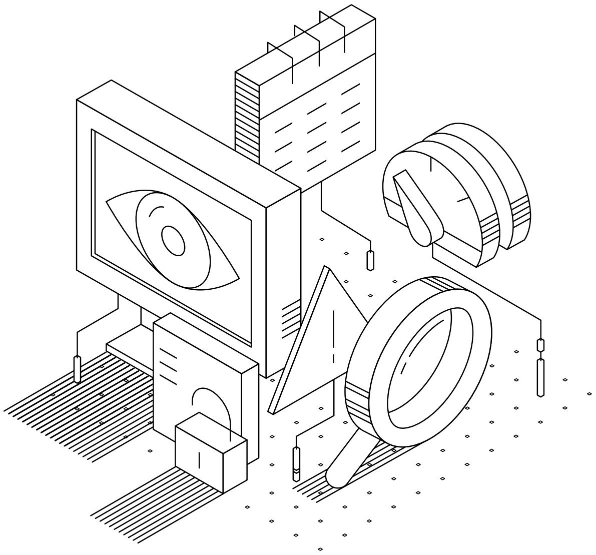
FIREMON

Immediate Insight

Security Analytics for Real-time Event Triage

Does security alert and data volume and complexity exceed the capacity of your teams?

The volume of security alerts far exceeds security team's capacity to assess if they represent risky security incidents or false positives. Moreover, new infrastructure paradigms, such as cloud/mobile–centric architectures and dynamic-by design infrastructures (e.g. SDN), are increasing the complexity of alert triage data analysis. Combine this with a more sophisticated, determined adversary and an avalanche of data, and it's clear that triage needs are exceeding the capabilities of SIEM-based data analysis, resulting an increased risk from security incidents.



What Is Immediate Insight?

Immediate Insight brings the speed and simplicity of a search engine to data analysis for security event triage. It merges machine learning, correlation and natural language in a simple, workflow-centric interface to reveal relationships in the data that users didn't even know to look for. It provides actionable data that accelerates threat detection and analysis without requiring a query language or customization.

Immediate Insight's real-time analysis across data silos provides the timely and detailed operational visibility necessary to:

- Make security alerts contextual and actionable
- Enrich alerts with important contextual information
- Find common themes and entities spanning alerts and alert clusters
- Identify changes in alert patterns – common and uncommon patterns, sources, and entities
- Gain insight from previous users' ovservations
- Add observations directly to the data
- Stage data for analysis by escalation teams

Solution Overview

01 THE DATA

Immediate Insight brings ease and flexibility to the data collection process so less of the event triage process is spent gathering data and more is spent determining the risk level of the security event.

- Automatically receive streams of structured and unstructured data
- Import data on demand through drag and drop interface
- Eliminate the need for parsing with natural-language technologies

02 ANALYZING THE DATA

Out-of-the-box analytics and correlations automatically enrich and optimize data for real-time analysis, so users can see anomalies and non-obvious associations across large datasets and directly navigate huge volumes of data.

Benefits include:

- Summary view of common entities (i.e. users, applications, networks, addresses, etc.)
- Automatic groupings of similar data
- Comparing arbitrary groups of data over time (new, missing, up/down)
- Local, learned context and reputation automatically applied as metadata

03 EXPLORING THE DATA

Analytics-enabled views and tailored data exploration workspace enables teams to see events and data associated with security alerts – all without learning a query language. There are five default exploration views for the results of any query: detailed events, entity associations, event clusters, comparisons and notes/tags/alerts.

Users can save searches to a PinBoard. For each pinned search:

- See volume and trends
- Filter views by any criteria
- Click through to see detailed data
- Access powerful data analytics using natural language

04 COLLABORATING IN THE DATA

An integrated "social" framework that enables operators to tag interesting data to inject context directly to, and collaborate in, the machine and human data used for incident response and threat detection. The system captures the context and leverages analytics to accelerate event triage.

Benefits include:

- Add custom context through tags
- Follow users, social style – learn and contribute

05 AUTOMATING ANALYSIS

The Workflow System and Data Router automate multi-step event triage processes and create sophisticated action policies for each step in the process. Workflows are configured with a drag-and drop interface, Plain English events are written for each step and the Data Router acts on those events in real time. Steps of the workflow are recorded so they can be used to improve the triage process.

WHY IMMEDIATE INSIGHT?

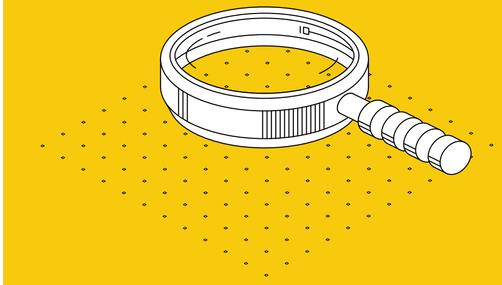
Reduces security risk by accelerating triage of security alerts as either a false positive or a real security incident.

IMMEDIATE INSIGHT:

- Tells you things you didn't know about your data
- Is real time – view and search live data
- Is easy to use – natural-language searches, point and click
- Automatically enriches data to highlight non-obvious associations
- Greatly simplifies data acquisition – no parsing required

FEATURES:

- Real-time data discovery and analysis
- Data association, clustering and comparison analytics
- Internal reputation engine
- Data tags for added custom context
- Pinboard of saved searches



FIREMON

Learn more about our solutions: www.firemon.com

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA

P: 1.913.948.9570
E: info@firemon.com