Immediate Insight + Palo Alto Networks Application Framework

Extend Analytics-Enabled Threat Hunting and Investigations to the Palo Alto Networks Application Framework

THE **CHALLENGE:** Inefficient and ineffective threat hunting and investigation increases risk

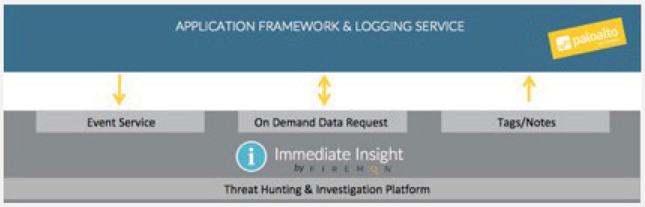
Detecting and protecting from threats requires systems and analysts to proactively and reactively analyze large volumes of data. The volume and speed of the data coming in prevents users from performing even the most basic security analysis for much of the data. Deploying systems to store, organize, and analyze the data is a lengthy and expensive process. It's called big data for a reason.

Firewall data is a good example. It contains useful information, however there's so much of it that it presents challenges for most organizations to store and effectively analyze. Additionally, the high volume can obscure an adversary's activities.

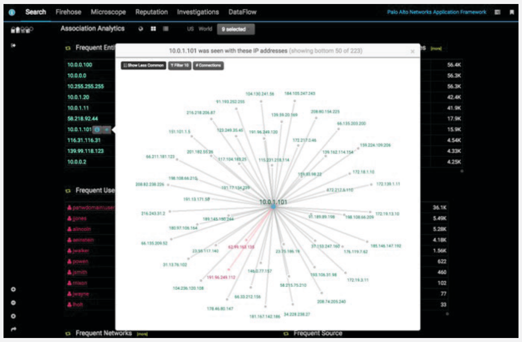
For a threat hunter or incident responder, life would be easier if they could receive an analyzed and meaningful subset of the firewall data including, but not limited to, critical threats, targeted inbound and outbound activity, correlated threat intelligence and anomalous behavior. When needed, the detailed source data (e.g. firewall logs) are just a mouse click away.

THE **SOLUTION:** FireMon Immediate Insight for Palo Alto Networks Application Framework

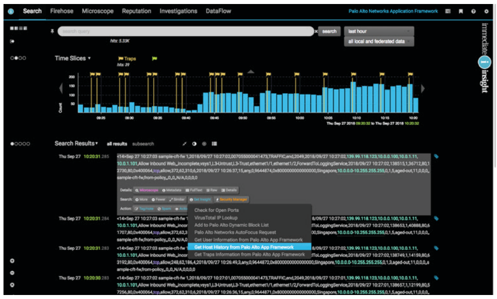
With FireMon Immediate Insight optimized for the Palo Alto Networks Application Framework, organizations can better leverage their Palo Alto Networks data in threat hunting and investigation activities. Simply forward your Palo Alto Networks data to the Palo Alto Networks Logging Service and Immediate Insight gives you the access to both the higher value analyzed data and the raw firewall data on-demand.



Threat Hunting is the human-driven process to detect and isolate malicious, suspicious, and high-risk activities that evade existing security systems. Analysts can use the Immediate Insight analytics-enabled threat hunting and investigation platform to seamlessly combine and analyze Application Framework and private infrastructure data, accelerating discovery and response to security threats.



Immediate Insight 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, accelerating threat detection and analysis without requiring a query language or customization.



```
Thu Sep 27  10:20:31.285  <14>Sep 27 10:27:03 sample-cft-fw 1,2018/09/27 10:27:02,007055000041473,TRAFFIC,end,2049,2018/09/27 10:27:02,139.99.118.123,10.0.0.100,10.0.1.11,
                          10.0.1.101,Allow Inbound Web_incomplete,vsys1,L3-Untrust,L3-Trust,ethernet1/1,ethernet1/2,ForwardToLoggingService,2018/09/27 10:27:02,138515,1,36712,80,1
                          2730,80,0x400064,tcp,allow,372,62,310,6,2018/09/27 10:26:37,15,any,0,9644874,0x8000000000000000,Singapore,10.0.0.0-10.255.255.255,0,1,5,aged-out,11,0,0,0,
                          sample-cft-fw,from-policy,,0,0,N/A,0,0,0,0
Thu Sep 27  10:20:31.284  <14>Sep 27 10:27:03 sample-cft-fw 1                                    8/09/27 10:27:02,139.99.118.123,10.0.0.100,10.0.1.11,
                          10.0.1.101,Allow Inbound Web_incor                                   ToLoggingService,2018/09/27 10:27:02,138653,1,40888,80,6
                          1707,80,0x400064,tcp,allow,372,62,3                                  00,Singapore,10.0.0.0-10.255.255.255,0,1,5,aged-out,11,0,0,0,
                          sample-cft-fw,from-policy,,0,0,N/A,0
Thu Sep 27  10:20:31.283  <14>Sep 27 10:27:03 sample-cft-fw 1                                    8/09/27 10:27:02,139.99.118.123,10.0.0.100,10.0.1.11,
                          10.0.1.101,Allow Inbound Web_incor                                   ToLoggingService,2018/09/27 10:27:02,138749,1,14159,80,6
                          3192,80,0x400064,tcp,allow,248,62,186,4,2018/09/27 10:26:49,3,any,0,9644872,0x8000000000000000,Singapore,10.0.0.0-10.255.255.255,0,1,3,aged-out,11,0,0,0,s
                          ample-cft-fw,from-policy,,0,0,N/A,0,0,0,0
Thu Sep 27  10:20:30.283  <14>Sep 27 10:27:02 sample-cft-fw 1,2018/09/27 10:27:01,007055000041473,TRAFFIC,end,2049,2018/09/27 10:27:01,139.99.118.123,10.0.0.100,10.0.1.11,
                          10.0.1.101,Allow Inbound Web_incomplete,vsys1,L3-Untrust,L3-Trust,ethernet1/1,ethernet1/2,ForwardToLoggingService,2018/09/27 10:27:01,138657,1,12199,80,5
                          7256,80,0x400064,tcp,allow,372,62,310,6,2018/09/27 10:26:36,15,any,0,9644871,0x8000000000000000,Singapore,10.0.0.0-10.255.255.255,0,1,5,aged-out,11,0,0,0,
```

Application Framework data provides a wealth of threat and log data that offers both vital contextual information and useful artifacts for threat hunting activities. For example, firewall records contain rich connection and contextual usage information that can indicate behavior anomalies identified by applications like Magnifier. All can provide useful artifacts, both streamed and on-demand, for Immediate Insight threat hunting activities.

IMMEDIATE INSIGHT - OPTIMIZED FOR THE PALO ALTO NETWORKS APPLICATION FRAMEWORK

- Automatically stream security events of interest into Immediate Insight as both threat hunting artifacts and context for on-premise data analysis to identify and investigate suspicious activity.
- Integrate Application Framework data, such as on-demand requests of host's activity history, into your threat hunting activities.
- Request contextual Active Directory user information from the Application Framework.
- Optionally share observations through Immediate Insight's tags and notes with other Application Framework-enabled applications.

For example, a security analyst needs to analyze a reference dataset for a specific problem (a packet capture of suspicious activity from a host). With Immediate Insight optimized for Application Framework, the dataset can be easily loaded via the drag/drop interface and analyzed with Application Framework data. The analyst can request the security and connectivity history from Application Framework for the host as affirmation of the threat and information on lateral movement. Root cause data can then be tagged for inclusion in the case management process, which uploads the information back to the Application Framework. The availability of tagged data can trigger other automated security processes available from the Application Framework.

Installation and configuration to enable data to/from the Application Framework takes minutes, allowing you to leverage Application Framework data as both a source of threat hunting artifacts and contextual data for any type of data being analyzed.

ADDITIONAL ADVANCED ANALYTIC AND AUTOMATION FEATURES FOR PALO ALTO NETWORKS SYSTEMS AND DATA

In addition to its functions optimized for the Palo Alto Networks Application Framework, Immediate Insight:

- Automatically extracts Palo Alto Networks User-ID and adds as context to other data
- Enriches alerts with important AutoFocus contextual information
- Finds common themes and entities spanning Palo Alto Networks alerts and event data
- Identifies changes in activity – common and uncommon patterns, sources, and entities
- Tag any Palo Alto Networks event to add custom context
- Add IP, URL, or domain to Dynamic Block List
- Deploy firewall policy through Firemon Security Manager

KEY FEATURES

Data discovery and analysis features enable your threat hunters and incident responders to more quickly discover and remediate threats.

- Leverages data from multiple structured and unstructured sources
- Supports parsing-free streaming and on-demand data ingestion
- Enriches data at index time
- Real-time data discovery and analysis
- Association, clustering, and comparison analytics
- Tagging to easily add custom context
- Internal reputation engine to define custom enrichment
- Operational and customizable views of favorite searches