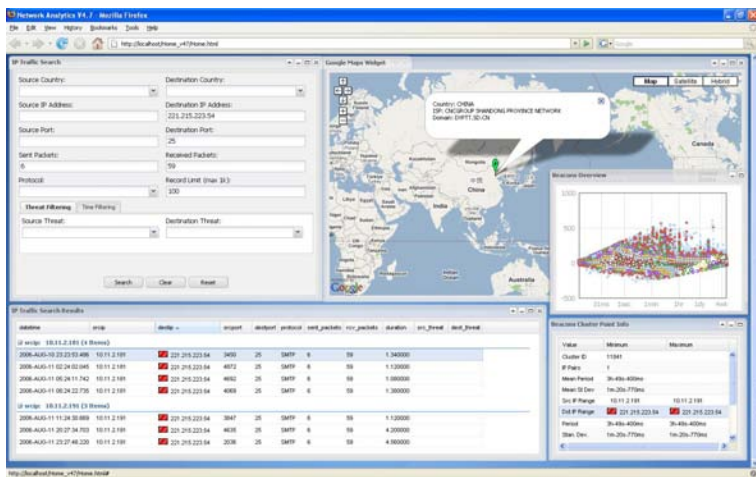


LexisNexis® Cyber Analytics Platform

Prevent network attacks through superior network traffic analysis

The LexisNexis® *Cyber Analytics Platform (CAP)* enables pattern analysis and anomaly detection for deep forensic analysis to uncover malicious network activity on your network. The *CAP* delivers a powerful ability to uncover and identify threats such as botnet beacons, data exfiltration and communication with compromised hosts, allowing you to discover unknown threat signatures and bolster your intrusion detection systems. Leveraging the speed and scalability of the LexisNexis *Data Analytics Supercomputer (DAS)* to analyze massive amounts of network traffic data, the Cyber Analytics Platform can ingest and analyze large volumes of net-flow and perimeter device session data, scaling to analyze more than 100 terabytes of network related data in a single query. Current network sensors and monitoring technologies provide limited views of network data because they are constrained by the volume of data they can process. These cyber security analytical applications built on typical relational databases can only effectively process 1-2 terabytes of data. Ninety days of traffic can add hundreds of terabytes of data, which would be impossible for a conventional network analysis system to process quickly enough to detect today's most sophisticated threats.



Above: The Cyber Analytics Platform provides an array of easy-to-use analytical tools, including “power” queries, cluster analysis charts and geospatial visualization

Search massive volumes of IP traffic for suspicious behavior across your entire network

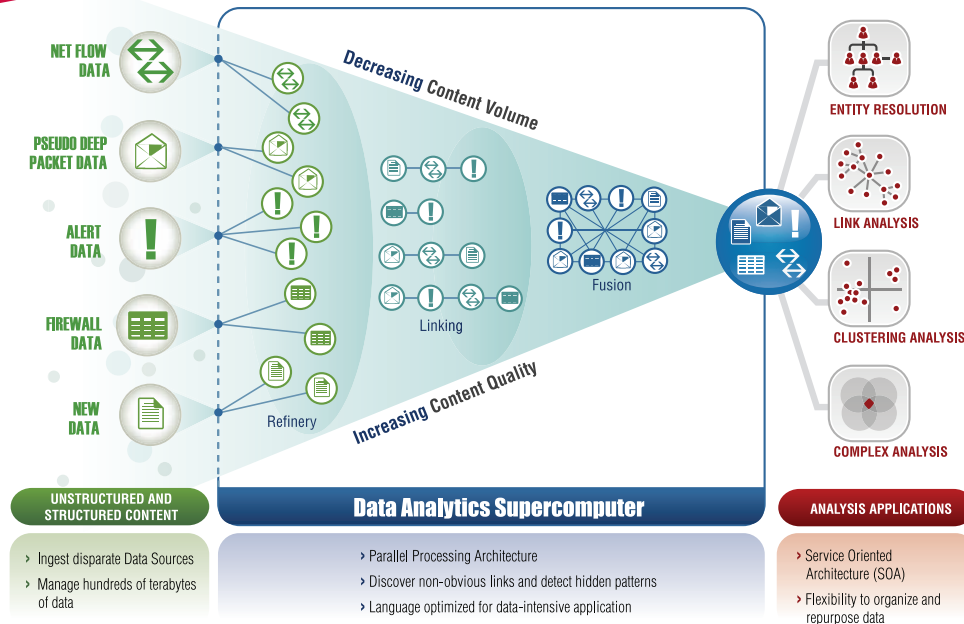
- Find patterns and anomalies that may be indicators of threats such as Botnets and Malware
- Quickly correlate and analyze system logs and IDS alerts to discover previously unknown threat patterns with “power” queries, cluster analysis charts, and geospatial visualization
- Enrich IP addresses with contextual information such as geospatial information, known hacker commands, system configuration information and other information for clearer analysis
- Identify hostile command and control nodes
- Identify “computer social networks” to identify other compromised systems on your network
- Discover non-obvious relationships between hacker-controlled nodes and target nodes
- Integrate other data sets for enriched analysis
- The Cyber Analytics Platform complements—rather than replaces—your existing SEM technologies

“It is no longer sufficient for the government to discover cyber intrusions in its networks, clean up the damage, and take steps to deter further intrusions. We must take proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage.”

***— Adm. Mike McConnell
Former Director of National Intelligence***



Identify system compromises through comprehensive network traffic analysis



Possible through DAS

Conventional high-performance computing platforms and database technologies can't handle the variety and volume of data you need to analyze to uncover key connections and relationships. Tasked with ingesting, linking, and analyzing this amount of complex data, conventional technologies are brought to a grinding halt. They're not scalable and they're not fast enough. They don't allow you to see the whole picture—the entirety of the data sets you need to analyze. The LexisNexis® *Data Analytics Supercomputer (DAS)* platform is designed to handle the diverse data sources, variety of data types, and massive amount of data you need to analyze in support of your mission.

LexisNexis Enterprise Control Language (ECL) is the query and control language developed to manage all aspects of the massive data joins, sorts and builds that truly differentiate *DAS* from other technologies in its ability to provide flexible data analysis on a massive scale. ECL is a declarative language optimized for the manipulation of massive data sets and its modular format will allow for the creation of attributes which can be stored and re-used for multiple analytical purposes. ECL allows information security analysts the maximum flexibility to “express” complex queries without needing to go through iterative, time-consuming data transformations and sorts associated with other programming languages. As cyber-threats and the tactics of cybercriminals and other bad actors evolve, ECL provides information security analysts with the flexibility to develop new analytical queries to keep pace with those evolving threats.

DAS offers a powerful, automated ETL capability that enables information security analysts to quickly update and refresh large volumes of network flow data without sacrificing days or even weeks to load new data for analysis. This ability to analyze current netflow data enhances situational awareness and allows analysts to more quickly respond to potential cyber attacks and incidents, and improve IDS capabilities.

High Performance

Results for 30 days of firewall logs—63 million non-indexed records processed on DAS



Summarized packets/day:
2 minutes 51 seconds



Tallied total bytes per day:
5 minutes 48 seconds



Ranked order distribution of protocols
3 minutes 20 seconds



Ranked order distribution of ports
3 minutes 22 seconds



Ranked order distribution of send IPs
1 minute 37 seconds



Ranked order distribution of receive IPs
1 minute 14 seconds

To learn more about LexisNexis Cyber Analytics Platform
call 1-888-579-7638 or visit www.lexisnexis.com/government