FIREMON

Immediate Insight

Analytics-Enabled Threat Hunting and Investigation Platform

THE **CHALLENGE:** Does security data volume and complexity exceed the capacity of your teams?

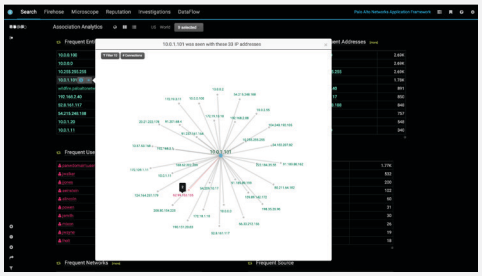
The volume of security data today far exceeds most security teams' capacity to assess if it indicates current or potential threats eluding current defenses. Moreover, new infrastructure paradigms, such as cloud/mobile-centric architectures and dynamic-by-design infrastructures (e.g. Software-Defined Networks (SDN)), are increasing the complexity of security and infrastructure data analysis. Combined with a more sophisticated, determined adversary and an avalanche of data, it's clear that analysis needs exceed the capabilities of current data analysis systems, resulting in increased risk from security incidents.

THE **SOLUTION:** FireMon Immediate Insight

Immediate Insight is an analytics-enabled threat hunting and investigation platform that allows IT security teams to accelerate the discovery of the unknown in the data. It merges machine learning, natural language and social media concepts in a simple, workflow-centric interface to reveal relationships in the data that you didn't even know to look for. Our analytics, orchestration, and workflow transform complex and disparate data into immediately actionable data across public and private cloud environments. Data analysis accelerates threat hunting and detection without customization or requiring analyst to learn a query language.

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

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



SOLUTION **FEATURES**

COLLECTING THE DATA

Immediate Insight brings ease and flexibility to the data collection process to quickly and effectively determine the risk level of a security event.

- Automatically receive streams of structured and unstructured data
- Eliminate parsing with natural-language-based entity extraction and field attribution
- Integrate with Palo Alto Networks Application Framework

ANALYZING THE DATA

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

- Configurable summary view of common entities
- Automatic groupings of similar data
- Comparing arbitrary groups of data over time
- Internal reputation system applies configured context as metadata

EXPLORING THE DATA

Analytics-enabled views and tailored data exploration workspaces enables you to see suspicious events and data 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. Users can save searches to the Pinboard. For each pinned search, you can:

- See volume and trends
- Filter views by any criteria
- Access powerful data analytics using natural language

COLLABORATING IN THE DATA

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

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

EXTENDING AND ORCHESTRATING ANALYSIS

The Data Router, Active Collectors, Investigations and Workflow systems streamline and automate your data assembly, enrichment, and analysis processes.

- Data Router enables sophisticated custom actions such as auto-tagging, programmable field extraction, JSON processing, and custom scripting
- Active Collectors can be configured to capture data that returned a command line program, script, or API call, either manually or automatically

WHY **IMMEDIATE INSIGHT?**

Increase your team's capacity to identify and analyze threats for faster, more effective threat hunting, detection, and response.

USE **IMMEDIATE INSIGHT TO:**

- Aggregate and analyze massive amounts of data
- Leverage data from multiple structured and unstructured sources in threat investigations
- Streamline assembly of data from disparate sources
- Provide rapid data analysis to reduce security risks.
- Integrate with workflows for threat hunting and incident response.

FEATURE **LIST**

- 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
- Integration with cloud data and analytics including the Palo Alto Networks Application Framework