SOLUTION BRIEF

Datiphy + Splunk Add-On: Identify Database Breaches

Datiphy's analytics agent enhances existing Splunk implementation

Organizations that have Splunk deployment tools and log management systems can greatly enhance visibility into their sensitive data repositories by adapting Datiphy's smart agent into the Splunk Universal Forwarder.

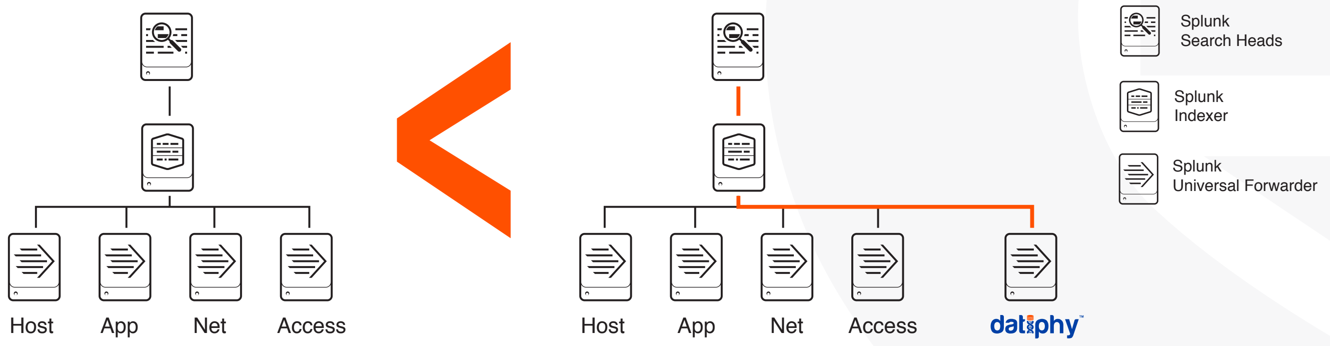
Many detection tools in the market are great at log aggregation. Splunk is no exception. However, with Datiphy augmented into the system log stream, security analysts can gain a greater level of granular visibility into their database transactions. The ultimate goal is to reduce the enterprise's database risk exposure.

Integration

- Light-weight Datiphy agents packaged with Splunk Universal Forwarders (UF)
- Zero-to-minimal configuration for immediate run-time, alerting, and reporting
- Works with new and existing log aggregation Splunk deployments
- Reports can be sent directly to Splunk Search Heads for security analysts and database administrators to review

Benefits

- In-depth and complete activity monitoring, policy management, and integrated event analysis of all data in motion
- Event and data driven alerts to reduce monitoring load and expedite the handling of malicious activity
- Seamless host agent or network tap configuration for immediate auditing, and breach and anomaly detection
- Normalize data to easily correlate with: host logs, network logs, access logs, application logs, web logs, etc.



Without Datiphy:
"John accessed HR application from 195.144.25.36 (client) on 8/21/2016 @ 21:01:35"

With Datiphy:
"John accessed HR application from 195.144.25.36 (client) on August 21st, 2016 @ 21:01:35.
Issuing **DELETE SQL** Command to table **(TABLE_HR)** on database **(DB_PROD_HR)** at host **(Linux_RHEL_HR_PROD @ 125.525.221.52)**"

Patented Database Event-Driven Engine

Datiphy's scan engine takes into account access anomalies, vulnerabilities, and threats to give an in-depth overview of database risks. Security analysts and auditors (both internal and external) can utilize reports to prioritize a defensive plan and to create mitigating controls. The patented non-intrusive technology can formulate a behavioral pattern well before hackers can exercise a means to exfiltrate your sensitive data.

Detection is necessary but prevention in paramount to ensuring knowledge of who is accessing sensitive data. Enhance your log aggregation tool with the help of Datiphy's data-centric visibility and security event detection capabilities.

Deploy our integration toolkit and immediately see where the biggest database threats are located!

ADDRESS
2290 N. First Street, Suite 204
San Jose, CA 95131

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938