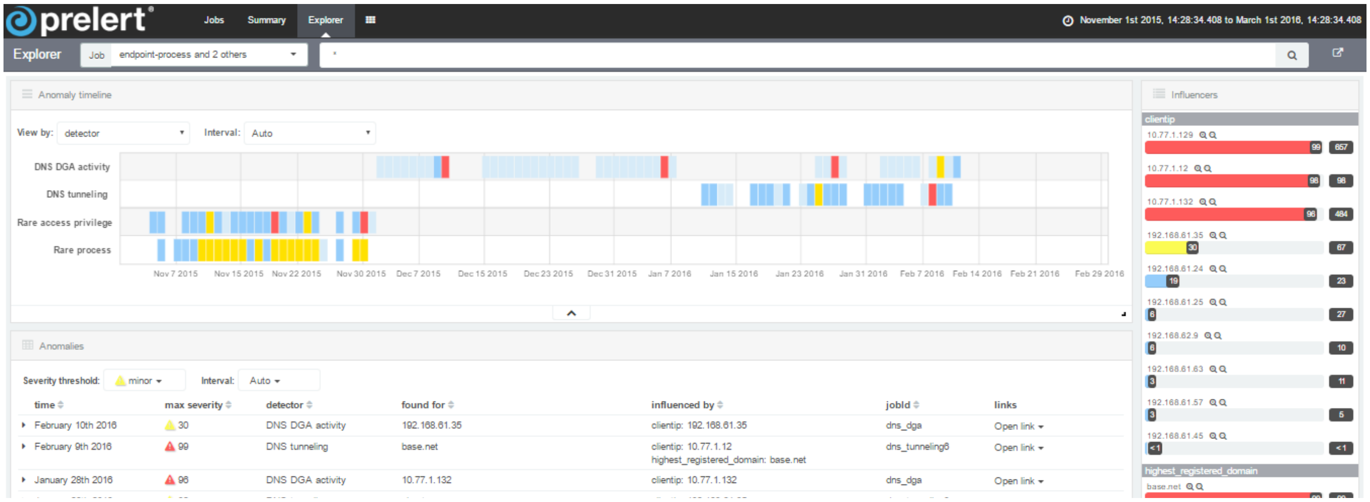
# Behavioral Analytics
for the Elastic Stack

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

Prelert Behavioral Analytics for the Elastic Stack analyzes security-related log data residing in Elasticsearch, finds anomalies within the data, links them together and lets your data tell the story behind advanced cyberthreats. Behavioral Analytics for the Elastic Stack extends the power of the Elastic Stack with automated machine learning-based analytics capabilities that can be applied to any type of security-related data in Elasticsearch. These capabilities include an innovative statistical influencer tracking capability that helps security analysts visualize multiple anomalous events that are related to a Cyber Kill Chain attack progression.

Behavioral Analytics for the Elastic Stack can automate the analysis of many different types of security-related data, including web proxy logs, Windows event logs, DNS logs, firewall logs - essentially any time-series log data that can be stored in Elasticsearch. Users simply choose the desired set of use cases to deploy. With easy-to-use parameterized configuration of anomaly search jobs, users can augment Prelert-supplied use cases by creating their own use cases leveraging their own subject-matter expertise. Anomaly Search jobs detect anomalies that represent elementary attack behaviors, the building blocks of advanced threat activity.



time	max severity	detector	found for	influenced by	jobId	links
February 10th 2016	⚠ 30	DNS DGA activity	192.168.61.35	clientip: 192.168.61.35	dns_dga	Open link
February 9th 2016	⚠ 99	DNS tunneling	base.net	clientip: 10.77.1.12 highest_registered_domain: base.net	dns_tunneling6	Open link
January 28th 2016	⚠ 96	DNS DGA activity	10.77.1.132	clientip: 10.77.1.132	dns_dga	Open link

clientip		
10.77.1.129	99	657
10.77.1.12	98	98
10.77.1.132	96	484
192.168.61.35	30	67
192.168.61.24	19	23
192.168.61.25	6	27
192.168.62.9	6	10
192.168.61.63	3	11
192.168.61.57	3	5
192.168.61.45	<1	<1
highest_registered_domain		
base.net		

"Anomaly timeline" dashboard showing anomaly search job "swimlanes" that help analysts understand relationships between anomalous behaviors. Here anomalies in DNS log data indicate DNS tunneling activity related to Domain Generation Algorithm (DGA) malware.

Executing as a Kibana app, Behavioral Analytics for the Elastic Stack is tightly integrated. Data is pulled from Elasticsearch for analysis, and anomaly results are displayed in Kibana dashboards. Behavioral Analytics for the Elastic Stack is also compatible with other Elastic Products such as Shield and Watcher. It's easy to download and deploy in minutes—no data import or export required.

Prelert Behavioral Analytics for the Elastic Stack helps you automate the analysis of massive Elasticsearch data sets using machine learning technology. Since the automated analysis operates in an online mode, it flags real problems in near-real-time, eliminating the need for traditional data monitoring rules and thresholds that return false positives if set too strictly, miss activity if set too loosely, and become outdated over time. Prelert analytics include statistical influencer tracking, which provides critical contextual data for each detected anomaly so entities that are associated with anomalous activity can be identified quickly for further investigation and remediation.

Behavioral Analytics for the Elastic Stack

Prelert Behavioral Analytics Offers:

Early Detection of Advanced Threats

Prelert uses machine learning to analyze log data in near real-time, detecting anomalies associated with advanced threat activities such as data exfiltration, malware command and control activity, network scanning, and suspicious logins and account activity. This allows security teams to identify security threats faster and more thoroughly, eliminating manual effort and human error.

Faster Root Cause Discovery

Using "online machine learning," Prelert algorithms continuously refine the model of what data behaviors are normal for your environment. With Prelert, security teams can now get the full story behind threat-related activity, while involving fewer people in incident response and remediation.

Reduced False Positives

Prelert's behavioral analytics capabilities help you identify and contain real threats. By analyzing your log data, finding anomalies in various log sources and linking them together, Prelert Behavioral Analytics for the Elastic Stack provides deeper context to help minimize false positives.

Why IT Security Teams Choose Prelert

Unsupervised Machine Learning

Proprietary 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 Prelert effectively.

More Accurate Anomaly Detection

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

Organization-Specific Insights

Prelert lets your data tell the story. Linked by common statistical influencers, related anomalies provide insight by telling you what you need to know now and what requires further investigation.

Speedy Data Analysis

Prelert 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

Just moments from the time your log data is indexed in Elasticsearch, Prelert analyzes your 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.

Behavioral Analytics for the Elastic Stack

IT Security Applications of Prelert Behavioral Analytics

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	Process starts, network connects
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 Address	External data scrapers, internal snoopers	Firewalls, web proxies, secure web gateways, Netflow, DPI logs

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

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, IT operations, and business 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 security threats, IT performance problems, and business disruptions. 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.