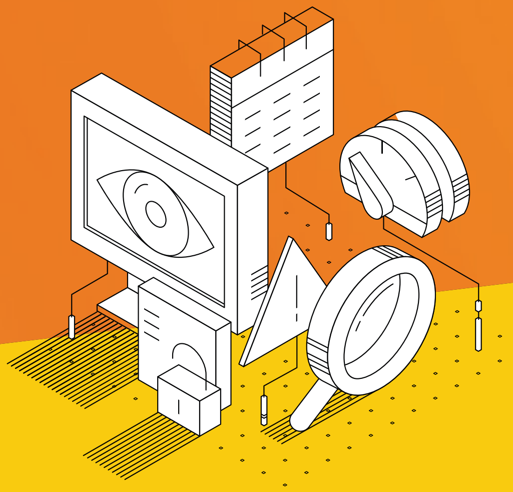
FIREMON

Accelerating Incident Response

Immediate Insight in action - Orchestration, automation and analytics for data assembly and discovery



The Challenge: Alert and Data Volume Exceeds Capacity of Security Teams

The volume of security alerts far exceeds security teams' capacity to assess whether they represent risky security incidents or false positives. Moreover, new infrastructure paradigms such as cloud/mobile-centric architectures and SDN are reducing organizations' capacity for incident response. Combine this with a more sophisticated, determined adversary and an avalanche of data, and it's clear that alert triage needs are exceeding the capabilities of SIEM-based data analysis, resulting in increased risk from security incidents.

It's a Big Data Problem

Every organization whose data volume, variety and velocity outpaces their ability to consume and extract value from it, has a big data problem. For most Incident Response teams, too much time is spent preparing disparate and increasingly complex data for analysis (parsing and normalizing internal data, collecting relevant external data, creating correlation rules, finding anomalies, etc.), resulting in longer resolution times. Furthermore, extending analysis to include unstructured data complicates or stops the analysis process altogether.

The Solution: Accelerated Incident Response with Immediate Insight

Immediate Insight offers a new approach to security event triage for incident response and threat detection. 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. Its orchestration, automation and analytics capabilities transform complex and disparate data into immediately actionable data, accelerating threat detection and analysis without requiring a query language or customization.

Immediate Insight's real-time assembly and analysis of structured and unstructured data:

- Makes security alerts contextual and actionable.
- Orchestrates assembly and correlation of external data.
- Enriches alerts with important contextual information.
- Finds common themes and entities spanning alerts and alert clusters.
- Identifies changes in alert patterns – common and uncommon patterns, sources and entities.
- Gain insight from previous users' observations.
- Adds observations directly to the data.
- Stages data for analysis by escalation teams.

WHY IMMEDIATE INSIGHT?

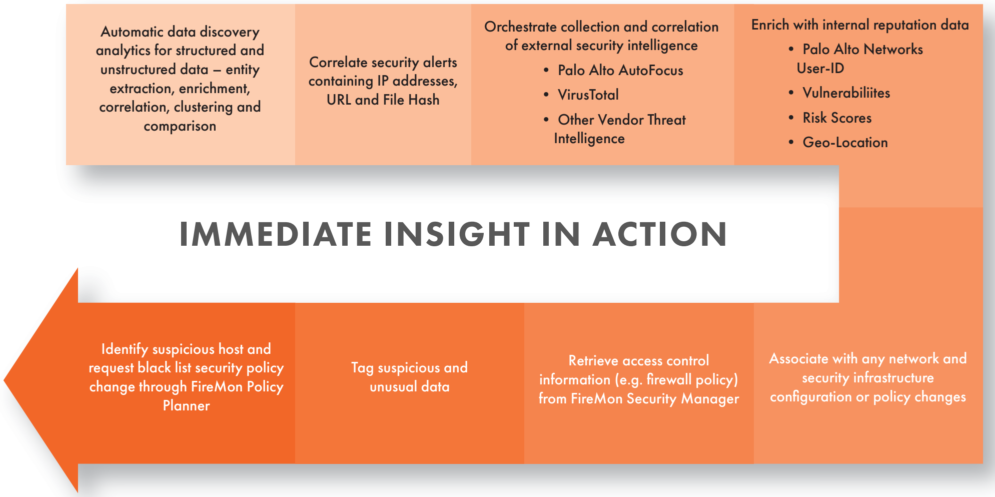
Reduces security risk by accelerating triage of security alerts as either a false positive or a real security incident.

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



Automatic data discovery analytics for structured and unstructured data – entity extraction, enrichment, correlation, clustering and comparison

Correlate security alerts containing IP addresses, URL and File Hash

Orchestrate collection and correlation of external security intelligence

- Palo Alto AutoFocus
- VirusTotal
- Other Vendor Threat Intelligence

Enrich with internal reputation data

- Palo Alto Networks User-ID
- Vulnerabiliites
- Risk Scores
- Geo-Location

Associate with any network and security infrastructure configuration or policy changes

Retrieve access control information (e.g. firewall policy) from FireMon Security Manager

Tag suspicious and unusual data

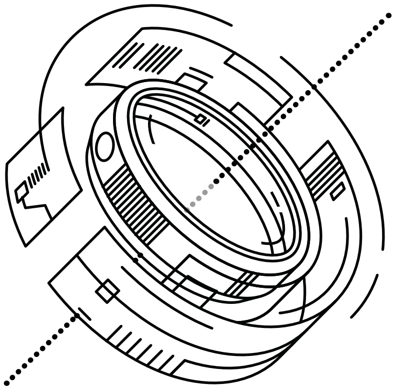
Identify suspicious host and request black list security policy change through FireMon Policy Planner

IMMEDIATE INSIGHT IN ACTION

Who is FireMon?

FireMon is the No.1 provider of Intelligent Security Management solutions worldwide, combining advanced benchmarking, simulation, and analysis to deliver next generation security intelligence. Since creating the first-ever network security management solution more than 15 years ago, FireMon solutions have continued to deliver visibility into and control over complex network security infrastructure, policies, and risk to over 1,500 customers around the world.

Using the FireMon Intelligent Security Management platform, today's leading enterprise organizations, government agencies, and managed security providers have dramatically improved effectiveness of network defenses, accelerating business agility and optimizing return on investment. For more information or a free 30-day trial, visit www.firemon.com.



Learn more about our solutions: www.firemon.com

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