LUMU ARCHIVE CASE STUDY: FINANCIAL INSTITUTION SLASHES SIEM LOG STORAGE COSTS BY 95%

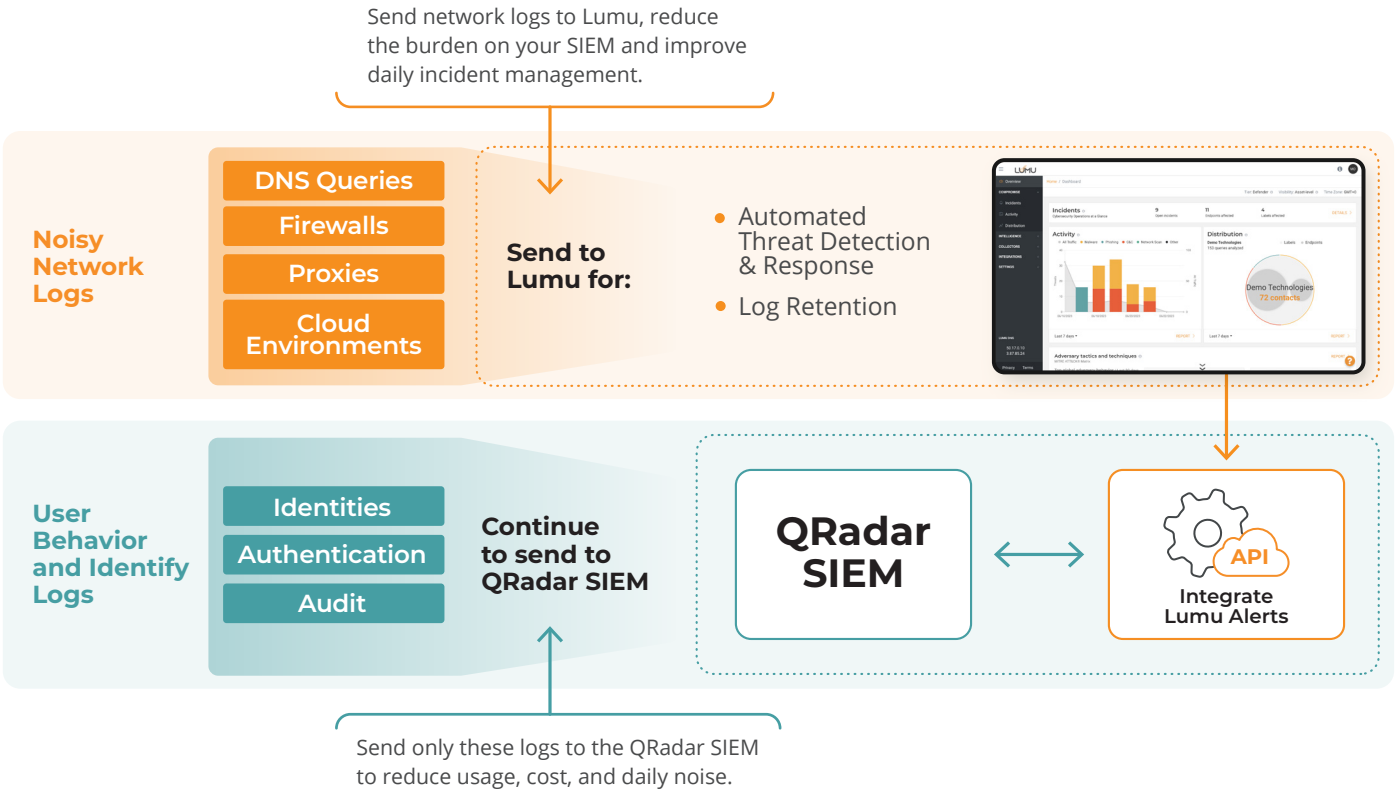
A Texas-based financial institution leveraged Lumu Archive to get more from their existing QRadar SIEM and FortiGate firewall deployments and significantly reduce costs.

SUMMARY

A Texas financial institution using the IBM QRadar SIEM platform sought a way to optimize its deployment and license usage. By integrating Lumu with their existing QRadar system, they were able to establish a new workflow for handling specific log sources, leading to significant operational efficiencies.

WHAT THEY NEEDED

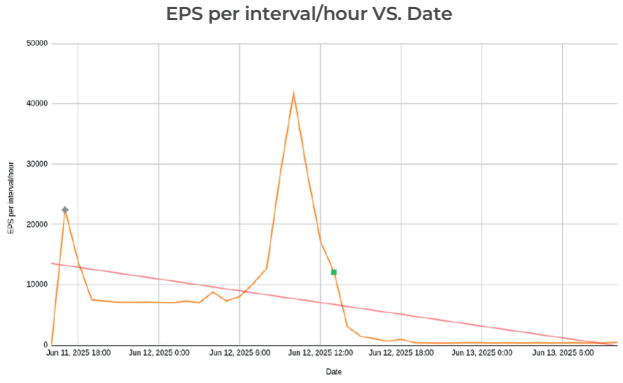
The institution needed to reduce its QRadar licensing costs, which are calculated based on the volume of Events Per Second (EPS) the platform ingests. An internal analysis identified that network logs from their FortiGate Firewall were the primary driver of the high EPS count. The challenge was to find a solution that could filter these high-volume firewall events from being processed by the main QRadar license without losing the crucial threat visibility contained within those logs.



THE SOLUTION

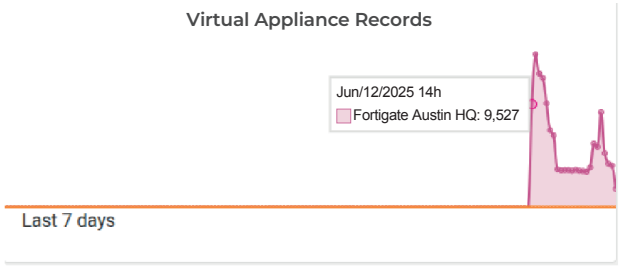
The institution harnessed Lumu to work with their existing QRadar deployment. Lumu's architecture for processing network logs provided what they needed to:

- **Implement strategic log routing:** A simple QRadar Log routing rule was created to forward all Fortinet Firewall logs to the Lumu Virtual Appliance. This change immediately diverted the data-heavy source away from QRadar, resulting in an average reduction of 95.71% in events per second being stored.
- **Slash SIEM ingestion and costs:** The reduction in license usage brought costs firmly under control.
- **Retain full threat visibility:** While the logs no longer bloated the SIEM, they continued to be analyzed by Lumu. This ensured that any contact with malicious infrastructure was identified, leaving no security gaps.
- **Integrate Lumu and QRadar:** An out-of-the-box integration ensures that all detected incidents and alerts are sent from Lumu to the QRadar SIEM.



QRadar Events per Second/Hour

This chart demonstrates the immediate impact of the routing rules on QRadar's data ingestion. The gray diamond marks the moment the FortiGate Firewall was added, causing an increase in events per second. The green square indicates when the Lumu routing rules were activated, which correlates with a sharp and sustained decline in EPS, confirming the effectiveness of the solution.



Lumu Events per Second/Hour

Following the implementation of the QRadar routing rule on June 12, 2025, the Lumu Virtual Appliance immediately began receiving the forwarded firewall logs, as shown by the sharp increase in collected records.

THE BENEFITS OF DEPLOYING LUMU ALONGSIDE QRADAR

Immediate return on investment: Delivered significant savings on QRadar licensing and data storage by cutting firewall log ingestion.

Optimized SIEM performance: Maximized the value of their QRadar investment by offloading network log analysis, letting the SIEM focus on high-fidelity alerts.

Visibility without bloat: Lumu's continuous analysis of the offloaded logs ensured that any communication with malicious actors was promptly identified.

Frictionless implementation: Deployed quickly through a simple log-forwarding rule and out-of-the-box integration

Increased analyst focus: Freed the security team from managing license limits to focus on investigating confirmed threats.

Continued log access: The institution is able to access their network logs through Lumu via self-service querying, ensuring compliance.

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io