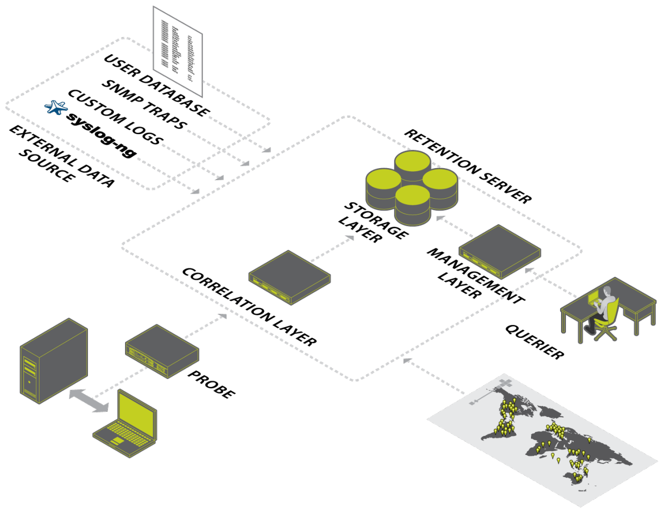
[secure]®

ISC8

Cyber NetFalcon

Real-time, Big Data Analytics

THE FIRST BIG DATA SOLUTION FOR ENTERPRISE NETWORK TRAFFIC



Combines Deep Packet Inspection with Big Data Analytics

Experience The Difference

A comprehensive enterprise cyber security infrastructure must combine on-line prevention and protection with off line historical visibility. Unfortunately, current off line visibility of network activity is limited to machine and log data or small scale packet capture. The result is a significant "coverage gap" in the ability of network security professionals and IT administrators to determine what happened over their networks.

Cyber NetFalcon provides advanced capabilities by extracting contextualized network data on a massive scale (hundreds of Gbps), retaining data for virtually unlimited time periods (months or years), and performing real time data correlation to provide instantaneous responses to queries. Cost-effective to deploy and scale, Cyber NetFalcon is currently deployed in a variety of demanding environments.

ISC8's Cyber NetFalcon solution offers:

- **Pre-correlates external information to expedite cyber investigations**
- **Returns all queries within seconds regardless of network size and time window**
- **Retains a summary of all network traffic for year**
- **Provides comprehensive coverage through versatile placement of probes throughout the core and at the edge of the network**
- **Addresses networks from 1 to over 100 Gbps**
- **Passively monitors all network activity according to administrative policies**

Sample Use Cases

- **Rapid and Effective Investigation of Insider/Outsider Threats**
- **Compliance Reporting: Internal or Regulatory**
- **Managing Acceptable Use Policies**
- **Network Event Attribution**
- **General Enterprise Security**

Fills Coverage Gap Into Historical Network Activity

Cyber NetFalcon

[secure]®
ISC8

www.ISC8.com CyberSecurity@isc8.com

ISC8 Cyber NetFalcon™

Cyber NetFalcon Architecture

At the heart of Cyber NetFalcon is a set of leading edge technologies combining proprietary record correlation, DPI network probing, and a purpose-built database structure to enable real time queries of long term, large scale network communication data.

Turn the Entire Network into a Searchable Medium

Cyber NetFalcon consists of three tiers. In the first tier, high performance probes connect to the network to classify and structure network traffic using Mass Metadata Extraction (MME). MME classifies the collected traffic into protocols and applications, extracting user and application-level information for each communication. Each of these attributes is a searchable element in the system. The conversion of raw network traffic into structured attributes turns the entire network into a searchable medium.

Shorter Time Intervals to Locate Actionable Information

In the second tier, Cyber NetFalcon Correlators collect the information from the probes and if required, combine it with information from other data sources. These additional data sources include DHCP, syslogs, SNMP traps, third party probes, and asynchronous sources, such as geo-location or user authentication data. Cyber NetFalcon's advanced technique for combining the various data elements results in a contextualized record of network activity. This vastly increases the quality and value of the information ultimately stored in the database. The result is a dramatically shorter time interval to locate actionable information.

Cyber NetFalcon Revolutionizes Investigations for Digital Networks

Cyber NetFalcon provides security analysts with the ability to perform real time queries on large scale, long term network communication activity. It represents the intersection of Big Data, Networking and IT Network Security, and promises to revolutionize investigative abilities for digital networks.

Queries Perform Instantaneously Regardless of Database Size

In the third tier, correlated records are stored in Cyber NetFalcon's proprietary database, which uses an advanced performance model and not a traditional relational database model. Unfortunately, relational databases exact a severe penalty in performance when faced with the size and performance demands of a big data system.

Cyber NetFalcon is based on a patent-pending proprietary database technology. The hallmark of the system is time independent query performance, independent of the search time window. Queries performed over search windows of 10 minutes, 10 days, or even 10 months, perform effectively and instantaneously, regardless of database size.

Associate the Action with the Actor

Cyber NetFalcon is designed to provide attribution to associate the action with the actor. As a user authenticates to the wired or wireless network, Cyber NetFalcon collects authentication data and correlates that to flow information as well as medium information. Through advanced correlation techniques, identification of the actor can be performed automatically by associating cyber identity with electronic identity and physical identity. Geolocation can also be included to further enhance the quality of attribution.

Collect, Correlate, Store and Retrieve

In addition to providing historical analysis of retained usage data, Cyber NetFalcon includes innovative dynamic triggering technology that can initiate real time actions throughout the collection, correlation, storage, and retrieval process. This powerful capability is easily customized using an open scripting mechanism and can immediately alert IT security professionals and/or trigger third party systems such as packet capture.

www.ISC8.com CyberSecurity@isc8.com

[secure]®
ISC8