VEMI

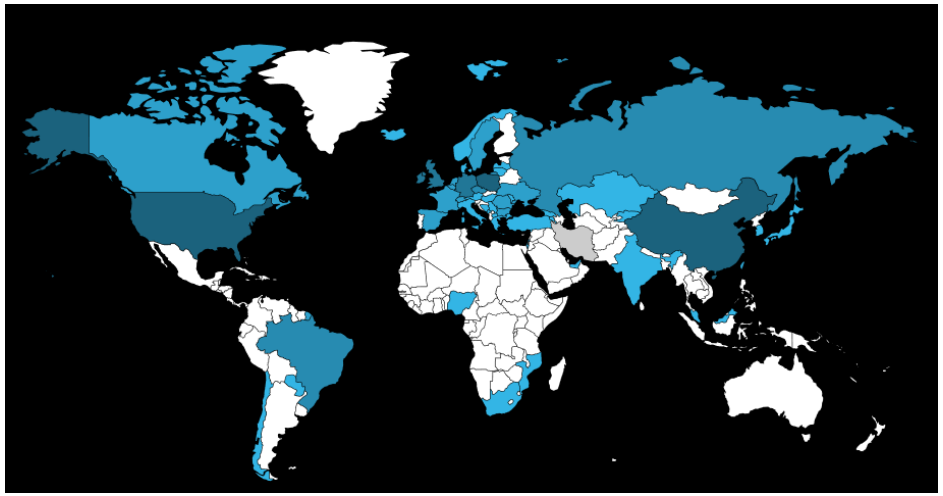
SECURITY SOLUTIONS

www.vemi.pl

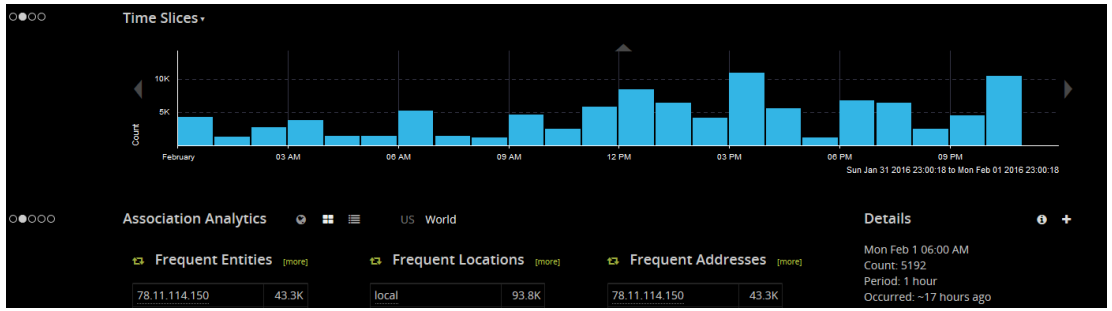

immediate
insight

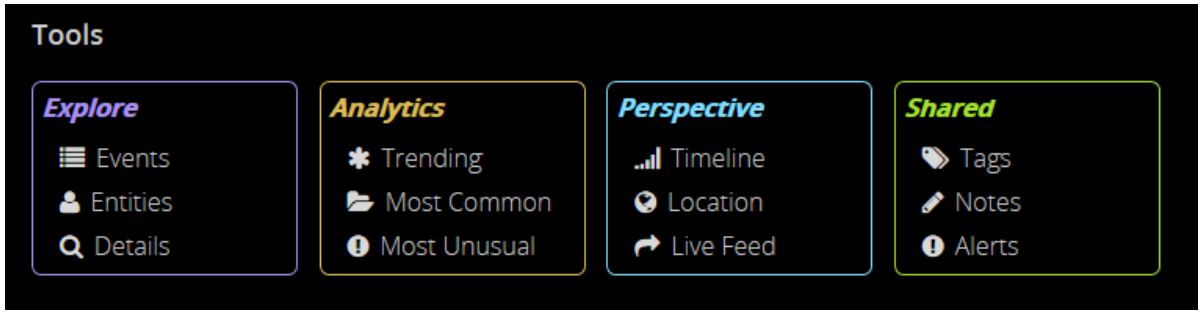
Zagadnienia

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



immediate insight





VEMI

Codzienność

- 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 koordynacja działań i wymiany informacji

FIREMON

immediate insight

Immediate Insight – uzupełnienie SIEM-a

VEMI

FIREMON

immediate insight

Platforma analityczna – odkryć nieznane

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

VEMI

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

Unk*NOW*ns

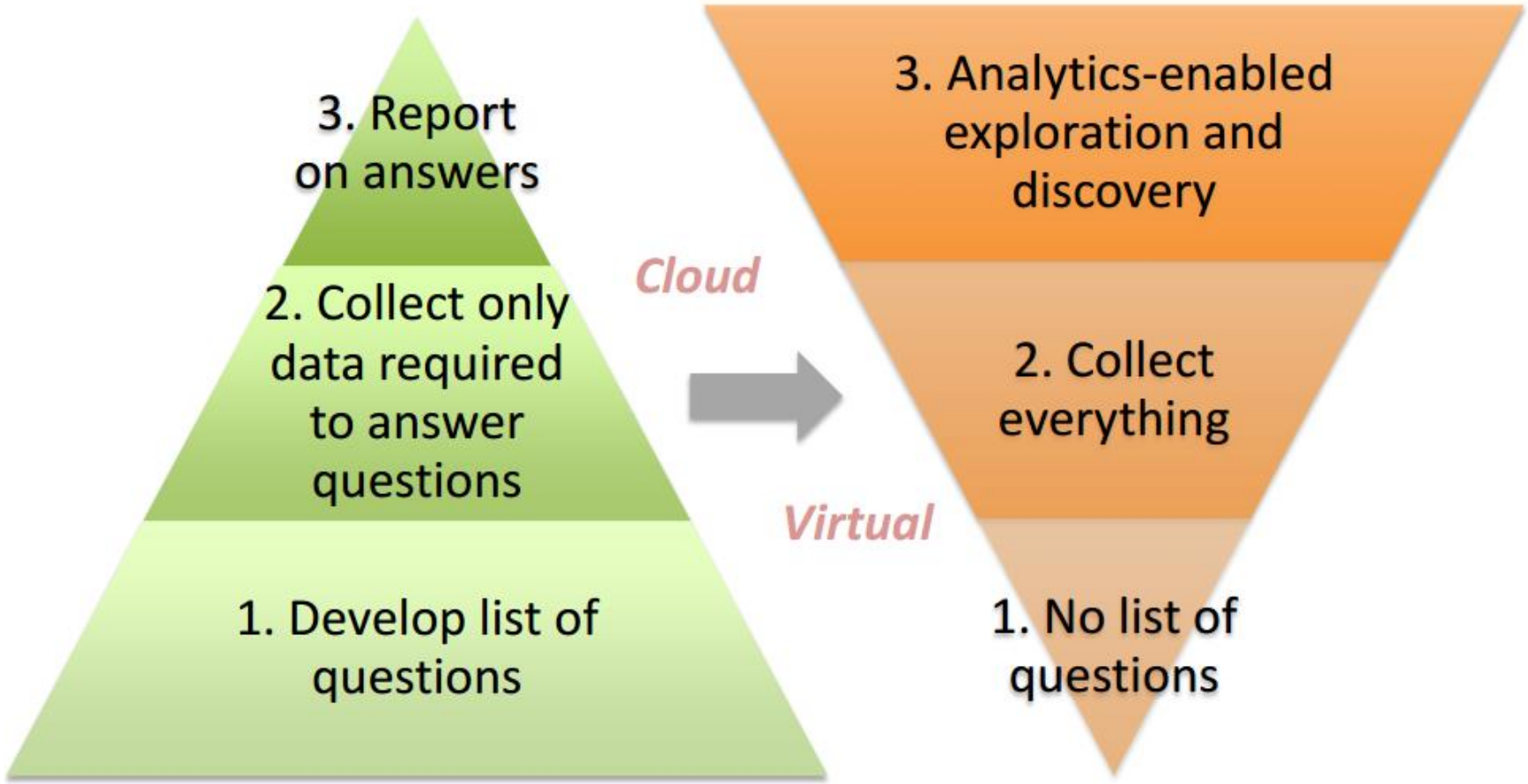
Gdzie zacząć jeśli mam problem, a nie mam na panelach „czerwonego światła" i alertów ?

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

FIREMON

immediate insight

Znane vs Nieznane

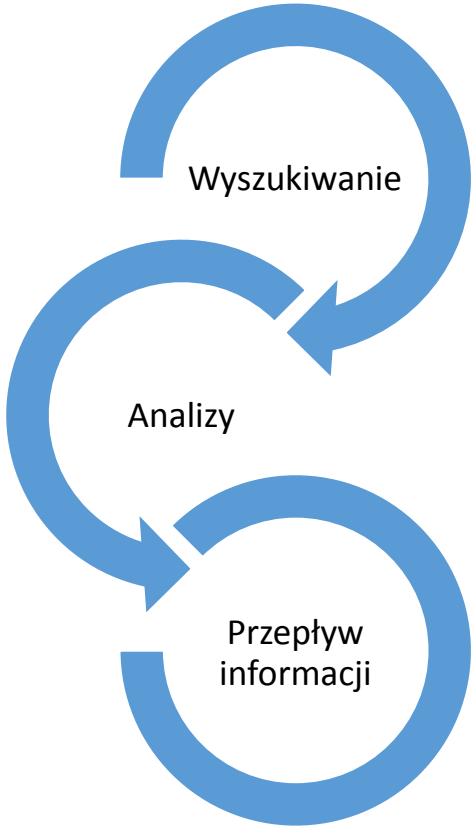


VEMI

FIREMON

immediate insight

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**

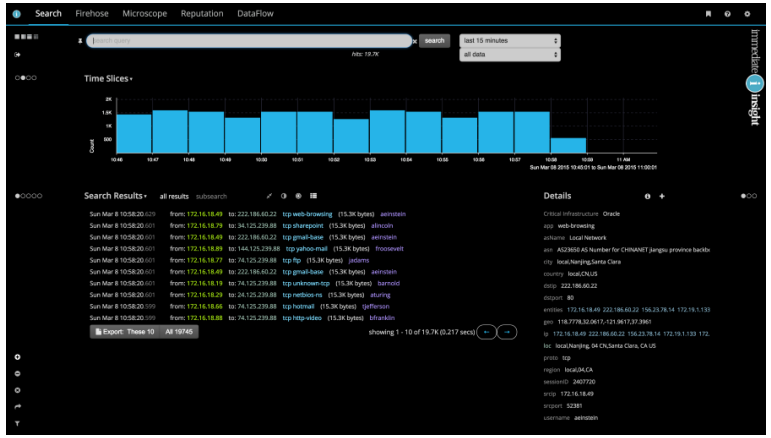
VEMI

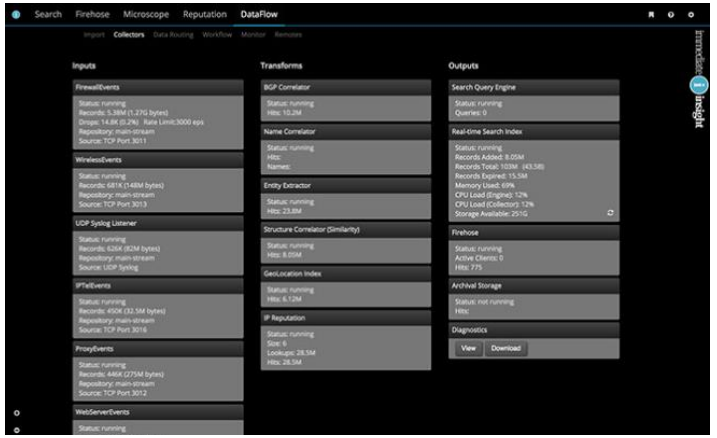
FIREMON

Platforma dla „myśliwych” i „tropicieli”

immediate insight

- Rozszerzenie funkcjonalności SIEM
- Analiza Big Data
- Paltforma do analityli śledczej i wsparcia reagowania na incydenty bezpieczeństwa



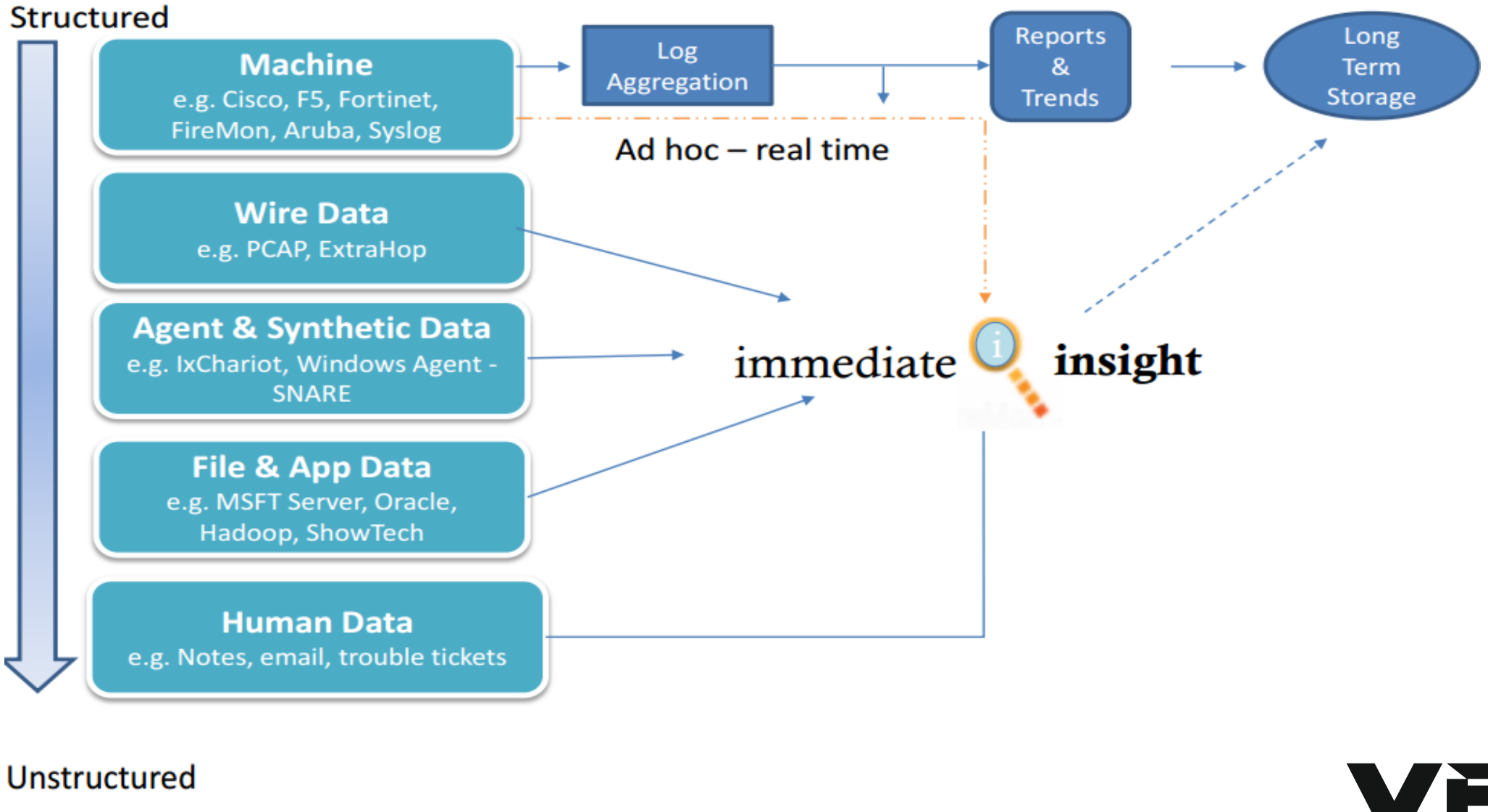


VEMI

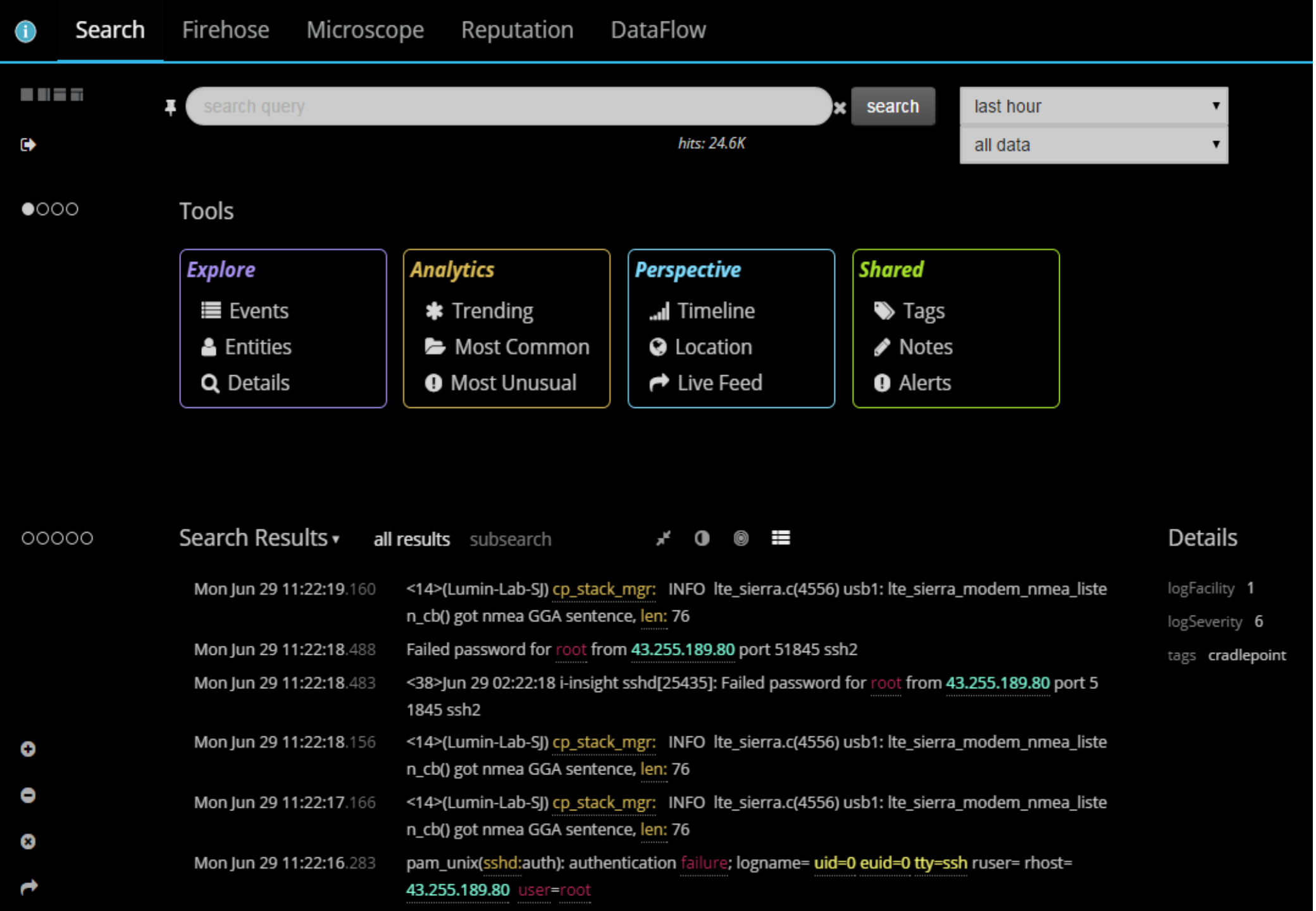
FIREMON

immediate insight

Źródła danych



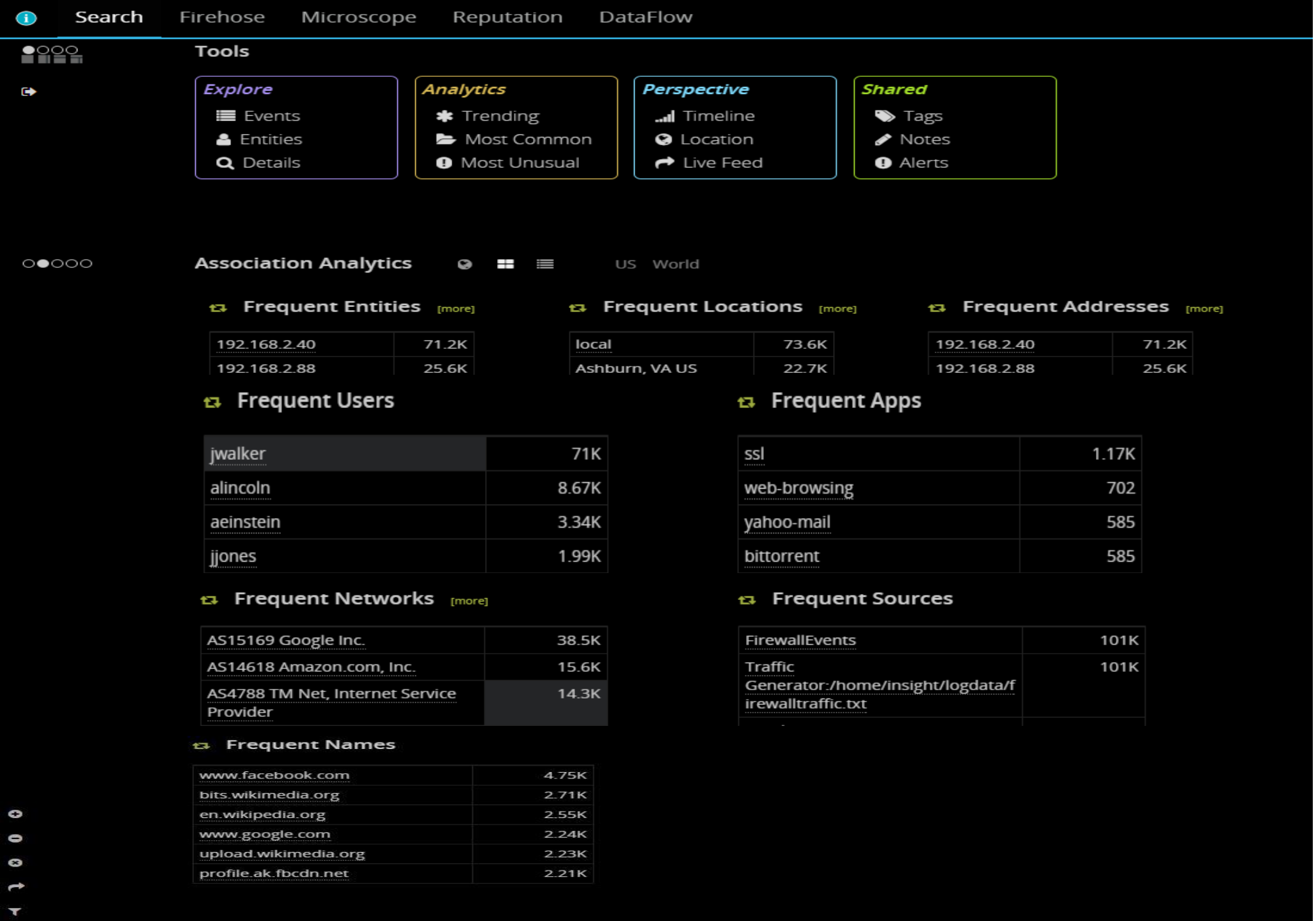
VEMI



FIREMON

immediate insight

VEMI



FIREMON

immediate insight

VEMI

FIREMON

immediate insight

Get Insight

Counts | Change

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

Priority FireEye Threats

11	+450% ↑	Malware on Critical Infrastructure - Oracle
8	+300% ↑	Malware Infection for IT Admin
		Command & Control traffic detected from an IT user with administrative privileges
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

VEMI

FIREMON

immediate insight

Search | Firehose | Microscope | Reputation | DataFlow

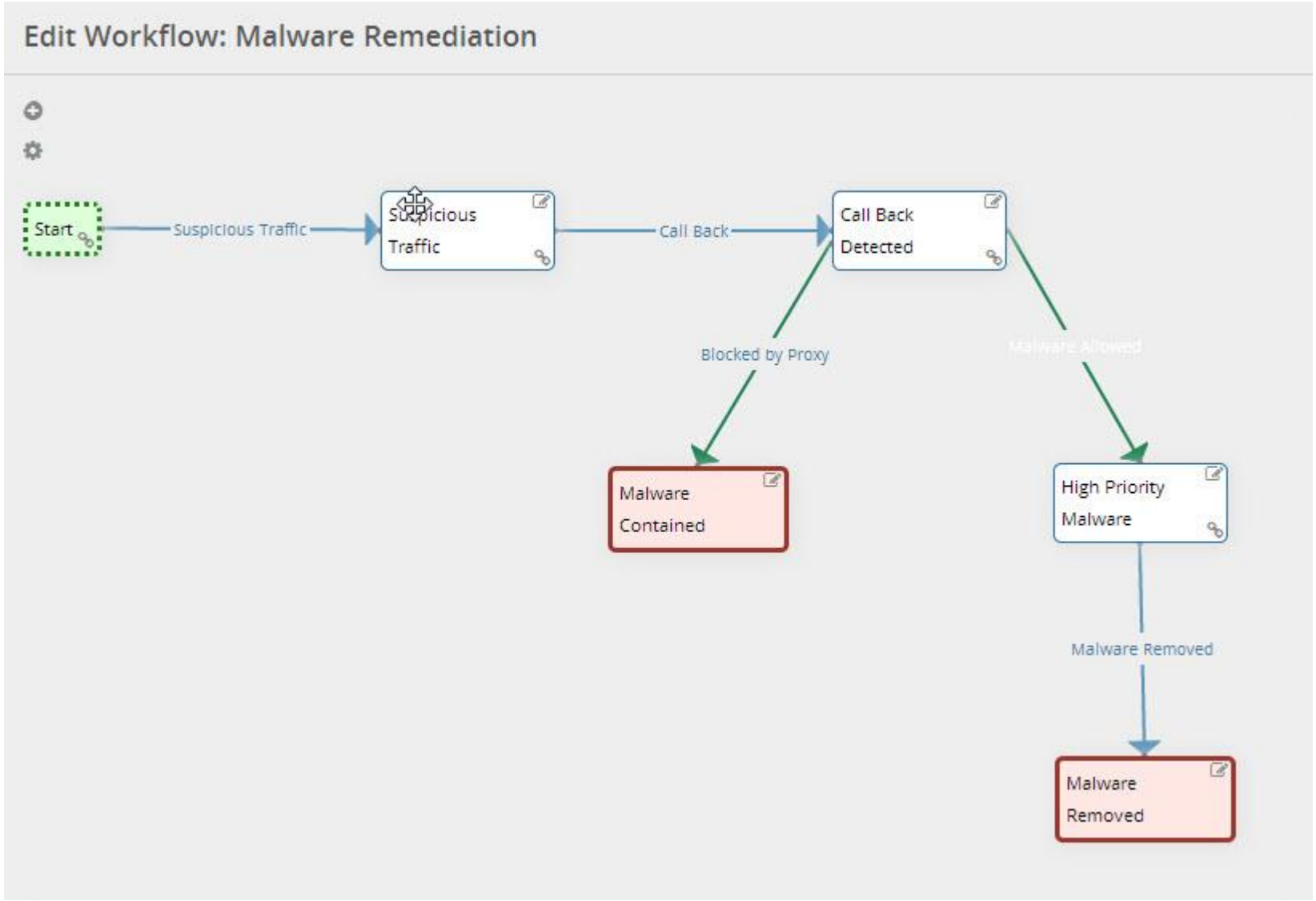
Workflow Tracking Summary

	Active	Completed
High Risk Epic Access: 4	Unmanaged Wireless Device:2 · Encryption Disabled:1 · Encryption Enabled:0 · High Risk Epic Access:1 · Medium Risk Epic Access: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

VEMI

FIREMON

immediate insight

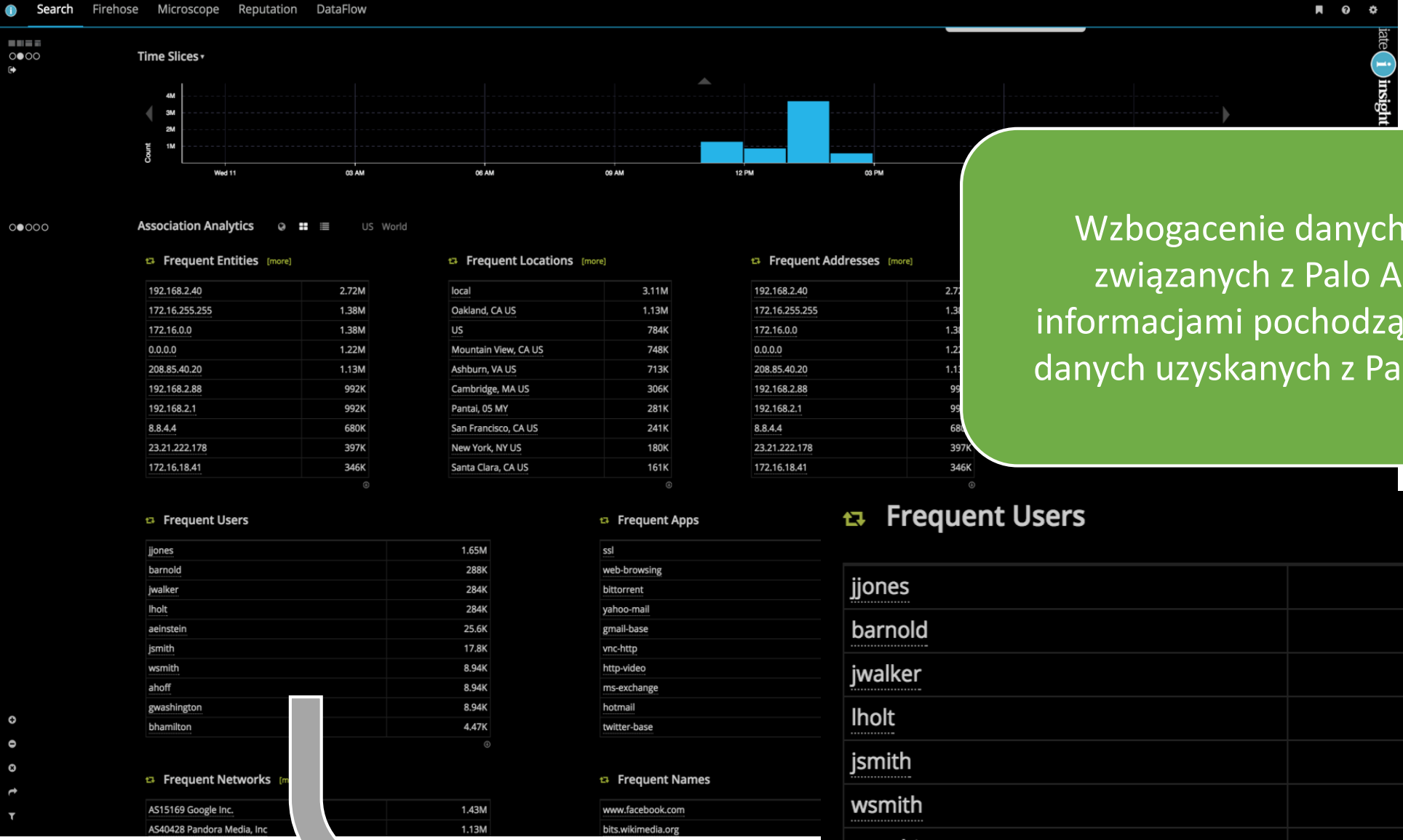


VEMI

FIREMON

immediate insight

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



Frequent Users

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

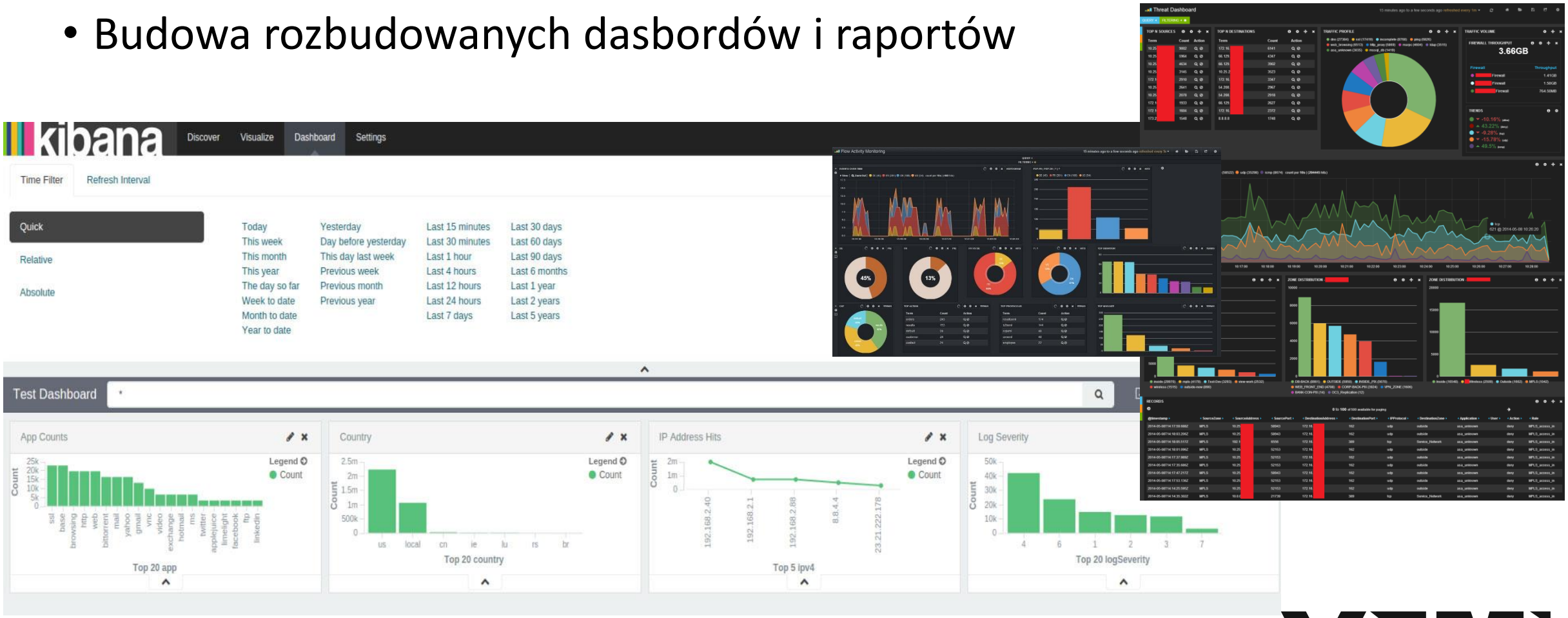
VEMI

FIREMON

immediate insight

Możliwości rozszerzenie wizualizacji

- Budowa rozbudowanych dasbordów i raportów

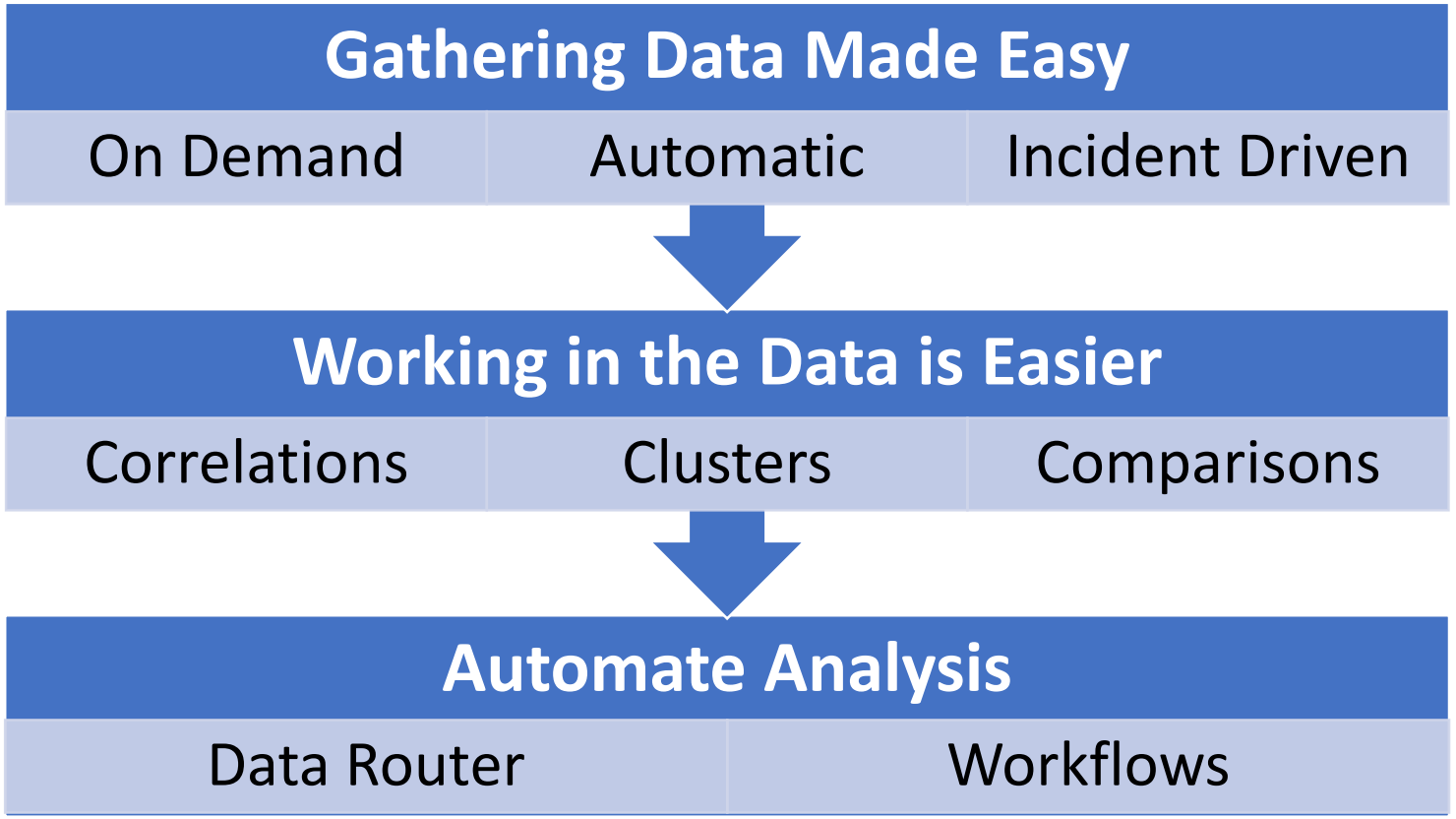


VEMI

FIREMON

immediate insight

Platforma Immediate Insight



Nie jest potrzebne parsowanie

Automatyczne wzbogacanie danych

Organizacja pracy, wykrywanie przepływów

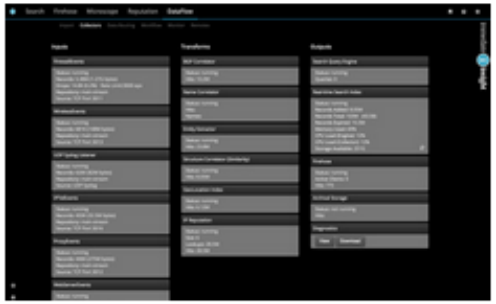
- Nowe podejście do analizy danych
- Wsparcie procesów operacyjnych

VEMI

Cechy Immediate Insight

FIREMON

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

FIREMON

immediate insight

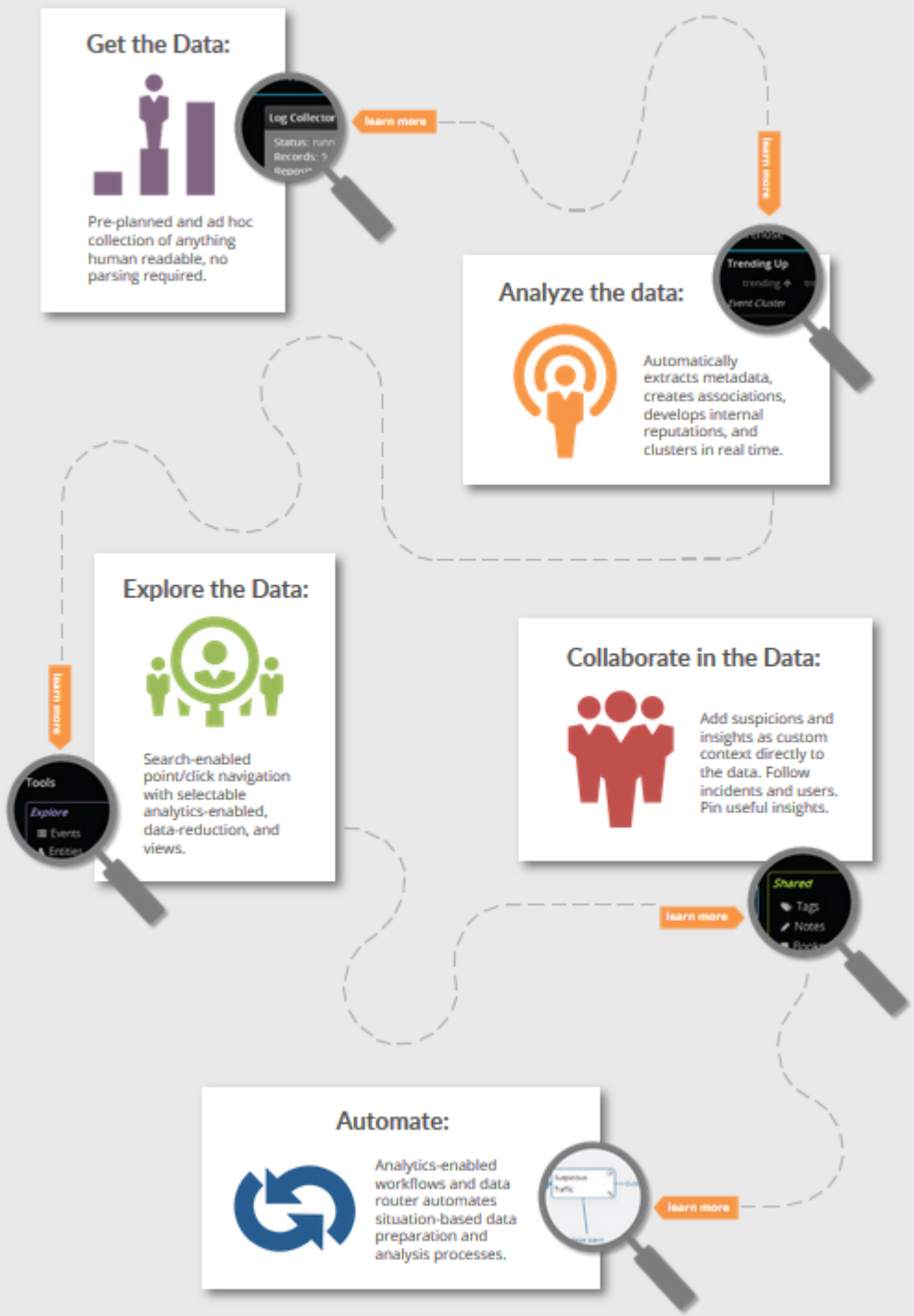
Security Incident Response
Security infrastructure identifies a potential breach. Immediate Insight enables teams to quickly separate real incidents from false positives.

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

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.

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



- 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*

VEMI

FIREMON

immediate insight

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

immediate insight

VEMI

Michal.Lewandowski@vemi.pl
Tomasz.Halasz@vemi.pl

VEMI

Value Added Security Distributor

www.vemi.pl

Tel. +48 22 3782353
Fax +48 22 3782353
e-mail office@vemi.pl