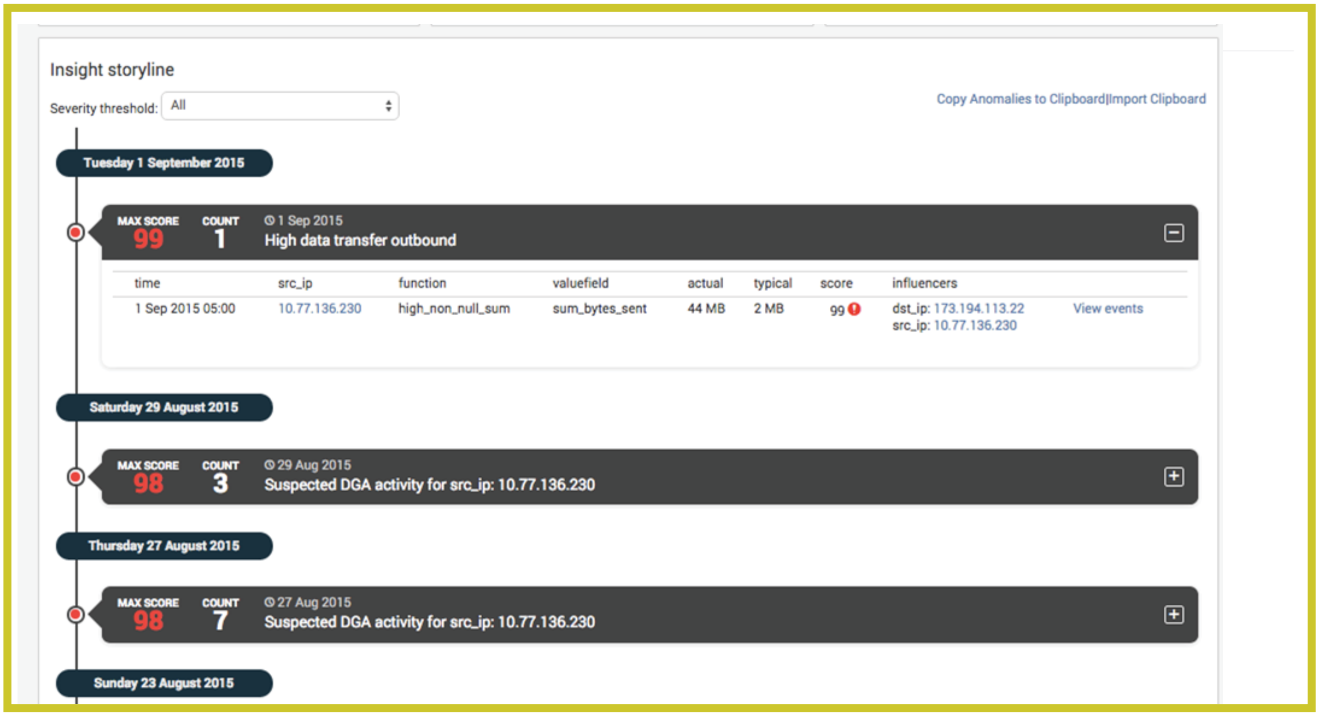
# Anomaly Detective® App
for Splunk®

Prelert Behavioral Analytics: Let Your IT Security Data Tell The Story

Prelert's Anomaly Detective app for Splunk analyzes log data, finds anomalies, links them together and lets your data tell the story behind advanced cyberthreats. The Anomaly Detective app extends the power of Splunk's platform with behavioral analytics capabilities that can be applied to any data source. These capabilities include an innovative new feature called the Insight Storyline that helps teams visualize security events and connect them to root causes faster and more easily.

Anomaly Detective can be used broadly across many different types of data, including Windows event logs, DNS logs, firewall logs and essentially any kind of time series data and log events that can be stored in Splunk (among other data platforms). It detects anomalies quickly, and in a very flexible way, based on individual use cases or elemental attack behaviors. It works across security, IT ops, business KPIs and many other types of data.

Tightly integrated with Splunk, the Anomaly Detective app is easy to download and deploy in minutes—no data import or export required. Anomaly Detective also supports Splunk Cloud™, Hunk® and the Enterprise Security application.



Insight storyline

Severity threshold: All

Tuesday 1 September 2015

MAX SCORE 99 COUNT 1 1 Sep 2015
High data transfer outbound

time	src_ip	function	valuefield	actual	typical	score	influencers	
1 Sep 2015 05:00	10.77.136.230	high_non_null_sum	sum_bytes_sent	44 MB	2 MB	99 !	dst_ip: 173.194.113.22 src_ip: 10.77.136.230	View events

Saturday 29 August 2015

MAX SCORE 98 COUNT 3 29 Aug 2015
Suspected DGA activity for src_ip: 10.77.136.230

Thursday 27 August 2015

MAX SCORE 98 COUNT 7 27 Aug 2015
Suspected DGA activity for src_ip: 10.77.136.230

Sunday 23 August 2015

Anomaly Detective helps you automate the analysis of massive Splunk data sets, eliminating manual effort and human error. Anomaly Detective operates within distributed environments, leveraging summary indexes for massive scalability. We analyze your data in Splunk, turning your existing dashboards into accurate, near real-time alerts and insights in under a minute.

Anomaly Detective® App for Splunk

Using machine learning anomaly detection, Prelert offers:

Early Detection of Advanced Threats

Anomaly Detective analyzes log data in near real-time, detecting advanced threats like snoopers, scrapers, rogue users and DNS-based command and control activity. This allows security teams to identify security threats faster and more thoroughly, eliminating manual effort and human error.

Faster Root Cause Discovery

Anomaly Detective's algorithms learn minute-to-minute what is normal for your environment. With Prelert, IT security teams can now get the full story of IT threats and problems, while involving fewer people in the triage process faster than with manual analysis.

Reduced False Positives

Anomaly Detective's behavioral analytics capabilities help you find and fix real problems. By analyzing your log data, finding anomalies in various log sources and linking them together, Anomaly Detective's insights provide more context than solutions that look at fewer log sources, eliminating false positives.

Why IT Security Teams Choose Prelert

Unsupervised Machine Learning

Anomaly Detective's unsupervised machine learning algorithms baseline normal behavior without the need for training data sets. Even better, organizations don't need a team of data scientists to use Anomaly Detective effectively.

Accurate Anomaly Detection

Anomaly Detective's sophisticated machine learning algorithms provide you with accurate information (read: fewer false positives) so you can quickly detect, investigate and respond to anomalous activity. No more manual effort writing rules or human error parsing alerts.

Organization-Specific Insights

Anomaly Detective's insights let your data tell the story. Arranged in time order and linked by common influencers, automated insights tell you what you need to know now and what requires further investigation.

Fast Data Analysis

Anomaly Detective is designed to analyze massive, high-cardinality data sets in moments, showing you what you need to know and making it easy to uncover what is worthy of your attention.

Near Real-Time Alerts

The moment it is aggregated, Anomaly Detective analyzes your Splunk log data, generating accurate models that evolve as fast as your data does, identifying outlying user behavior and alerting you about what is most important in your environment.

Anomaly Detective® App for Splunk

IT Security Applications of Prelert

Threat Indicator Category	Helps you identify...	... By Finding Anomalies In
Data Exfiltration	Credit card, health record theft	Firewalls, web proxies, secure gateways, DNS logs
Malware Command & Control Activity	Infected systems beaconing	Firewalls, web proxies, DNS request logs
Compromised Endpoints	Spreading malware internally	EDR/AV logs, Netflow records
Suspicious Server Behaviors	New bit torrents, chat rooms, file services	Process starts, network connects
Suspicious Account Activity	Account creation, privilege changes	Servers, directories, audit logs
Unauthorized Login Attempts/Activity	Smart brute force attacks	Servers, directories, audit logs
Unusual IDS/IPS Events	Unusual security threats	IDS/IPS, IDP, NGFW logs
Disabled/Interrupted Logging	Attempts to hide tracks	All types of log data
Unusual Network Activity	DDoS attack, excessive DNS requests	Firewalls, web Proxies, secure web gateways, Netflow, DPI logs
Abusive/Attacking IP Adress	External data scrapers, internal snoopers	Firewalls, web Proxies, secure web gateways, Netflow, DPI logs

System Requirements:
info.prelert.com/system-requirements

DOWNLOAD FREE TRIAL
www.prelert.com

Or Call Us to Learn More: (888) PRELERT or +1 (508) 319-5322

About Prelert

Prelert is the leading provider of behavioral analytics for IT security and operations teams. The company's solution analyzes an organization's log data, finds anomalies, links them together and lets the data tell the story behind advanced cyberthreats and IT performance problems. Leveraging machine learning anomaly detection and other behavioral analytics capabilities, the solution automates the analysis of massive data sets, eliminating manual effort and human error. Hundreds of progressive IT organizations rely on Prelert to detect advanced threat activity, reduce false positive alerts and enable faster root cause analysis. Prelert lets your data tell the story.