THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

LYNXeon

Cyber Pattern Analysis Platform

***EXPAND** investigation*
***DETECT** patterns and get fast answers for incident response*
***FIND** true source of an attack quickly*

Your network data has a story to tell. Northrop Grumman's LYNXeon Cyber Pattern Analysis Platform empowers cyber analysts to detect and disrupt cyber threats. Through an unparalleled combination of data fusion, big data analytics and network visualization, LYNXeon provides cyber protection teams with unprecedented network situational awareness to enhance cyber hunt operations.

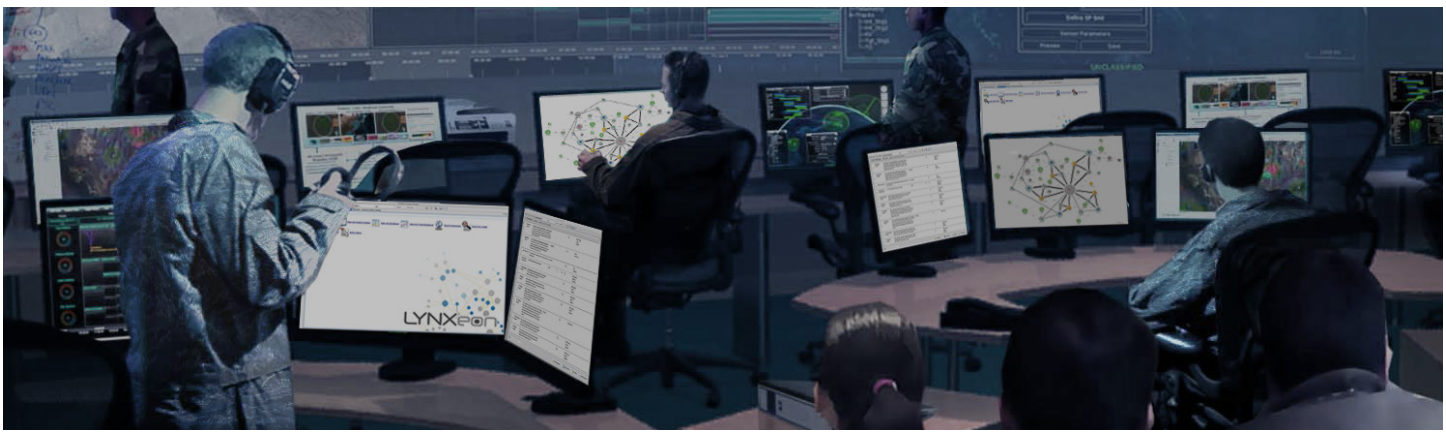
Uncovers threat patterns, activity and behaviors hiding in your data. Correlate, monitor and analyze network data from your existing data sources.

Simplifies your analysis. Preloaded with a robust catalog of more than 70 adaptable search queries, plus the ability to create your own.

Accelerates investigation and mitigation. Optimized query engine to provide rapid results for even the most complex queries.

Allows visibility into data typically missed due to capacity filtering. Scalability to process very large amounts of data over long periods of time.

Provides situational awareness of target anomalies quickly. Visualization canvas allows security teams to analyze, interact, and collaborate together.



LYNXeon

Developed by Analysts for Analysts

Data Fusion · Security Analytics · Network Visibility

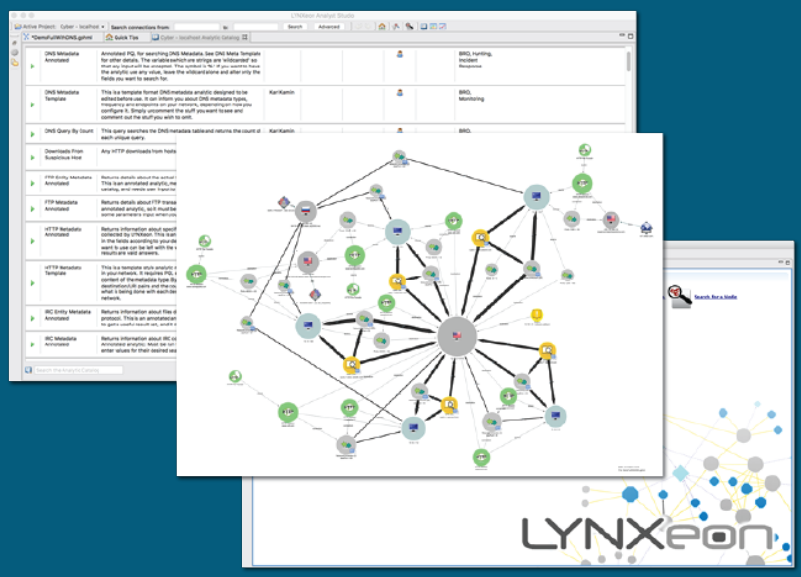
Gain Complete Situational Awareness on Your Network to Detect and Disrupt Cyber Threats

LYNXeon collects and fuses all your cyber data together so you can get a complete picture of your network activity.

- Centralize your organization's data from sources such as NetFlow, Bro, Intrusion Protection Systems (IPS), endpoint protection, and malware detection systems.
- Eliminate stovepipes across your organization's data sources (data repositories and sensors) and find the subtle trails of evidence and patterns of an attacker.

LYNXeon security analytics eliminate labor-intensive manual filtering.

- Create reusable patterns to detect Advanced Persistent Threats (APTs), compromised hosts, malicious probes, and exfiltrated data.
- Obtain results rapidly using LYNXeon's optimized query engine and automate your analytics to be notified whenever suspicious behavior is detected.



LYNXeon includes a catalog of analytics to:

- Identify data exfiltration
- Find DNS covert channels
- Visualize communications with known bad actors on a threat list
- Detect malicious email campaigns
- Identify compromised hosts
- Warn against potential insider threat activity

LYNXeon delivers visualization and correlation of network data in one place.

- Network traffic and alert-based data is displayed in highly interactive graphs, dramatically increasing your situational awareness.
- Quickly and easily see connections between internal and external servers with rich metadata to provide immediate situational context.

LYNXeon provides Cyber Protection and Hunt Teams with unprecedented network visibility.

- Enhances the value of existing cyber detection systems, providing Cyber Protection and Hunt Teams correlation and querying across networks to get answers.
- Increases network security insight from alerts and logs.
- Reduces root cause analysis time.
- Finds previously hidden malicious behavior.
- Analyzes full activity history before and after a breach to determine the full impact of an incident.

For more information, please contact:

Northrop Grumman
Mission Systems

Don Hupp
Donald.Hupp@ngc.com
512.374.4109

Manuel Juarez
Manuel.Juarez@ngc.com
703.556.1822

THE VALUE OF *PERFORMANCE.*

NORTHROP GRUMMAN

www.northropgrumman.com