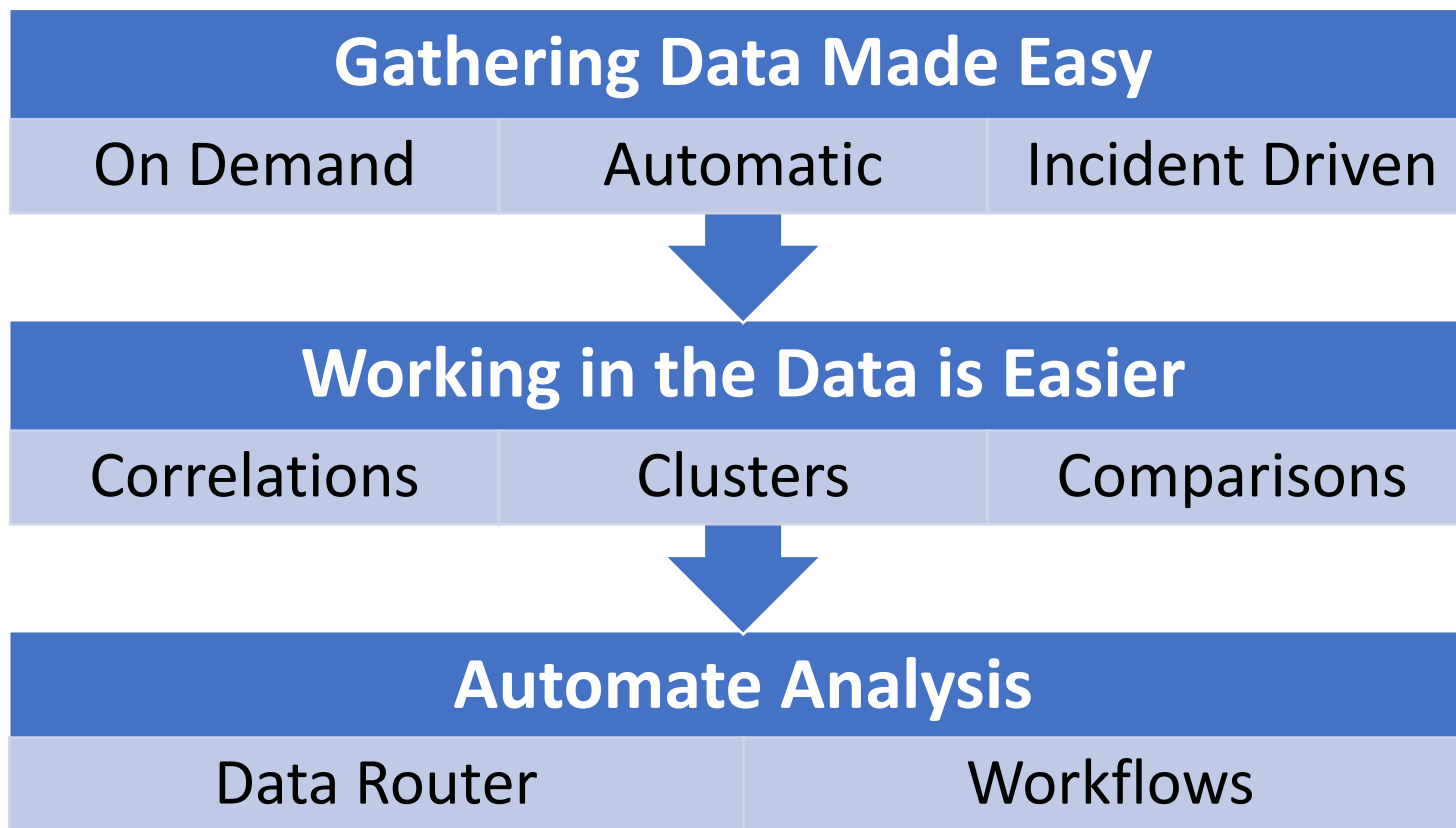
# Możliwości rozszerzenie wizualizacji

- Budowa rozbudowanych dasbordów i raportów





# Platforma Immediate Insight



Nie jest  
potrzebne  
parsowanie

Automatyczne  
wzbogacanie  
danych

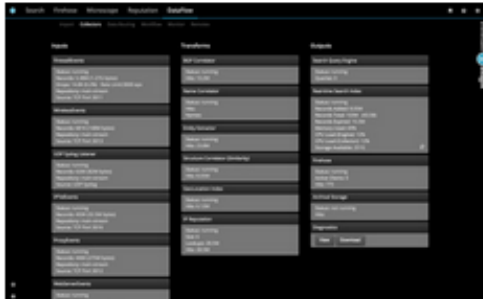
Organizacja pracy,  
wykrywanie  
przeptywów

- Nowe podejście do analizy danych
- Wsparcie procesów operacyjnych

# Cechy Immediate Insight

F I R E M  N

immediate  insight



Natural-Language  
Technology

*Reduces data collection costs –  
no custom writing.*



Automatic Data  
Enrichment

*Highlights non-obvious  
relationships in the data.*



PinBoard Searches

*Displays volume and trends and  
filters by any criteria for each  
pinned search.*



Real-Time Analysis

*Enables teams to work with data  
at the speed of thought.*



Workflow & Data Router

*Automates complex data analysis  
processes.*



Social Stream

*Allows users to follow incidents  
and other users and share useful  
insights.*

**VEMi**

# Przykłady użycia

F I R E M  N

immediate  insight



## INCIDENT RESPONSE

### Security Incident Response

Security infrastructure identifies a potential breach. Immediate Insight enables teams to quickly separate real incidents from false positives.



## RAPID TRIAGE

### Forensic Investigation

Existing visibility infrastructure answers the "what." Immediate Insight answers the "why" and "how" to identify the root cause.



## PROACTIVE RECONNAISSANCE

### Proactive Reconnaissance

Find the unusual, new and changing in the data for any arbitrary search. Find the event that occurred once without knowing what to search for.



## AD-HOC ANALYSIS

### On-Demand & Ad Hoc Data Analysis

Correlation and analysis of multiple sources of data. Load and analyze a 2GB log file and a 1GB PCAP as easily as uploading a file to a server.

**VEMi**

### Get the Data:



Pre-planned and ad hoc collection of anything human readable, no parsing required.



learn more

learn more

### Analyze the data:



Automatically extracts metadata, creates associations, develops internal reputations, and clusters in real time.



### Explore the Data:



Search-enabled point/click navigation with selectable analytics-enabled, data-reduction, and views.



learn more

### Collaborate in the Data:



Add suspicions and insights as custom context directly to the data. Follow incidents and users. Pin useful insights.



learn more

### Automate:



Analytics-enabled workflows and data router automates situation-based data preparation and analysis processes.



learn more

- ✓ Identify and investigate the suspicious.
- ✓ Search for indicators of breach and operational inefficiencies.
- ✓ Get real-time analysis of security data.
- ✓ Accelerate incident resolution and reduce escalations.
- ✓ Automatically connect and correlate data silos.
- ✓ Stage data for analysis by escalation teams.

### Immediate Insight:

- Real Time
- Built for unstructured data analysis
- Run custom queries, no query language to learn
- Automatically contextualizes data - threat intelligence, geo-location, DNS, etc.
- Correlates data without rule creation

### One-Click Analytics:

- *More like this*
- *Fewer like this*
- *Similar*
- *Most Common*
- *Most Unusual*
- *Trending Up*
- *Trending Down*
- *New*
- *Missing*
- *Active - Increasing*
- *Active - Decreasing*
- *Tag*



# Podsumowanie

- Rozszerzenie dla SIEM-a – wykrycie nieznanego
- Wsparcie analityki śledczej i rozwiązywania problemów oraz wsparcie procesu reakcji na incydenty
- Narzędzie wspierające proaktywne działania w obszarze bezpieczeństwa – „tropienie i polowanie”
- Analiza danych w czasie rzeczywistym i danych historycznych
- Skrócenie czasu wykrywania problemów
- Wykrywanie nieoczywistych powiązań i zależności – analiza Big Data





Michal.Lewandowski@vemi.pl

Tomasz.Halasz@vemi.pl

**VEMI**

Value Added Security Distributor



[www.vemi.pl](http://www.vemi.pl)

Tel. +48 22 3782353

Fax +48 22 3782353

e-mail [office@vemi.pl](mailto:office@vemi.pl)